EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

NOKIA CORPORATION,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. ____________________
	)	
APPLE INC.,	)	JURY TRIAL DEMANDED
	)	
Defendant.	)	

COMPLAINT FOR PATENT INFRINGEMENT AND DECLARATORY JUDGMENT

Plaintiff Nokia Corporation ("Nokia"), on personal knowledge as to its own acts, and on information and belief as to all others based on its investigation, alleges as follows:

INTRODUCTION

1. This is an action brought by Nokia against Apple Inc. ("Apple") for Apple's infringement of Nokia's patents. In particular, Nokia seeks remedies for Apple's infringement of Nokia's U.S. Patent Nos. 5,802,465 ("the 465 Patent"), 5,862,178 ("the 178 Patent"), 5,946,651 ("the 651 Patent"), 6,359,904 ("the 904 Patent"), 6,694,135 ("the 135 Patent"), 6,775,548 ("the 548 Patent"), 6,882,727 ("the 727 Patent"), 7,009,940 ("the 940 Patent"), 7,092,672 ("the 672 Patent"), and 7,403,621 ("the 621 Patent") (collectively, "the patents-in-suit").

2. Each of the patents-in-suit is essential to one or more of the following standards: the Global System for Mobile Communications ("GSM") Standard, the Universal Mobile Telecommunications System ("UMTS") Standard, and the Institute of Electrical and Electronic Engineers ("IEEE") 802.11 Standard.

3. Nokia has declared each of the patents-in-suit as essential to the GSM, UMTS, and/or 802.11 Standards, where applicable, and undertaken -- in accordance with the

applicable rules of the standard setting organizations ("SSO") -- to grant licenses under each of the patents-in-suit on fair, reasonable, and nondiscriminatory ("FRAND") terms and conditions (in some cases, alternatively referred to as "reasonable and non-discriminatory," or "RAND," terms).

4. On the basis of Nokia's licensing commitments, Apple has the right to be granted license(s) under F/RAND terms and conditions with respect to a Standard.

5. Prior to filing this Complaint, Nokia has made various offers to Apple for the F/RAND terms and conditions of a license agreement under which each of the patents-in-suit could be licensed either individually or together with other Nokia essential patents (i.e., a portfolio license). In its offers to Apple, Nokia has specified both a portfolio rate and an average per-patent royalty rate which Apple could have accepted within a reasonable time for each of the patents-in-suit.

6. Apple has rejected Nokia's offers for the F/RAND terms and conditions both on a portfolio and on a per-patent basis and thereby refused to compensate Nokia on F/RAND terms for its use of Nokia's patented technologies, including each of the patents-in-suit.

7. In order to be fairly and adequately rewarded for the use of Nokia patented technology in the implementation of the standards, Nokia seeks by this action F/RAND compensation for Apple's use of the patents-in-suit. In addition, Nokia seeks a declaration (i) that the patents-in-suit are infringed by Apple's products complying with the respective Standards and that the patents-in-suit are not invalid or unenforceable (ii) that Nokia has complied with its obligations under the F/RAND undertakings by negotiating in good faith and offering and specifying F/RAND terms and conditions for the patents-in-suit, (iii) that Apple has refused to compensate Nokia on F/RAND terms for the patents-in-suit in breach of its obligation

to pay for the use of the Nokia patents, and (iv) that Nokia is entitled to an injunction until and unless Apple pays F/RAND compensation, together with interest, for past infringement of the patents-in-suit and irrevocably commits to pay such compensation in the future.

PARTIES

8. Plaintiff Nokia is incorporated under the laws of Finland and has its principal place of business at Keilalahdentie 4, Espoo, Finland.

9. Nokia was founded in 1865 and is the world's largest manufacturer of mobile telephones. Nokia is one of the champions of wireless cellular communications and has received numerous awards and accolades for its achievements, including introducing the first car phone on the first international cellular mobile network in 1981.

10. Nokia's innovations continue today. In 1991, the world's first genuine call on GSM was made with a Nokia phone. In 1996, Nokia introduced the Nokia 9000 Communicator, which was the first all-in-one phone, fax, calendar, e-mail and Internet device in a hand-portable size. The Nokia 8110i, introduced in 1997, was the first mobile phone with a dynamic menu supporting Smart Messaging. Just two years later, Nokia introduced the Nokia 7110, which was the first mobile phone compliant with the Wireless Application Protocol 1.1, which provided access to mobile Internet services, such as banking, e-mail, and news, as well as the first phone with predictive text input.

11. In 2001, Nokia made the world's first 3G WCDMA voice call on a commercial system, and launched its first imaging phone with an integrated camera, the Nokia 7650. In 2002, Nokia introduced the world's first UMTS/GSM dual mode phone, and the first Nokia phone to record video simultaneously with sound. The Nokia 5140, launched in 2003 was

the first Push-to-Talk GSM handset. In 2006, Nokia introduced the N95, which was the first Nokia phone with built-in GPS.

12. Research is one of the keys to Nokia's success. As of December 2008, Nokia had research and development presence in 16 countries and employed over 39,000 people in research and development. Such research and development led to the innovations found in the patents-in-suit.

13. In the 1980s, Nokia led the charge to establish the communications protocols that are still used today. Without Nokia's contributions and innovation, the world would not have the communications standards that it has today. Nokia continues to be a leader in mobile communications worldwide and continues to invest millions of dollars annually in new developments in mobile communications.

14. Upon information and belief, Defendant Apple is a corporation duly organized and existing under the laws of the state of California and has a principal place of business at 1 Infinite Loop, Cupertino, California 95014.

15. Upon information and belief, Apple did not make telephones, much less mobile telephones, until 2007. Apple's wireless communication devices take advantage of the decades of continued investments by Nokia to build today's communication protocols. By refusing to compensate Nokia for its patented technologies, Apple is attempting to get a "free-ride" on the billions of dollars that Nokia has invested in research and development to provide the public with the wireless communications it enjoys today.

JURISDICTION AND VENUE

16. This is an action arising under the patent laws of the United States. Accordingly, this Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

17. This Court has personal jurisdiction over Apple because Apple has established minimum contacts with the forum. Apple manufactures (directly or indirectly through third party manufacturers)and/or assembles products that are and have been used, offered for sale, sold, and purchased in Delaware. Apple, directly and/or through its distribution network, places wireless communication devices within the stream of commerce, which stream is directed at this district, with the knowledge and/or understanding that such products will be sold in the State of Delaware. Therefore, the exercise of jurisdiction over Apple would not offend traditional notions of fair play and substantial justice.

18. Apple does business in this district, including providing products that are used, offered for sale, sold, and have been purchased in Delaware. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b), (c), (d) and 1400(b).

FACTUAL BACKGROUND

The Mobile Wireless Industry

19. The wireless devices developed and marketed by Nokia and Apple connect to a variety of wireless networks, including the networks of wireless carriers to provide telecommunications service. Carriers operate wireless systems that enable users to place and receive telephone calls, send and receive e-mails, and connect to the internet through wireless devices. Leading carriers in the United States include AT&T (formerly Cingular), T-Mobile USA, Verizon Wireless, and Sprint.

20. Companies around the world manufacture wireless devices. These manufacturers typically sell their phones to the mobile wireless carriers, which in turn sell the phones to users. Wireless devices contain, among other components, one or more computer chipsets that enable the phone to communicate with the carriers' wireless systems. Carriers, device manufacturers, and chipset manufacturers must create equipment and devices compatible with each other by using common mobile wireless technology. Since carriers, device manufacturers, and chipset manufacturers must create equipment and devices compatible with each other to provide mobile wireless services, developers and manufacturers participate in the crucial process of standards development.

21. The progression from cell phones, which primarily focus on voice communications, to smart phones required more advanced mobile wireless technologies for communications involving transmission of data such as e-mail. Since the mass market introduction of the cell phone in the 1980s, mobile wireless technology has evolved to keep pace with the rising volume of voice traffic as well as to incorporate the data transmission capabilities necessary to support increasingly sophisticated phones and other handheld devices. The technology has evolved in what are commonly referred to as "generations" of mobile wireless technology.

22. The first generation of mobile wireless technology (1G) consisted of analog devices and networks that carried only voice traffic. The second generation of mobile wireless technology (2G) began the transition to digital devices and networks providing more efficient use of available spectrum for voice traffic and limited support for data-intensive applications such as paging and text messaging. The emergence of 2G technologies coincided with the growing commercial use of the Internet. The greater data capacity of advanced 2G

networks allowed for the development of the first smart phones, which offered new capabilities such as taking and transmitting photographs, sending and receiving email, and limited web browsing. Third generation (3G) wireless technology supports more advanced data intensive services, such as multimedia, web browsing, music and video downloads, e-commerce, and position location. Fourth Generation (4G) wireless technology is currently being developed. 4G technologies will provide voice, data, and streamed media at much higher data rates compared to the previous generations. Almost all wireless carriers currently support and provide 2G technology, and most have also introduced 3G networks and services. Some carriers have announced plans for migration to 4G networks and services in the coming years.

The Importance of Standards

23. The UMTS and GSM standards, as well as other mobile radio standards, were developed under the patronage of the European Telecommunications Standards Institute ("ETSI"). ETSI is a non-profit institution that was founded in 1988 through an initiative of the European Commission by several companies active in mobile communication with the objective to develop a common mobile radio standard for Europe. Since it was founded, ETSI has grown to include approximately 700 members from 56 countries. Among these members are virtually every company active in the mobile radio sector, who together account for a substantial share of the supply of mobile telecommunications equipment and services. Nokia and Apple are both members of ETSI.

24. ETSI brings important market participants in the mobile radio sector together. Within the context of ETSI, the members develop technical standards, which often lead to a factually binding industry standard. In some cases, national or international regulatory bodies require adherence to particular ETSI standards.

25. Many ETSI members, including Nokia, are engaged in research and development of new telecommunications technologies, and own intellectual property rights relating to different elements of such technologies. Accordingly, when ETSI adopts technical standards, it must take into account that many elements of the standards are likely to be covered by such intellectual property rights. Therefore, others wishing to exploit the standard may need licenses for the essential intellectual property rights to do so. ETSI has therefore adopted an Intellectual Property Policy ("the ETSI IPR Policy") to govern the manner in which ETSI will take account of such intellectual property rights in the process leading to the adoption of ETSI standards.

26. The ETSI IPR policy was adopted in 1994 and the policy has been part of the "ETSI Directives" since December 2004. Its provisions are further explained in the ETSI Guide on Intellectual Property Rights.

27. The objectives of the ETSI IPR Policy are defined in its Clause 3. Clause 3.1 provides as follows:

> It is ETSI's objective to create STANDARDS and TECHNICAL SPECIFICATIONS that are based on solutions which best meet the technical objectives of the European telecommunications sector, as defined by the General Assembly. In order to further this objective the ETSI IPR POLICY seeks to reduce the risk to ETSI, MEMBERS, and others applying ETSI STANDARDS and TECHNICAL SPECIFICATIONS, that investment in the preparation, adoption and application of STANDARDS could be wasted as a result of an ESSENTIAL IPR for a STANDARD or TECHNICAL SPECIFICATION being unavailable. In achieving this objective, the ETSI IPR POLICY seeks a balance between the needs of standardization for public use in the field of telecommunications and the rights of the owners of IPRs.

28. In order to achieve its objectives, the ETSI IPR Policy contains rules regarding the disclosure of essential IPR and rules regarding their licensing on FRAND terms. Members are obligated to use their reasonable endeavors to inform ETSI of essential IPRs in a timely manner, and voluntarily undertake to grant licenses on FRAND terms and conditions.

Therefore, ETSI allows its members to hold and benefit from any IPRs which they may own, including the right to refuse the granting of licenses.

29. Clause 6.1 of the ETSI IPR Policy provides:

> When an essential IPR relating to a particular standard or technical specification is brought to the attention of ETSI, the director-general of ETSI shall immediately request the owner to give within three months an irrevocable undertaking in writing that it is prepared to grant irrevocable licenses on fair, reasonable, and non-discriminatory terms and conditions under such IPR to at least the following extent . . .

30. The ETSI IPR Policy provides that firms owning potentially essential patents will provide undertakings of the kind envisaged by clause 6.1 of the ETSI IPR Policy preferably before adoption of the respective standard. If an owner of an essential IPR does not submit this declaration, keeping its technology proprietary, alternatives are sought to the essential technology, which would not require the infringement of the IPR, pursuant to Clause 8.1.1 of the ETSI IPR Policy. If no technical alternative is available, the development of the respective standards is ceased, under Clause 8.1.2 of the ETSI IPR Policy.

31. Pursuant to the ETSI IPR Policy, Nokia has submitted declarations for certain of the patents-in-suit. For example, with respect to the 465 Patent, Nokia submitted a declaration stating the following:

> The signatory has notified ETSI that it is the proprietor of the IPRs listed above and has informed ETSI that it believes that the IPRs may be considered ESSENTIAL to the Standards listed above. The SIGNATORY and/or its AFFILIATES hereby declare that they are prepared to grant irrevocable licences under the IPRs on terms and conditions which are in accordance with Clause 6.1 of the ETSI IPR Policy, in respect of the STANDARD, to the extent that the IPRs remain essential. …
>
> The construction, validity and performance of this DECLARATION shall be governed by the laws of France.

32. Like ETSI, the Institute of Electrical and Electronics Standards Association (IEEE-SA) is a developer of industry standards in a number of industries, including

telecommunications, information technology, nanotechnology, and information assurance. Among the standards developed by IEEE-SA is IEEE 802.11, the standard for WLAN and IEEE 802.16, the standard for WiMax.

33. Like ETSI, many IEEE-SA members, including Nokia, are engaged in the research and development of new technologies and own intellectual property rights relating to different elements of such technologies. Accordingly, IEEE-SA has adopted a similar intellectual property policy as ETSI in the IEEE-SA Standards Board Bylaws ("IEEE-SA Bylaws").

34. Clause 6.2 of the IEEE-SA Bylaws states that when a standard includes the use of Essential Patent Claims, a "letter of assurance" with regard to the essential patent may be requested. That letter of assurance may include:

> . . . .
>
> A statement that a license for a compliant implementation of the standard will be made available to an unrestricted number of applicants on a worldwide basis without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination. At its sole option, the Submitter may provide with its assurance any of the following: (i) a not-to-exceed license fee or rate commitment, (ii) a sample license agreement, or (iii) one or more material licensing terms.

35. Clause 6.2 of the IEEE-SA Bylaws further provides for an instance where a party providing a letter of assurance discovers additional claims that are essential to a standard:

> If, after providing a Letter of Assurance to the IEEE, the Submitter becomes aware of additional Patent Claim(s) not already covered by an existing Letter of Assurance that are owned, controlled, or licensable by the Submitter that may be or become Essential Patent Claim(s) for the same IEEE Standard but are not the subject of an existing Letter of Assurance, then such Submitter shall submit a Letter of Assurance stating its position regarding enforcement or licensing of such Patent Claims. For the purposes of this commitment, the Submitter is deemed to be aware if any of the following individuals who are from, employed by, or otherwise represent the Submitter have personal knowledge of additional potential Essential Patent Claims, owned or controlled by the Submitter, related to a [Proposed] IEEE Standard and not already the subject of a previously submitted

> Letter of Assurance: (a) past or present participants in the development of the [Proposed] IEEE Standard, or (b) the individual executing the previously submitted Letter of Assurance.

36. Clause 6.2 of the IEEE-SA Bylaws also provides that a letter of assurance, once submitted, is irrevocable.

37. Pursuant to the IEEE-SA Bylaws, Nokia has submitted letters of assurance for certain of the patents-in-suit. For example, with respect to the 465 Patent, Nokia submitted a letter of assurance stating the following:

> In accordance with Clause 6.2 of the *IEEE-SA Standards Board Bylaws*, the Submitter hereby declares the following: …
>
> The Submitter may own, control or have the right to license Patent Claims that might be or become Essential Patent Claims. With respect to such Essential Patent Claims, the submitter's licensing position is as follows: …
>
> The Submitter will grant a license under reasonable rates to an unrestricted number of applicants on a worldwide basis with reasonable terms and conditions that are demonstrably free of unfair discrimination.

F/RAND

38. Standards Setting Organizations ("SSOs") are formed to allow wide promulgation and utilization of commonly defined standards. These standards must be available and accessible in order to produce the intended efficiency gains and benefits and thereby for the standardization process itself to comply with competition law. Intellectual Property Rights policies ("IPR Policies"), like those described above, provide essential IPR holders committing to license on F/RAND terms with the benefit of collecting F/RAND compensation from a far larger market than they would have enjoyed if the protected technology had not been incorporated in the standard. Because competing proprietary technologies and systems have been abandoned in favor of a single, universal, and standardized system and set of technologies, a holder of an essential IPR can collect royalties on a large volume of standards-compliant

products from a wide variety of manufacturers worldwide. In contrast, if the IPR holder's protected technology was only used in one of a number of competing systems or proprietary technologies, the patent holder could only generate returns on its R&D investments through differentiation and -- if it chose to license -- only collect royalties from manufacturers who chose to market and sell products for the narrow proprietary technology. This is why committing to F/RAND licensing is advantageous and rarely refused by essential IPR holders.

39. An IPR holder that has voluntarily undertaken to license its IPRs on F/RAND terms (instead of keeping the inventions proprietary) has irrevocably committed to allow the standard to be implemented under its IPR on F/RAND basis and thereby waived -- absent exceptional circumstances -- its legally defined right to exclude others from practicing the standard under its IPR. This also means that the IPR holder cannot use its hold-up power resulting from the incorporation of its technology into the standard and the IPR holder's right to exclude to extort royalties that do not comply with F/RAND.

40. Once an IPR holder has made a F/RAND commitment, all manufacturers have the right to implement the standard in their products and use the inventions from any declared essential IPRs. There is no need to wait until all the particular F/RAND terms and conditions have been negotiated with the IPR holder or until a definitive license agreement is executed setting out those terms. However, it is clear that in return for the right to practice the standard under the essential IPRs, implementing manufacturers have the obligation to pay F/RAND compensation for the IPR used (to the extent not invalid or unenforceable). For example, according to the ETSI IPR Policy Clause 3.2:

> IPR holders whether members of ETSI and their AFFILIATES or third parties, should be adequately and fairly rewarded for the use of their IPRs in the implementation of STANDARDS and TECHNICAL SPECIFICATIONS.

41. Save for cases where the manufacturer refuses to take a license altogether, it follows from F/RAND licensing commitments that the IPR holder has a duty to negotiate in good faith and propose F/RAND terms. Negotiations over F/RAND terms may cover the essential IPR portfolio as a whole but, if requested, F/RAND terms should be available for each patent separately.

42. If the implementer refuses to take a license altogether or refuses to pay F/RAND compensation for valid and enforceable IPRs used by it, exceptional circumstances are present and the IPR holder may seek an injunction to prevent the implementer from continuing to manufacture standard-compliant products without payment. The injunction only extends for so long as the manufacturer refuses to pay F/RAND compensation.

Apple's Refusal to pay F/RAND Compensation

43. Nokia has irrevocably undertaken the obligation to grant license(s) on F/RAND terms and conditions to its essential patents, including the patents-in-suit, and Apple has the corresponding right to claim licenses on F/RAND terms on the basis of Nokia's undertakings.

44. In compliance with its declarations and undertakings which Nokia submitted with regard to the patents-in-suit, prior to filing this complaint Nokia has negotiated in good faith over the F/RAND licensing terms with Apple. Nokia has made various offers to Apple for the F/RAND terms and conditions of a license agreement under which the patents-in-suit could be licensed either individually or in combination with other Nokia essential patents. In its offers, made subject to reciprocity, Nokia has defined both a portfolio rate and an average per patent royalty rate which Apple could have accepted within a reasonable time. Nokia has also provided Apple with information on the method used to calculate royalties as well as claim charts assisting Apple with its technical analysis.

45. Apple has rejected Nokia's offers for the F/RAND terms and conditions both on a portfolio and on a per patent basis and thereby refused to compensate Nokia on F/RAND terms for the use of Nokia patented technology, including the patents-in-suit.

46. Due to Apple's violation of its obligation to pay F/RAND compensation for the use of Nokia's patents, Nokia has no choice but to file this Complaint in order to enforce its right to be compensated on a F/RAND basis for the use of the patents in suit in Apple's standards-compliant products, and to prevent further infringement unless and until Apple pays F/RAND compensation, together with interest, for its past infringement and irrevocably commits to payment of such compensation in the future.

OVERVIEW OF THE PATENTS-IN-SUIT.

47. The patents-in-suit are a reflection of Nokia's research and development and achievements in the world of mobile communications. To provide a few examples, Nokia is a leader in wireless data and owns important patents in this area. Today's wireless devices are used for a wide variety of tasks, such as sending email, browsing the Internet, and downloading applications. These tasks all involve Nokia's advances in wireless data. Without these advances, it would be difficult to work remotely from a coffee shop or download a new game to a phone.

48. Nokia is also a leader in speech coding and owns important patents in this area. In order to send audio, today's phones transmit the audio as a series of 1's and 0's. Speech coding is the backbone of any digital wireless system. Without speech coding, it would be difficult to talk clearly or listen to music without overwhelming the limited resources of the network.

49. Nokia is also a leader in security and encryption and owns important patents in this area. Today's wireless devices are frequently used for e-commerce and other purchases. Nokia's technology allows people to use their wireless devices to conduct business without their confidential information being intercepted.

Wireless Data Patents

50. The 465 Patent, entitled *Data Transmission in a Radio Telephone Network*, was duly and lawfully issued on September 1, 1998. Nokia is the current owner of all rights, title, and interest in the 465 Patent. A true and correct copy of the 465 Patent is attached hereto as Exhibit A.

51. The 465 Patent is essential and has been declared essential to at least the GSM, UMTS, and IEEE 802.11 standards. The 465 Patent invention allows communication over wireless networks while conserving resources on the network. It provides for the formation of a virtual data channel, such that a real data channel can be quickly established when data transmission is desired.

52. The 904 Patent, entitled *Data Transfer in a Mobile Telephone Network*, was duly and lawfully issued on March 19, 2002. Nokia is the current owner of all rights, title, and interest in the 904 Patent. A true and correct copy of the 904 Patent is attached hereto as Exhibit B.

53. The 904 Patent is essential and has been declared essential to at least the GSM and IEEE 802.11 standards. The 904 Patent allows for simpler communication on the networks. The invention provides that, in a radio block to be coded, user data is transferred in octet form to simplify the flow of data in the network.

54. The 135 Patent, entitled *Measurement Report Transmission in a Telecommunications System*, was duly and lawfully issued on February 17, 2004. Nokia is the

current owner of all rights, title, and interest in the 135 Patent. A true and correct copy of the 135 Patent is attached hereto as Exhibit C.

55. The 135 Patent is essential and has been declared essential to at least the GSM standard. The 135 Patent provides an efficient method of communicating information about a mobile device operating in downlink transfer by enabling the mobile device to respond to polling codes with messages that indicate the condition of the mobile device.

56. The 548 Patent, entitled *Access Channel for Reduced Access Delay in a Telecommunications System*, was duly and lawfully issued on August 10, 2004. Nokia is the current owner of all rights, title, and interest in the 548 Patent. A true and correct copy of the 548 Patent is attached hereto as Exhibit D.

57. The 548 Patent is essential and has been declared essential to at least the UMTS standard. The 548 Patent enables a mobile station to access the network with less delay. The '548 invention enables access requests to be adjusted based on channel conditions, reducing overall access delays.

58. The 672 Patent, entitled *Reporting Cell Measurement Results in a Cellular Communication System*, was duly and lawfully issued on August 15, 2006. Nokia is the current owner of all right, title, and interest in the 672 Patent. A true and correct copy of the 672 Patent is attached hereto as Exhibit E.

59. The 672 Patent is essential and has been declared essential to at least the GSM standard. The 672 Patent enables a mobile device to report an increased number of signal quality measurements to a mobile network.

Speech Coding Patents

60. The 178 Patent, entitled *Method and Apparatus for Speech Transmission in a Mobile Communications System*, was duly and lawfully issued on January 19, 1999. Nokia

is the current owner of all rights, title, and interest in the 178 Patent. A true and correct copy of the 178 Patent is attached hereto as Exhibit F.

61. The 178 Patent is essential and has been declared essential to at least the GSM standard. The 178 Patent ensures clear, efficient speech communications over mobile networks. The 178 Patent invention enables multiple speech coding methods to operate at different transmission rates by using two stages of channel encoding, one of which is dependent on the speech coding method, and one of which is not dependent on the speech coding method.

62. The 651 Patent, entitled *Speech Synthesizer Employing Post-Processing for Enhancing the Quality of the Synthesized Speech*, was duly and lawfully issued on August 31, 1999. Nokia is the current owner of all rights, title, and interest in the 651 Patent. A true and correct copy of the 651 Patent is attached hereto as Exhibit G.

63. The 651 Patent is essential and has been declared essential to at least the GSM standard. The 651 Patent ensures clear voice and audio communications over mobile networks. The 651 Patent invention provides for a postfilter for processing speech signals derived from an excitation code book and adaptive code book of a speech decoder.

Security and Encryption Patents

64. The 727 Patent, entitled *Method of Ciphering Data Transmission in a Radio System*, was duly and lawfully issued on April 19, 2005. Nokia is the current owner of all rights, title, and interest in the 727 Patent. A true and correct copy of the 727 Patent is attached hereto as Exhibit H.

65. The 727 Patent is essential and has been declared essential to at least the UMTS standard. The 727 Patent ensures secure transmission of data over mobile networks. The '727 invention prevents data from falling into the wrong hands by using a ciphering algorithm with a channel-specific parameter among its inputs.

66. The 940 Patent, entitled *Integrity Check in a Communication System*, was duly and lawfully issued on March 7, 2006. Nokia is the current owner of all rights, title, and interest in the 940 Patent. A true and correct copy of the 940 Patent is attached hereto as Exhibit I.

67. The 940 Patent is essential and has been declared essential to at least the UMTS standard. The 940 Patent ensures secure transmission of data over mobile networks. The 940 Patent protects communications using an integrity algorithm calculated from values including channel identity information.

68. The 621 Patent, entitled *System for Ensuring Encrypted Communication After Handover*, was duly and lawfully issued on July 22, 2008. Nokia is the current owner of all rights, title, and interest in the 621 Patent. A true and correct copy of the 621 Patent is attached hereto as Exhibit J.

69. The 621 Patent is essential and has been declared essential to at least the GSM and UMTS standards. The 621 Patent ensures continued secure transmissions during a handover by communicating information about encryption algorithms supported by a mobile station between radio access networks.

APPLE'S INFRINGEMENT

70. Upon information and belief, Apple has infringed and continues to infringe each of the patents-in-suit by engaging in acts constituting infringement under 35 U.S.C. § 271, including but not necessarily limited to one or more of making, using, selling and offering to sell, in this District and elsewhere in the United States, and importing into this District and elsewhere in the United States, one or more products and services that comply with the GSM, UMTS, and/or IEEE 802.11 standards, including wireless communication devices such as the Apple iPhone, the Apple iPhone 3G, and Apple iPhone 3GS.

HARM TO NOKIA FROM APPLE'S INFRINGEMENT

71. Nokia is harmed by Apple's failure to pay F/RAND compensation for its use of Nokia patented technology in a way that cannot necessarily be compensated for by a payment of a past due F/RAND royalty alone. Apple's failure to pay a F/RAND rate for the use of the patents-in-suit in its products at the time of their sale allows it to charge less for its products because it does not have to recover the costs of development of the technology used in the device. This allows it to obtain market share that it would otherwise not be able to obtain were its products to bear the costs for the patented technology.

72. Nokia's products, in turn, must bear the costs of the development of the technology that allows them to function in compliance with the relevant standards. This puts Nokia in a competitive disadvantage to "free-riders" such as Apple.

73. Even if Apple were to subsequently pay past due F/RAND royalties, it would still enjoy a market share it otherwise would not have but for the period of "free riding." Nokia would likewise lose its portion of the market share for the period of the "free riding." Due to the difficulty in predicting whether, if at all, such market share can be recovered, Nokia's harm cannot be compensated by payment of past due F/RAND royalties alone.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 5,802,465

74. Nokia incorporates by reference the allegations set forth in Paragraphs 1-73 of this Complaint as though fully set forth herein.

75. Apple has infringed and is infringing the 465 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services including wireless communication devices such as the Apple iPhone, the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 465 Patent.

76. Apple is inducing the infringement of the 465 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

77. Apple is contributing to the infringement of the 465 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

78. Apple's infringement of the 465 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

79. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 5,862,178

80. Nokia incorporates by reference the allegations set forth in Paragraphs 1-79 of this Complaint as though fully set forth herein.

81. Apple has infringed and is infringing the 178 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services that include an encoder and decoder for simultaneous bi-directional voice and/or data communications, including wireless communication devices such as the Apple iPhone, the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 178 Patent. Nokia does not allege infringement by Apple based on the making, using, offering for sale, or selling in the United States any product that does not include an encoder and decoder for simultaneous bi-directional voice and/or data communications.

82. Apple is inducing the infringement of the 178 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

83. Apple is contributing to the infringement to the infringement of the 178 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

84. Apple's infringement of the 178 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

85. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 5,946,651

86. Nokia incorporates by reference the allegations set forth in Paragraphs 1-85 of this Complaint as though fully set forth herein.

87. Apple has infringed and is infringing the 651 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services that include an encoder and decoder for simultaneous bi-directional voice and/or data communications, including wireless communication devices such as the Apple iPhone, the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 651 Patent. Nokia does not allege infringement by Apple based on the making, using, offering for sale, or selling in the United States any product that does not include an encoder and decoder for simultaneous bi-directional voice and/or data communications.

88. Apple is inducing the infringement of the 651 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

89. Apple is contributing to the infringement to the infringement of the 651 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

90. Apple's infringement of the 651 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

91. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 6,359,904

92. Nokia incorporates by reference the allegations set forth in Paragraphs 1-91 of this Complaint as though fully set forth herein.

93. Apple has infringed and is infringing the 904 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services including wireless communication devices such as the Apple iPhone, the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 904 Patent.

94. Apple is inducing the infringement of the 904 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

95. Apple is contributing to the infringement to the infringement of the 904 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

96. Apple's infringement of the 904 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

97. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 6,694,135

98. Nokia incorporates by reference the allegations set forth in Paragraphs 1-97 of this Complaint as though fully set forth herein.

99. Apple has infringed and is infringing the 135 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services including wireless communication devices such as the Apple iPhone, the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 135 Patent.

100. Apple is inducing the infringement of the 135 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

101. Apple is contributing to the infringement to the infringement of the 135 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

102. Apple's infringement of the 135 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

103. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 6,775,548

104. Nokia incorporates by reference the allegations set forth in Paragraphs 1-103 of this Complaint as though fully set forth herein.

105. Apple has infringed and is infringing the 548 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services including wireless communication devices such as the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 548 Patent.

106. Apple is inducing the infringement of the 548 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

107. Apple is contributing to the infringement to the infringement of the 548 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

108. Apple's infringement of the 548 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

109. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT VII
INFRINGEMENT OF U.S. PATENT NO. 6,882,727

110. Nokia incorporates by reference the allegations set forth in Paragraphs 1-109 of this Complaint as though fully set forth herein.

111. Apple has infringed and is infringing the 727 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services including wireless communication devices such as the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 727 Patent.

112. Apple is inducing the infringement of the 727 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

113. Apple is contributing to the infringement to the infringement of the 727 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

114. Apple's infringement of the 727 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

115. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT VIII
INFRINGEMENT OF U.S. PATENT NO. 7,009,940

116. Nokia incorporates by reference the allegations set forth in Paragraphs 1-115 of this Complaint as though fully set forth herein.

117. Apple has infringed and is infringing the 940 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services

including wireless communication devices such as the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 940 Patent.

118. Apple is inducing the infringement of the 940 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

119. Apple is contributing to the infringement to the infringement of the 940 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

120. Apple's infringement of the 940 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

121. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT IX
INFRINGEMENT OF U.S. PATENT NO. 7,092,672

122. Nokia incorporates by reference the allegations set forth in Paragraphs 1-121 of this Complaint as though fully set forth herein.

123. Apple has infringed and is infringing the 672 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services including wireless communication devices such as the Apple iPhone 3G, and Apple iPhone 3GS, that infringe one or more claims of the 672 Patent.

124. Apple is inducing the infringement of the 672 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

125. Apple is contributing to the infringement to the infringement of the 672 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

126. Apple's infringement of the 672 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

127. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT X
INFRINGEMENT OF U.S. PATENT NO. 7,403,621

128. Nokia incorporates by reference the allegations set forth in Paragraphs 1-127 of this Complaint as though fully set forth herein.

129. Apple has infringed and is infringing the 621 Patent by making, using, offering for sale, and selling in the United States, without authority, products and services including wireless communication devices such as the Apple iPhone, the Apple iPhone 3G, and Apple iPhone 3GS, that are covered by one or more claims of the 621 Patent.

130. Apple is inducing the infringement of the 621 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

131. Apple is contributing to the infringement to the infringement of the 621 Patent by others in the United States. The direct infringement occurs by the activities of end users of the accused products.

132. Apple's infringement of the 621 Patent is exceptional and entitles Nokia to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

133. Apple's acts of infringement have caused damage to Nokia and Nokia is entitled to recover from Apple F/RAND compensation as a result of Apple's wrongful acts in an amount subject to proof at trial, and such other relief as may be appropriate.

COUNT XI
DECLARATORY JUDGMENT REGARDING F/RAND RIGHTS

134. Nokia incorporates by reference the allegations set forth in Paragraphs 1-133 of this Complaint as though fully set forth herein.

135. The patents-in-suit are infringed, not invalid, and enforceable.

136. Prior to filing this lawsuit, Nokia made various offers to Apple for a license to make, use, offer to sell, and/or sell products embodying the claims of the patents-in-suit, and/or the methods of the claims of the patents-in-suit.

137. Nokia has met its obligations under its F/RAND undertakings through, among other things, the offers made by Nokia to Apple.

138. Despite Nokia's offers for the F/RAND terms and conditions for a license under the patents-in-suit to Apple, Apple has refused to compensate Nokia on F/RAND terms for the use of the patents-in-suit in breach of its obligation to pay for the use of Nokia's patents.

139. Apple's continued use of the patents-in-suit without paying F/RAND compensation has caused and will continue to cause Nokia irreparable harm unless enjoined by the Court until Apple pays to Nokia F/RAND compensation for past infringement, and irrevocably commits to payment of such compensation in the future.

140. Once the appropriate compensation on F/RAND terms is determined, Apple should be enjoined from importing, making, using, selling, or offering for sale products and services embodying the claimed inventions of the patents-in-suit until and unless it pays

Nokia F/RAND compensation for past infringement, and irrevocably commits to payment of such compensation in the future.

141. This Court's equitable powers are hereby invoked by this Count, and Nokia accordingly requests that the Court consider such other relief, equitable or otherwise, as it may find appropriate at the time for entry of judgment in this case.

DEMAND FOR JURY TRIAL

142. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Nokia demands a trial by jury of this action.

PRAYER FOR RELIEF

WHEREFORE, Nokia prays for judgment and seeks relief against Apple as follows:

(a) For judgment that the patents-in-suit have been and continue to be directly and/or indirectly infringed by Apple;

(b) For judgment that the patents-in-suit are not invalid and are enforceable;

(c) For judgment that Nokia has complied with its legal obligations with respect to negotiating F/RAND terms and conditions of licenses to the patents-in-suit to Apple;

(d) For judgment that Apple has refused to compensate Nokia on a F/RAND basis for Apple's use of the patents-in-suit;

(e) Once the appropriate F/RAND compensation is determined, for a permanent injunction preventing further infringement, contributory infringement, and inducement of infringement until and unless Apple pays to Nokia such F/RAND compensation for past infringement, and irrevocably commits to payment of such compensation in the future.;

(f) For actual F/RAND damages together with prejudgment interest;

(g) For an award of attorneys' fees pursuant to 35 U.S.C. § 285 or as otherwise permitted by law;

(h) For all costs of suit; and

(i) For such other and further relief as the Court may deem just and proper.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

Jack B. Blumenfeld (#1014)
Rodger D. Smith II (#3778)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
rsmith@mnat.com

Attorneys for Plaintiff Nokia Corporation

OF COUNSEL:

Patrick J. Flinn
John D. Haynes
ALSTON & BIRD LLP
One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309
(404) 881-7000

October 22, 2009

EXHIBIT A

US005802465A

United States Patent [19]

Hamalainen et al.

[11] **Patent Number: 5,802,465**

[45] **Date of Patent: Sep. 1, 1998**

[54] **DATA TRANSMISSION IN A RADIO TELEPHONE NETWORK**

[75] Inventors: **Jari Hamalainen**, Tampere; **Timo Jokiaho**, Vantaa, both of Finland

[73] Assignee: **Nokia Mobile Phones Ltd.**, United Kingdom

[21] Appl. No.: **724,375**

[22] Filed: **Oct. 1, 1996**

Related U.S. Application Data

[63] Continuation of Ser. No. 301,340, Sep. 6, 1994, abandoned.

[30] **Foreign Application Priority Data**

Sep. 6, 1993 [FI] Finland 933894

[51] **Int. Cl.**^{6} **H04Q 7/20**

[52] **U.S. Cl.** **455/403**; 455/452; 455/560

[58] **Field of Search** 455/403, 422, 455/450, 452, 455, 509, 516, 550, 560, 435; 370/389, 338

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,763,319	8/1988	Rozenblit	370/84
4,837,800	6/1989	Freeburg et al.	379/59
4,887,265	12/1989	Felix	370/94.1
4,972,506	11/1990	Uddenfeldt	455/33
5,008,883	4/1991	Eizenhofer et al.	370/95.1
5,081,704	1/1992	Umeda et al.	455/33
5,103,445	4/1992	Ostlund	370/79
5,109,527	4/1992	Akerberg	455/33.2
5,142,533	8/1992	Crisler et al.	370/95.1
5,159,702	10/1992	Aratake	455/33.1
5,166,929	11/1992	Lo	370/85.3

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0048854 A1	4/1982	European Pat. Off. .	
0048861 A1	4/1982	European Pat. Off. .	
0 369 535 A3	5/1990	European Pat. Off.	H04Q 7/04
0 399 611 A3	11/1990	European Pat. Off.	H04Q 7/04
0399612A2	11/1990	European Pat. Off. .	
0587980 A2	3/1994	European Pat. Off. .	
2 270 815	3/1994	United Kingdom .	
WO 94/10767	5/1994	WIPO .	

OTHER PUBLICATIONS

IEEE Transactions On Vehicular Technology, "Voice and Data Integration in the Air-Interface of a Microcellular Mobile Communication System", vol. 42, No. 1, Feb. 93.

DeVile, J.M., "A Reservation Based Multiple Access Scheme For A Future Universal Mobile Telecommunications System", Seventh IEE European Conf. On Mobile And Personal Communications, 15 Dec. 1993, pp. 210–215.

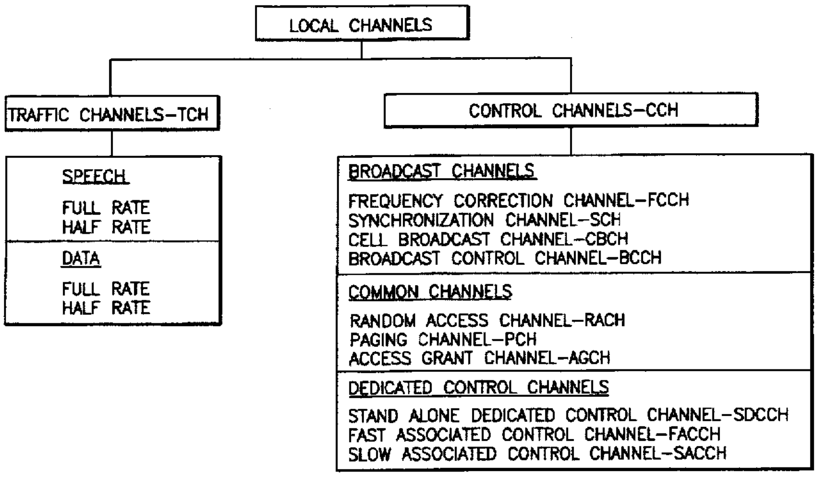
(List continued on next page.)

Primary Examiner—Dwayne D. Bost
Assistant Examiner—William G. Trost
Attorney, Agent, or Firm—Perman & Green, LLP

[57] **ABSTRACT**

For bidirectional transmission of packet data, a packet data service unit (Agent) is disposed in a digital cellular system connected to be in association with a Mobile Switching Center, and connecting the cellular network to the date network. As a mobile station is connected to the packet data service unit, signalling related to connection formation characteristics of the network is first accomplished. As a result thereof, the mobile station and the data service unit are provided with a number of stored parameters relating to each other. This situation creates or is called a virtual channel. When a mobile station wants to transmit or receive data packets between the mobile station and the data service unit a packet data transfer channel is established making use of the parameters of the virtual channel and thereby using substantially less signalling than the channel establishment signalling characteristic of the network, one part thereof being a radio channel and the other part a time slot in a digital trunk line. On termination of data packet transfer, at least said radio channel is disassembled but the virtual channel is maintained until the disconnection of the mobile station from the data service.

32 Claims, 7 Drawing Sheets


LOCAL CHANNELS
TRAFFIC CHANNELS–TCH
SPEECH
FULL RATE
HALF RATE
DATA
FULL RATE
HALF RATE
CONTROL CHANNELS–CCH
BROADCAST CHANNELS
FREQUENCY CORRECTION CHANNEL–FCCH
SYNCHRONIZATION CHANNEL–SCH
CELL BROADCAST CHANNEL–CBCH
BROADCAST CONTROL CHANNEL–BCCH
COMMON CHANNELS
RANDOM ACCESS CHANNEL–RACH
PAGING CHANNEL–PCH
ACCESS GRANT CHANNEL–AGCH
DEDICATED CONTROL CHANNELS
STAND ALONE DEDICATED CONTROL CHANNEL–SDCCH
FAST ASSOCIATED CONTROL CHANNEL–FACCH
SLOW ASSOCIATED CONTROL CHANNEL–SACCH

U.S. PATENT DOCUMENTS

5,199,031	3/1993	Dahlin	370/110.1
5,239,678	8/1993	Grube et al.	455/54.1 X
5,276,680	1/1994	Messenger	379/63 X
5,359,603	10/1994	McTiffin	370/94.1
5,404,355	4/1995	Raith	370/95.1
5,404,392	4/1995	Miller et al.	379/59 X
5,420,864	5/1995	Dahlin et al.	370/95.3
5,430,724	7/1995	Fall et al.	370/95.3 X
5,434,847	7/1995	Kou	370/17
5,487,065	1/1996	Acampora et al.	379/63 X

OTHER PUBLICATIONS

Ziegeler, R. et al., "An Experimental Implementation of the PRMA Protocol for Wireless Communication", IEEE, 1993, pp. 909–912.

Mouly, et al., The GSM System for Mobile Communications, 1992, France, pp. 215–216, 231–241, 346–349.

Hodges, M.R.L., The GSM radio interface, British Telecom Technology Journal vol. 8 No. 1, Jan. 1990, pp. 31–43.

"European digital cellular telecommunications system (Phase 2); Mobile radio interface layer 3 specification(GSM) 04.08)", ESTI, May 1995, pp. 37–40, 183–186.

"European digital cellular telecommunications system (Phase 2); Physical layer on the radio path General description (GSM 05.01)" ETSI, May 1995, pp. 1–19.

"European digital cellular telecommunications system (Phase 2); Channel coding (GSM 05.03)", ESTI, Aug. 1995, pp. 1–5 and Mar. 1995, pp. 1–31.

Electronics and Communication Journal, vol. 5, No. 3, 1 Jun. 1993, pp. 180–186, Dunlop, J., "A Reservation Based Access Mechanism For 3rd Generation Cellular Systems".

IEEE Transactions On Vehicular Technology, vol. 39, No. 4, 1 Nov. 1990, pp. 340–351, Mitrou et al. "A Reservation Multiple Access Protocol For Microcellular Mobile–Communicatin Systems".

Finnish Office Action dated 2 Aug. 1994 on Finnish priority application No. 933894 and English translation thereof.

S. Chakraborty, Data interworking with GSM, Proceedings of 5th Nordic Seminar on Digital Mobile Radio Communications, pp. 389–395, DMR V, Helsinki '92.

R. Tafazolli, B. G. Evans, Interworking and integration of the Inmarsat Standard–M with the Pan–European GSM system, Proceedings of 3rd.

International Mobile Satellite Conference, Jet Propulsion Lab, CA, 1993.

E. J. Younger, K. H. Bennet, R. Hartley–Davies, A Model for a broadband cellular wireless network for digital communications, Compter Networks and ISDN Systems, vol. 26, No. 4, Netherlands, 1993.

Data Networks, D. Bertsekas, R. Gallager, Prentice–Hall Inc., 1987 New Jersey, Chapters 2.7 and 2.8.3, pp. 91, 92, 99, 100, 101.

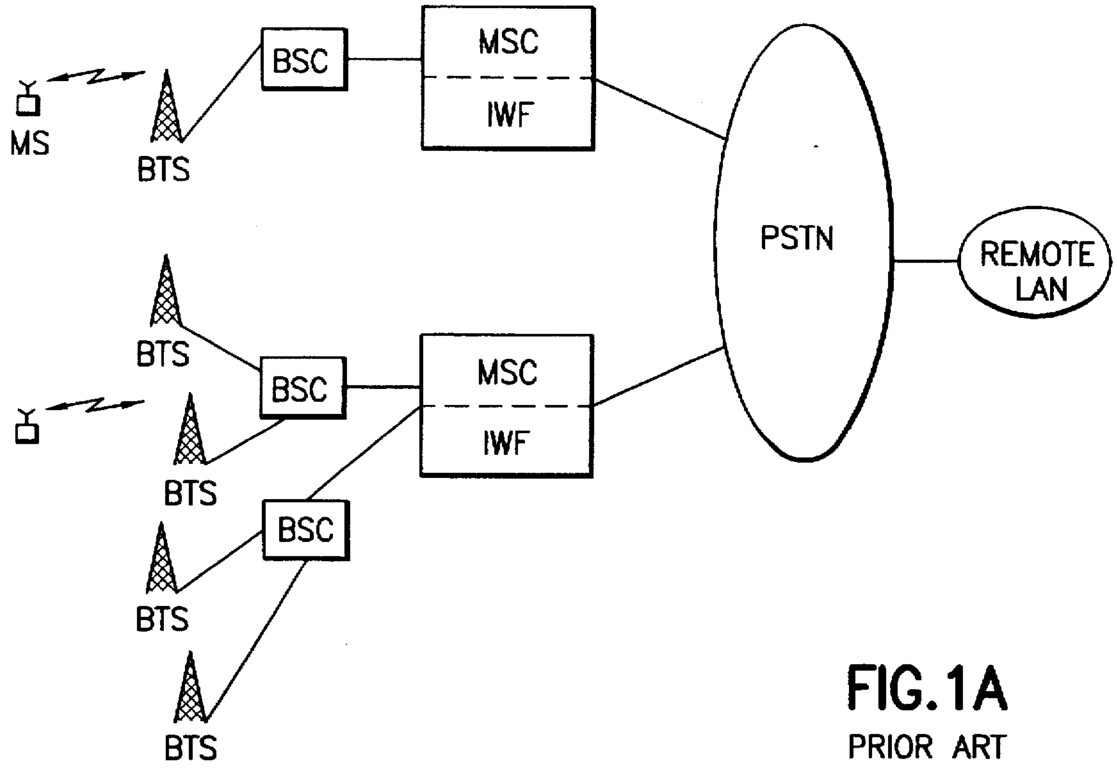


FIG. 1A
PRIOR ART

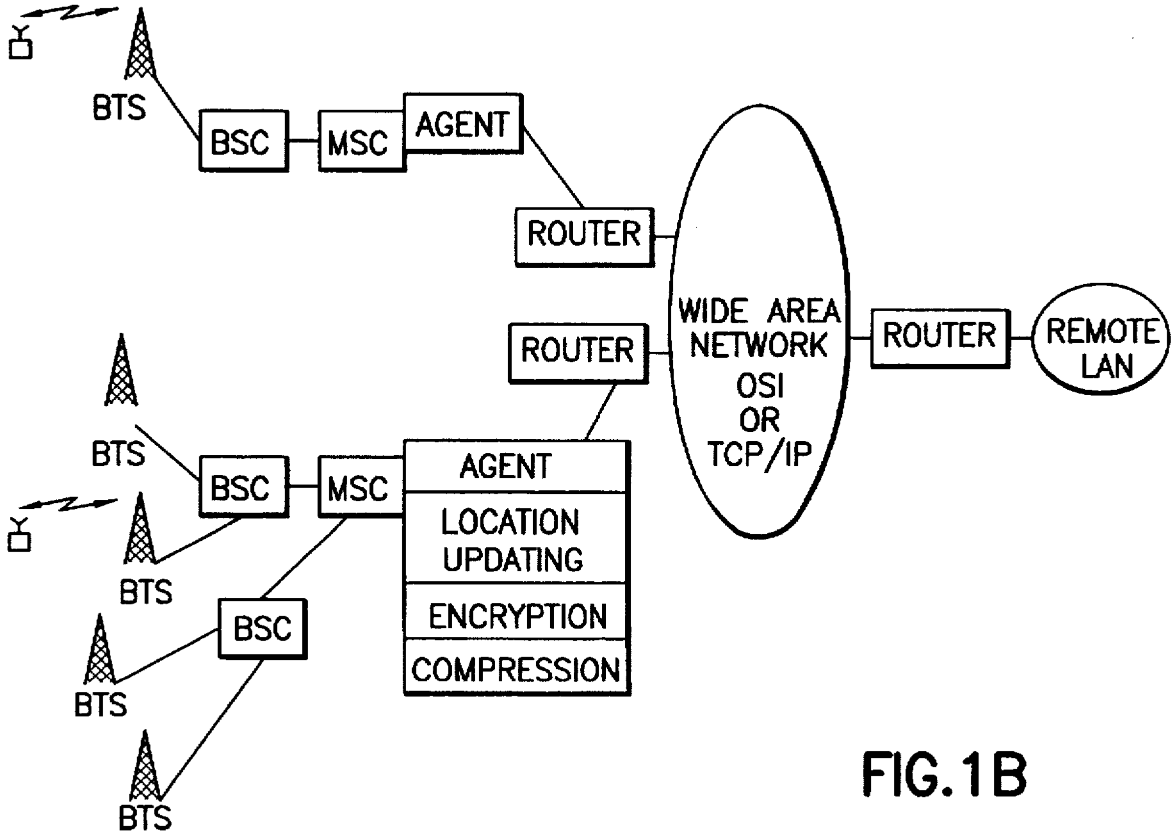


FIG. 1B

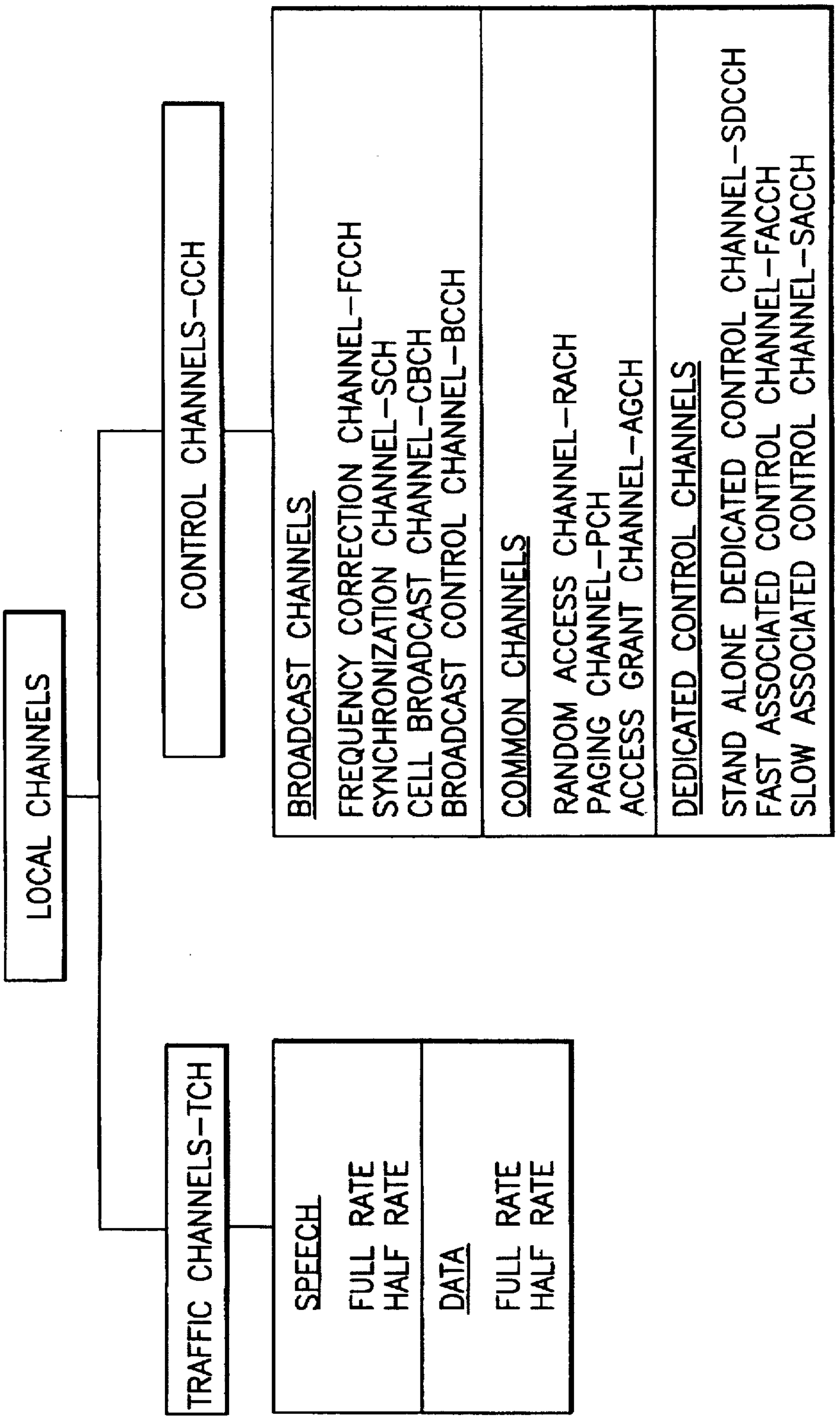

LOCAL CHANNELS
CONTROL CHANNELS-CCH
BROADCAST CHANNELS
FREQUENCY CORRECTION CHANNEL-FCCH
SYNCHRONIZATION CHANNEL-SCH
CELL BROADCAST CHANNEL-CBCH
BROADCAST CONTROL CHANNEL-BCCH
COMMON CHANNELS
RANDOM ACCESS CHANNEL-RACH
PAGING CHANNEL-PCH
ACCESS GRANT CHANNEL-AGCH
DEDICATED CONTROL CHANNELS
STAND ALONE DEDICATED CONTROL CHANNEL-SDCCH
FAST ASSOCIATED CONTROL CHANNEL-FACCH
SLOW ASSOCIATED CONTROL CHANNEL-SACCH
TRAFFIC CHANNELS-TCH
SPEECH
FULL RATE
HALF RATE
DATA
FULL RATE
HALF RATE

FIG.2

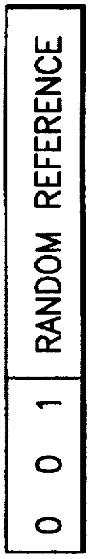

0 0 1
RANDOM REFERENCE

FIG.3

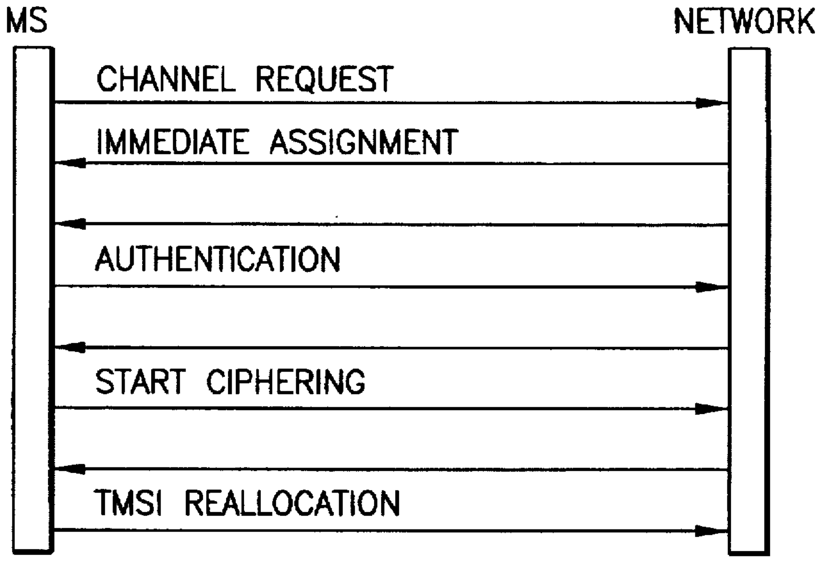


FIG.4

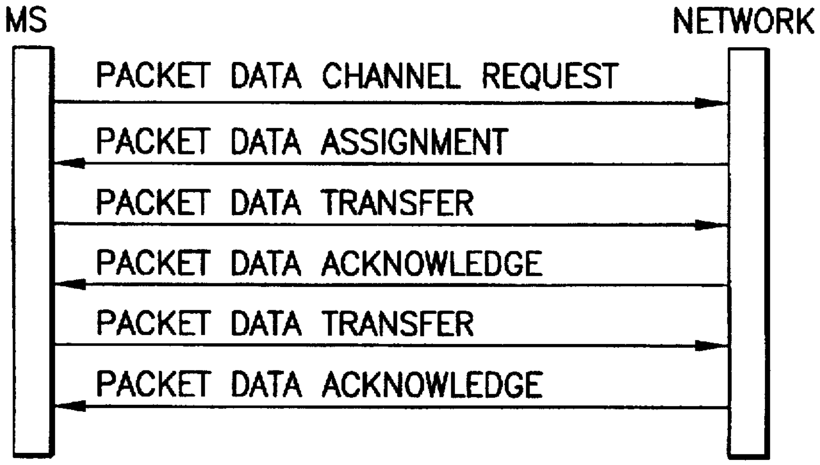


FIG.5

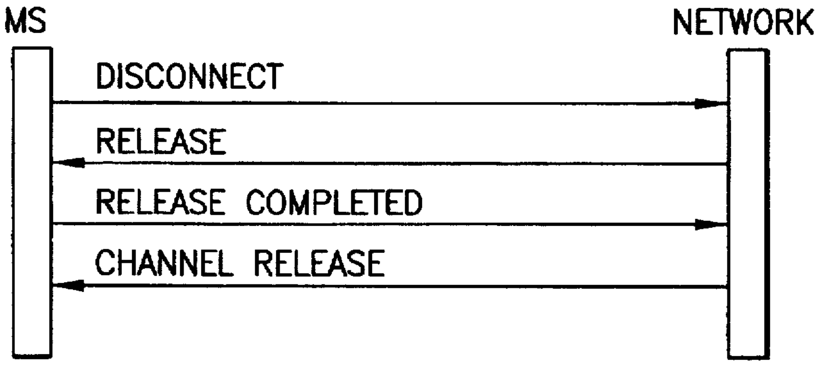


FIG.6

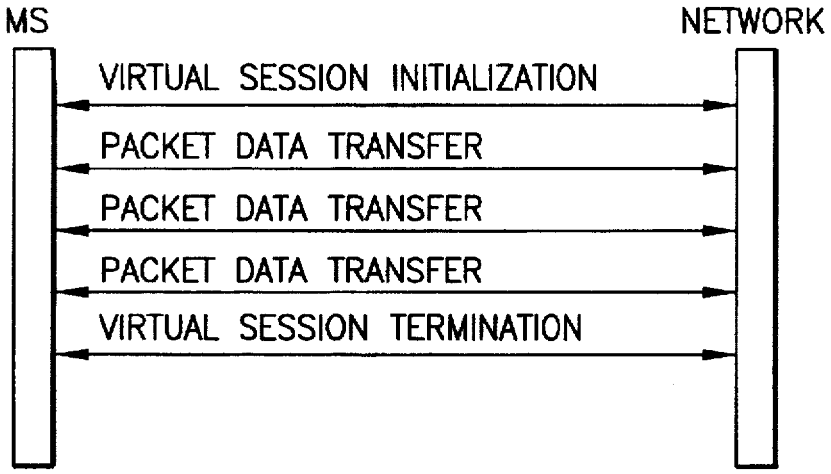


FIG.7

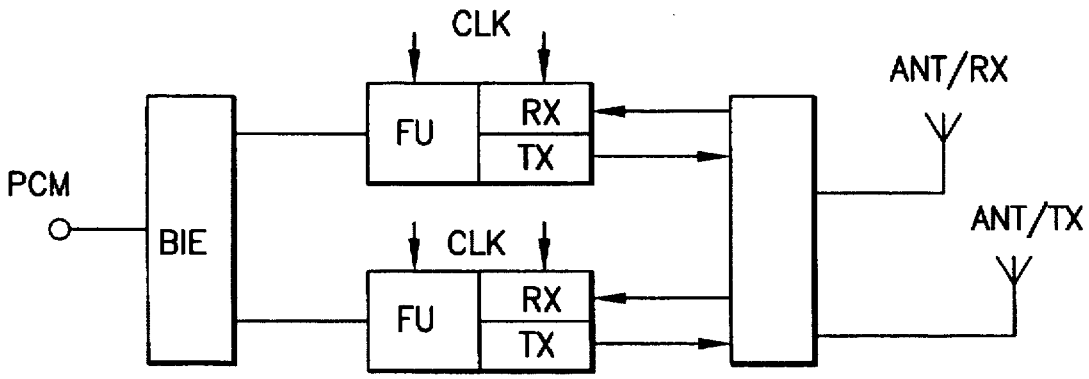


FIG.8

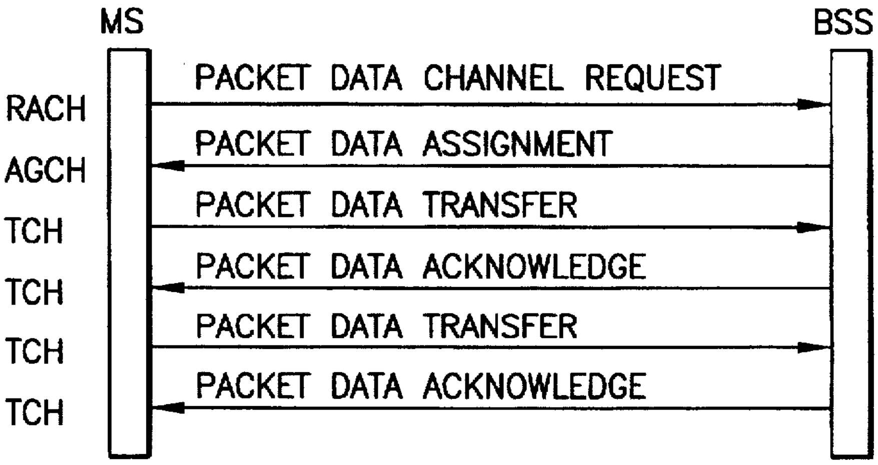


FIG.9

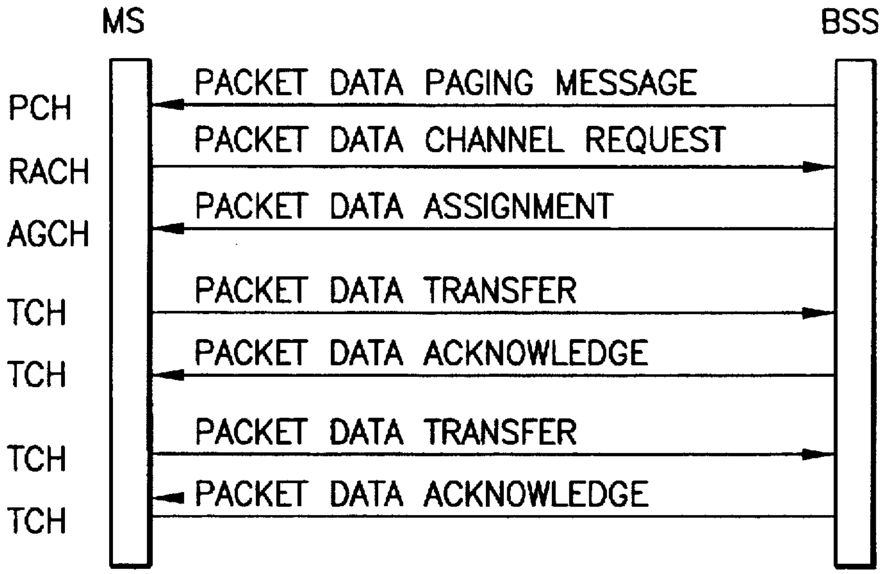


FIG.10

HEADER	VARIABLE LENGTH OF DATA BITS

FIG.11

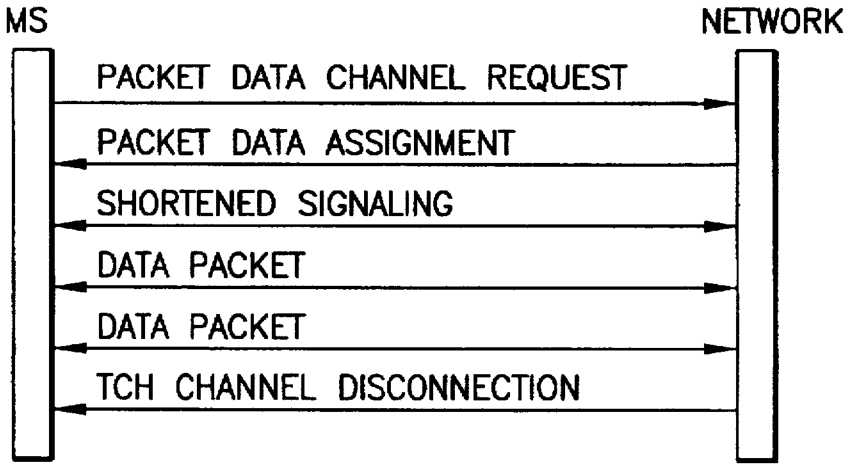


FIG.15

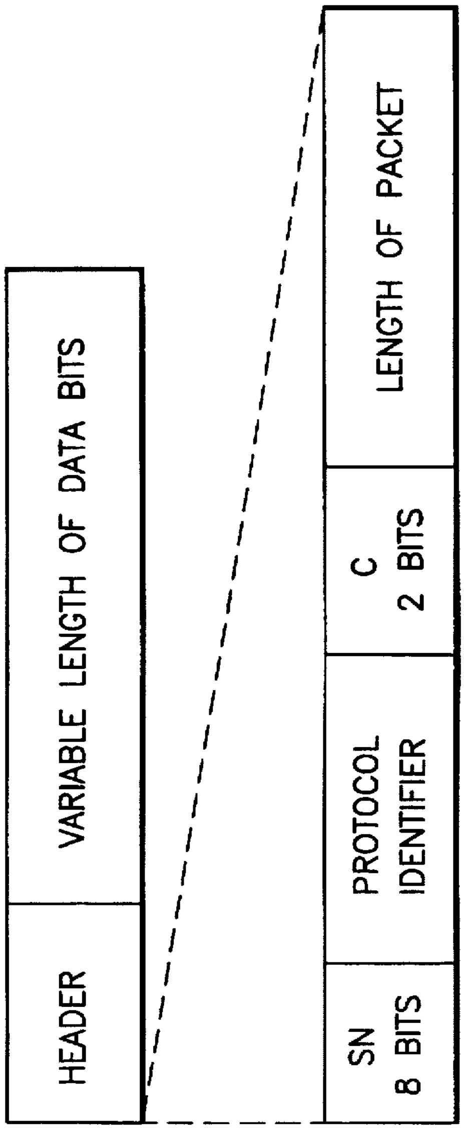

HEADER
VARIABLE LENGTH OF DATA BITS
SN
8 BITS
PROTOCOL
IDENTIFIER
C
2 BITS
LENGTH OF PACKET

FIG.12

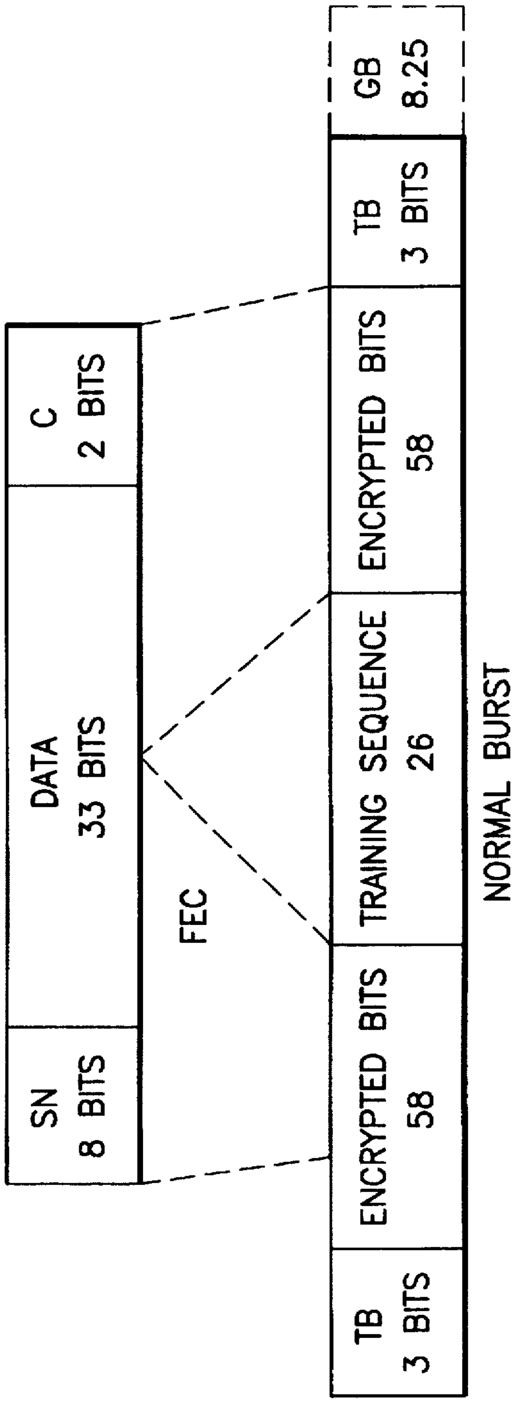

SN
8 BITS
DATA
33 BITS
C
2 BITS
FEC
TB
3 BITS
ENCRYPTED BITS
58
TRAINING SEQUENCE
26
ENCRYPTED BITS
58
TB
3 BITS
GB
8.25
NORMAL BURST

FIG.13

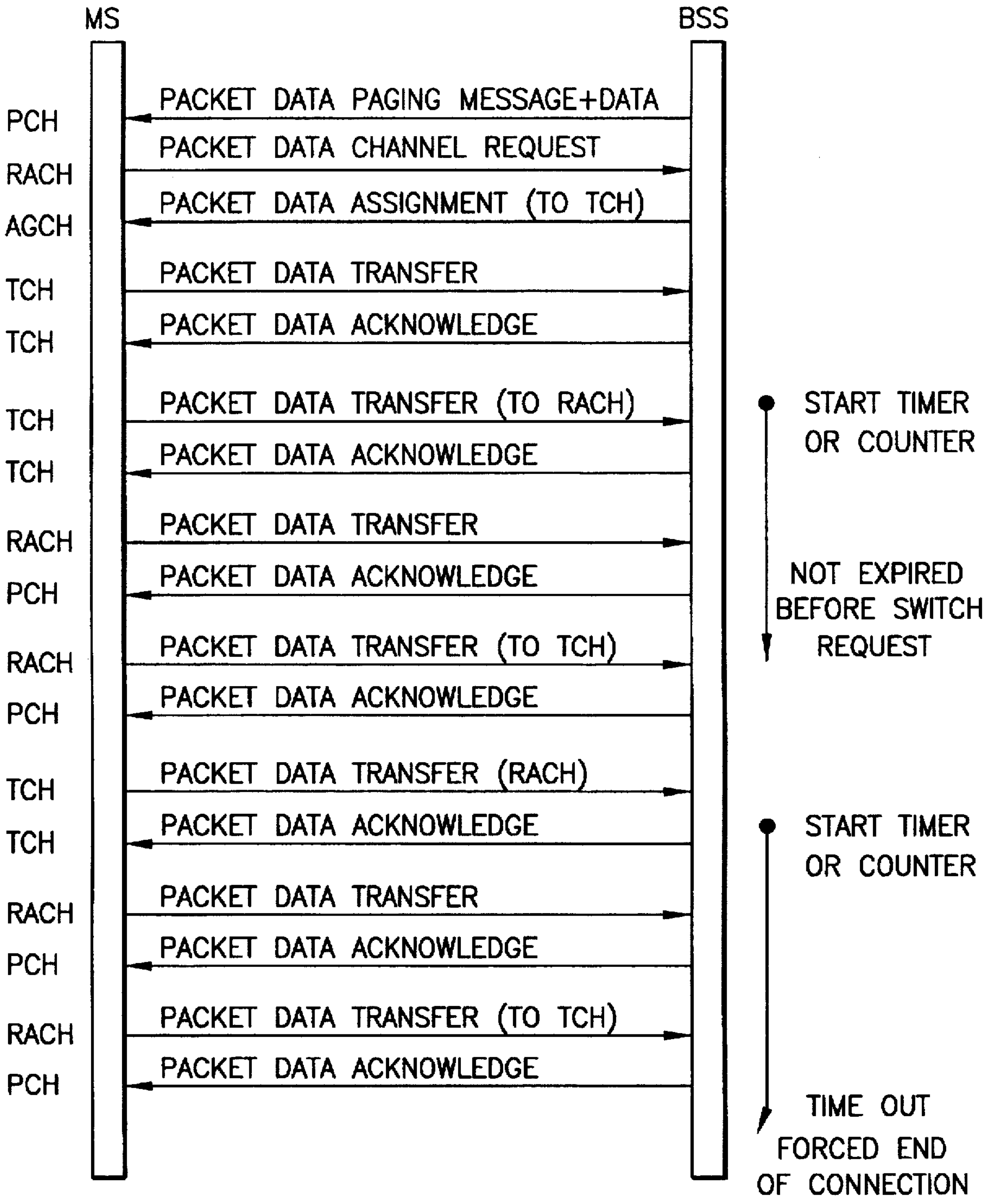

MS
BSS
PCH
PACKET DATA PAGING MESSAGE+DATA
RACH
PACKET DATA CHANNEL REQUEST
AGCH
PACKET DATA ASSIGNMENT (TO TCH)
TCH
PACKET DATA TRANSFER
TCH
PACKET DATA ACKNOWLEDGE
TCH
PACKET DATA TRANSFER (TO RACH)
START TIMER OR COUNTER
TCH
PACKET DATA ACKNOWLEDGE
RACH
PACKET DATA TRANSFER
PCH
PACKET DATA ACKNOWLEDGE
NOT EXPIRED BEFORE SWITCH REQUEST
RACH
PACKET DATA TRANSFER (TO TCH)
PCH
PACKET DATA ACKNOWLEDGE
TCH
PACKET DATA TRANSFER (RACH)
TCH
PACKET DATA ACKNOWLEDGE
START TIMER OR COUNTER
RACH
PACKET DATA TRANSFER
PCH
PACKET DATA ACKNOWLEDGE
RACH
PACKET DATA TRANSFER (TO TCH)
PCH
PACKET DATA ACKNOWLEDGE
TIME OUT FORCED END OF CONNECTION

FIG.14

DATA TRANSMISSION IN A RADIO TELEPHONE NETWORK

This is a continuation of application Ser. No. 08/301,340 filed on Sep. 6, 1994, now abandoned.

FIELD OF INVENTION

The present invention relates to the transmission of data in a radio telephone network.

BACKGROUND OF THE INVENTION

An example of a radio telephone network, in this case a conventional digital cellular network, is shown in FIG. 1A. The network comprises Base Station Controllers (BSC), each of which control a number of Base Transceiver Stations (BTS). The BTS and mobile stations (MS) are connected via a radio communications channel. A Base Station Controller and the base stations with which it is connected form a Base Station Subsystem. The BSCs are connected to Mobile Switching Centres (MSC) via digital trunk lines which control the Base Station Subsystems. The MSCs route communication traffic to a general Public Service Telephone Network (PSTN) or private networks such as a Local Area Network (LAN). A Base Station Controller may also be physically located with the Mobile Switching Center. The service range of a base station forms a cell and a mobile station within the service range is typically served by that base station. The mobile station is able to move from one cell to another and roam from under the control of one Base Station Controller to be under the control of another Controller without losing a connection to the radio telephone network.

In known cellular networks data information can be transmitted between the home network of a mobile station and a terminal or destination network. The terminal network can include a home network, another network of the same system, a fixed telephone network, or a data network. The network services typically include synchronous and asynchronous circuit-switched data transfer from the cellular network to the external telephone network PSTN, to a circuit-switched date network or an ISDN network. Suggestions have also been made on implementing asynchronous packet switching to an external packet switched data network.

As shown in FIG. 1A, data transmitted by a mobile station enters a data Inter Working Functions unit, IWF, associated with the Mobile Switching Centre, from there via a modem to the Centre wherefrom it is further transmitted, e.g., via the PSTN, to a target means or target data network, such as a private LAN network. The transition network is thus the general telephone network.

A typical method of data transmission between networks and also within a network is circuit switching, in which a transfer channel is established for the transfer of data. Establishing a channel is a time-consuming operation and requires a lot of signalling, such as sending a control channel request and assignment of a channel, authentication checks, installation of an encrypting mode and others, before the channel is set up for transferring data information. Circuit switching, when applied for data transfer, is uneconomical since the transfer needs a wide frequency band. Also a user is charged irrespective of whether data is transmitted or not. This is because in a circuit-switched network the channel has to be maintained until all data information has been transmitted, which regarding the capacity is uneconomical. Since charging of the user is usually based on the length of

the reserved connection time in the circuit-switched network, the user is obliged to pay for "nil" because the time used for the actual data transfer is a minor part of the total connection time. Typically, cellular networks have primarily been optimized for speech transfer, and for that purpose, circuit-switched data transfer is appropriate.

In a digital cellular network, such as in the European GSM network and in the American network of the EIA/TIA (Electronic Industries Association/Telecommunication Industry Association) standards, suggestions have been made on data communication as packets, as so-called packet data e.g., in the patent U.S. Pat. No. 4,887,265. This patent discloses a system in which several mobile stations send packet data to one base station using the same channel. When the Base Station Controller receives an assignment request for a data channel from the mobile station, it transmits a channel assignment to the mobile station, whereby the mobile station moves on that data channel. The same channel is also available for use for all other mobile stations within the range of said cell. A request, a channel assignment and transfer on a channel require a considerable amount of signalling. Handover of a data connection from one base station to another is also possible in this system. In the system disclosed by the patent, a permanent channel is provided for packet transfer, being constantly available, irrespective of a momentary need.

SUMMARY OF THE INVENTION

According to a first aspect of the invention there is provided a radio telephone system comprising:

a mobile station; and

a fixed station, wherein a parameter of the mobile station for setting up a data communication channel is capable of being stored by the fixed station and a parameter of the fixed station for setting up a data communication channel is capable of being stored by the mobile station, for forming a virtual data communication channel between the mobile station and the fixed station, thereby expediting establishment of a real data communication channel.

According to a second aspect of the invention there is provided a method of transmitting data in a radio telephone network comprising:

storing a parameter of a mobile station for setting up a date communication channel at a fixed station; and

storing a parameter of the fixed station for setting up a data communication channel at the mobile station, for forming a virtual data communication channel between the mobile station and the fixed station, thereby expediting establishment of a real data communication channel.

According to a third aspect of the invention there is provided a radio telephone adapted to store a parameter for setting up a communication channel of a fixed station for forming a virtual data communication channel with the fixed station thereby expediting establishment of a real data communication channel.

These aspects of the invention provide the advantage that a real data communication channel can be established quickly and when a mobile station desires to transmit data. In between the transmission of data the real data communication channel can be switched to a virtual data communication channel ready for quick reestablishment. Thus, a communication channel does not have to be continually open, even during no actual transmission of data. Thus, the costs of transmitting data are reduced.

Alternatively, the virtual data communication channel can be formed if a mobile station having data transmission capability registers with the fixed station, or if a mobile station registered with the fixed station requests a data communication channel. An advantage of forming a virtual data communication channel only when a mobile station requests a data communication channel is that unnecessary signalling is avoided.

Optionally, the data communication channel can be a channel usually reserved for speech transmissions, or signalling or control transmissions. A particular advantage of using signalling or control channels is that the transmission of data does not reduce the number of speech channels available to the users of the system.

Advantageously, the data communication channel is adapted for transmitting packet data, which is a transmission form particularly suitable for use with a data communication channel which can quickly be opened or closed.

Another advantage is that data packets can be created at the mobile stations and transferred directly to a data network without the need for transition networks, such as Packet Assembler/Disassemblers (PADs) or using the PSTN. Additionally, the mobile station itself can receive packet data, i.e. the system is bidirectional.

An appropriate existing cellular system currently in use is, for instance, the European GSM system.

Embodiments of the invention will now be described by way of example only and with reference to the drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A presents a cellular network in accordance with the prior art,

FIG. 1B presents a cellular network in accordance with the present invention

FIG. 2 is a schematic presentation of the logical channels of the GSM system,

FIG. 3 illustrates the configuration of a channel request,

FIG. 4 presents the starting signalling of a virtual channel,

FIG. 5 presents the steps of transferring packet data,

FIG. 6 presents the terminating signalling of the virtual channel,

FIG. 7 presents a phase after a channel has been assembled,

FIG. 8 is a diagrammatic presentation of a base station,

FIG. 9 illustrates mobile phone originated data transfer,

FIG. 10 illustrates data transfer terminating in a mobile phone,

FIG. 11 presents a format of a packet data message,

FIG. 12 presents a format of another packet data message,

FIG. 13 presents an order of a RACH frame for a standard burst,

FIG. 14 presents the phases of a packet data transfer, and

FIG. 15 presents signalling when a connection is broken at interfaces.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

In a particular example of a cellular network, the physical channel of a mobile station and a base station, that is, a radio frequency channel, consists of consecutive frames which in turn consist of time slots, in one of which the transmission is performed, the reception in another, in another listening to paging calls, etc. The respective time slots constitute a logical channel, of which a great number may be available.

In digital cellular networks, a mobile station can send and receive data on a traffic channel particularly intended for speech and data transfer. Both of them cannot be transmitted simultaneously but the user or the network makes a selection which thereof is to be transferred. Data as well as speech are sent as bursts on a radio channel. This means that in a transmission time slot a brief data burst is transmitted in the middle of the time slot so that a considerable part of the total time used for transmission means the time between the bursts when no information is transferred.

A particular type of data service known as packet data service has been defined in the GSM network. In this service, the number selected by a data transmitting mobile station informs the network that a circuit-switched connection has to be created to a packet assembling or disassembling unit performing the connection with a data network, such as X.25, which can be a Packet Assembler/Disassembler (PAD) or a Packet Handler (PH). The Packet Assembler/Disassembler can be placed in association with or also behind the ISDN network. The mobile station sends data as continuous data flow, not as packets, to PAD or PH, which forms the data packets and transmits them onwards via the data network to the target. If PH is a so-called Basic Packet Handler, the data connection is always located via a given point PH, even in any network. The Basic Data Handler also supports the mobile terminated direction in data transmission. On the other hand, the mobile terminated direction is not supported by the so-called dedicated Packet Handler, nor PAD. The traffic between the mobile station and the packaging means imitates synchronous or asynchronous data transfer, wherebelow a radio traffic protocol RLP is located.

In the data packet service of the GSM network no packets are produced in the mobile stations, but in PAD. The traffic is unidirectional also in the sense that the connection is mobile station-originated, i.e., the station should send a request to the network for creation of a data connection. No packets can be sent to the mobile station unless the station itself has first requested the opening of a line. It is also to be noted that data is conducted via the telephone network, the pricing of the data transfer whereof being much higher than pricing of transfer within a data network.

The sending and reception function of data packets can be arranged to be positioned in all mobile stations or in some of them only. For the mobile stations without such function, a packet data transfer is to be completely opaque so that mobile stations of different types are enabled to function without any problems in the network simultaneously. Thus, the packet data feature is an additional service provided by the network, though requiring that the mobile station possesses a property to use such service. The implementation of the system must be such that it requires only a few changes in digital cellular systems in current use and, as an additional feature, it is well appropriate for use in current systems such as GSM, DCS 1800 operating in 1.8 GHz range or PCN.

In new networks a so-called Short Message Service is most often determined, wherewith a mobile station is enabled to transmit and receive temporally short messages. A transfer of a short message requires, however, standard connection formation routines, thus requiring part of the frequency band and limiting the amount of data to be transferred.

For transferring packet data no allocated radio channel and data route via the network are maintained continuously.

In accordance with the invention, a virtual channel is arranged for data packet transfer in the network between the mobile station and the Mobile Switching Center. When a phone provided with a packet data function enters the range of the Mobile Switching Center, assigned as a user of the packet data service, all necessary signalling is executed, whereafter the Center, or more specifically, the packet data service unit (Agent) in association therewith is provided with all the information it needs concerning the phone and establishing a true transfer channel. Such data, containing in fact information about the location of the phone, is called a virtual channel. The virtual channel is thus a virtual connection between the mobile station and the data service unit, enabling fast transition into data transfer mode, paying regard to the parameters stored in the memories of the mobile station and the data service unit. When packet data has to be transferred from the phone to the network, or vice versa, no complete signalling is needed between the phone and the Center, since that was carried out earlier; instead, a true transfer route can be set up extremely fast and with very low-level signalling between the mobile station and the packet data service unit (Agent), whereupon the packets are transferred. The transfer route, or at least the radio channel, is released as soon as there is no packet data to be transferred. Instead, the virtual channel is kept in constant preparedness as long as the mobile station is listed in the data service. In accordance with the present invention, a very rapid connection to the packet data transfer mode can be made, and the transfer route is kept reserved only when there is something to be transferred.

A means to control the transfer of packet data is arranged to be in conjunction with the Mobile Switching Center, and is known as a data service unit (Agent), which can be a computer or a process. It is a data service center provided with a number of connection services and which has access to other networks and the services thereof. The Agent has been placed logically in association with a Mobile Switching Center MSC, though the physical location can be inside the Center as part of the processes thereof or outside the Center in the form of one or more computers connected via a transmission link to the Center. The basis of the Agent is an Interface Unit IFU connecting the cellular network to another network, such as to TCP/IP or OSI networks (TCP=Transmission Control Protocol, IP=Internet Protocol, OSI=Open Systems Interconnection). Thus, a mobile station MS provided with a packet data function communicates by means of the data service unit (Agent) with the other networks, and the virtual channel is placed specifically between it and the data service unit (Agent). Therefore, each mobile station utilizing the packet data service under the control of the Mobile Switching Center is supervised by the data service unit (Agent) in association with the Mobile Switching Center.

The Agent performs at least some of the following functions: It

registers all telephones provided with a packet data function under the control of the Mobile Switching Center,

informs the phone of a message to arrive,

removes the phone from the register after terminating of connection,

transfers the messages of the phone to the rest of the network,

transfers the messages from the rest of the network to the phone,

buffers messages with a view to efficient transmission via the network,

when necessary, performs encrypting/decrypting,

when necessary, performs compression/decompression between the phone and the Agent,

updates the data base thereof (location updating),

receives messages addressed to the paging channel.

Normally, the virtual channel is initialized when the user starts using the packet data service, and the channel is terminated after the user leaves the service. During the time between the start and the termination, i.e., while being connected with the service, the mobile station is able to move and transfer from one cell to another. The handover function prerequires disassembling the virtual channel and assembling a new one. The handover is practically unobservable by the user.

When entering the cell area, a mobile station listens to the System Info channel, characteristic of all cellular networks and constant transmission from the base station, being therethrough informed if the packet data service is in use in the network or in the cell. A System Info message may include an identification referring e.g., to the packet data service. When a mobile station wants to be connected to a packet data service, it transmits via a base station to the network a request for setting up a virtual channel. The request commences in the network a standard control signalling sequence utilized thereby and characteristic of said network, in which the authentication of the requester is checked, encrypting is started and the requester is provided with an interim identification number. The Agent in association with the Mobile Switching Center controlling the packet service, is also informed, whereby it includes the supervision of the mobile phone under the control thereof. The Mobile Switching Center maintains an ongoing register on the location of the mobile station, whereby handover from one cell to another is possible and a fast preparedness to transfer to data transmission or reception exists because there is no need for the phone to request separately for a traffic channel.

Instead of a System Info message, it is also possible to operate so that the mobile station requests the network via a short message service whether the packet data function is engaged. The network responds by an equal message of the short message service. The short message services (SMS) are a service mostly included in the digital networks.

The control signalling associated with the management of the data connection between the data service unit (Agent) in association with the Mobile Station and the Mobile Switching Center MSC is executed along with the data messages in the signalling plane. The functions in the signalling plane are provided with functions for setting up, maintaining and terminating a connection between the cellular network and the other networks. It also includes functions for updating the register, authentication, and a function for providing an interim subscriber number TMSI.

A plurality of protocols are available for use in the transfer of data packets between the mobile station and the data service unit (Agent). The radio interface sets, however, certain limits, such as a requirement for minimizing the amount of data transmitted across the interface. The amount can be minimized by compressing the data section of the packets. The data are compressed prior to transmission, e.g., by means of V.42bis compression algorithm, and the receiver decompresses the data using the same algorithm. Also the bit amount in the header of the data packets may be reduced. Such functions are attended to by a Virtual Channel Protocol, which also attends to the control messages between the agent and the mobile station, as well as adapts the packets of the upper protocols into the Radio Link

Protocol (RLP) frames. A paging message transmitted to all mobile stations (broadcast) of the cell or to certain mobile stations (multicast) is transmitted on the data section of the broadcast or the multicast protocols, respectively.

After the virtual channel has been assembled between the mobile station and the base station, the mobile station can neither start nor receive ordinary calls. Instead, the transmission and reception of short messages SMS is possible.

When wishing to transmit data packets, a mobile stations ends a request to the network for channel assignment. Since the majority of the signalling needed in establishing a channel has been already executed at the beginning of creating the virtual connection, the setting up of a data packet transfer channel extending from the mobile station to the Agent, required at this moment, is fast. This means a short time from the channel assignment request to transmission of packets.

The transmission may be accomplished according to a first or second embodiment of the invention. When a user of the mobile station switches off the packet data function on termination of data transmission or when the network terminates the connection, the data route is disassembled and the radio channel is released; optionally, the virtual channel may be maintained.

A packet data session refers to the time commencing when a user starts a packet data function (informs of his desire to be connected to the service), and ending when the user terminates the service. In the course of the session the user may transmit packets both to a terminal network and receive them from the source network. Roaming and handover are possible. In the course of a session one or several virtual channel connections are created, though only one at a time.

In accordance with a first embodiment, the radio channel for a data route is a standard traffic channel of a cellular system which is intended for transfer of speech and non-packet shape data via broadcasting between a mobile station and a base station. When wishing to transmit data from a mobile station (i.e., mobile originated), the station requests the network via a base station for a channel using the same signalling channel as normally used when the station sends a request to connect a call. The signalling channel is a random access channel which all mobile stations of the call use. The channel runs from the mobile station to the base station, that is, it is a so-called uplink direction channel. Due to the random access, collisions may occur when channel requests enter simultaneously. In such an event the request has to be repeated. The request message includes a special bit configuration, an identification block with which the station reports of a service it wants to have, such as speech, data, packet data; in the present case, the identification configuration indicates that the desired service is transmission of packet data.

After the network has processed the request and allocated the traffic channel, it transmits to the mobile station on the signalling channel a response containing information as to which traffic channel the station should move onto in order to transmit packet data. The channel on which the network responds to channel requests is a common Access Grant CHannel and is in a downlink direction. The mobile station tunes its transmitter onto the allocated traffic channel, and immediately starts transmitting packet data. The transmission lasts until all the data has been transmitted. The network may also start a particular counter or timer when the traffic channel has been allocated, whereby the transmission continues until the counter or timer expires. It is preferred to store the data to be transmitted in a buffer memory of the mobile station and to erase the memory by transmission.

When packet data is transferred according to the first embodiment via the network to a mobile station (mobile terminated transfer), the only difference from a transfer in the opposite direction is that the network informs the mobile station of a packet data transmission to come. For transmitting such information, a common paging channel is used. All mobile stations within the range of the cell continuously listen to this common downlink paging channel (speech pagings are transmitted on this channel). When the mobile station has received a message indicating that packet data is coming in, it acts in the same way as in the mobile-originated case: It transmits a traffic channel request to the base station, receives data on the channel, and moves immediately on to the traffic channel assigned thereto, thus being prepared to receive data packets. On termination of data flow, the network disassembles the traffic channel, so that it is released for use of other mobile stations present within the range of the cell. The data to be transmitted is preferably stored in a data buffer of the data service unit (Agent) and the buffer is erased all at once.

In accordance with the first embodiment, when transmitting packet data one traffic channel is reserved for such date which is normally used for transferring speech. On termination of transmission, the traffic channel is again free for use by any mobile station. The same mobile station may send another request for packet data transmission, whereby the sequence "channel request-transmission—channel release" can be repeated until the mobile station leaves the packet data service, and the virtual channel is disassembled.

In accordance with a second embodiment of the invention, a signalling channel or a control channel is used either exclusively or as an alternative to the use of the traffic channel for the transmission of packet data.

In accordance with the second embodiment, when a mobile station wishes to transmit data packets, i.e., mobile originated transfer, it sends a channel request page to a base station using the same random access channel upon which ordinary channel requests are transmitted. Said channel is in an uplink direction. All mobile stations of the cell employ the same channel for speech channel requests. The Mobile Switching Center decides, after receiving the request, which channel the mobile station should move to for data transmission. The channel can be either a standard traffic channel or a control channel. The control channel can be the same random access channel on which the channel requests are transferred from the mobile stations to the base station. The network establishes a traffic channel provided it has been selected to be the transfer channel. The base station transfers information to the mobile station on whether it is expected to use the standard traffic channel or the control channel for data transmission. Such information is transmitted on the Common Control CHannel, on the Access Grant CHannel, upon which channel the channel assignment is sent to the mobile stations. The mobile station moves to the traffic or control channel thus assigned, starting immediately to transmit packet data. In the course of the transmission, the channel may be handed over from the traffic channel to the control channel, and vice versa, even several times. On termination of transmission, the channel is disassembled and it is released for other uses. The transfer ends after a given time elapses or when a "packets over" message is received from the station.

If the network is required to transfer packet data to a mobile station, i.e., mobile terminated transfer, it informs the station via the standard common paging channel of a data packet transmission on the way. The paging includes a particular identification part (bit configuration) indicating that a packet data transfer is in question. In such paging the identification of a second mobile station has been replaced by the user's data section, including a packet coming in to the user from outside. If a packet from outside cannot be accommodated in one data section of the paging message, it is divided into several paging messages, all of which the mobile station receives, gathering one packet therefrom. When the mobile station has received the packet, it acts thereafter in the same way as when desiring to transmit data packets: it transmits a channel request to the base station, receives a channel assignment, moves on the assigned channel, the traffic channel or the control channel, and acknowledges the packet it has received.

The data route connection between the base station and the Agent connected with the Mobile Switching Center can be implemented in a number of ways. One possibility is to reserve a direct connection and to maintain the connection reserved continuously for packet data traffic. This means an ongoing existence of the connection so that no extra delays are formed. The connection can be a PCM time slot or several PCM time slots in the digital trunk line between the Base Station System (BSS) and the Mobile Station Center (MSC). When a mobile station provided with a packet data reception and transmission property enters the range of the cell in association with the base station, e.g., a BTS in FIG. 1A, the network immediately establishes a direct connection between the base station and the Mobile Switching Center provided for transmission of packet data. The connection can be one or several time slots in the PCM trunk line commonly used by all mobile stations provided with the packet data function. The entry of the mobile station into the cell is known because it has been transferred either as a result of a handover function, or, if entry from outside into the reception area is in question, or the phone is switched on, the phone is registered in the network.

In an embodiment such as the one described above the PCM channel within the network is constantly maintained but the radio route channel is reserved only when needed.

The use of the PCM time slots may also be optimized in that a direct connection is maintained only if the Base Station System (BSS) includes existing virtual connections, that is, at least one cell under the control of the Base Station Controller includes a mobile station connected to the packet data service, being in readiness to receive and transmit packet data. The direct connection is disconnected when no users of the service are found to be in the range of the BSS, and it is set up again when a first mobile station joins the packet data service.

A second possibility is that connections between the network and radio path are assembled and disassembled when need be. The examples described below include the connections provided according to the second possibility.

FIG. 1B shows a typical cellular network such as a GSM network provided with a data packet service in accordance with the invention. A data service unit (Agent) has been connected to a Mobile Switching Center, from where the packet data are conducted directly to a data network according to the OSI or TCP/IP protocol, and from there to a target network, such as a LAN. A difference between this network and the network of FIG. 1A lies in the fact that no data passes via the circuit-switched telephone network PSTN.

According to FIG. 2, the logical channels are divided into traffic channels TCH and control channels CCH. The traffic channels are intended for transferring coded speech and data. Each of them can be transferred at full rate or half rate. The control channels CCH are intended to transfer signalling and synchronization data, and three types of channels can be distinguished thus: Broadcast Channels, Common Channels and Dedicated Control Channels. Below, "uplink" refers to the direction from a mobile station to a base station and "downlink" the direction from a base station to a mobile station.

The Broadcast Channels comprise the following:

- a Frequency Correction CHannel, FCCH, transferring frequency correction data to the mobile station, downlink,
- a Synchronization CHannel, SCH, transferring synchronization data to the mobile station and identification data of the base station, downlink
- a Cellular Broadcast CHannel, CBCH, short message service, bi-directional channel, and
- a Broadcast Control CHannel, BCCH, transferring general information on the base station, downlink.

The Common Channels comprise the following:

- a Random Access CHannel, RACH, uplink direction only, on which the mobile stations send a request for a dedicated channel
- a common Paging CHannel, PCH, whereby a base station sends a paging to a mobile station to inform of an incoming call, the channel being in downlink direction only,
- an Access Grant CHannel, AGCH, whereby the base station reports of a Stand-alone Dedicated Control CHannel, SDCCH, or directly of a Traffic CHannel, TCH, said channel being only downlink.

The Dedicated Control CHannels comprise the following:

- a Stand-alone Dedicated Control Channel, bi-directional, and
- a Slow Associated Control Channel and a Fast Associated Control Channel, the channels being bi-directional.

In accordance with the present invention, a Traffic CHannel (bidirectional), TCH, a Paging CHannel, PCH, (unidirectional, downlink), a Random Access CHannel, RACH, (unidirectional, uplink), and an Access Grant CHannel, AGCH, (unidirectional, downlink) are made use of. Channels of equivalent types can also be found in digital cellular systems other than GSM.

The mobile station listens to the Broadcast Transmission Control CHannel BCCH transmitted continuously by the base station of the cell and is therethrough informed of a packet data service being engaged in the network. Another procedure is that the mobile station requests on the Cellular Broadcast CHannel by transmitting a short message service whether the packet data function is in use in the network or not. The base station sends a short message response on the same channel.

When a mobile station sends a request to be a user of a packet data service, a message sequence as shown in FIG. 4 is carried out therebetween and the Mobile Switching Center. The events are read from top to the bottom. After the channel request is transmitted by the Mobile Station an immediate assignment of the control channel follows (FACCH), and on the assigned channel the authentication of the requester is checked (the network inquires on the authentication data and the mobile station sends a response), encryption is started, and an interim identification number TMSI is allocated. A Radio Link Protocol is established and maintained thereafter permanently. This means that in the course of a session the transmission of data packets can be performed without reassembling the radio link protocol. The data service unit (Agent) in association with the Mobile Switching Center controlling the packet data service is informed, thus transferring the control of the mobile station under the control of its own. The data service unit is now able to detect the mobile station and carry out the encryption and authentication without extra signalling. The virtual channel from the Mobile Switching Center to the mobile station has now been assembled. The radio link protocol is not disassembled before the end of the session (the phone is released from the data packet service) whereby the virtual channel is disassembled.

When a mobile station wants to transmit data, it transmits a request to set up a transfer channel for real packet data. The request is transmitted on a common Random Access CHannel RACH which is similar in configuration to the one shown in FIG. 3. By means of the first three bits of the message the nature of the connection is determined, and sequence 001 refers to a request to set up a data packet connection. The end of the message is a random reference number. The message is a modification of a standard GSM message. The base station receives the request, and after coding the sequence, it informs the mobile station on which control channel the signalling to be performed next is carried out and on which transfer channel the transfer of the packets is to take place. These phases are described by the two topmost phases in FIG. 15. The transmission channel has been assembled from the mobile station to the Base Station Controller. On a channel produced as above, the mobile station transmits first control messages, the third phase in FIG. 15, wherewith a data connection from the station to the data service unit (Agent) is provided, whereafter the channel from the mobile station to the Agent is complete for data transfer.

When a true channel, the first part thereof comprising a radio channel and the latter part a PCM time slot, has in the above described manner been established between the mobile station and the base station, the mobile station is able to transmit immediately packet data on that channel. After a demand on data transmission by the network the station transmits data packets, the network acknowledges the packets and sands requests for a repeated transmission if a transmission has been defective. The phases up to that point are presented in FIG. 5.

After transmission of all packets, the mobile station sends a request to the network to disassemble the true connection. After receiving the request the network sends an order to the mobile station to terminate the data activities, and the station acknowledges termination of those activities. The phases are presented in FIG. 6. The data packet transfer channel to the base station controller BSC and from there on to the data service unit (Agent) is disassembled. If a method based on direct PCM connection is used, the channel is left on.

Transfer of packet data may also be directed at the mobile station (i.e., it is mobile terminated). A base station sends on a common paging channel a paging to a mobile station, informing of a packet data transmission on the way. The mobile station then sends a channel request signal to the base station on the common Random Access CHannel RACH, whereby the process from that moment onwards is the same as in the mobile oriented case described above: establishing a virtual channel and immediate reception of packet data. In FIG. 7, each of the cases are presented step by step.

FIG. 8 shows a block diagram of a base station related to the present invention. The base station includes several parallel branches formed by the Framing Unit (FU) and the Transmitter/Receiver Unit RX/TX. A Base Band Interconnection Element (BIE) connects the base station to a digital PCM link. Part of the channels of the link are reserved for signalling and the rest for data transfer. The digital signals from the PCM link are conducted to the Framing Unit in which they are arranged into TDMA frames, channel-coded, interlaced and transmitted as bursts onto the radio path via antenna TX. Prior to the transmission, the bursts have been modulated in the transceiver unit RX/TX and transferred to a carrier wave frequency. When the base station receives a TDMA signal from the mobile station, the signal is conducted via the necessary filters to the transceiver unit RX/TX where it is demodulated, transferred to a carrier frequency, and the modulation is indicated. The channel decoding and discharge of interlacing are performed in the Framing Unit (FU). Finally, the data signal is conducted to the PCM line and therefrom via the Mobile Switching Center to the receiving network.

The Base Station Controller produces all messages transmitted to the radio path, and all received messages are transferred via the Base Station to the base station Controller. Therefore, compared with the GSM currently used, the embodiment of the invention requires only minor changes in the software of the Base Station Controller. Changes have to be made also in the softwares of the mobile station and of the Center. The mobile station has to be able to detect and transmit all messages related to packet data transfer. The messages transmitted by a mobile station can be originated by the user's keyboard or by a separate data terminal connected to the station.

The invention is described above with a view to assembling a virtual channel without mentioning more closely on which particular radio channel the transmission of data packets will take place.

In accordance with the first embodiment, the radio channel reserved for packet data transmission is a traffic channel TCH normally used for transmitting speech. On termination of transmission said packet data channel is free for use of any other mobile station. Such first embodiment is described below.

Reference is made to FIG. 9 showing packet data transfer in mobile station originated mode. The figure is equivalent to FIG. 5 and the description thereof, with an additional remark that also a mentioning has been added therein on which channel each message is transmitted. So, a mobile station sends a packet data channel request to a base station using a common Random Access CHannel RACH, which all stations in the cell use when requesting a radio channel. The base station replies by a traffic channel assignment on the common Access Grant CHannel AGCH, whereafter the packet data transfer and acknowledgement of reception are carried out on the traffic channel. The paging transmitted on the Random Access CHannel RACH contains a value 001 in the "Establishment Cause" as in FIG. 3. Said channel paging request is a modification of a standard channel paging of the GSM system. The value "001" would mean that the direction of the packets is from the network to the mobile station. The purpose thereof is so that the value of the "Establishment Cause" field is different in the mobile originated case and the mobile terminated case is to ensure that the priority of the mobile terminated case is higher because the network has already been made to prepare a connection.

The network responds to the paging on the Access Grant CHannel AGCH with a message called "Packet Data Assignment". The message is a modification from the standard GSM message "Immediate Assignment". The modification is such that the bit configuration of the "message type" block of said standard message is 00111101 in the present invention, said configuration not being used for any other purposes in GSM. After the message "Packet Data Assignment" the signalling is not continued on the Stand-alone Dedicated Slow Control Channel SDCCH, as the case would be in standard traffic channel trafficking, but on a Faster Associated Control Channel. This should be included in the message sent to the mobile station. The standard message includes an information part "channel description" and it includes an element "channel type". This element informs that the traffic channel has to be connected with. The bit configuration illustrating the full rate traffic channel TCH and the control channel FACCH associated thereto is "00001". In this element also the timing advance TA and power control are transmitted, these being necessary data for the mobile station.

When the mobile station has received the above-described modified message, it immediately moves to the traffic channel and starts data packet transmission. If the assembly of the connection between the mobile phone and the Mobile Switching Center requires more signalling prior to transfer of the mobile phone to data packet transmission, the signalling can be carried out on the full rate control channel FACCH.

The operating time of the traffic channel can be limited relative to the time available or the number of packets. The simplest and most effective method is possibly to transmit all data from the transmission buffer and to release the traffic channel TCH after the buffer is empty. Since the reservation of a true channel takes a few hundreds of milliseconds, a timer can be provided in the telephone counting the time after emptying the buffer. The traffic channel is not released until a set time has elapsed, not immediately after the transmission of the last packet. So, a transmission can be repeated or more transmitted (if more data have been accumulated in the buffer) without setting up a channel. The use of a timer increases the sense of interaction because the channel need not be established again and again in each case. If the transmission rate of the packets is high, the timer keeps the traffic channel TCH continuously reserved and the user receives the replies immediately. The time setting of the timer can be set by the user.

The operator may also select one traffic channel only in the cell for transferring data packets or equally a great number or even all traffic channels.

FIG. 10 schematically shows the functions of the first embodiment when packet data are to be sent via the network from a mobile station. The only difference to the opposite case is that the network first informs the mobile station of the packet data transmission to come. The report takes place on the common paging channel PCH in a paging message. When the mobile station has received the paging, the activity is continued, as in the mobile station originated case, that is, the station transmits a channel request to the base station, and the operation goes on as described in association with FIG. 9.

FIG. 11 shows the formats of a packet data message of an arrangement in accordance with the first embodiment. The packets of the Virtual Channel Protocol, VCP, are produced using the OSI terminology in layer 3, above the link layer, and conducted via Layer 2 Relay Functions, L2R, to the Radio Link Protocol for transmission via the broadcast interface (radio path). The packet includes a header and a data part. The header includes the identification of the upper level protocol to be used. One of the upper level protocols is the protocol of the packet used in the signalling between the station and the Agent in association with the Mobile Switching Center. Other potential protocols are Internet Protocol (IP), Open Systems Interconnection (OSI) protocol and some fax protocols. The operator of the network may also add services of his own to be attended to by the Agent, these being provided with identifications of their own. The header may alternatively be also provided with a field informing of the length of the packets. The length of the data part of the packets, or the number of higher level octets, varies. One packet can be transferred in one or more RLP frames.

A second embodiment of the invention is described, according to which packet data can be transmitted either on a traffic channel TCH or on a common Random Access CHannel RACH, using a channel request, which can be, as above, an 8 bit byte with a bit sequence "001" at the beginning. Thereafter, the network transmits on the Access Grant Channel, AGCH, a message requesting transmission of packet data, the message being a modification of the standard GSM message. The element determining the message type thereof includes bit configuration "00111101", indicating that a packet data case is in question. In block "Channel Type" the bit configuration "00001" indicates that the mobile station should move to the traffic channel TCH to transfer the packet data thereon, and the bit configuration "10000" indicates that it has to stay on the Random Access CHannel RACH and to transfer the data packets on that channel. The network makes a decision which channel is to be used. If the telephone traffic in the cell is large scale, the transmission is carried out on the traffic channel, but if it is minor, the Random Access CHannel RACH is used.

The duration of transmission on the Random Access CHannel RACH is limited by means of a timer or counter as the Timing Advance, TA, changes very rapidly and the channel reservation occupies the possibilities from the others to request for a connection to be formed.

FIG. 12 shows the formats of a packet data message of an arrangement in accordance with the second embodiment. Each frame is provided with an 8-bit ordinal number SN acting as identification of a connection. It is generated by the base station and transmitted to the mobile station in conjunction with the assignment message of the packet data. The identification is released after the connection ends. The identification is necessary so that the data included in the same connection with the random access channel and the traffic channel can be combined. FIG. 13 presents a case in which packet data are transmitted on a random access channel. On that channel the packet data are transmitted as standard bursts, and the figure shows the equivalence of the RACH channel frame as standard bursts.

The mobile station is enabled to present in the form of a wish, which of the channels it wants to use for transmitting data. Each TCH and RACH frame is provided with two command bits, informing the channel of the subsequent frame. The connection via the RACH channel can be discontinued if a request to move to the traffic channel TCH arrives, and likewise, the connection via the TCH channel can be discontinued if a request to move to the RACH channel arrives. The command bits C at the ends of the frames are available for use of the mobile station for a channel shift request and moreover, the termination of a data transfer can be reported therethrough. These two bits can therefore be used as follows:

bits "11"=move to the same channel

bits "01"=move to traffic channel TCH

bits "10"=switch to the common Random Access CHannel and the common Paging CHannel PCH

bits "00"=transmission over.

The switching onto the transmission channel can be implemented in two ways. After the switch-on-the-channel command transfer, the mobile station is allowed to request for a channel in a "packet data channel request" message and to wait for a channel assignment message to be able to select the channel on which the data traffic will take place. Another alternative is to read the message on the network side and if a channel switching is requested in the command bits, the "packet data assignment" message is sent without any "packet data request" message. The packet has been transferred to a plurality of RLP frames. One of the RLP frames is interlaced into 22 standard bursts of the TCH channel.

The transmission of data packets is described above in mobile station-originated mode in an instance according to the second embodiment. The instance in which packet data are transmitted via the network to a mobile station differs from the above-mentioned case only in that the network reports the mobile station of future transmission in a particular "packet data paging request" message which it sends on a common Paging CHannel. The message is a modification of the paging of the GSM system being provided with a free bit configuration for this purpose. "001000011" is selected for the bit configuration. As an extension. a data field is added in the message, wherein the data to be transmitted to the user is transferred. After receiving this paging message (or a series of paging messages including the packet), the mobile station opens a connection and acknowledges the packet.

FIG. **14** presents schematically the events in temporal order when transmitting data packets via the network to the mobile station. The packet transfer first takes place on a traffic channel, moves onto a random access channel, returns on the traffic channel and then on the random access channels. On the random access channels the trafficking time runs out, and the connection is terminated forcedly.

In view of the foregoing description it will be evident to a person skilled in the art that various modifications may be made within the scope of the invention.

The scope of the present disclosure includes any novel feature or combination of features disclosed therein either explicitly or implicitly or any generalisation thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed by the present invention. The applicant hereby gives notice that new claims may be formulated to such features during prosecution of this application or of any such further application derived therefrom.

What we claim is:

1. A radio telephone system comprising:

a mobile station having means for storing a first parameter, relating to another station, for setting up a real data communication channel having a reserved physical path between said mobile station and said another station; and

said another station comprising a fixed station having means, wherein a second parameter relating to the mobile station for setting up said real data communication channel is capable of being stored, for forming a virtual data communication channel between the mobile station and the fixed station, said virtual data communication channel being a non-physical registration relationship using said first and second parameters and lacking a reserved path between said mobile station and said fixed station preparatory to the establishment of said real data communication channel, whereby the establishment of a real data communication channel is expedited when data is to be communicated between said mobile and fixed stations.

2. A system according to claim **1**, further comprising means for communicating a first parameter relating to said mobile station to be stored in the fixed station parameter storing means to form the virtual data communication channel when a mobile station having data communication capability registers with the fixed station.

3. A system according to claim **1**, further comprising means for forming the real data communication channel when a mobile station registered with the fixed station requests the setting up of a data communication channel.

4. A system according to claim **1**, further comprising means for forming traffic channels, usually reserved for speech communication, and control channels between the mobile station and the fixed station, and wherein the real data communication channel is a traffic channel usually reserved for speech communication.

5. A system according to claim **1**, further comprising means for forming traffic channels, usually reserved for speech communication, and control channels between the mobile station and the fixed station, and wherein the real data communication channel is a control channel.

6. A system according to claim **1**, further comprising control means for controlling communication between the mobile station, the fixed station and an external communication network.

7. A system according to claim **1**, further comprising means for adapting the real data communication channel for transmitting packet data.

8. A digital time-division cellular network having a base station and a plurality of mobile stations, wherein radio channels between the mobile stations and the base station comprise:

a plurality of Traffic CHannels (TCH) for transferring speech and data between the mobile stations and the base station,

a control channel in association with each of said TCH channels, said control channels comprising:

a Random Access CHannel (RACH), for conducting signals from the mobile stations to the base station requesting a TCH channel,

a common Paging CHannel (PCH), for conducting a paging signal from the base station to a mobile station,

an Access Grant CHannel (AGCH), for conducting a signal from the base station to inform a mobile station of the TCH channel assigned thereto,

and further comprising:

a packet data service unit (Agent) for connecting the cellular network to a data network,

means for switching a mobile station to the Agent and signalling for the setting up of a connection to the data network,

means in a mobile station and the Agent for storing a number of parameters relating to each other, said parameters including a Radio Link Protocol (RLP) and forming a virtual channel, said virtual channel being a non-physical registration relationship using said parameters and lacking a reserved path between said mobile station and said Agent preparatory to the establishment of a packet data transfer channel,

means, responsive to a request from a mobile station to transfer or receive data packets, for assembling a packet data transfer channel between the mobile station and the Agent, making use of the parameters of the virtual channel, and wherein said packet data transfer channel comprises a first part comprising a radio channel between said mobile station and the base station and a second part comprising a time slot in a digital trunk line between said base station and said Agent,

means for transferring data packets over said packet data transfer channel, means, responsive to the termination of data packet transfer over said packet data transfer channel, for disassembling at least said radio channel, and

means for maintaining the virtual channel until the release of a mobile station from the Agent.

9. A network according to claim 8, wherein the Agent comprises:

means for registering all mobile stations connected to the Agent,

means for informing a mobile station of any data packets addressed thereto,

means for transferring data packets from a mobile station addressed to the data network,

means for transferring messages to the mobile station entering the Agent from the data network,

means for buffering data packets,

means for performing encrypting/decrypting,

means for performing compression/decompression of the data to and from a mobile station,

means for updating a data base of the location of the mobile stations,

means for receiving data packets from the data network addressed to the cellular network and transferring them to the mobile stations, and

means for removing a mobile station from the register after it is disconnected from the Agent.

10. A network according to claim 8, wherein the packet data service unit (Agent) comprises means for adapting the data packets from the data network to virtual channel protocol packets, said virtual channel protocol packets being composed of one or more radio link traffic protocol (RLP) frames.

11. A network according to claim 10, wherein the virtual channel protocol packets comprise an identification part indicating whether the contents of a packet contain signalling data or upper layer data.

12. A network according to claim 8, further comprising means, in a mobile station, for initiating the transmitting of data packets by sending a request on the RACH channel for establishing a packet data transfer channel, said request being a modification of the standard channel establishing request of the cellular network.

13. A network according to claim 8, further comprising means in the base station, responsive to data packets to be transferred to a mobile station, for sending a message on the common PCH channel to the mobile station about said data packets to be transferred and means at the mobile station, responsive to said message for sending on the RACH channel a request to the base station for establishing a packet data transfer channel, said request being a modification of the standard channel establishing request of the cellular network.

14. A network according to claim 8, further comprising means, in the base station, for transmitting control channel data used in channel establishment signalling and packet data transfer channel data to the mobile stations.

15. A network according to claim 14, further comprising means for establishing, after the channel establishment signalling between the mobile station and the base station, said second part of the packet data transfer channel with said Agent, whereby the entire packet data transfer channel is ready for packet transfer.

16. A network according to claim 8, wherein said cellular network comprises a Dedicated Fast Access Channel (FACCH), and further comprising means for causing said

channel establishment signalling to be carried out on a Dedicated Fast Access CHannel, FACCH of the cellular network.

17. A network according to claim 8, further comprising a base station controller connected to the base station and wherein the second part of the packet data transfer channel is a direct PCM connection from the base station controller to the Agent, whereby said second part of the packet data transfer channel is active irrespective of the packet data transfer.

18. A network according to claim 8, wherein the second part of the packet data transfer channel is a variable time slot on the PCM trunk line, and further comprising means whereby said second part is disassembled after the termination of the data packet transfer.

19. A network according to claim 8, wherein the first part of the packet data transfer channel is a TCH channel.

20. A network according to claim 8, further comprising means for causing the first part of the packet data transfer channel to be a RACH channel when packet data are transferred from the mobile station to the Agent, and to be the common PCH channel when packet data are transferred from the Agent to the mobile station.

21. A network according to claim 8, further comprising means for causing, in the course of a transfer of packet data, the first part of the packet data transfer channel to be any one of the TCH channel, the RACH channel, and the common PCH channel.

22. A network according to claim 8, wherein a broadcast paging message transmitted to all mobile stations of the cellular network and a multicast paging message transmitted to certain mobile stations of the cellular network are transmitted on the data section of the broadcast and the multicast protocols, respectively.

23. A method of transmitting data in a radio telephone network comprising:

storing at a fixed station a first parameter relating to a mobile station and the setting up of a real data communication channel between the mobile station and the fixed station; and

storing at the mobile station a second parameter relating to the fixed station and the setting up of a real data communication channel between the mobile station and the fixed station, for forming a virtual data communication channel between the mobile station and the fixed station, the virtual data communication channel being a non-physical registration relationship using the first and second parameters and lacking a reserved path between the mobile station and the fixed station preparatory to the establishment of a real data communication channel, thereby expediting establishment of a real data communication channel between the mobile station and the fixed station in response to an appropriate request.

24. A method according to claim 23, further comprising forming the virtual data communication channel when a mobile station having data communication capability registers with the fixed station.

25. A method according to claim 23, further comprising forming the virtual data communication channel when a mobile station registered with the fixed station requests the setting up of a real data communication channel.

26. A method according to claim 23, wherein said network comprises traffic channels usually reserved for speech communication, and control channels, and further comprising utilising a traffic channel usually reserved for speech communication for the real data communication.

27. A method according to claim 23, wherein said network comprises traffic channels usually reserved for speech communication, and control channels, and further comprising utilising a control channel as the real data communication channel.

28. A radio telephone having storage means therein to store a parameter relating to a fixed station for setting up a real data communication channel with said fixed station and for forming a virtual data communication channel with the fixed station by utilizing a parameter relating to said radio telephone stored in said fixed station, the virtual data communication channel being a non-physical registration relationship using the respective stored parameters and lacking a reserved path between the radio telephone and the fixed station preparatory to the establishment of a real data communication channel, thereby expediting establishment of a real data communication channel between said radio telephone and said fixed station in response to an appropriate request.

29. A radio telephone according to claim 28, further comprising means adapted to store said parameter in said storage means when said radio telephone has a data communication ability and when said radio telephone registers with the fixed station.

30. A radio telephone according to claim 28, further comprising means adapted to store said parameter in said storage means when said radio telephone is registered with the fixed station and requests the setting up of a data communication channel.

31. A radio telephone system according to claim 1 wherein said mobile station comprises a radio telephone.

32. A method according to claim 23 wherein said mobile station comprises a radio telephone.

* * * * *

EXHIBIT B

US006359904B1

(12) **United States Patent**
Hämäläinen et al.

(10) **Patent No.: US 6,359,904 B1**
(45) **Date of Patent: Mar. 19, 2002**

(54) **DATA TRANSFER IN A MOBILE TELEPHONE NETWORK**

(75) Inventors: **Jari Hämäläinen**; **Arto Leppisaari**, both of Tampere; **Kari Huttunen**, Oulu, all of (FI)

(73) Assignee: **Nokia Mobile Phone Ltd.**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/134,615**

(22) Filed: **Aug. 14, 1998**

(30) **Foreign Application Priority Data**

Aug. 18, 1997 (FI) 973373

(51) **Int. Cl.**^{7} **H04J 3/16**; H04J 3/22
(52) **U.S. Cl.** **370/469**; 370/328; 455/422
(58) **Field of Search** 370/328, 329, 370/336, 337, 345, 347, 465, 469; 455/422, 450

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,257,257	A		10/1993	Chen et al.	
5,396,653	A		3/1995	Kivari et al.	
5,430,740	A		7/1995	Kivari et al.	
5,563,895	A	*	10/1996	Malkamaki et al.	714/748
5,570,353	A		10/1996	Keskitalo et al.	
5,577,024	A		11/1996	Malkamaki et al.	
5,606,548	A		2/1997	Vayrynen et al.	
5,640,395	A		6/1997	Hamalainen et al.	
5,642,354	A	*	6/1997	Spear	370/329
5,708,656	A		1/1998	Noneman et al.	
5,726,981	A		3/1998	Ylitervo et al.	
5,729,534	A		3/1998	Jokinen et al.	
5,729,541	A		3/1998	Hamalainen et al.	
5,742,592	A	*	4/1998	Scholefield et al.	370/329
5,745,503	A		4/1998	Kuusinen	
5,745,695	A	*	4/1998	Gilchrist et al.	709/227
5,752,193	A	*	5/1998	Scholefield et al.	455/452
5,764,632	A		6/1998	Ylitervo	
5,790,156	A		8/1998	Mutton et al.	
5,790,534	A		8/1998	Kokko et al.	

FOREIGN PATENT DOCUMENTS

WO	WO 96/27959	9/1996
WO	WO 96/27960	9/1996
WO	WO 97/16899	5/1997
WO	WO 97/28607	8/1997
WO	WO 98/21840	5/1998

OTHER PUBLICATIONS

UK Search Report.
"Digital Cellular Telecommunications System(Phase 2+)"; General Packet Radio Service (GPRS); Service description: Stage 2 (GSM 03.60 version 5.2.0).

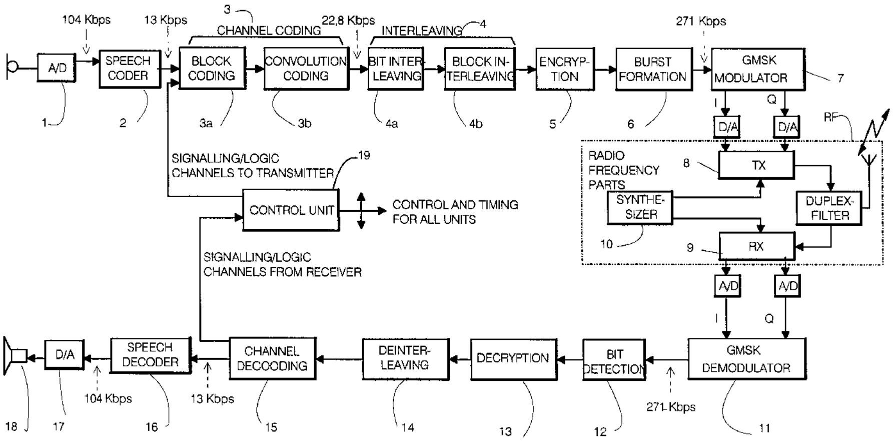
(List continued on next page.)

Primary Examiner—Ajit Patel
Assistant Examiner—Bob A. Phunkulh
(74) *Attorney, Agent, or Firm*—Perman & Green, LLP

(57) **ABSTRACT**

The scope of the present invention is a method for data transfer in a digital mobile communications system, in which method it is handled data in certain layers according to certain protocols, in a certain layer out of said layers it is transferred user data in radio blocks (RB) over a physical radio channel between a mobile station and a fixed mobile communications network, for the transfer of said certain layer it is formed in the radio block (RB) a payload of a certain size comprising check bits (CHB) connected with the performing of the transfer and transfer bits (TB) available for the transfer of user data, each radio block (RB) is channel coded using a certain coding method and the size of said payload is dependent on the coding method. In the transfer bits (TB) of the radio block to be coded using at least a certain coding method it is transferred user data in a first part of the transfer bits and in a second part of the transfer bits it is transferred fill bits in such a way that it is chosen for the transfer of user data a number of transfer bits divisible by eight.

12 Claims, 3 Drawing Sheets



OTHER PUBLICATIONS

"Digital Cellular Telecommunications System"; General Packet Radio Service (GPRS); Mobile Station—Serving GPRS Support Node (MS–SGSN) Logical Link Control (LLC) Layer Specification (GSM 04.64 version 5.1.0).
"Digital Cellular Telecommunications System(Phase 2+)"; General Packet Radio Service (GPRS); Mobile Station (MS)—Serving GPRS Support Node (SGSN): Subnetwoork Dependent Convergence Protocol (SNDCP) (GSM 04.65 version 5.0.0).
"Digital Cellular Telecommunications System(Phase 2+)"; General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2 (GSM 03.64 version 5.0.0).
PCT International Search Report.

* cited by examiner

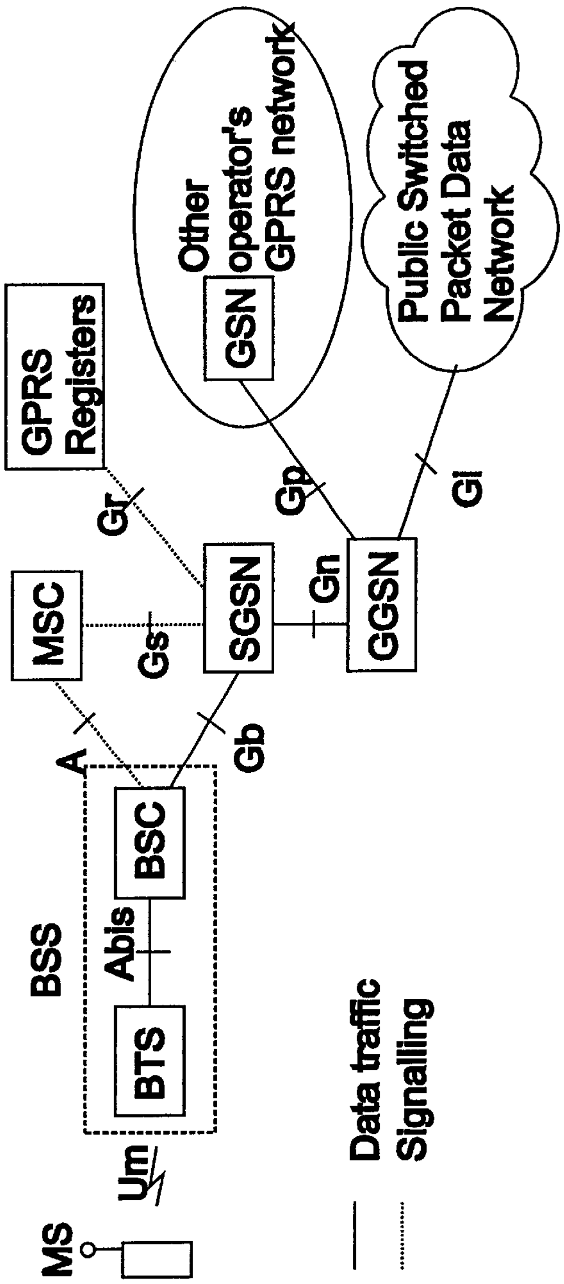

MS
Um
BSS
BTS
Abis
BSC
A
Gb
MSC
Gs
SGSN
Gn
GGSN
GPRS Registers
Gr
Gp
Gi
GSN
Other operator's GPRS network
Public Switched Packet Data Network
Data traffic
Signalling

Fig. 1

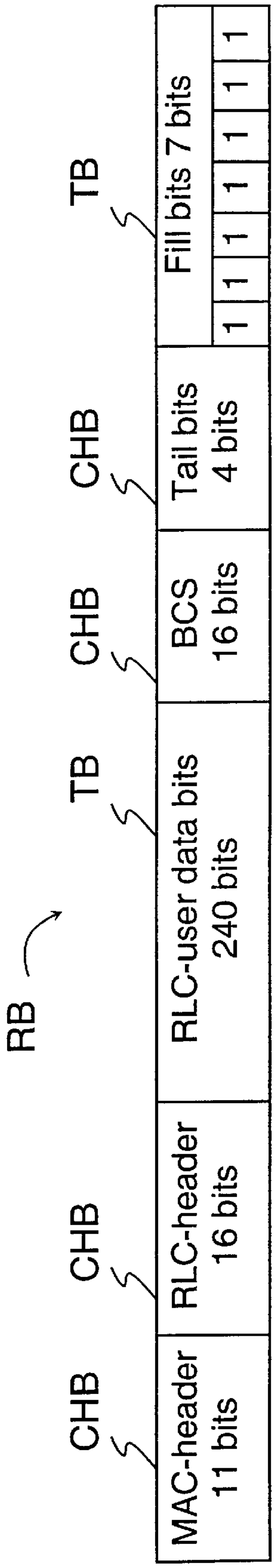

RB
CHB
CHB
TB
CHB
CHB
TB
MAC-header 11 bits
RLC-header 16 bits
RLC-user data bits 240 bits
BCS 16 bits
Tail bits 4 bits
Fill bits 7 bits
1
1
1
1
1
1
1

Fig. 4

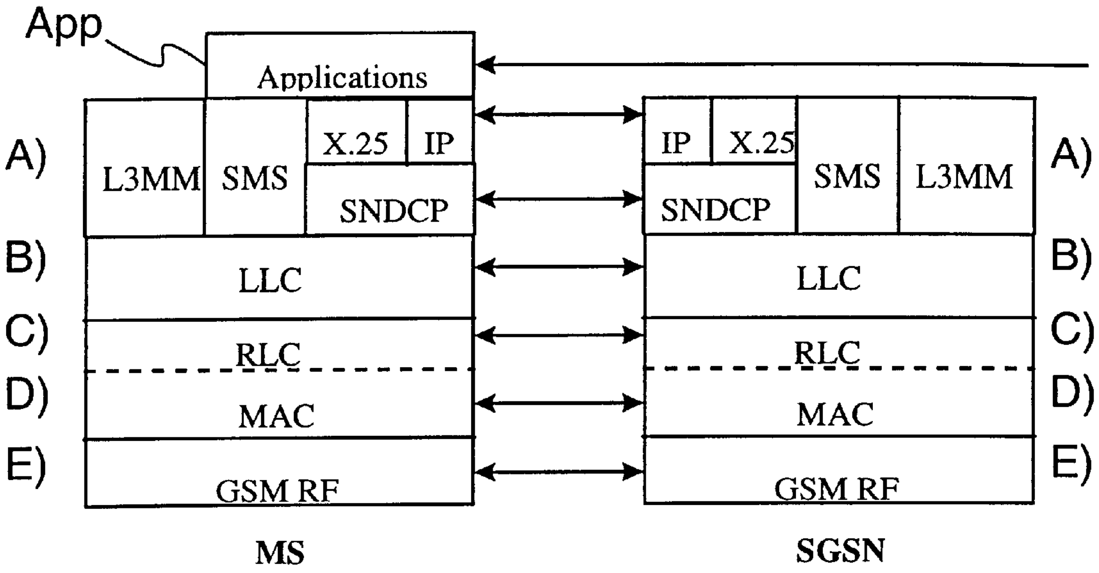


Fig. 2a

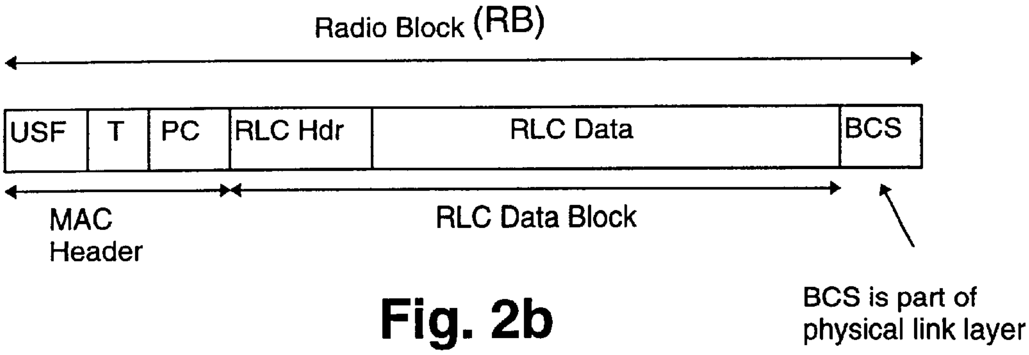


Fig. 2b

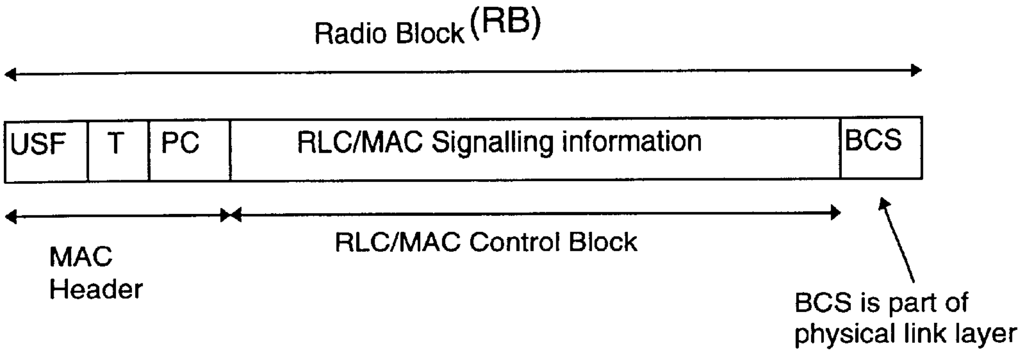

Radio Block (RB)
USF
T
PC
RLC/MAC Signalling information
BCS
MAC Header
RLC/MAC Control Block
BCS is part of physical link layer

Fig. 2c

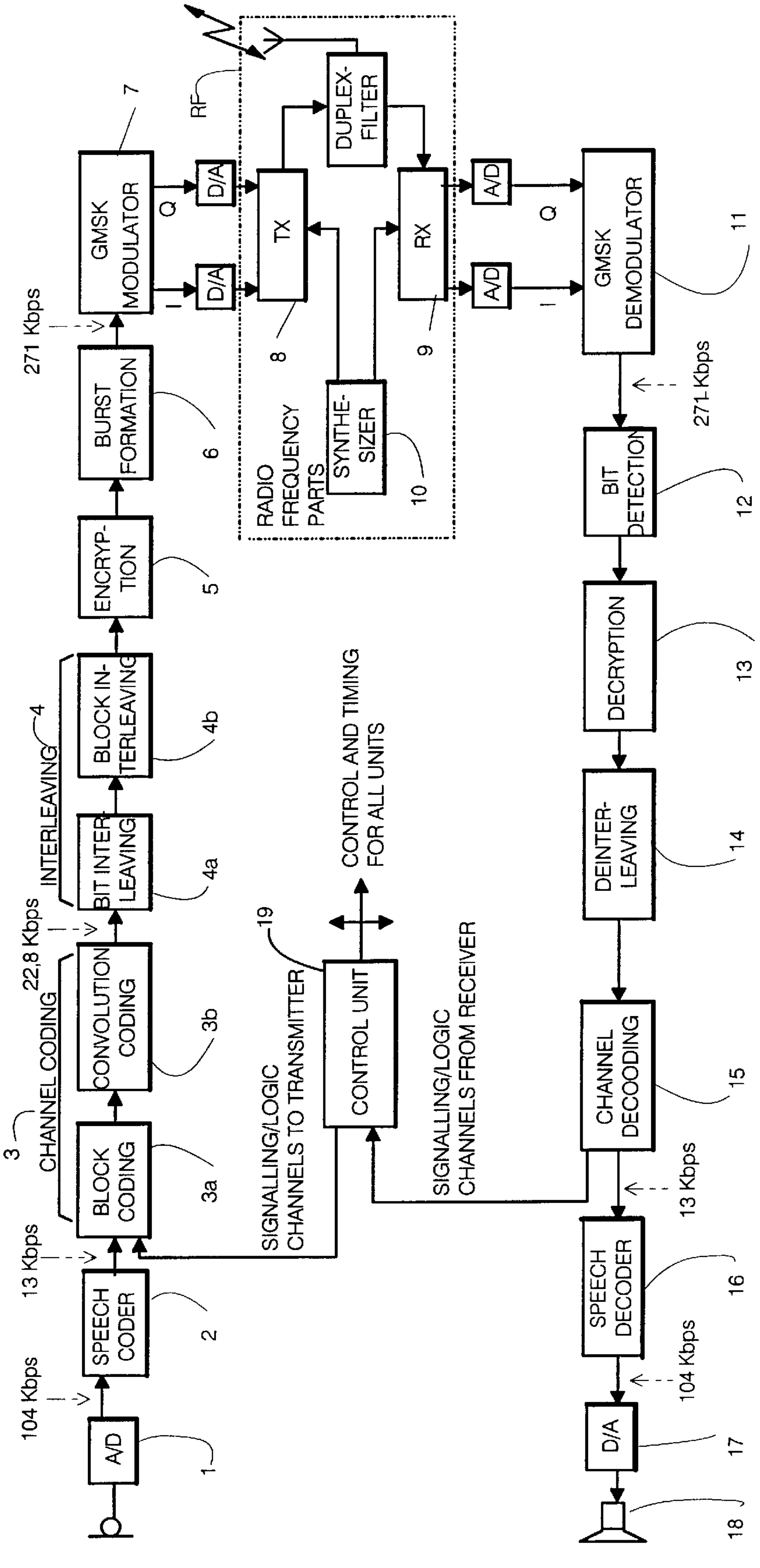

A/D
1
104 Kbps
SPEECH CODER
2
13 Kbps
BLOCK CODING
3a
CONVOLUTION CODING
3b
CHANNEL CODING
3
22,8 Kbps
BIT INTER-LEAVING
4a
BLOCK IN-TERLEAVING
4b
INTERLEAVING
4
ENCRYP-TION
5
BURST FORMATION
6
271 Kbps
GMSK MODULATOR
7
I
Q
D/A
D/A
TX
8
RX
9
DUPLEX-FILTER
SYNTHE-SIZER
10
RADIO FREQUENCY PARTS
RF
A/D
A/D
I
Q
GMSK DEMODULATOR
11
271 Kbps
BIT DETECTION
12
DECRYPTION
13
DEINTER-LEAVING
14
CHANNEL DECOODING
15
13 Kbps
SPEECH DECODER
16
104 Kbps
D/A
17
18
CONTROL UNIT
19
CONTROL AND TIMING FOR ALL UNITS
SIGNALLING/LOGIC CHANNELS TO TRANSMITTER
SIGNALLING/LOGIC CHANNELS FROM RECEIVER

FIG. 3

DATA TRANSFER IN A MOBILE TELEPHONE NETWORK

FIELD OF THE INVENTION

The present invention relates to a method for data transfer in a digital mobile communications network, in which method it is handled user data in certain layers according to certain protocols, in a certain layer of said layers it is transferred user data over a physical radio channel between a mobile station and a fixed mobile communications network in radio blocks, for the transfer of said layer it is formed in the radio block a payload of a certain size comprising check bits connected with the performing of the transfer and transfer bits available for the transfer of user data, each radio block is channel coded using a certain coding method and the size of said payload is dependent on the coding method. The invention also relates to a transmitter/receiver device operating according to the method and a mobile communications system. The invention relates in particular to data transfer in the GSM-system in the GPRS-packet switched service.

BACKGROUND OF THE INVENTION

Out of the present mobile communications systems a majority is offering data- and voice services based upon circuit switched technique. In the circuit switched technique a transfer connection is maintained during the whole connection even if no information would be transferred time to time. This unnecessarily consumes the transfer resources, shared by also many other users, in which case the maintaining of a circuit switched transfer connection to one user consumes unnecessarily the transfer resources of other users. Because of the bursts in the GSM-transmission, data services are not optimal in the circuit switched technique. However, the packet switched information transfer for the increasing of the efficiency of the utilization of a channel is known.

As well as the fixed network also a future mobile communications network must be able to transfer both circuit switched and packet data transfer, e.g. ISDN-transfer (Integrated Services Digital Network) and ATM-transfer (Asynchronous Transfer Mode). For information transfer using packet switching it is known in mobile communications systems a protocol based upon packet reservation multiple access called PRMA (PRMA, Packet Reservation Multiple Access). It is also spoken of as packet radio. PRMA is a technique for multiplexing digital speech or data in a time division carrier wave, i.e. PRMA uses in a radio channel a time division multiple access (TDMA, Time Division Multiple Access), in which case transmission and reception take place at certain moments using time division. The PRMA-protocol has been developed to utilize the discontinuity of speech transfer in order to support more users than the number of speech channels in a time division carrier wave. In such a case a channel is allocated to a mobile station, for example a speech channel when speech is being produced and when the speaking ends the channel is released, in which case the mobile station does not unnecessarily reserve capacity, but the channel is channel is free for other purposes, for example the transmissions of other mobile stations in the cell. The PRMA-protocol is used in cellular mobile communications systems in the communication between a mobile station and a base station. The GSM GPRS (General Packet Radio Service)-system is an example of a system based upon a PRMA-type protocol.

GPRS is a new GSM-service, by using which the packet radio operation can be made available to GSM-users. GPRS

reserves radio resources only when there is something to transmit, in which case the same resources are shared between all mobile stations as needed. The normal circuit switched network of the GSM-system has been designed for circuit switched speech transmissions. The main goal of the GPRS-service is to realize the connection from a mobile station to a public data network using prior known protocols, such as TCP/IP and X.25. However, there is a connection between the packet switched GPRS-service and the circuit switched services of the GSM-system. In a physical channel resources can be reused and certain signalling can be common to both. It is possible to reserve in the same carrier wave time slots for circuit switched use and for the packet switched GPRS-use.

FIG. **1** presents telecommunication network connections in a packet switched GPRS-service. The main element of the infrastructure of the network for GPRS-services is a GPRS-support node, so called GSN (GPRS Support Node). It is a mobility router which realizes the connecting and co-operation between different data networks, for instance to PSPDN (Packet Switched Packet Data Network) through interface Gi or to another operator's GPRS-network through interface Gp, mobility management using GPRS-registers over interface Gr and the transfer of data packets to mobile stations MS independent of their location. It is possible to integrate physically GPRS-node GSN with mobile switching center MSC (Mobile Switching Center) or it can be a separate network element based upon the architecture of data network routers. User data passes directly between support node GSN and base stations system BSS, consisting of base stations BTS and base station controllers BSC, through interface Gb, but between support node GSN and mobile switching center MSC there is signalling interface Gs. In FIG. **1** the uninterrupted lines between blocks represent data traffic (i.e. the transfer of speech or data in a digital form) and the interrupted lines represent signalling. Physically the data can pass transparently over mobile switching center MSC. The radio interface between mobile station MS and the fixed network passes through base station BTS and it has been marked with reference Um. References Abis and A represent the interface with base station BTS and base station controller BSC, and respectively between base station controller BSC and mobile switching center MSC, which is a signalling connection. Reference Gn represents an interface between the different support nodes of the same operator. The support nodes are normally divided into gateway support nodes GGSN (Gateway GSN) and serving or home support nodes SGSN (Serving GSN) as presented FIG. **1**.

The GSM-system is a time division multiple access-type (TDMA, Time Division Multiple Access) system, in which the traffic in the radio path is time-divided and takes place in repeated TDMA-frames, each of which consists of several (eight) time slots. In each time slot it is transmitted an information packet in form of a radio frequency burst of finite duration consisting of a number of modulated bits. The time slots are mainly used as control channels and traffic channels. On the traffic channels it is transferred speech and data and in the control channels it is carried out signalling between base station BTS and mobile station MS.

In the following it is explained the protocols of GPRS and the protocol hierarchy in radio interface Um between mobile station MS and a fixed network (home support node SGSN) with reference to FIG. **2***a*. User data is handled hierarchically on different levels, when it is converted into a form suited for the physical radio path and the public data network. On the highest level A) the user data (coming e.g.

from an application App) is in a form suited for the protocol of the public data network, such as TCP/IP and X.25 and on the lowest level E) the data is in a form suited for transferring in the GSM-radio path.

The highest level A) protocol SNDCP (Subnetwork Dependent Convergent Protocol), i.e. a convergence protocol dependent of a subnetwork is explained in more detail in GSM radio specifications 04.65 and 03.60. According to SNDCP a network protocol data unit is segmented between mobile station MS and home support node SGSN into one or several SNDCP data units, the maximum size of the payload of which is approximately 1600 octets. The SNDCP-data unit is transferred in one LLC-fame (Logical Link Control) over the radio interface. The SNDCP-protocol includes multiplexing of user data, segmenting and compressing, and the compressing of the TCP/IP-header. It is possible to transfer in the SNDCP-protocol different network level protocols, such as IP, X.25, PTM-M and PTM-G. The size of a SNDCP user data field is, as to the total number of bits, divisible by eight bits, i.e. it is octet oriented.

The protocol of the next B) level, the LLC-protocol or the logical link control protocol has been explained in more detail in GSM standard specifications 04.64 and 03.60. The LLC-protocol provides a reliable logical link between a mobile station and home support node SGSN. SNDCP-, short messages and GPRS signalling messages are transmitted in LLC-frames which have a frame header containing numbering and a temporary address field, an information field of variable length and a frame check sequence. The functionality of LLC includes maintaining the communication context of mobile station MS and home support node SGSN, the transmitting of acknowledged and unacknowledged frames, the detection and retransmitting of corrupted frames. LLC-frames are transmitted in one or several radio blocks. The logical link is maintained when mobile station MS moves between cells within the area of one home support node SGSN. If mobile station MS moves into the area of another home support node SGSN, a new logical link must be established. The size of a LLC-protocol user data field is, as to the total number of bits, divisible by eight bits, i.e. it is octet oriented.

The next level C) after LLC, the RLC-level (Radio Link Control) has been explained in more detail in GSM standard specifications 03.64. The LLC-frame is being transmitted continuously. The variable length LLC-frames is transmitted in one or more RLC-blocks. The functionality of RLC between mobile station MS and home support node SGSN is to detect the corrupted RLC-blocks and to ask for a selective retransmission of the corrupted blocks. A retransmission request comprises a bit map indicating each air path block to be either corrupted or successfully received. Based upon the bit map the transmitter retransmits the corrupted blocks. The total size of an RLC-block is, the header and user data included, as to the number of bits, is divisible by eight bits, i.e. it is octet oriented.

Also level D), the MAC-level (Medium Access Control) has been explained in more detail in GSM standard specifications 03.64. MAC is used for dividing radio channels between mobile stations and for the allocating of a radio channel for a mobile station for transmission and reception as needed. The functionality of MAC includes a separate header containing uplink state flag USF (Uplink State Flag), block type indicator T and eventual power control information PC (Power Control). The MAC-header and the RLC-data block are placed in radio block RB (see FIGS. **2***b* and **2***c*) to be transmitted on the physical layer.

Protocol level E) describes the physical layer or GSM-radio path, in which messages are transferred in radio blocks RB presented in FIGS. **2***b* and **2***c*. Radio block RB includes a MAC-header, an information part containing the data or the signalling (RLC-data block, FIG. **2***b* or an RLC/MAC-signalling-information block, FIG. **2***c*) and block check sequence BCS (Block Check Sequence). Each radio block is interleaved in four standard bursts. Before the interleaving it is performed a channel coding on the radio block. For the channel coding there are four different coding schemes CS-**1**, CS-**2**, CS-**3** and CS-**4** (Coding Scheme). A mobile station must support all four alternatives. In the channel coding a convolutional coding is performed on the information part. A pre-coding is performed on uplink state flag USF (Uplink State Flag), in which case the length of USF after the pre-coding is dependent on the channel coding method CS-**1** . . . CS-**4** used. After the channel coding the size of the radio block is according to the GSM-specification 456 bits. Prior to the convolutional coding the payload according to the different coding method varies, and an octet oriented data stream is not achieved with all coding methods CS-**1** . . . CS-**4**. Only CS-**1** produces an octet oriented data stream, but the other the channel coding methods CS-**2** . . . CS-**4** do not do it according to the present protocols. This hampers data stream between different layers A)–E) in mobile station MS and in the mobile communications network, i.e. in base station system BSS and in home support node SGSN.

SUMMARY OF THE INVENTION

Now it is introduced such a method, with which data flow can be made simpler between all hierarchy levels or between mobile station MS and the different protocols of mobile communications network BSS; SGSN. This is achieved by bringing the user data flow into octet form on all protocol levels of the GPRS-service, in particular on the lower levels, by setting a certain number of bits as fill bits instead of using them for the transfer of user data. With this method it is possible to make the payload of a radio block octet oriented when any of channel coding methods CS-**1** . . . CS-**4** is used. A certain number of the bits of radio block RB, the being determined according to the method, are set prior to channel coding and the interleaving of the radio block (in four bursts) to transfer fill bits in such a way that the number of bits in the radio block transferring user data is divisible by eight prior to the channel coding. By using the method the handling of data, in particular that of the user data to be transferred, is made octet oriented on all GPRS-protocol levels. Because the radio block is made octet oriented the operation can after the channel coding be carried out fully in accordance with the GSM-specifications.

If this method were not used, the transmissions of two radio blocks would be mixed in such a way that the last bits of the preceding radio block would be transferred in the same burst with the first bits of the next radio block. This would make the handling of the data and protocols, and the equipment executing them difficult when octets coming from a higher protocol level should be distributed to different blocks on lower protocol levels.

The method according to the invention is characterized in that in the transfer bits of a radio block coded using at least a certain coding method it is transferred user data in a first part of the transfer bits and fill bits in a second part in such a way that it is chosen such a number bits for the of transfer user data which is divisible by eight.

The transmitter/receiver device according to the invention is correspondingly characterized in that it comprises control means for transferring user data in a first part of radio block transfer bits coded using at least a certain coding method and for transferring fill bits in a second part of said transfer bits, and said first part of transfer bits comprises a number of bits divisible by eight.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described in detail in the following with reference to enclosed figures, of which

FIG. **1** presents the structure of a telecommunication network in the GSM GPRS-packet service data transfer,

FIG. **2***a* presents the different protocols levels of the GPRS-service,

FIG. **2***b* presents a radio block to be transferred in the radio interface,

FIG. **2***c* presents another radio block to be transferred in the radio interface,

FIG. **3** presents the block diagram of a GSM-system transceiver,

FIG. **4** presents a radio block according to the invention to be transferred in the radio interface.

DETAILED DESCRIPTION

In order to illustrate the handling of a transmitter/receiver and a physical layer according to the invention, it is explained in the following the transmitter- and receiver function of the GSM-system with reference to FIG. **3**, in which it is presented a block diagram of a transmitter/receiver in a mobile telephone according to the GSM-system. The transmitter/receiver of a base station differs from the transmitter/receiver of a mobile telephone usually in the respect that it is a multi-channel one and it has no microphone nor loudspeaker, in other respects it is in structure and operating principle similar to the transmitter/receiver of a mobile telephone.

The first stage of a transmission sequence is digitizing **1** of analogue speech and encoding **2**. Sampling with A/D-converter **1** is carried out a 8 kHz frequency and the speech encoding algorithm assumes the input signal to be 13 bit linear PCM. The samples obtained from the A/D-converter are segmented into 160-sample speech frames, in which case the duration of each speech frame is 20 ms. Speech encoder **2** handles 20 ms speech frames, i.e. prior to the commencing of the encoding it is taken 20 ms of speech in a buffer. The coding operations are performed frame by frame or on their subframes (in 40-sample blocks). As a result of the encoding by speech encoder **2** it is obtained 260 bits out of one frame.

After speech encoding **2** it is performed channel coding **3** for example in two stages depending on the coding method used, when at first one part of the bits (e.g. 50 most significant of 260 bits) are protected using block code **3***a* (=CRC, 3 bits) and after that these and the next most important bits (132) are further protected using convolutional code **3***b* (coding ratio 1/2) ((50+3+132+4)*2=378, and a part of the bits are taken unprotected (78). As presented in FIG. **3**, signalling- and logical messages and the data to be transmitted come directly from control unit **19** controlling the blocks of the telephone to block coding block **3***a*, and thus naturally no speech encoding is performed on these data messages. Correspondingly, signalling- and logical messages and the received data are taken from channel decoding block **15** to control unit **19**. In block encoding **3***a* a bit string is attached at the end of a speech frame, using which bit string it is possible to detect transfer errors at reception. In convolutional coding **3***b* it is increased the redundancy of a speech frame. All in all, a total of 456 bits per each 20 ms frame is transmitted.

These 456 bits are interleaved **4** and also interleaving **4** is performed in two stages. At first **4***a* the order of bits is mixed and the mixed bits are divided into eight blocks of equal size. These blocks are further distributed **4***b* into eight subsequent TDMA-frames, in which case the interleaved 456 bits are transmitted in eight time slots of the radio path (57 bits in each). With the interleaving it is striven for to spread transfer errors, which usually occur as error bursts, evenly over all the data to be transmitted, in which case the channel decoding operates at its most effective. After the deciphering of the interleaving an error burst is converted into individual error bits which can be corrected in the channel decoding. The following stage in the transmission sequence is the ciphering **5** of data. Ciphering **5** is carried out using an algorithm which is one of the most guarded secrets of GSM. With the ciphering it is striven for to prevent any unauthorized listening of calls.

Out of the ciphered data it is formed **6** a bust to be transmitted by adding in it a learning sequence, tail bits and a protection time. The burst to be transmitted is brought to GMSK-modulator **7** which modulates the burst for transmission. The GMSK-modulation method (Gaussian Minimum Shift Keying) is a digital, constant amplitude modulation method, in which the information is contained in the shifts of phase. Transmitter **8** mixes the modulated burst through one or more intermediate frequencies into 900 MHz and transmits it through an antenna to the radio path. Transmitter **8** is one of three radio frequency blocks RF. Receiver **9** is the first block on the reception side and it performs the operations inverted to those of transmitter **8**. The third RF-block is synthesizer **10** which takes care of the forming of frequencies. In the GSM-system it is used frequency jumping, in which transmission- and reception frequencies are changed in each TDMA-frame. The frequency jumping improves the quality of the connection, but sets strict requirements on synthesizer **10**. Synthesizer **10** must be capable of moving from one frequency to another very quickly, in less than one millisecond.

In reception it is carried out operations inverted to transmission. After RF-receiver **9** and demodulator **11** it is carried out bit detection **12** using for example a channel correction unit, in which bits are detected from the received samples i.e. it is tried to find out the transmitted bit sequence. After the detection ciphering **13** and interleaving **14** are deciphered and channel decoding **15** is performed on the detected bits and the check sum is checked using a cyclic redundance check (CRC, Cyclic Redundance Check). In channel decoding **15** it is striven for to correct the bit errors occurred at the transfer of the burst. In a 260 bit speech frame after channel decoding **15** there are the transmitted parameters representing the speech, by using which speech decoder **16** forms the digital samples of the speech signal. The samples are D/A-converted **17** for reproduction with loudspeaker **18**.

In a transmitter/receiver as the central control unit of a mobile station there is control unit **19** which essentially controls all blocks **1**–**18** and coordinates their operations and controls timing. Control unit **19**usually comprises for example a microprocessor. The protocols according to hierarchy level A)–D), presented in FIG. **2***a*, are executed preferably in control unit **19** and the processing of user data to the physical channel (in transmission beginning from channel coding an in reception until channel decoding) is performed in blocks **3**–**15**.

For channel coding **3** there are four different coding schemes CS-**1**, CS-**2**, CS-**3** and CS-**4** (Coding Scheme). A mobile station must support each method. The data rates of these coding methods are 9.05, 13.4, 15.6 and 21.4 kbps respectively. Coding method CS-**1** contains a convolutional coding having a coding ratio of 1/2, which is used in the GSM-system on the SDCCH-channel. In coding methods CS-**2** and CS-**3** it is also at first performed a convolutional coding having a coding ratio of 1/2, after which fill bits are removed by puncturing in order to achieve the desired 456 bits. Coding method CS-**4** has no FEC-error protection (Forward Error Protection), i.e. no convolutional coding is performed on the data.

In the following it is explained in more detail the channel coding carried out in a packet data traffic channel (PDTCH, Packet Data Traffic Channel). Radio block RB presented in FIG. **2***b*, in which the RLC-data block is transferred, can be coded using one of the above channel coding methods CS-**1** . . . CS-**4**, while radio block RB presented in FIG. **2***c*, in which the RLC/MAC-control block is transferred is always coded using channel coding method CS-1.

In the first stage of coding it is added at the end of a radio block a block check sequence BCS (Block Check Sequence) for error detection. After this in coding methods CS-**1** . . . CS-**3** it is performed on the uplink status flag or USF a pre-coding (except in method CS-**1**), four tail bits are added and convolutional coding is performed according to above description, and puncturing in methods CS-**2** and CS-**3** in order to achieve the desired coding rate (456 bits).

The coding parameters of the different methods are presented below in Table 1.

TABLE 1

Scheme	Code rate	USF	Precoded USF (a)	Radio Block excl. USF and BCS (b)	BCS (c)	Tail (d)	Coded bits (e)	Punctured bits (f)	Data rate kb/s
CS-1	½	3	3	181	40	4	456	0	9.05
CS-2	≈⅔	3	6	268	16	4	588	132	13.4
CS-3	≈¾	3	6	312	16	4	676	220	15.6
CS-4	1	3	12	428	16	—	456	—	21.4

Table 1 shows that the length of USF after pre-coding/bit processing is 3, 6, 6 and 12 bits respectively in the different methods (column a). Block check sequence BCS is 40 bits in CS-**1** method and in the other methods 16 bits (column c). After convolutional coding **3***b* with code rate 1/2 it is obtained 456, 588 and 676 coded bits in methods CS-**1** . . . CS-**3** and in method CS-**4** it is obtained directly 456 bits without convolutional coding (column e). By adding together the bits in columns a–d it is obtained the payload according to each method. It is then seen that the payload in methods CS-**1**, CS-**2** and CS-**3** is 228, 294 and 338 bits and the number of bits is doubled in the convolutional coding in accordance with column e. In method CS-**4** it is obtained a payload of 456 bits. When it is known that the length of a pre-coded USF varies 3–12 bits and that the total length of T and PC is 5 bits, it is obtained as the size of a MAC-header field 8, 11, 11 and 17 bits. The number of tail bits is 4 in methods CS-**1** . . . CS-**3** and 0 in method CS-**4**. In this way the number of bits available for the transfer of the other data is as presented in Table 2.

TABLE 2

Payload bits	MAC header	BCS	Tail bits	Remaining bits
CS-1: 228 –	8 –	40 –	4 =	176
CS-2: 294 –	11 –	16 –	4 =	263
CS-3: 338 –	11 –	16 –	4 =	307
CS-4: 456 –	17 –	16 –	0 =	423

In these bits it is transferred the RLC-header and the RLC-data containing the actual user data. These are in the RLC-layer (layer C in FIG. **2***a*) divisible by eight. In order to keep the handling and transfer of user data octet oriented according to the invention, two octets or 16 bits are reserved for the header field, and the number of RLC-data block bits shown in Table 3 is transferred, when in certain methods bits are left over for user data transfer.

TABLE 3

Payload bits	MAC header		RLC header		RLC data bits		BCS		Tail bits		Additional bits
CS-1: 228 =	8	+	16	+	160	+	40	+	4	+	0
CS-2: 294 =	11	+	16	+	240	+	16	+	4	+	7
CS-3: 338 =	11	+	16	+	288	+	16	+	4	+	3
CS-4: 456	17	+	16	+	400	+	16	+	0	+	7

According to the invention it is not user data that is transferred in these additional bits of a radio block but fill bits in order to arrange the handling and transfer of user data to be octet oriented, i.e. divisible by eight. According to the invention in the fill bits of a radio block, i.e. in a certain amount of bits reserved for the transfer of user data it is transferred fill bits, depending on channel coding method CS-**1** . . . CS-**4**. This is done by giving the concerned bits a predetermined value, either logical "1" or logical "0". However, in order to get as much user data as possible transferred in a radio block, it is preferably transferred only such a quantity of fill bits, less than an octet, which leaves as many as possible octets available for the transfer of user data. Such quantities are presented in Table 3.

Thence 0 bits (i.e. none) is set as fill bits in channel coding method CS-**1**. In channel coding method CS-**2** for example the seven last bits are chosen as the fill bits, in channel coding method CS-**3** 3 additional bits (for example 3 last bits) are chosen as the fill bits and in channel coding method CS-**4** it is selected 7 additional bits (for example the last 7 bits) as the fill bits. FIG. **4** presents an example of the contents of a radio block payload in the method according to the invention when coding method CS-**2** is used. The payload comprises check bits CHB connected with the performing of the transfer, in which bits it is transferred the MAC-header bits, RLC-header bits, BCS-bits and the tail bits, and transfer bits TB used for the transfer of user data, in which bits it is here transferred the RLC-user data bits and the seven fill bits at the end, which bits otherwise could be used for the transfer of user data. In a radio block according to FIG. **4** it is transferred user data in octets (bytes), in which case handling between different hierarchy levels is kept simple. According to the invention the maximum amount of user data bits transferred in a radio block is obtained by dividing the number of transfer bits TB by eight and by transferring user data in the number of octets (bytes) corresponding to the quotient and by transferring fill bits in the number of transfer bits corresponding to the remainder.

By utilizing the invention it is obtained in each channel coding method an octet oriented number of user data bits or RLC-data bits. At the same it is further obtained after the channel coding and the puncturing presented in Table 1, in each method the desired number of bits, 456. In this way the puncturing need not be changed. This is achieved because the size of the payload is in the method according to the invention kept unchanged with respect to the payloads defined in GSM standard specification 03.64.

Alternatively the payloads of methods CS-**2** and CS-**3** are increased, for example in CS-**2** by one bit to 295 and in CS-**3** by five bits to 343, in which case it would be obtained one more octet for the transfer of user data (with the additional bits noted in Table 3 regarded). Then the number of bits after the convolutional coding would be 590 and 686, in which case the puncturing should be altered by puncturing 134 and 230 bits respectively. If correspondingly the payload should be reduced by 7 and 3 bits, the puncturing should be reduced. Such alternative methods would however require the changing of both the payload and the puncturing in the GSM standard specification 03.64, which is not desirable.

Thanks to the invention data stream through different layers from the higher layers down to the lowest physical layer is made octet oriented, which simplifies the executing of protocols between mobile station MS and fixed network BSS, SGSN. At the same a certain number of bits is lost (0, 7, 3, 7), which bits otherwise could be used for the transfer of user data. When the certain number of bits according to the invention is chosen in such a way that the number is less than an octet and at the same the number of bits in a RLC-data block is adjusted to divisible by eight, the achieving of simpler protocols is however more important than the loss of a few bits for the transfer of user data.

The above has been an introduction of the realization of the invention and its embodiments using examples. It is self evident to persons skilled in the art that the invention is not limited to the details of the above presented examples and that the invention can be realized also in other embodiments without deviating from the characteristics of the invention. The presented embodiments should be regarded as illustrating but not limiting. Thus the possibilities to realize and use the invention are limited only by the enclosed claims. Thus different embodiments of the invention specified by the claims, also equivalent embodiments, are included in the scope of the invention.

What is claimed is:

1. A method for data transfer in a digital mobile communications system, in which method

user data is handled in layers according to protocols,

in one layer of said layers user data is transferred over a physical radio channel between a mobile station and a fixed mobile communications network in radio blocks,

for the transfer of said one layer a payload of a size comprising check bits connected with the performing of the transfer and transfer bits available for the transfer of the user data is formed in the radio block,

each radio block is channel coded using a coding method and the size of said payload is dependent on the coding method, wherein

in the transfer bits of a radio block to be coded using at least said coding method, user data is transferred in a first part of the transfer bits and fill bits are transferred in a second part so that, for the transfer of user data, such a number of transfer bits is chosen which is divisible by eight.

2. A method according to claim **1**, wherein

as the first part of transfer bits for use for the transfer of user data it is chosen the number of octets indicated by the quotient when the number of transfer bits is divided by eight, and

as the second part of transfer bits for use for the transfer of the fill bits it is chosen the number of transfer bits indicated by the remainder of said division.

3. A method according to claim **1**, wherein the radio block is one of the radio blocks according to the GSM standard specification 03.64, except for said fill bits.

4. A method according to claim **1**, wherein in said second part of transfer bits fill bits are set prior to the channel coding performed in the channel coding and prior to interleaving of the bits of the radio block into bursts to be transmitted.

5. A transmitter/receiver device for transmitting user data in a digital mobile communications system, which device comprises

user data handling means for the handling of user data in layers according to protocols,

transmitting means for transmitting user data in radio blocks over a physical radio channel in one layer of said layers,

payload forming means for the forming of a payload of a predetermined size in a radio block for the transfer of said one layer, said payload comprising check bits connected with the performing of the transfer and transfer bits available for the transfer of user data,

channel coding means for the channel coding of a radio block using a coding method, and said size of the payload is dependent on the coding method used, wherein the device comprises

control means for transferring user data in a first part of radio block transfer bits, the radio block being coded using at least said coding method, and for transferring fill bits in a second part of said transfer bits, and said first part of the transfer bits comprises a number of bits divisible by eight.

6. A transmitter/receiver device according to claim **5**, wherein said control means have been arranged to choose as the first part of transfer bits to be used for the transfer of user data the number of octets obtained by the quotient when the number of transfer bits is divided by eight, and

said control means have been arranged to choose as the second part of transfer bits to be used for the transfer of the fill bits the number of bits indicated by the remainder of said division.

7. A transmitter/receiver device according to claim **5**, wherein it has been arranged to transfer transfer bits according to the GSM standard specification 03.64, except for said fill bits.

8. A digital mobile communications system comprising

at least one mobile station and a fixed mobile communications network, which system comprises means for transferring user data over a physical radio channel between the mobile station and the fixed mobile communications network,

user data handling means for the handling of user data in layers according to protocols,

data transfer means for the transfer of user data in radio blocks over a physical radio channel in one layer of said layers,

payload forming means for the forming of a payload of a size in a radio block for the transfer of said one layer, said payload comprising check bits connected with the performing of the transfer and transfer bits available for the transfer of user data,

channel coding means for the channel coding of the radio block using a coding method and the size of said payload is dependent on the coding method,

wherein the system comprises

control means for transferring user data in a first part of transfer bits of the radio block to be coded using at least said coding method, and for the transfer of fill bits in a second part of said transfer bits, and said first part of transfer bits comprises a number of bits divisible by eight.

9. A digital mobile communications system according to claim **8**, wherein

said control means have been arranged to choose as the first part of transfer bits to be used for the transfer of user data the number of octets according to the quotient obtained when the number of transfer bits is divided by eight, and

said control means have been arranged to choose as the second part of transfer bits to be used for the transfer of fill bits the number of transfer bits according to the remainder of said division.

10. A mobile communications system according to claim **8**, wherein it has been arranged to transfer transfer bits according to the GSM standard specification 03.64, except for said fill bits.

11. A method for transceiving a first user data in a digital mobile communications system having a first mobile station and a first fixed mobile communications system, the method comprising the steps of:

selecting a first protocol coding format;

translating the first user data in a first layer according to the first protocol format;

transceiving the first user data over a physical communications channel between the first mobile station and the first fixed mobile communications system, wherein transceiving the first user data comprises the steps of:

selecting a first channel code;

encoding the first user data according to the first channel code, wherein the step of encoding the first user data further comprises the steps of:

using dummy bits where necessary to make the first user data divisible by eight;

encoding the now divisible by eight first user data; and

transceiving the first user data.

12. A method according to claim **11**, wherein the step of encoding the first user data to be divisible by eight further comprises the steps of:

determining a first number of octets of the first user data from the quotient of dividing the first user data by eight; and

determining a second number of dummy bits from the remainder of dividing the first user data by eight.

* * * * *

EXHIBIT C

US006694135B1

(12) **United States Patent**
Oksala et al.

(10) **Patent No.: US 6,694,135 B1**
(45) **Date of Patent: Feb. 17, 2004**

(54) **MEASUREMENT REPORT TRANSMISSION IN A TELECOMMUNICATIONS SYSTEM**

(75) Inventors: **Jarkko Oksala**, Tampere (FI); **Kari Hautamaki**, Oulu (FI)

(73) Assignee: **Nokia Mobile Phones Ltd.**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/473,789**

(22) Filed: **Dec. 29, 1999**

(30) **Foreign Application Priority Data**

Dec. 31, 1998 (GB) 9828875

(51) **Int. Cl.**^{7} **H04Q 7/20**

(52) **U.S. Cl.** **455/424**; 455/69; 455/522

(58) **Field of Search** 455/424, 69, 423, 455/522, 67, 170, 68, 88, 403, 575, 464, 466, 67.4, 226, 73; 370/346, 349, 469, 449, 347, 331, 332, 465, 550; 379/346, 349; 714/748, 749

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,475,010	A	*	10/1984	Huensch et al.	179/2 EB
4,910,794	A	*	3/1990	Mahany	455/67.4
5,093,924	A	*	3/1992	Toshiyuki et al.	455/33
5,633,875	A	*	5/1997	Hershey et al.	370/346
5,960,335	A	*	9/1999	Umemoto et al.	455/226.2
5,966,657	A	*	10/1999	Sporre	455/425
6,356,759	B1	*	3/2002	Mustajarvi	455/450
6,359,904	B1	*	3/2002	Hamalainen et al.	370/469
6,430,163	B1	*	8/2002	Mustajarvi	370/310

FOREIGN PATENT DOCUMENTS

WO	WO 98/44639	10/1998

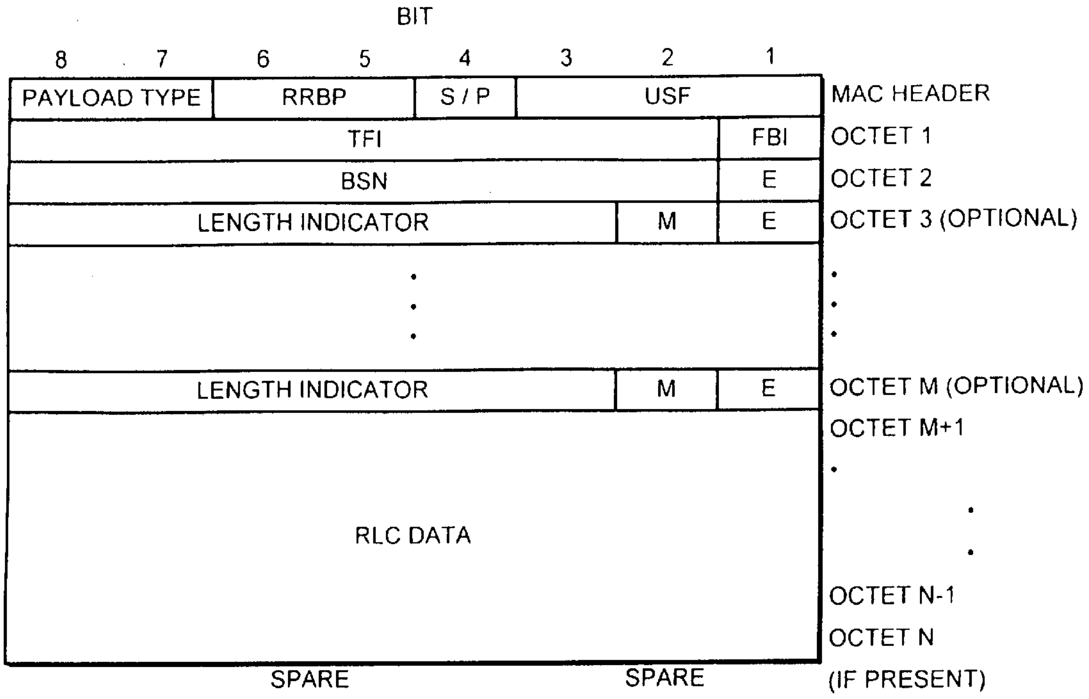
* cited by examiner

Primary Examiner—Edward F. Urban
Assistant Examiner—C. Chow
(74) *Attorney, Agent, or Firm*—Perman & Green, LLP

(57) **ABSTRACT**

A method of obtaining data messages at a radio communication network from a mobile station operating therein during downlink transfer, the method comprising the network providing a header portion of the downlink transfer with one or more unique polling codes for requesting the mobile station to transmit one or more respective data messages indicative of one or more corresponding conditions at the mobile station.

17 Claims, 2 Drawing Sheets



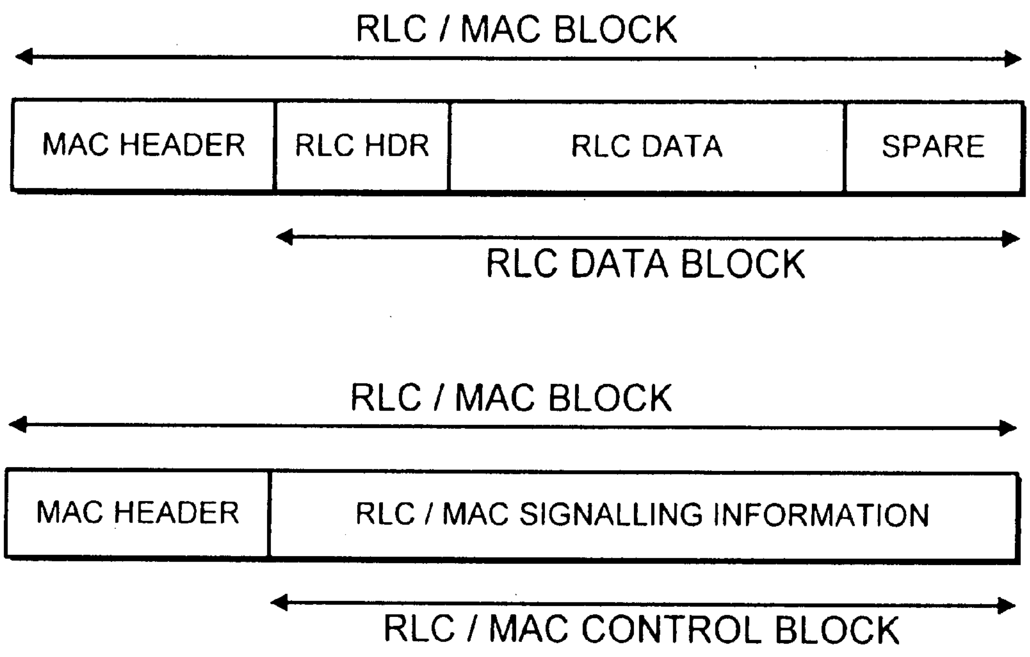

RLC / MAC BLOCK
MAC HEADER
RLC HDR
RLC DATA
SPARE
RLC DATA BLOCK
RLC / MAC BLOCK
MAC HEADER
RLC / MAC SIGNALLING INFORMATION
RLC / MAC CONTROL BLOCK

FIG. 1

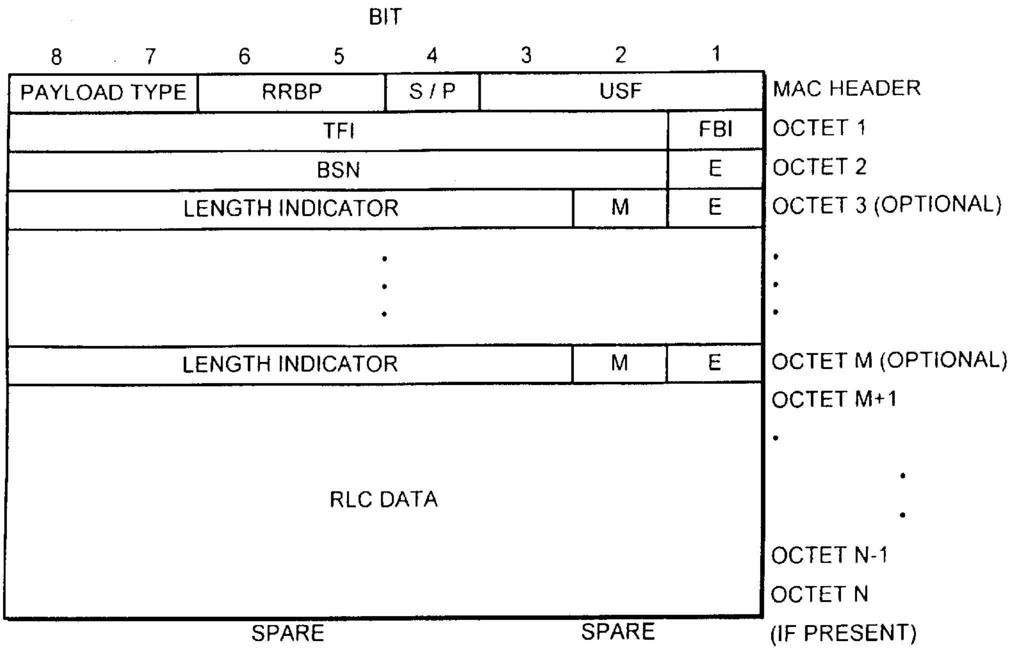

BIT
8
7
6
5
4
3
2
1
PAYLOAD TYPE
RRBP
S / P
USF
MAC HEADER
TFI
FBI
OCTET 1
BSN
E
OCTET 2
LENGTH INDICATOR
M
E
OCTET 3 (OPTIONAL)
LENGTH INDICATOR
M
E
OCTET M (OPTIONAL)
OCTET M+1
RLC DATA
OCTET N-1
OCTET N
SPARE
SPARE
(IF PRESENT)

FIG. 2

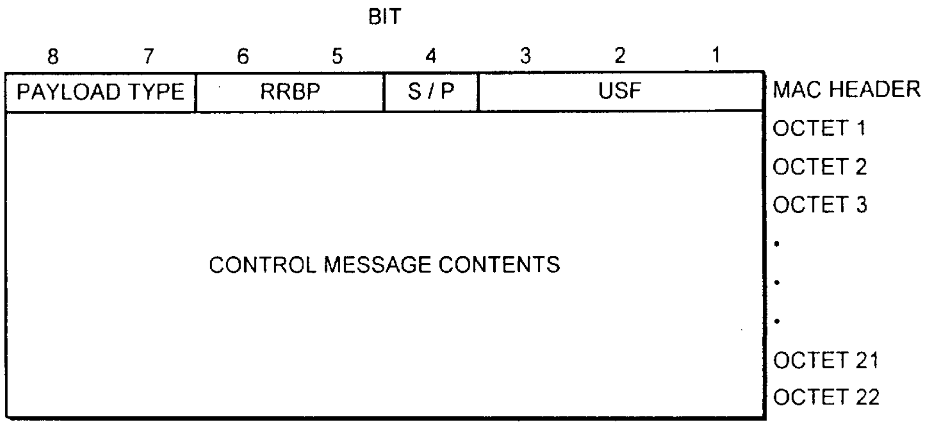

BIT
8
7
6
5
4
3
2
1
PAYLOAD TYPE
RRBP
S / P
USF
MAC HEADER
OCTET 1
OCTET 2
OCTET 3
CONTROL MESSAGE CONTENTS
OCTET 21
OCTET 22

FIG. 3

MEASUREMENT REPORT TRANSMISSION IN A TELECOMMUNICATIONS SYSTEM

BACKGROUND OF THE INVENTION

The present invention relates to information transfer between a mobile station and a radio communication network, and more particularly to a method designed to be employed in a radio communication network to obtain information from a mobile station about conditions at the mobile station during downlink transfer.

In normal wireless voice communications the telecommunication system sets up a two way communication link between a mobile station and a base station of the cellular network in which the mobile station is operating. By mobile station is meant any kind of radio communication device which operates in a cellular telecommunication system. The data stream for the voice communication is continuous and operates on a real time basis. The two way communication link consists of simultaneous transmission and reception, the base station transmits on one set of radio channels called the uplink and receives on another set of channels called the downlink. The transmit and receive channels assigned for a particular cell are separated by a fixed amount of frequency called the duplex spacing.

In addition to voice communications, digital cellular telecommunication systems increasingly support advanced high speed data services such, as short message service (SMS), broadcast paging, imaging services and fax services.

Both data and voice transmissions are improved by the emerging use of GPRS (General Packet Radio Services) protocol. GPRS provides for high speed packet radio access for GSM mobile station and routing protocols for the GSM network by the dynamic allocation of communication channels for voice and data transmissions. GPRS is defined in GSM 03.64 standard specification.

A feature of certain data services is that unlike voice transmissions, data services can be transferred unidirectionally and on a non-real time basis. For example, because paging messages can be delayed for several minutes without significant disadvantages to the receiver of the message, it allows short paging messages to be placed in a queuing system. Furthermore, the transfer of the paging message takes place in a unidirectional link from the network to the mobile station of the receiver, i.e. exclusively in a downlink transfer. When the network is transferring data in a unidirectional downlink transmission, the network must nevertheless obtain certain information from the mobile station in order to keep a check of its operation and be updated of its position in the cellular network.

One requirement is for the network to obtain information from the mobile stations on whether the downlink data which it is transmitting to the mobile station has been received. In the context of GSM, GPRS this is defined in GSM 04.60. Briefly, the approach in GPRS is to make use of a header portion of the data stream—the RLC/MAC (Radio Link Control/Medium Access Control) layer—which defines certain control criteria of the communication link.

The Medium Access Control (MAC) procedures include the functions related to the management of the common transmission resources, eg. the packet resource requests and packet resource configuration changes. The MAC procedures support the provision of Temporary Block Flows (TBFs) that allow the point-to-point transfer of signalling and user data within a cell between the network and the mobile station. Additionally, the MAC functions provide for measurement reporting for cell selection and re-selection.

The RLC function is responsible for: interface primitives allowing the transfer of Logical Link Control (LLC) layer PDU's between the LLC layer and the MAC function; segmentation of LLC PDU's in the RLC data blocks in reassembly of RLC data blocks into LLC/PDU, and Backward Error Correction (BER) procedures enabling the selective retransmission of RLC data blocks.

In ETSI standards MAC function is combined with RLC as one layer. RLC/MAC control blocks are used to transport RLC control messages, and only one RLC/MAC control message can be transported per RLC control block. The RLC/MAC layer comprises a series of block periods each of which is a sequence of four time slots on a packet data physical channel (PDCH) used to convey one radio block carrying one RLC/MAC protocol data unit.

Whenever the mobile station receives a RLC data block addressed to itself and with a valid RRBP (Relative Reserved Block Period) field in the RLC data block header (i.e. is polled) the mobile station transmits a packet downlink acknowledgement (ACK/NACK) message in the uplink radio block specified by the RRBP field. The acknowledgement message relates to the received downlink blocks and the quality measurement results calculated from the received blocks together with interference measurement results, and are transmitted in the uplink block based on the information in the downlink blocks (according to a certain number of bits in the downlink MAC header).

That is unless another RLC/MAC control message relating to some other information about the mobile station is waiting to be transmitted, in which case the other RLC/MAC control message is sent. However, the mobile station can only transmit an RLC/MAC control message relating to information other than packet downlink ACK/NACK at most every fourth time it is polled.

For the network to be aware of the position of the mobile station and the available options for handover the network directs a mobile station to send in measurement reports including neighbour cell information. In this context the behaviour of the mobile station is controlled by the parameter NETWORK_CONTROL_ORDER which may have the following values: NC0: 'Normal MS Control'; the mobile station does not send measurements reports and makes autonomous cell reselection, NC1: 'Mobile Station control, with the measurement report'; the mobile station sends measurement reports but makes autonomous cell reselection, NC2: 'Network Control'; the mobile station sends a measurements reports, suspend normal cell re-selection and accept network control of cell re-selection.

Accordingly, the mobile station may be directed by the network to perform neighbour cell power measurements in predefined gaps. The network indicates the location of these gaps in the packet downlink assignment message and the location and time and the size of the gaps are signalled by the following parameters: the starting time of the first TDMA frame of the first gap; a bit map indicating the time slots that are part of the gap; and the number of RLC/MAC Block periods between gaps. Once the network has signalled the gap parameters to the mobile station the network does not send an RLC/MAC block addressed to the mobile station in the time slot immediately before an assigned measurement gap, during any of the time slots of a gap or during the time slot immediately after a gap.

Neighbour cell information results are sent to the network on uplink blocks normally allocated for downlink data acknowledgement transmission. As already mentioned only a certain number of allocated uplink blocks can be used for messages other than acknowledgements and quality measurements results. In order to be able to transmit the neighbour cell measurement results as well as the required amount of acknowledgement messages, the network must send polling messages more often.

The shortest measurement period for neighbour cell re-selection measurements is 104 TDMA-frames as the maximum acknowledgement time is 64 blocks. If only one downlink time slot is allocated, the transmission of the 64 blocks last approximately 256+20 TDMA-frames (idle-frames included). Together with the fact that only every fourth of the uplink blocks allocated for the downlink ACK/NACK messages is allowed to be used for some other purposes, the neighbour message transmission with the current solution in the most stringent case will need the transmission of three extra pollings for the downlink ACK/NACK messages within every measurement period, to make it possible to send the measurement report.

Against this background the present invention aims to improve the efficiency of the use of uplink resources.

SUMMARY OF THE INVENTION

Accordingly the present invention provided a method for a radio communication network to obtain data messages from a mobile station operating therein during a unidirectional downlink transfer, the data messages being indicative of conditions at the mobile station, the method comprising the network providing a header portion of the downlink transfer having one or more unique polling codes for requesting the mobile station to transmit one or more respective data messages indicative of one or more corresponding conditions at the mobile station.

In a complementary aspect, the invention provides a radio communication system comprising a cellular network in downlink radio communication transfer with a mobile station operating therein, wherein the network provides a header portion of the transfer having one or more unique polling codes for requesting the mobile station to transmit one or more respective data messages indicative of one or more corresponding conditions at the mobile station.

By means of the invention, one or more dedicated polling messages can be transmitted for different purposes thereby separating the different cases. Thus, superfluous polling can be avoided because the messages are separated.

In a preferred embodiment, the header portion comprises the downlink RLC/MAC message header.

A BRIEF DESCRIPTION OF THE DRAWINGS

To further aid understanding of the present invention, a preferred embodiment thereof will now be described with reference to the accompanying drawings in which:

FIG. **1** is schematic diagram of a RLC/MAC block structure;

FIG. **2** is schematic diagram of a downlink RLC data block; and

FIG. **3** is schematic diagram of a downlink RLC control block.

DETAILED DESCRIPTION OF THE INVENTION

Referring to the drawings, FIG. **1** shows a RLC/MAC block structure consisting of a MAC header and a RLC data block or RLC/MAC control block.

The format of the downlink RLC data block is shown in greater detail in FIG. **2**, and that of the RLC control block is shown in FIG. **3**.

The Supplementary/Polling (S/P) bit is used to indicate whether the RRBP field is valid or not valid as shown in Table 1

TABLE 1

Supplementary/Polling (S/P) bit	
bit	
1	S/P
0	RRBP field is not valid
1	RRBP field is valid

The interpretation of the Relative Reserved Block Period (RRBP) field depends on the value of the S/P field: the two cases are when the S/P field is valid and invalid.

When the S/P field is valid the RRBP value specifies a single uplink block in which the mobile station transmits either a PACKET CONTROL ACKNOWLEDGEMENT or a Packet Associated Control Channel (PACCH) block to the network. If the RRBP field is received as part of a RLC/MAC block containing an RLC/MAC control block, the mobile station transmits a PACKET CONTROL ACKNOWLEDGEMENT in the uplink radio block specified. If the RRBP field is received as part of a RLC/MAC block containing an RLC data block, the mobile station shall transmit a PACCH block in the specified uplink radio block.

The mobile station does not need to monitor the Uplink State Flag (USF: is used by the network to control multiplexing of different mobile stations on uplink Packet Data Channel (PDCH) measurement report) bits in the downlink RLC/MAC block before the uplink block is transmitted.

Table 2 indicates the number of TDMA frames the mobile station should wait before transmitting. The delay is relative to the first TDMA frame (N) of the downlink block containing the RRBP value.

TABLE 2

Relative Reserved Block Period (RRBP) field when S/P valid	
bits	
2 1	Relative Reserved Block Period (RRBP)
0 0	uplink block with TDMA frame number = N + 8 or N + 9
0 1	uplink block with TDMA frame number = N + 13
1 0	uplink block with TDMA frame number = N + 17 or N + 18
1 1	uplink block with TDMA frame number = N + 21 or N + 22

In the case where the S/P field is not valid the RRBP value specifies that the mobile station send a PACKET MEASUREMENT REPORT in single uplink block or is the value of RRBP field unused.

The mobile station need not monitor the USF bits in the downlink RLC/MAC block before the uplink block is transmitted.

Table 3 indicates the number of TDMA frames the mobile station must wait before transmitting. The delay is relative to the first TDMA frame (N) of the downlink block containing the RRBP value.

TABLE 3

Relative Reserved Block Period (RRBP) field when S/P not valid

bits	
2 1	Relative Reserved Block Period (RRBP)
0 1	uplink block with TDMA frame number = N + 13
1 0	uplink block with TDMA frame number = N +17 or N + 18
0 0	no measurement reports are sent
1 1	no measurement reports are sent

The network allocates uplink block for sending the measurement report by setting the RRBP and S/P bits in the downlink block MAC-header according to the values specified in Table 4.

TABLE 4

S/P	RRBP	Description
0	00	No polling
0	01	Polling for the measurement report, uplink block with TDMA-frame number = N + 13
0	10	Polling for the measurement report, uplink block with TDMA-frame number = N + 17 or N = 18
0	11	Extra polling for measurement report supported by network
1	Any value	Polling for downlink ACK/NACK, as stated in the ETSI GPRS specification 04.60

By modifying the downlink RLC/MAC header in this way, the pollings for the neighbor measurement and the packet acknowledgement messages are seperated, and the network can allocate uplink resources more efficiently because the extra packet downlink messages do not be need to be sent.

The present invention may be embodied in other specific forms without departing from its essential attributes. The embodiments that have been described concern feeding backing information at the network's request from the mobile station to the network; information such as an acknowledgement that certain transmitted data has been received, or information about the characteristics of surrounding cells. The invention is not limited to such applications and could be used to feed back other types of information, for example information about the radio link itself such as the transmission power for either or both of network base stations and mobile stations, and other situational and environmental information. Accordingly reference should be made to the appended claims and other general statements herein rather than to the foregoing specific description as indicating the scope of invention.

Furthermore, each feature disclosed in this specification (which term includes the claims) and/or shown in the drawings may be incorporated in the invention independently of other disclosed and/or illustrated features. In this regard, the invention includes any novel features or combination of features disclosed herein either explicitly or any generalisation thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed.

The appended abstract as filed herewith is included in the specification by reference.

What is claimed is:

1. A method for a radio communication network to obtain data messages from a mobile station operating therein during unidirectional downlink transfer, a first data message being indicative of downlink data acknowledgement/non-acknowledgement, and a second data message being indicative of measurement result conditions at the mobile station, the method comprising the steps of:

the network providing in a header portion of the downlink transfer a first polling code representative of a first polling state for requesting the mobile station to transmit said first data message,

and the method being characterised in that the network provides in a header portion of the downlink transfer a second polling code representative of a second polling state for requesting the mobile station to transmit said second data message, said second polling code being different from the first polling code such that the second polling state is different from the first polling state.

2. A method according to claim **1**, wherein the radio communication system comprises a GPRS system and the first and second polling codes are transmitted in a downlink RLC/MAC block.

3. A method according to claim **2**, wherein the first and second polling codes comprise S/P bits in a header of the RLC/MAC block, and said first polling state is representative of a valid S/P state and said second polling state is representative of an invalid S/P state, so that when the S/P bits provide an invalid state the mobile station is requested to transmit said second data message.

4. A method according to claim **1**, wherein said second polling code that is representative of said second polling state requests the mobile station to transmit said second data message, wherein said second data message is provided for determining transfer conditions.

5. A method according to claim **4**, wherein said transfer conditions comprise neighbour cell measurement report.

6. A method according to claim **1**, wherein said second polling code that is representative of said second polling state requests the mobile station to transmit said second data message, wherein said second data message is provided for determining data flow between the mobile station and the network.

7. A method according to claim **1**, wherein said second polling code is provided for requesting the mobile station to provide transmission power level information.

8. A radio communication system comprising a cellular network in downlink radio communication transfer with a mobile station operating therein, the system providing for the network to obtain first and second data messages from the mobile station, wherein the network provides in a header portion of the transfer a first polling code representative of a first polling state for requesting the mobile station to transmit a first data message indicative of downlink data acknowledgement/non-acknowledgement, the system being characterised in that the network provides in a header portion of the downlink transfer a second polling code representative of a second polling state for requesting the mobile station to transmit a second data message indicative of measurement result conditions at the mobile station, said second polling code being different from the first polling code such that the second polling state is different from the first polling state.

9. A control system for a radio communication network, the network being capable of downlink radio communication transfer with a mobile station, the control system comprising means for configuring a header portion of the downlink transfer, said means for configuring the header portion comprising:

means for generating a first polling code representative of a first polling state for requesting the mobile station to transmit a first data message indicative of downlink data acknowledgement/non-acknowledgement, the system being characterised in that said means for configuring the header portion comprises means for generating a second polling code representative of a second polling state for requesting the mobile station to transmit a second data message indicative of measurement result conditions at the mobile station, said second polling code being different from the first polling code such that the second polling state is different from the first polling state.

10. A radio communication system network element comprising a control system, the network element being capable of downlink radio communication transfer with a mobile station, the network element comprising means configuring a header portion of the downlink transfer, said means for configuring the header portion comprising:

means for generating a first polling code representative of a first polling state for requesting the mobile station to transmit a first data message indicative of downlink data acknowledgement/non-acknowledgement, the network element being characterised in that said means for configuring the header portion comprises means for generating a second polling code representative of second polling state for requesting the mobile station to transmit a second data message indicative of measurement result conditions at the mobile station, said second polling code being different from the first polling code such that the second polling state is different from the first polling state.

11. A mobile station for use in a radio communication system, the mobile station being capable of downlink radio communication transfer with the radio communication system, the mobile station having a controller and the controller being adapted to be responsive to a first polling code representative of a first polling state provided in a header portion of the downlink transfer so as to transmit a first data message indicative of downlink data acknowledgement/non-acknowledgement, characterised in that the controller is adapted to be responsive to a second polling coded representative of a second polling state provided in a header portion of the downlink transfer so as to transmit a second data message indicative of measurement result conditions at the mobile station, said second polling code being different from the first polling code such that the second polling state is different from the first polling state.

12. A method for a radio communication network to obtain data messages from a mobile station operating therein during unidirectional downlink transfer, a first data message being indicative of downlink data acknowledgement/non-acknowledgement, and a second data message being indicative of measurement result conditions at the mobile station at least including data indicative of measurement report, the method comprising the network providing in a header portion of the downlink transfer a first polling code for said data acknowledgement/non-acknowledgement, and the method being characterised in that the network provides in a header portion of the downlink transfer a second polling code for requesting the mobile station to transmit said measurement report, said second polling code being different from, the first polling code, and wherein the first and second polling codes are transmitted in a header of a downlink RLC/MAC block.

13. A method according to claim **12**, wherein the measurement report comprises channel quality report.

14. A method according to claim **12**, wherein the second data message includes data relating to the first data message.

15. A method for a radio communication network to obtain data messages from a mobile station operating therein during unidirectional downlink transfer, the method comprising:

the network providing in a header portion of the downlink transfer a first polling code for obtaining from the mobile station a data message indicative of downlink data acknowledgement/non-acknowledgement; and

the network providing in a header portion of the downlink transfer a second polling code for obtaining from the mobile station a data message indicative of said downlink data acknowledgement/non-acknowledgement and indicative of one or more other conditions at the mobile station at least including data indicative of measurement report, said second polling code being different from the first polling code, and wherein the first and second polling codes are transmitted in a header of a downlink RLC/MAC block.

16. A method according to claim **15**, wherein the second data message includes data relating to the first data message.

17. A method for a radio communication network to obtain data messages from a mobile station operating therein during unidirectional downlink transfer, the method comprising:

the network providing, in a header portion of the downlink transfer, a first polling code for obtaining from the mobile station a data message indicative of downlink data acknowledgement/non-acknowledgement and

the network providing, in a header portion of the downlink transfer, a second polling code for obtaining from the mobile station a data message indicative of said downlink data acknowledgement/non-acknowledgement and indicative of one or more other conditions at the mobile station at least including data indicative of measurement report, said second polling code being different from the first polling code, and wherein the first and second polling codes are transmitted in a header of a downlink RLG/MAC block.

* * * * *

EXHIBIT D

US006775548B1

(12) United States Patent
Rong et al.

(10) Patent No.: US 6,775,548 B1
(45) Date of Patent: Aug. 10, 2004

(54) ACCESS CHANNEL FOR REDUCED ACCESS DELAY IN A TELECOMMUNICATIONS SYSTEM

(75) Inventors: **Zhigang Rong**, Fort Worth, TX (US); **Steven D. Gray**, Carrollton, TX (US)

(73) Assignee: **Nokia Mobile Phones Ltd.**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/102,222**

(22) Filed: **Jun. 22, 1998**

(51) **Int. Cl.**^{7} **H04Q 7/20**
(52) **U.S. Cl.** **455/452**; 370/468; 455/67.1
(58) **Field of Search** 455/455, 452, 455/422, 67.1, 67.4, 68, 70, 73, 522, 69, 63; 375/216, 225; 370/465–468, 252, 253

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,592,049	A	*	5/1986	Killat et al.	370/87
4,815,073	A	*	3/1989	Grauel et al.	370/95
4,910,794	A	*	3/1990	Mahany	455/67
5,404,355	A		4/1995	Raith	370/95.1
5,425,101	A	*	6/1995	Woo et al.	380/23
5,483,676	A		1/1996	Mahany et al.	455/67.4
5,533,004	A	*	7/1996	Jasper et al.	370/11
5,563,895	A		10/1996	Malkamaki et al.	371/32
5,612,950	A		3/1997	Young	370/276
5,703,902	A	*	12/1997	Ziv et al.	375/200
5,706,428	A	*	1/1998	Boer et al.	395/200
5,740,166	A	*	4/1998	Ekemart et al.	370/331
5,822,318	A	*	10/1998	Tiedemann, Jr. et al.	370/391
5,857,147	A	*	1/1999	Gardner et al.	455/67.1
5,872,775	A	*	2/1999	Saints et al.	370/342
5,923,648	A	*	7/1999	Dutta	370/280
5,963,548	A	*	10/1999	Virtanen	370/335
5,974,032	A	*	10/1999	Snowden et al.	370/316
5,978,414	A	*	11/1999	Nara	375/225
6,005,855	A	*	12/1999	Zehavi et al.	375/200
6,128,322	A		10/2000	Rasanen et al.	370/536
6,219,343	B1		4/2001	Honkasalo et al.	370/355
2001/0012271	A1		8/2001	Berger	370/230

* cited by examiner

Primary Examiner—Edward F. Urban
Assistant Examiner—C. Chow
(74) *Attorney, Agent, or Firm*—Brian T. Rivers

(57) **ABSTRACT**

A method and apparatus for accessing a telecommunications system. A channel having a plurality of data rates and a plurality of frame sizes is utilized by a mobile station to gain access to the system. If channel conditions allow, a faster data rate of the available data rates and a smaller frame size of the available frame sizes may be used to request access over the channel. By dynamically determining the data rate based on channel conditions, overall access delays for mobile stations using packet data services and making many access attempts may be reduced.

30 Claims, 4 Drawing Sheets

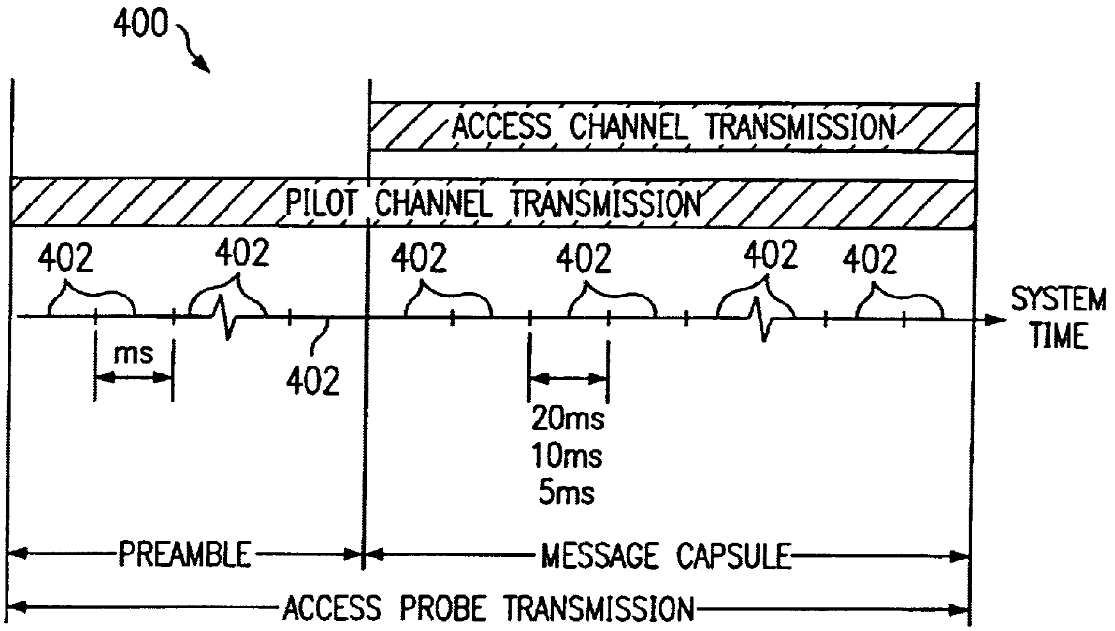
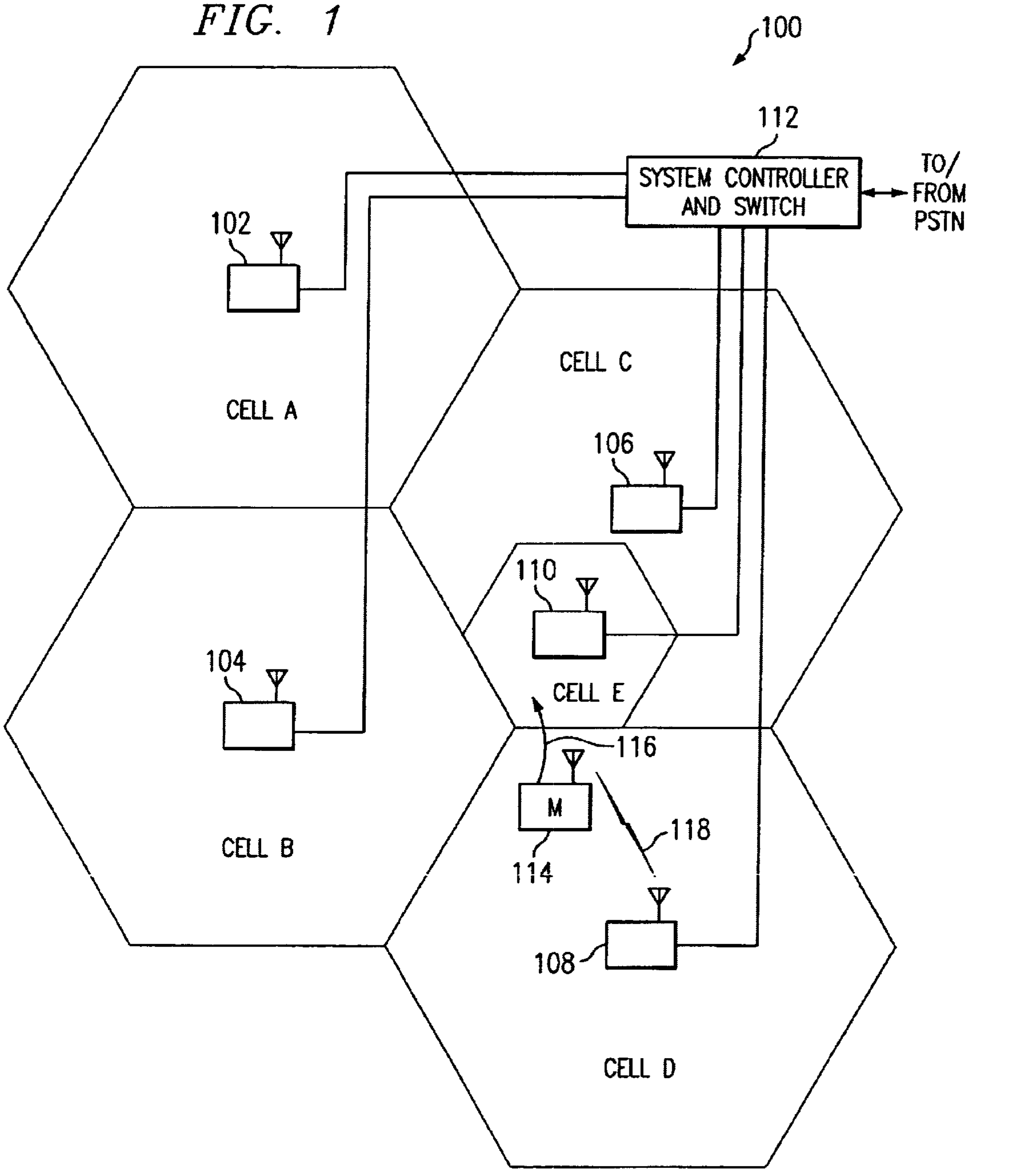

400
ACCESS CHANNEL TRANSMISSION
PILOT CHANNEL TRANSMISSION
402
402
402
402
402
402
SYSTEM TIME
ms
402
20ms
10ms
5ms
PREAMBLE
MESSAGE CAPSULE
ACCESS PROBE TRANSMISSION

FIG. 1


100
112
SYSTEM CONTROLLER AND SWITCH
TO/ FROM PSTN
102
CELL A
CELL C
106
110
CELL E
104
CELL B
116
M
118
114
108
CELL D

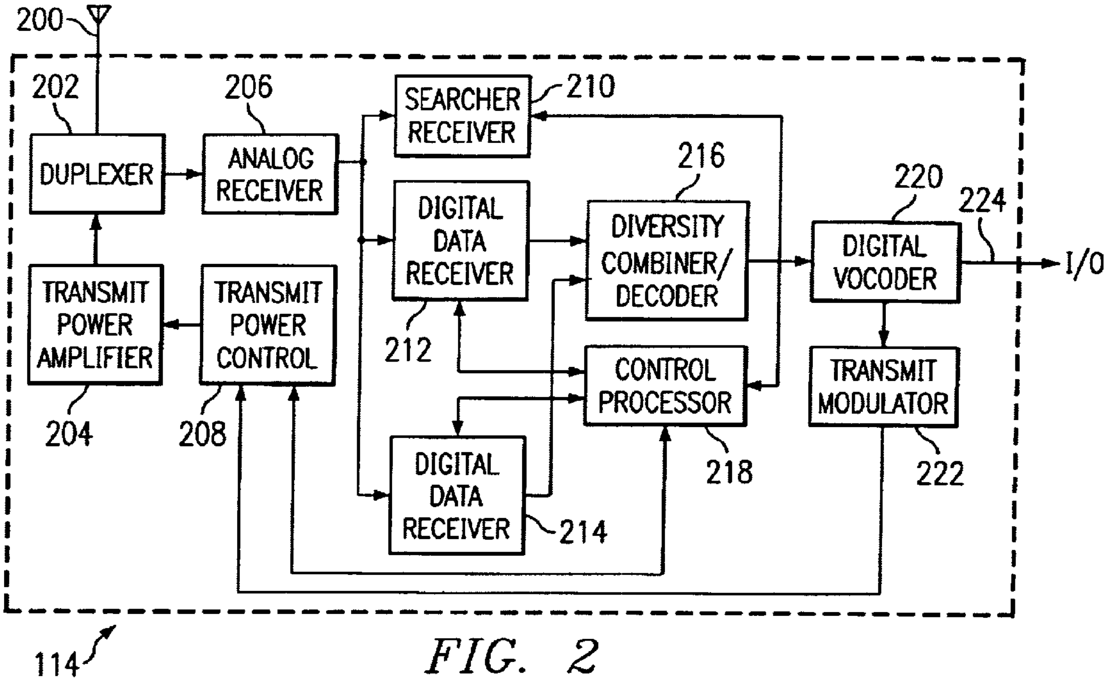

200
202
206
DUPLEXER
ANALOG RECEIVER
SEARCHER RECEIVER
210
DIGITAL DATA RECEIVER
216
DIVERSITY COMBINER/ DECODER
220
224
DIGITAL VOCODER
I/O
TRANSMIT POWER AMPLIFIER
TRANSMIT POWER CONTROL
212
CONTROL PROCESSOR
TRANSMIT MODULATOR
204
208
DIGITAL DATA RECEIVER
218
222
214
114

FIG. 2

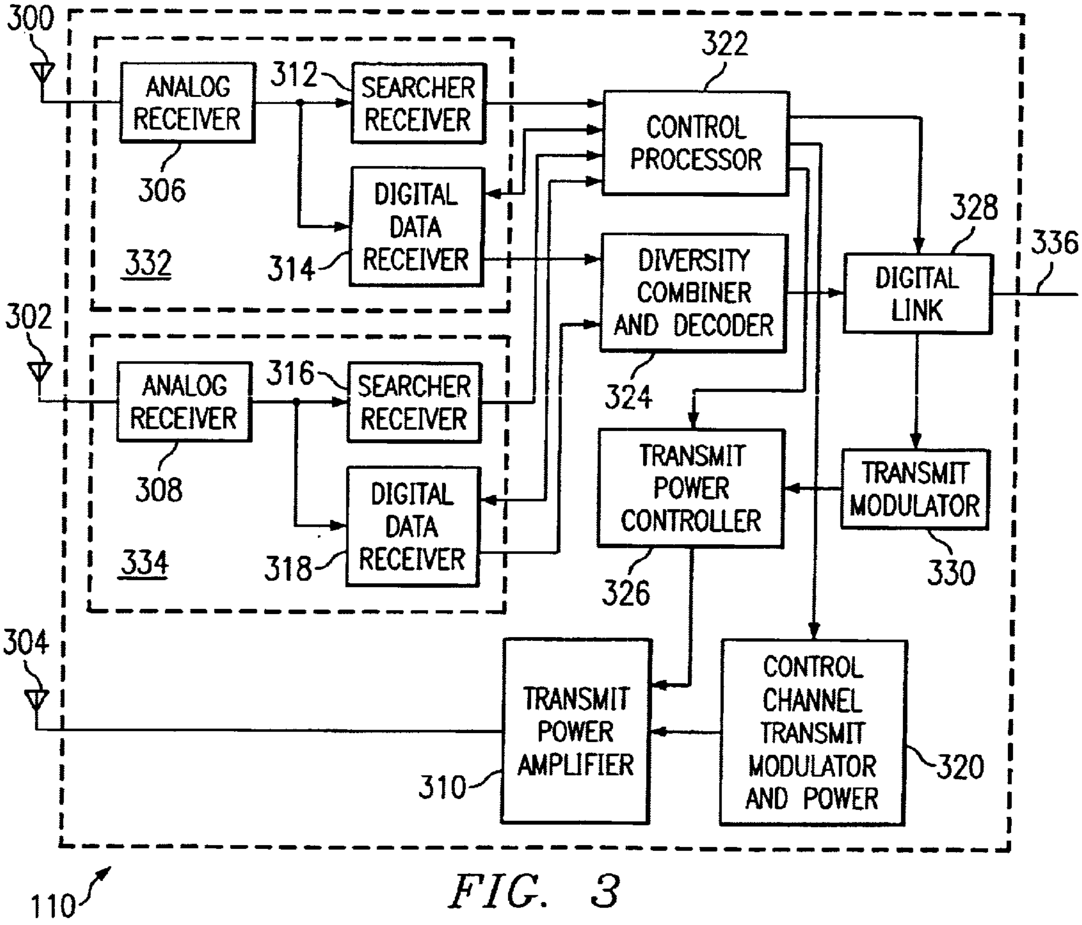

300
322
ANALOG RECEIVER
312
SEARCHER RECEIVER
CONTROL PROCESSOR
306
DIGITAL DATA RECEIVER
328
336
332
314
DIVERSITY COMBINER AND DECODER
DIGITAL LINK
302
324
ANALOG RECEIVER
316
SEARCHER RECEIVER
TRANSMIT POWER CONTROLLER
TRANSMIT MODULATOR
308
DIGITAL DATA RECEIVER
334
318
330
326
304
TRANSMIT POWER AMPLIFIER
CONTROL CHANNEL TRANSMIT MODULATOR AND POWER
310
320
110

FIG. 3

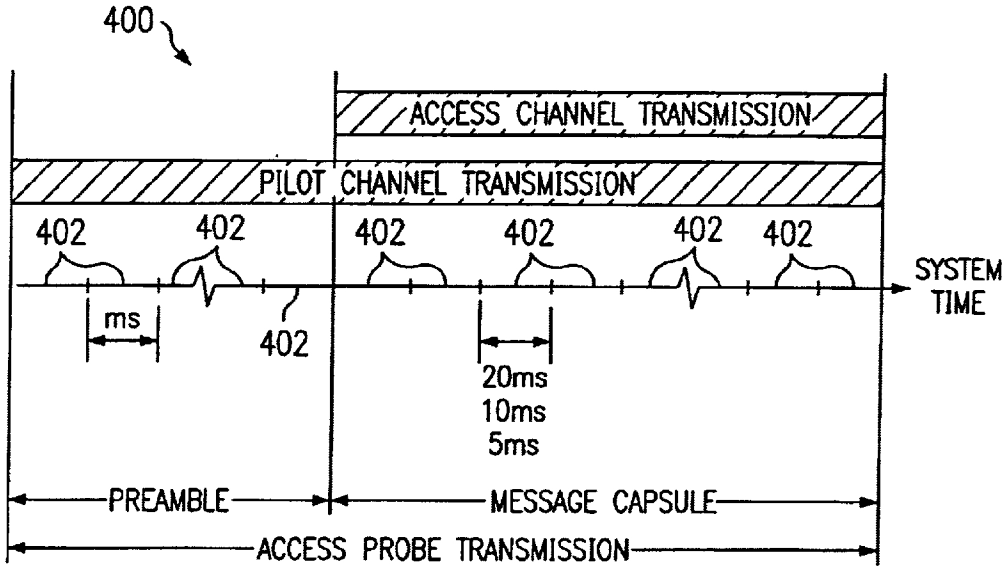

400
ACCESS CHANNEL TRANSMISSION
PILOT CHANNEL TRANSMISSION
402
402
402
402
402
402
402
ms
SYSTEM TIME
20ms
10ms
5ms
PREAMBLE
MESSAGE CAPSULE
ACCESS PROBE TRANSMISSION

FIG. 4A

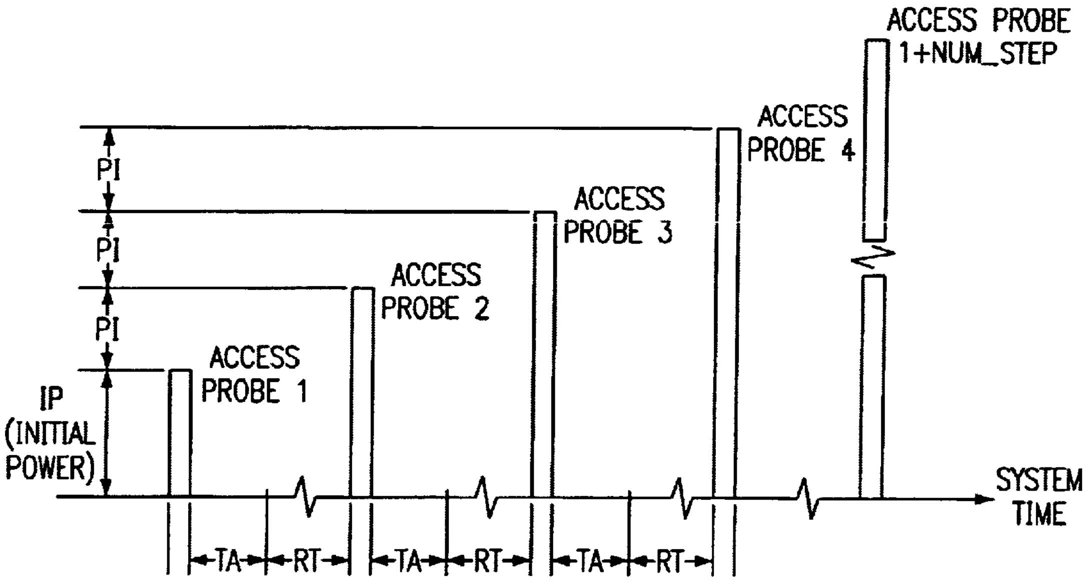
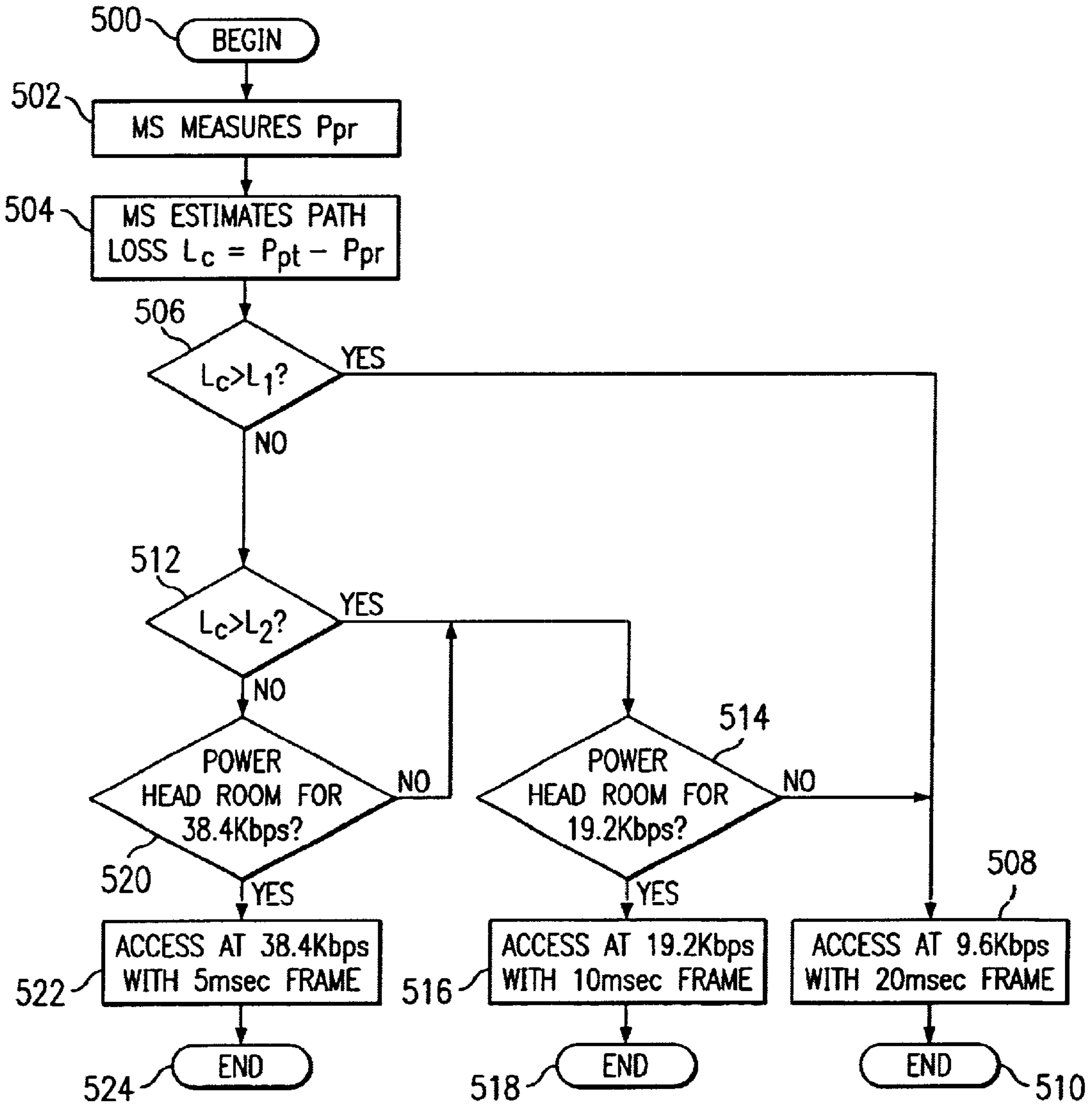

ACCESS PROBE 1+NUM_STEP
ACCESS PROBE 4
ACCESS PROBE 3
ACCESS PROBE 2
ACCESS PROBE 1
PI
PI
PI
IP (INITIAL POWER)
SYSTEM TIME
TA
RT
TA
RT
TA
RT

FIG. 4B

FIG. 5


500
BEGIN
502
MS MEASURES Ppr
504
MS ESTIMATES PATH LOSS $L_c = P_{pt} - P_{pr}$
506
$L_c > L_1$?
YES
NO
512
$L_c > L_2$?
YES
NO
POWER HEAD ROOM FOR 38.4Kbps?
NO
520
YES
514
POWER HEAD ROOM FOR 19.2Kbps?
NO
YES
508
522
ACCESS AT 38.4Kbps WITH 5msec FRAME
516
ACCESS AT 19.2Kbps WITH 10msec FRAME
ACCESS AT 9.6Kbps WITH 20msec FRAME
524
END
518
END
END
510

ACCESS CHANNEL FOR REDUCED ACCESS DELAY IN A TELECOMMUNICATIONS SYSTEM

FIELD OF THE INVENTION

This invention relates to telecommunications systems and, more particularly, to a method and apparatus for accessing a system utilizing an access channel providing reduced access delay in a telecommunications system.

BACKGROUND OF THE INVENTION

Major cellular telecommunications systems types include those operating according to the Global Services for Mobile (GSM) Standard, the TIA/EIA/IS-95 Mobile Station-Base Station Compatibility Standard for Dual Mode Wide Band Spread Spectrum Cellular Systems (IS-95A, currently being updated as IS-95B in the document TIA/EIA SP-3693), the TIA/EINIS-136 Mobile Station-Base Station Compatibility Standard (IS-136), and the TIA/EIA 553 Analog Standard (AMPS/TACS). Other major cellular systems include those operating in the personal communications system (PCS) band according to the IS-95 based ANSI-J-STD-008 1.8–2.0 GHz standard or those operating according to the GSM-based PCS 1900/1910 MHz frequency range standard. Currently, each of the major cellular system standards bodies is implementing packet data services into its digital cellular specifications. A packet data specification has been finalized for GSM and IS-95A. Packet data specifications compatible with the IS-136 and IS-95B standards are also being prepared.

In a typical cellular system a call establishment begins either by a base station transmitting a paging message to a mobile station on a paging channel and then the mobile station transmitting a paging response message to the base station on an access channel, or by a mobile station accessing the system on an access channel by transmitting an origination message to a base station. In either of these call establishment cases, the mobile station must access the system on an access channel, and information unique to the particular call establishment must be exchanged between the mobile station and base station over the access channel or other channels of the system air interface. The paging response message and origination message typically carry a large portion of the information. The information unique to the particular call establishment could include called number data, mobile station identification and capability related data, authentication information, etc. After receiving this information, the system must then use the information to set up the different layers of communication necessary in the system to implement the call.

In packet data applications, a mobile station establishes a connection with the base station when it has one or more data packets in the buffer of the mobile station to send or when it is paged by a base station having data packets to send. The mobile station accesses the system for a channel connection and transmits until it is determined that no data exists in the buffer for transmission. Since data may be received from a data server at the mobile or base station intermittently, it may be necessary to release the channel connection in order to maximize the use of the channel by other mobile stations. This means that the mobile station will be making multiple access attempts to establish a channel connection, each access attempt being made when the mobile or base station has enough data to transmit. Each access attempt may in itself involve more than one access

attempt if initial access attempts are unsuccessful. In the current packet data system for GSM, IS-95A, IS-95B and IS-136, the access channel has a fixed frame size and data rate. For example, the IS-95B packet data access channel is the same channel used to originate regular calls. The IS-95B access channel has a frame size of 20 msec and a data rate of 4.8 kbps.

As third generation systems which will replace GSM, IS-136 and IS-95B are developed and packet data usage becomes more common, solutions must be found to handle packet data service delays that may be caused by the delays incurred when requesting access to the system each time packet data is to be sent. If many packet data users are in the system competing for channels, there will be a need to release access channels as often as possible and a need to perform new accesses following release of the accessed channel if new data is accumulated for transmission. An improved access procedure will be required for packet data services in these systems.

OBJECTS OF THE INVENTION

It is, therefore, an object of this invention to provide an improved method and apparatus for accessing a telecommunications system that overcomes the foregoing and other problems.

Another object of this invention is to provide a method and apparatus for accessing a telecommunications system using a channel providing reduced access delay.

Another object of this invention is to provide a method and apparatus for accessing a telecommunications system using a channel having variable data rates and frame sizes for access.

A further object of this invention is to provide a method and apparatus for accessing a telecommunications system using a channel having variable data rates and frame sizes assignable to a mobile station based on channel conditions and service type required.

SUMMARY OF THE INVENTION

The present invention provides an improved method and apparatus for accessing a telecommunications system. The method and apparatus utilizes a channel having variable data rates and frame sizes. In the method and apparatus, access to the system may be requested via at least one channel having variable data rates. Each of the available data rates is associated with at least one transmission frame size of a plurality of frame sizes. If channel conditions allow, a higher data rate of the available data rates may be used to request access over the channel. The method and apparatus has an advantage for use in packet data services. By dynamically determining the data rate based on channel conditions, overall access delays for mobile stations using packet data services and making many access attempts may be reduced.

In an embodiment of the invention, a plurality of access channel data rates and frame durations are available for use by a mobile station requesting access. The data rates and frame durations may be set so that the number of data bits per frame is constant for ease of processing. A mobile station accessing the system selects a data rate and associated frame duration based on channel conditions, mobile station power conditions or the type of service required. Packet data service users requiring shorter access delay may select a higher data rate and associated frame duration for a particular type of service under certain channel conditions, subject to transmission power requirements. Since a higher data rate requires a higher transmitted power to achieve a comparable Eb/No as at a lower data rate, transmission power of the mobile station at the higher rate must be increased compared to that at the lower rate without exceeding the maximum allowable transmitted power for the mobile station so the frame error rate (FER) and bit error rate (BER) remain within acceptable limits.

Transmission power requirements may be determined on the basis of a desired Eb/No to be received at the base station antenna for access attempts by the mobile station. The mobile station determines whether an estimated path loss is less than a maximum allowable path loss for a desired data rate for access. If the estimated path loss is less than the maximum allowable path loss at the desired data rate for access and the mobile station transmission power necessary to achieve the desired Eb/No does not exceed the maximum allowed power the mobile station is limited to for acceptable system performance, the desired data rate is selected. If the estimated path loss is greater than the maximum allowable path loss for the desired data rate for access or the necessary mobile station transmission power exceeds the allowable maximum for the mobile station, a lower data rate having a maximum allowable path loss greater than the estimated path loss and/or greater than the maximum allowed power for the mobile station is selected.

BRIEF DESCRIPTION OF THE DRAWINGS

The above set forth and other features of the invention are made more apparent in the ensuing Detailed Description of the Invention when read in conjunction with the accompanying drawings wherein:

FIG. **1** illustrates a block diagram of a telecommunications system constructed according to an embodiment of the present invention;

FIG. **2** is a block diagram of portions of a mobile station of the embodiment of the invention shown in FIG. **1**;

FIG. **3** is a block diagram of portions of a base station of the embodiment of the invention shown in FIG. **1**;

FIGS. **4**A and **4**B are illustrations of an access probe transmission and access probe sequence, respectively, according to an embodiment of the invention; and

FIG. **5** is a flow diagram illustrating process steps performed when accessing a system according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1** illustrates a block diagram of a telecommunications system **100** constructed according to an embodiment of the present invention. System **100** comprises mobile station **114**, and an infrastructure comprising system controller and switch **112** and base stations **102**, **104**, **106**, **108** and **110**. A subscriber who subscribes to service provided by the operator of cellular system **100** may use mobile station **114** to make and receive phone calls over a radio interface, such as shown by radio interface **118** between mobile station **114** and base station **108**, as the subscriber moves throughout the coverage area of cellular system **100**. The subscriber also may use mobile station **114** to make and receive packet switched data calls over the radio interface **118**. During a packet data call, mobile station **114** may function as a data terminal for transmitting or receiving data. As such, mobile station **114** may be connected to a portable computer or fax machine. Each of base stations **102**, **104**, **106**, **108** and **110** provides coverage over a separate area of system **100**, shown as cell A, cell B, cell C, cell D and cell E, respectively, in FIG. **1**. Base stations **102**, **104**, **106**, **108** and **110** are connected to system controller and switch **112** by connections as in a conventional cellular system. System controller and switch **112** may be connected to a public switched telephone network to allow subscribers of cellular system **100** to make and receive phone calls from the landline public network. In the embodiment of FIG. **1**, cell A, cell B, cell C and cell D are shown to be of about the same size and may be the size of what is commonly called a “microcell” or a cell of about 500 meters in width. A micro cell of system **100** may require a maximum mobile station transmission power level of approximately 200 mw. Cell E of system **100** is shown to be contained within the coverage area of cell C and may be the size of what is commonly called a “picocell” or a cell of about 100 meters in width. A picocell of system **100** may require a maximum mobile station transmission power level of approximately 20 mw. The embodiment of the invention has particular application to packet data users operating in a microcell or picocell environment. In this type of environment, signal path loss between the mobile station **114** and base stations **102**–**108** may be small, allowing necessary transmission power increases by mobile station **114** required for faster data rate and small frame access attempts. However, the embodiment has application to cellular systems having all sizes of cells. In the embodiment of FIG. **1**, cellular system **100** may operate according to the Code Division Multiple Access (CDMA) cellular system standard specified in the document, “The CDMA 2000 ITU-R RTT Candidate Submission,” published by the Telecommunications Industry Association, TR45.5 Subcommittee, Apr. 2, 1998 (CDMA 2000). The method and apparatus of the invention has application to all types of telecommunications systems that use similar access principles, such as, for example, time division multiple access (TDMA) systems.

Referring now to FIG. **2**, therein is a block diagram of portions of mobile station **114** of the embodiment of the invention shown in FIG. **1**. Mobile station **114** comprises antenna **200**, duplexer **202**, transmit power amplifier **204**, analog receiver **206**, transmit power controller **208**, searcher receiver **210**, digital data receiver **212**, digital data receiver **214**, diversity combiner/decoder **216**, control processor **218**, user digital vocoder **220**, transmit modulator **222** and user interface **224**.

Antenna **200** is coupled to analog receiver **206** through duplexer **202**. Signals received at antenna **200** are input to analog receiver **206** through duplexer **202**. The received signals are then converted to an IF frequency and then filtered and digitized in analog receiver **206** for input to digital data receiver **212**, digital data receiver **214** and searcher receiver **210**. The digitized IF signal input to digital data receiver **212**, digital data receiver **214** and searcher receiver **210** may include signals from many ongoing calls, together with the pilot carriers transmitted by the base station of the cell site in which the mobile station is currently located, plus the pilot carriers transmitted by the base stations in all neighboring cell sites. Digital data receiver **212** and digital data receiver **214** perform correlation on the IF signal with a pseudo random noise (PN) sequence of a desired received signal. The output of digital data receivers **212** and **214** is a sequence of encoded data signals from two independent paths. Searcher receiver **210** scans the time domain around the nominal time of a received pilot signal of a base station for other multi-path pilot signals from the same base station and for other signals transmitted from different base stations. Searcher receiver **210** measures the strength of any desired waveform at times other than the nominal time. Searcher receiver **210** generates signals to control processor **218** indicating the strengths of the measured signals to control processor **218**.

The encoded data signals output from digital data receiver **212** and digital data receiver **214** are input to diversity combiner/decoder **216**. In diversity combiner/decoder **216** the encoded data signals are aligned and combined, and the resultant data signal is then decoded using error correction and input to digital vocoder **220**. Digital vocoder **220** then outputs information signals to the user interface **224**. User interface may be a handset with a keypad or another type of user interface, such as a laptop computer monitor and keyboard.

For transmission of signals from mobile station **114**, a signal received at user interface **224** is input to user digital vocoder **220** in digital form as, for example, data or voice that has been converted to digital form at user interface **224**. In digital vocoder **220** the signal is encoded and output to transmit modulator **222**. Transmit modulator **222** Walsh encodes the signal and then modulates the Walsh encoded signal onto a PN carrier signal, with the PN carrier sequence being the PN carrier sequence of the CDMA channel to which the mobile station is assigned. The PN carrier information is transmitted to mobile station **114** from the system **100** and transferred to control processor **218** from digital data receivers **212** and **214** after being received from the system. Control processor **218** sends the PN carrier information to transmit modulator **222**. The PN modulated signal is then output from transmit modulator **222** to transmit power controller **208**. Transmit power controller **208** sets the level of the transmission power of mobile station **114** according to commands received from control processor **218**. In the embodiment of the invention, the transmission power is dependent on the data rate and frame size used for access. Control processor **218** also generates commands that set the transmission data rate and frame sizes used for access. The power control commands may be generated by control processor **218** according to commands received from the system or may be generated by software of control processor **218**, according to the embodiment of the invention, in response to data received from th e system through digital data receivers **212** and **214**.

The modulated signal is then output from transmit power controller **208** to transmit power amplifier **204** where the signal is amplified and converted to an IF frequency signal. The IF frequency signal is then output from power amplifier **204** to duplexer **20 2** and transmitted from antenna **200**.

Referring now to FIG. **3**, therein is a block diagram of portions of a base station **110** of the embodiment of the invention shown in FIG. **1**. The block diagrams of any of the other base stations **102**, **104**, **106**, and **108** of FIG. **1** may be equivalent to that shown in FIG. **3** for base station **110**. Base station **110** includes a first receiver section **332**, a second receiver section **334**, control processor **322**, diversity combiner/decoder **324**, transmit power controller **326**, digital link **328**, input/out I/O **336**, transmit modulator **330**, control channel transmitter/modulator **320**, transmit power amplifier **310**, and antenna **304**. First receiver section **332** comprises antenna **300**, analog receiver **306**, searcher receiver **312** and digital data receiver **314**. Second receiver section **334** comprises antenna **302**, analog receiver **308**, searcher receiver **316** and digital data receiver **318**.

First receiver section **332** and second receiver section **334** provide space diversity for a single signal that may be received at both antennas **300** and **302**. The signals received at antenna **300** are input to analog receiver **306** where the signal is filtered, converted to an IF frequency and digitized to generate a digital signal. The digital signal is then output from analog receiver **306** to searcher receiver **312** and digital data receiver **314**. Searcher receiver **312** scans the time domain around the received signal to verify that digital data receiver **314** tracks the correct signal. Control processor **322** generates the control signals for digital data receiver **314** according to a signal received from the searcher receiver **312**, so that the correct signal is received at digital data receiver **314**. Digital data receiver **314** generates the proper PN sequence necessary to decode the digital signal received from analog receiver **306** and generates weighted output symbols for input to diversity combiner/decoder **324**. Antenna **302**, analog receiver **308**, searcher receiver **316** and digital data receiver **318** of second receiver section **334** function identically to the components of first receiver section **332** to generate a second set of weighted output symbols. The weighted symbols from digital data receiver **314** and digital data receiver **318** are then combined and decoded in diversity combiner/decoder **324** to generate received digital data which is then output through digital link **328** and I/O **336** to system controller and switch **112** of FIG. **1**.

When data received from system controller and switch **112** is to be transmitted from base station **110** on a traffic channel, the data is received at digital link **328** over I/O **336** and sent to transmit modulator **330**. Transmit modulator **330** then modulates the data using the appropriate Walsh function assigned to the mobile station to which the base station is transmitting. The Walsh modulated data is then spread by a voice channel PN sequence having the appropriate time shift and input to transmit power controller **326**. Transmit power controller **326** controls the transmission power in response to control signals received from control processor **322**. The power control commands may be generated by software in control processor **322**. The signal output from power controller **326** is input to transmit power amplifier **310** and then transmitted from antenna **304**. Base station **100** may have multiple transmit modulator and transmit power controllers for transmitting to multiple mobile stations.

In system **100**, a pilot channel that may be used for handoff measurements is generated by each base station. The pilot channel generated for each base station of system **100** is unique, with each pilot identified by the time shift (or phase) of the PN sequence transmitted from the particular base station rather than by a unique PN sequence. The pilot channel for base station **110** may be generated in control channel transmitter/modulator **320** in response to control signals generated by control processor **322**. The pilot channel signal may be generated by using a Walsh code sequence of all zeros and multiplying the Walsh code sequence by the system PN sequence to generate a pilot channel signal having the appropriate phase for the base station **110**. System **100** also utilizes at least one reverse pilot channel and at least one access channel from mobile station **114** to base station **108**. Each access channel is associated with a reverse pilot channel that is generated by using a Walsh code sequence of all zeros. The reverse pilot channel and access channel are used to obtain access to the system.

Referring now to FIGS. **4**A and **4**B, therein are illustrated the access channel structure and an access probe sequence, respectively, of an embodiment of the invention. In FIG. **4**A the system time is shown as a series of consecutive access channel frames **402** on the system time access. The access probe transmission **400** comprises a preamble and a message capsule. The access probe transmission **400** has a duration of

M×X msec preamble frames transmitted on the reverse pilot channel plus N×L msec message capsule frames transmitted on the access channel, where L and X are variable lengths. The value of X, M and N may be system constants. In the embodiment, the N×L msec message capsule frames may be of duration 20 msec, 10 msec or 5 msec with data rates of 38.4 kbps, 19.2 kbps and 9.6 kbps, respectively. The data rates and frame sizes are set so that the number of data bits per frame is constant for ease of processing. It is not required that each data rate be fixed to a specific frame size. For example, in an alternative of the embodiment, each data rate may be used with multiple frame sizes of 20 msec, 10 msec or 5 msec. For normal voice of circuit switched operations, the message capsule frames are typically 20 msec in duration. For packet switched applications, the message capsule frame duration is variable.

Access probes are transmitted as shown in FIG. **4**B. An access probe sequence comprises up to 1+NUM_STEP access probes, where NUM_STEP is a system-defined parameter. The preamble is transmitted on a reverse pilot channel associated with the access channel. The reverse pilot channel space is continuously searched by the base station so mobile station access on the associated access channel can be acquired by the system. In the embodiment of the invention, searcher receivers **312** and **316**, and digital data receivers **314** and **318** are configured to search and receive access probes having multiple frame durations of 5 msec, 10 msec and 20 msec, with multiple data rates of 38.4 kbps, 14.2 kbps and 9.6 kbps. Control processor **322** generates the appropriate control signals to cause data and frame rate determination to be performed, so that an access probe is received correctly. The reverse pilot channel and channel used for access are spaced by the same long code. Each access probe begins with access probe **1** and continues up until access probe 1+NUM_STEP if no acknowledgment is received from the base station after a time-out period denoted by TA. Access probe **1** is transmitted at an initial power level, and each succeeding access probe is transmitted at a-power level incremented by PI. In the embodiment of the invention, the power levels used for access are dependent on the message capsule data rate used. The power levels for 9.6 kbps are as set for the CDMA 2000 system. The initial power level, IP, plus power increment, PI, for different access capsule data rates may be scaled such that for a rate of 19.2 kbps transmit power is 3dB above IP for 9.6 kbps, and for a rate of 38.4 kbps transmit power is 6dB above IP for 9.6 kbps. Access probes are separated by the period TA and a random probe backoff time (RT) that are system constants. If no response is received during an access probe sequence, the access probe sequence may be repeated. In an access attempt, the access probe may be repeated up to a number, MAX_SEQ, that is set by the system.

In the embodiment of the invention, when mobile station **114** is involved in a packet data call, mobile station **114** may utilize the variable data rate access probes of the invention to minimize the time needed to obtain access to the system. Mobile station **114** may transmit an access probe to base station **108** in response to a page received on a paging channel or autonomously when mobile station **114** has packet data to be sent.

Referring now to FIG. **5**, therein is a flow diagram illustrating process steps performed when accessing a system using variable rate and variable length frames according to an embodiment of the invention. The process begins at step **500**. The process may begin at initial access for a packet data call or sometime during the duration of an ongoing packet data call, when a physical channel needs to be re-accessed for continued packet data transmission. This may include mobile station **114** or base station **110** initiated accesses. At step **502**, searcher receiver **210** of mobile station **114** measures the received signal strength, P_{pr}, of the forward link pilot channel from base station **108**. Next, at step **504**, control processor **218** calculates an estimated path loss, L_c. $L_c=P_{pt}-P_{pr}$ where P_{pt} is the forward link pilot channel transmit power of base station **108**. P_{pt} may be fixed based upon the operating environment, cell type, etc., and the value of P_{pt} may be transmitted to mobile station **114** from base station **108** via message signaling. The forward link pilot channel measurements of step **502** and calculations of step **504** need not be done after access is required, as these forward link measurements and calculations may be continuously made and already available when mobile station **114** begins the process at step **500**.

At step **506**, a determination is made by control processor **218** as to whether or not the calculated path loss L_c is greater than a threshold path loss L_1, where L_1 is the maximum path loss a signal transmitted from mobile station **114** can incur when transmitting at 19.2 kbps at a reference transmission power. The reference transmission power may be the maximum possible transmit power for mobile station **114**. The threshold path loss L_1 may be a system value determined based on a desired Eb/No to give a desired frame error rate (FER) and bit error rate (BER) rate. Typically, the transmitted power required to achieve a desired Eb/No at base station **118** increases with an increased data rate. Based on a desired FER and BER, then the allowable path loss for transmitting at 9.6 kbps will be greater than the maximum allowable path loss when transmitting at 19.2 kbps at a selected transmission power.

If, at step **506**, a determination is made that L_c is greater than L_1, the process moves to step **508**. At step **508**, control processor **218** generates the appropriate control signals so that mobile station **114** transmits the access probes of FIGS. **4**A and **4**B using a message capsule with data transmitted at a rate of 9.6 kbps having a frame of 20 msec in length and initial power IP set for 9.6 kbps. The process then ends at step **510**. If, however, at step **506**, a determination is made that L_c is not greater than L_1, the process moves to step **512**.

At step **512**, a determination is made by control processor **218** as to whether or not the calculated path loss L_c is less than or equal to L_1 and greater than L_2, where L_2 is the maximum path loss a signal transmitted from mobile station **114** can suffer when transmitting at 38.4 kbps at the reference transmission power. The threshold path loss L_2 may be a value determined based on a desired FER and BER.

If, at step **512**, a determination is made that L_c is less than or equal to L_1 and greater than L_2, the process moves to step **514**. At step **514**, control processor **218** then determines if the transmit power head room for transmitting at 19.2 kbps exists by determining whether the necessary transmit power for 19.2 kbps to achieve the desired Eb/No with a loss of L_c is within the maximum allowable transmit power for mobile station **114**. If a determination is made that the transmit power head room for transmitting at 19.2 kbps exists, the process moves to step **516**. At step **516**, control processor **218** generates the appropriate control signals so that mobile station **114** transmits the access probes of FIGS. **4**A and **4**B using a message capsule with data transmitted at a rate of 19.2 kbps having a frame of 10 msec in length and initial power IP set for 19.2 kbps. The process then ends at step **518**. If, however, at step **514**, a determination is made that the transmit power head room for transmitting at 19.2 kbps does not exist, the process moves to step **508** and transmits the access probes of FIGS. **4**A and **4**B using a message capsule with data transmitted at a rate of 9.6 kbps having a frame of 20 msec in length and initial power IP set for 9.6 kbps. The process then ends at step **510**.

If, however, at step **512**, a determination is made that L_c is not greater than L_2, the process moves to step **520**. At step **520**, control processor **218** determines if the transmit power head room for transmitting at 38.4 kbps exists by determining whether the necessary transmit power for 38.4 kbps to achieve the desired Eb/No with a loss of L_c is within the maximum allowable transmit power for mobile station **114**. If the transmit power head room for transmitting at 38.4 kbps exists, the process moves to step **522**. At step **522**, control processor **218** generates appropriate control signals so that mobile station **114** transmits the access probes of FIGS. **4**A and **4**B using a message capsule with data transmitted at a rate of 38.4 kbps having a frame of 5 msec in length and initial power IP set for 38.4 kbps. The process then ends at step **524**. If, however, at step **520**, a determination is made that power head room for transmitting at 38.4 kbps does not exist, the process moves to step **514**. At step **514**, control processor **218** determines if the transmit power head room for transmitting at 19.2 kbps exists. If a determination is made that the transmit power head room for transmitting at 19.2 kbps exists, the process moves to step **516**. At step **516**, control processor **218** generates the appropriate control signals so that mobile station **114** transmits the access probes of FIGS. **4**A and **4**B using a message capsule with data transmitted at a rate of 19.2 kbps having a frame of 10 msec in length and initial power IP set for 19.2 kbps. The process then ends at step **518**. If, however, at step **514**, a determination is made that the transmit power head room for transmitting at 19.2 kbps does not exist, the process moves to step **508** and transmits the access probes of FIGS. **4**A and **4**B using a message capsule with data transmitted at a rate of 9.6 kbps having a frame of 20 msec in length and initial power IP set for 9.6 kbps. The process then ends at step **510**.

While the embodiment shown utilizes a set frame size for each of the different data rates that may be used for access, it is within the scope of the invention to provide multiple frame sizes for use with each possible data rate. For example, 38.4 kbps could be used with frame sizes of 5, 10 or 20 msec; 19.2 kbps could be used with frame sizes of 10 or 20 msec; and 9.6 kbps could be used with frame sizes of 20 msec. In this case, process steps **516** and **522** may involve access using varying frame sizes. Also, it is within the scope of the invention to determine the access data rate based on predetermined algorithms using parameters other than path loss or to perform the access data rate determination within other than the mobile station. For example, the access data rate may be calculated at the base station, and the appropriate information could then be transmitted to the mobile station to inform the mobile station of the data rate and frame size to use on the access channel.

Therefore, while the invention has been particularly shown and described with respect to preferred embodiments thereof, it will be understood by those skilled in the art that changes to form and details may be made therein without departing from the spirit and scope of the invention.

What is claimed is:

1. A method for accessing a telecommunications system, said method comprising the steps of:

determining, based on channel conditions and access time requirements for a type of service, a selected data rate from a plurality of data rates and a selected frame size from a plurality of frame sizes, wherein each of said plurality of frame sizes includes the same number of bits; and

accessing said system by transmitting an access probe from a mobile station, said access probe including a message capsule having said selected data rate and said selected frame size, selecting during said step of determining.

2. The method of claim **1**, wherein said step of determining a selected data rate and a selected frame size comprises the steps of:

determining an estimated path loss for transmissions from a mobile station to a base station; and

determining a selected data rate from a plurality of data rates, said selected data rate being the maximum data rate of said plurality of data rates that may be transmitted from said mobile station to said base station while incurring a path loss at the level of said estimated path loss.

3. The method of claim **2**, wherein said step of determining an estimated path loss comprises the steps of:

receiving, at a mobile station, a signal transmitted from a base station at a transmission power level P_{pt};

measuring received signal strength P_{pr} of said signal at said mobile station; and

calculating an estimated path loss as the difference between P_{pt} and P_{pr}.

4. The method of claim **1**, wherein said plurality of data rates comprises data rates of 9.6 kbps, 19.2 kbps and 38.4 kbps, and said plurality of data frames comprises data frames of sizes 20 msec, 10 msec and 5 msec.

5. The method of claim **1**, wherein said selected data rate at a first data rate has a first frame size, and said selected rate at a second data rate slower than said first data rate has a second frame size larger than said first frame size.

6. The method of claim **1**, wherein said plurality of frame sizes comprises frame sizes of 20 msec, 10 msec, and 5 msec.

7. The method of claim **6**, wherein said step of determining a selected data rate comprises the steps of:

determining an estimated path loss for transmission from a mobile station to a base station; and

determining, at a mobile station, a selected data rate from a plurality of data rates, said selected data rate being the maximum data rate of said plurality of data rates that may be transmitted from said mobile station to said base station while incurring a path loss at the level of said estimated path loss.

8. The method of claim **7**, wherein said step of determining an estimated path loss comprises the steps of:

receiving, at a mobile station, a signal transmitted from a base station at a transmission power level P_{pt};

measuring received signal strength P_{pr} of said signal at said mobile station; and

calculating an estimated path loss as the difference between P_{pt} and P_{pr}.

9. The method of claim **1**, wherein said plurality of data rates comprises a data rate of 9.6 kbps, 19.2 kbps and 38.4 kbps, and wherein said data rate of 9.6 kbps is associated with at least a frame size of 20 msec, said data rate of 19.2 kbps is associated with at least a frame size of 10 msec, and said data rate of 38.4 kbps is associated with at least a frame size of 5 msec.

10. A method of accessing a telecommunications system, said method comprising the steps of:

determining whether channel conditions for transmissions from a mobile station to a base station do not meet predetermined criteria for transmission of an access signal at a first data rate and first frame size including a selected number of bits, wherein said first data rate and first frame size allow access to said system with a first access time and are preferred for accessing the system for a selected type of service; and

if it is so determined, transmitting an access signal to access the telecommunication system, the access signal transmitted at a second data rate and second frame size including said selected number of bits, wherein said second data rate is less than said first data rate, and said second frame size is larger than said first frame size, wherein said second data rate and said second frame size allow access to said system with a second access time and are less preferred for accessing said selected type of service than said first data rate and first frame size; else

if it is determined that said channel conditions meet said predetermined criteria, transmitting said access signal to access the telecommunications system at said first data rate and said first frame size including said selected number of bits.

11. The method of claim **10**, wherein said step of determining comprises the steps of:

determining an estimated path loss for transmissions from a mobile station to a base station; and

determining whether said estimated path loss is greater than a maximum path loss, said maximum path loss being the maximum path loss for an access signal transmitted at a first data rate.

12. An apparatus for accessing a telecommunications system, said apparatus comprising:

a processor, said processor for determining a selected data rate from a plurality of data rates and a selected frame size from a plurality of frame sizes, wherein each of said plurality of frame sizes includes the same number of bits, based on channel conditions and access time requirements for a type of service, wherein said processor determines said selected data rate by determining an estimated path loss from said mobile station to a base station, and wherein said selected data rate is determined as the maximum data rate of said plurality of data rates that may be transmitted from said mobile station to said base station while incurring a path loss at the level of said estimated path loss, said processor further for generating at least one control signal; and

a transmitter, said transmitter for receiving said at least one control signal and transmitting, in response to receiving said at least one control signal, an access probe to access the telecommunications system, the access probe including a message capsule having said selected data rate and said selected frame size.

13. The apparatus of claim **12**, further comprising a receiver for receiving a signal transmitted from said base station at a transmission power level P_{pt} and measuring a received signal strength P_{pr} of said signal, and wherein said processor determines said estimated path loss as the difference between P_{pt} and P_{pr}.

14. The apparatus of claim **12**, wherein said plurality of data rates comprises data rates of 9.6 kbps, 19.2 kbps and 38.4 kbps, and said plurality of data frames comprises data frames of sizes 20 msec, 10 msec and 5 msec.

15. The apparatus of claim **12**, wherein said selected data rate at a first data rate has a first frame size, and said selected data rate at a second data rate slower than said first data rate has a second frame size larger than said first frame size.

16. The apparatus of claim **12**, wherein said plurality of frame sizes comprises frame sizes of 20 msec, 10 msec and 5 msec.

17. The apparatus of claim **16**, wherein said processor determines said selected data rate by determining an estimated path loss from said mobile station to a base station, and said selected data rate is determined as the maximum data rate of said plurality of data rates that may be transmitted from said mobile station to said base station while incurring a path loss at the level of said estimated path loss.

18. The apparatus of claim **17**, further comprising a receiver for receiving a signal transmitted from said base station at a transmission power level P_{pt} and measuring a received signal strength P_{pr} of said signal, and wherein said processor determines said estimated path loss as the difference between P_{pt} and P_{pr}.

19. The apparatus of claim **12**, wherein said plurality of data rates comprises a data rate of 9.6 kbps, 19.2 kbps and 38.4 kbps, and wherein said data rate of 9.6 kbps is associated with at least a frame size of 20 msec, said data rate of 19.2 kbps is associated with at least a frame size of 10 msec, and said data rate of 38.4 kbps is associated with at least a frame size of 5 msec.

20. An apparatus for accessing a telecommunications system, said apparatus comprising:

means for determining whether channel conditions for transmissions from a mobile station to a base station do not meet predetermined criteria for transmission of an access signal at a first data rate and first frame size including a selected number of bits, wherein said first data rate and first frame size allow access to said system with a first access time and are preferred for accessing the system for a selected type of service;

means for transmitting an access signal, to access the telecommunications system, at a second data rate and second frame size including said selected number of bits, wherein said second data rate is less than said first data rate and said second frame size is larger than said first frame size, if said channel conditions do not meet said predetermined criteria, wherein said second data rate and second frame size allow access to said system with a second access time and are less preferred for accessing said selected type of service than said first data rate and first frame size; and

means for transmitting said access signal, to access the telecommunications system, at said first data rate and first frame size including said selected number of bits, if it is determined that said channel conditions meet said predetermined criteria.

21. The apparatus of claim **20**, wherein said means for determining comprises:

means for determining an estimated path loss for transmissions from a mobile station to a base station; and

means for determining whether said estimated path loss is greater than a maximum path loss, said maximum path loss being the maximum path loss for an access signal transmitted at a first data rate.

22. An apparatus for accessing a channel in a telecommunication system, said apparatus comprising:

a processor for selecting, for an access transmission on the channel, at least a first or a second transmission frame from a plurality of available transmission frames, wherein each of said available transmission frames has a selected data rate of a plurality of data rates and a selected frame size of a plurality of frame sizes, wherein said first and second transmission frames each have different frame sizes of said plurality of frame sizes and different data rates of said plurality of data rates, wherein said first and second transmission frames each carry the same number of bits, the transmission frame selected of said first or second transmission frames by said processor carries said same number of bits, and wherein available transmission frames include a transmission frame of data rate 9.6 kbps and duration 20 msec., a transmission frame of data rate 19.2 kbps and duration 10 msec., and a transmission frame of data rate 38.4 kbps and a duration 5 sec.

23. The apparatus of claim **22**, wherein said access transmission includes a preamble portion and a message portion, wherein said processor selects a selected transmission frame from said at least a first or a second transmission frame, wherein said message portion includes said selected transmission frame and, wherein said apparatus further comprises a transmitter for transmitting said access transmission.

24. A mobile station, said mobile station for transmitting to a base station, an access transmission on a channel, the access transmission comprising a preamble and at least one message frame, wherein said mobile station is configured to transmit said message frame having at least a first duration and first data rate carrying a selected number of bits or a second duration, different from said first duration, and second data rate, different from said first data rate, also carrying said selected number of bits.

25. The mobile station of claim **24**, wherein said mobile station transmits said preamble on a pilot channel and transmits said at least one message frame on an access channel.

26. The mobile station of claim **24**, wherein said mobile station transmits packet data within said at least one message frame.

27. The mobile station of claim **24**, wherein said at least one message frame has said first duration and first data rate, said second duration and said second data rate or, a third duration and third data rate also carrying said selected number of bits, and wherein said first, second, and third durations comprise 20 msec., 10 msec., and 5 msec., respectively, and wherein said first, second and third data rates comprise 9.6 kbps, 19.2 kbps, and 38.4 kbps, respectively.

28. A base station for receiving an access transmission from a mobile station on a channel, wherein said access transmission comprises a preamble and at least one message frame, and said message frame having at least a first duration and first data rate carrying a selected number of bits or a second duration, different from said first duration, and second data rate, different from said first data rate, also carrying said selected number of bits.

29. The base station of claim **28**, wherein said message frame has at least said first duration and said first data rate carrying said selected number of bits, said second duration and said second data rate also carrying said selected number of bits, or a third duration, different from said first and second duration, and third data rate, different from said first and second data rate, carrying said selected number of bits.

30. The base station of claim **29**, wherein said first data rate comprises 9.6 kbps., and said first duration comprises 20 msec., wherein said second data rate comprises 19.2 kbps., and said second duration comprises 10 msec., and wherein said third data rate comprises 38.4 kbps and said third duration comprises 5 msec.

* * * * *

EXHIBIT E

US007092672B1

(12) **United States Patent**
Pekonen et al.

(10) **Patent No.: US 7,092,672 B1**
(45) **Date of Patent: Aug. 15, 2006**

(54) REPORTING CELL MEASUREMENT RESULTS IN A CELLULAR COMMUNICATION SYSTEM

(75) Inventors: **Johanna Pekonen**, Espoo (FI); **Leif Friman**, Järvenpää (FI); **Harri Jokinen**, Hiisi (FI)

(73) Assignee: **Nokia Corporation**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 234 days.

(21) Appl. No.: **10/088,460**

(22) PCT Filed: **Sep. 19, 2000**

(86) PCT No.: **PCT/EP00/09206**

§ 371 (c)(1),
(2), (4) Date: **Aug. 29, 2002**

(87) PCT Pub. No.: **WO01/22759**

PCT Pub. Date: **Mar. 29, 2001**

(30) **Foreign Application Priority Data**

Sep. 20, 1999 (GB) 9922217.6

(51) **Int. Cl.**
H04B 17/00 (2006.01)

(52) **U.S. Cl.** **455/67.11**; 455/422.1

(58) **Field of Classification Search** 455/515, 455/226.1, 226.2, 226.3, 436, 439, 464, 446, 455/67.11, 422.1, 69, 522, 115.3, 524, 513, 455/429, 442, 443, 437
See application file for complete search history.

(56) References Cited

U.S. PATENT DOCUMENTS

5,594,949 A		1/1997	Andersson et al.	455/62
5,966,657 A	*	10/1999	Sporre	455/425
6,223,037 B1	*	4/2001	Parkkila	455/434
6,308,071 B1	*	10/2001	Kalev	455/446

FOREIGN PATENT DOCUMENTS

EP	0 920 143 A	6/1999
GB	2 327 014 A	1/1999
WO	WO 99 05878 A	1/1997

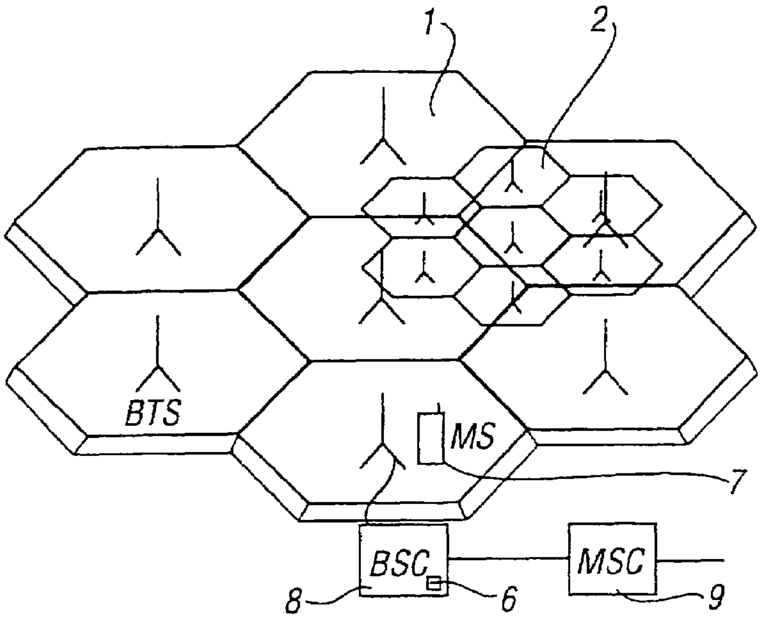
* cited by examiner

Primary Examiner—Edward F. Urban
Assistant Examiner—Tu X. Nguyen
(74) *Attorney, Agent, or Firm*—Cohen, Pontani, Lieberman & Pavane

(57) ABSTRACT

The present invention relates to reporting cell measurement results associated with a plurality of cells of a cellular communication system. The reporting is transmitted from a station via a radio interface to receiver element of a cell serving the station. The cells are arranged in a reporting order that is to be used by the station for the reporting. The cell measurements are performed by the transceiver station for getting cell measurement results associated with a number of the cells. Relevant cell measurement results are then selected and the selected results are transmitted in the defined reporting order.

30 Claims, 3 Drawing Sheets



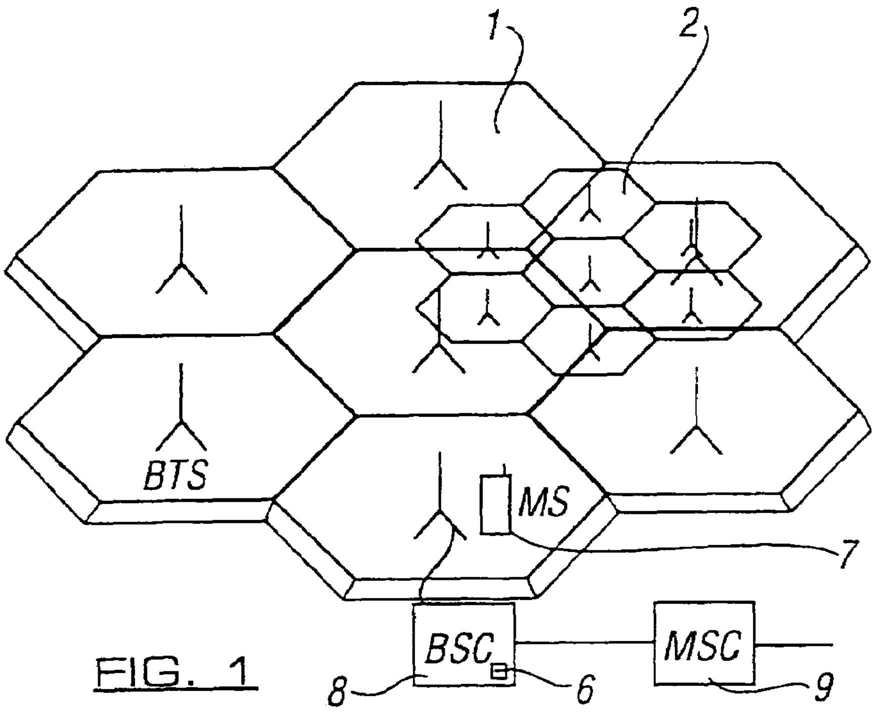


FIG. 1

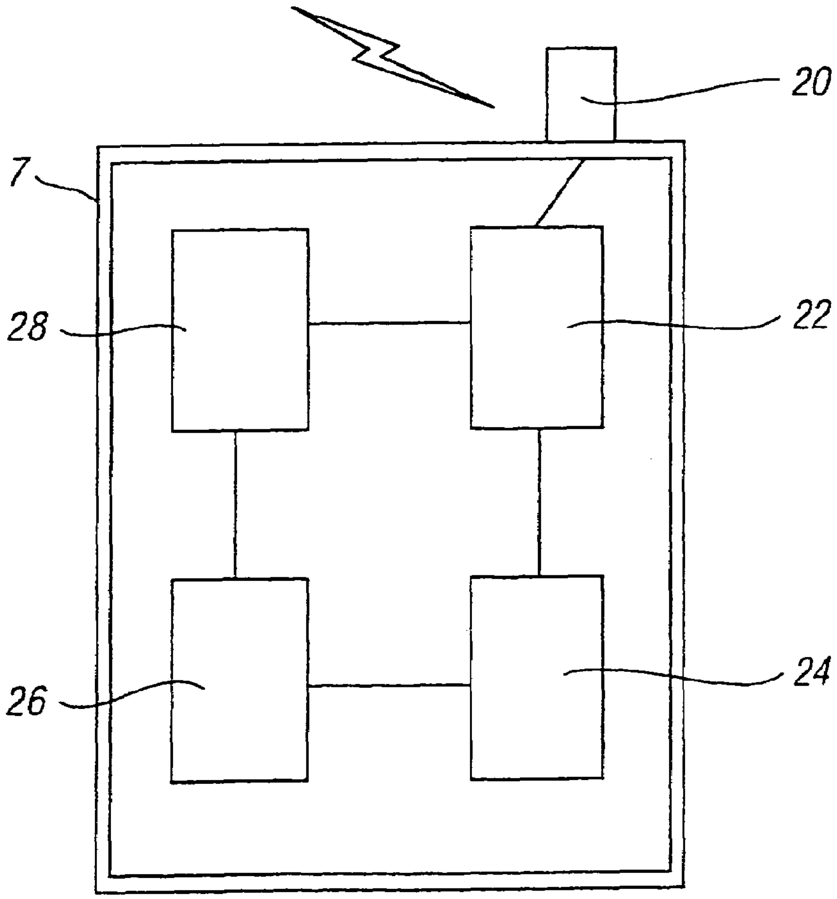


FIG. 2

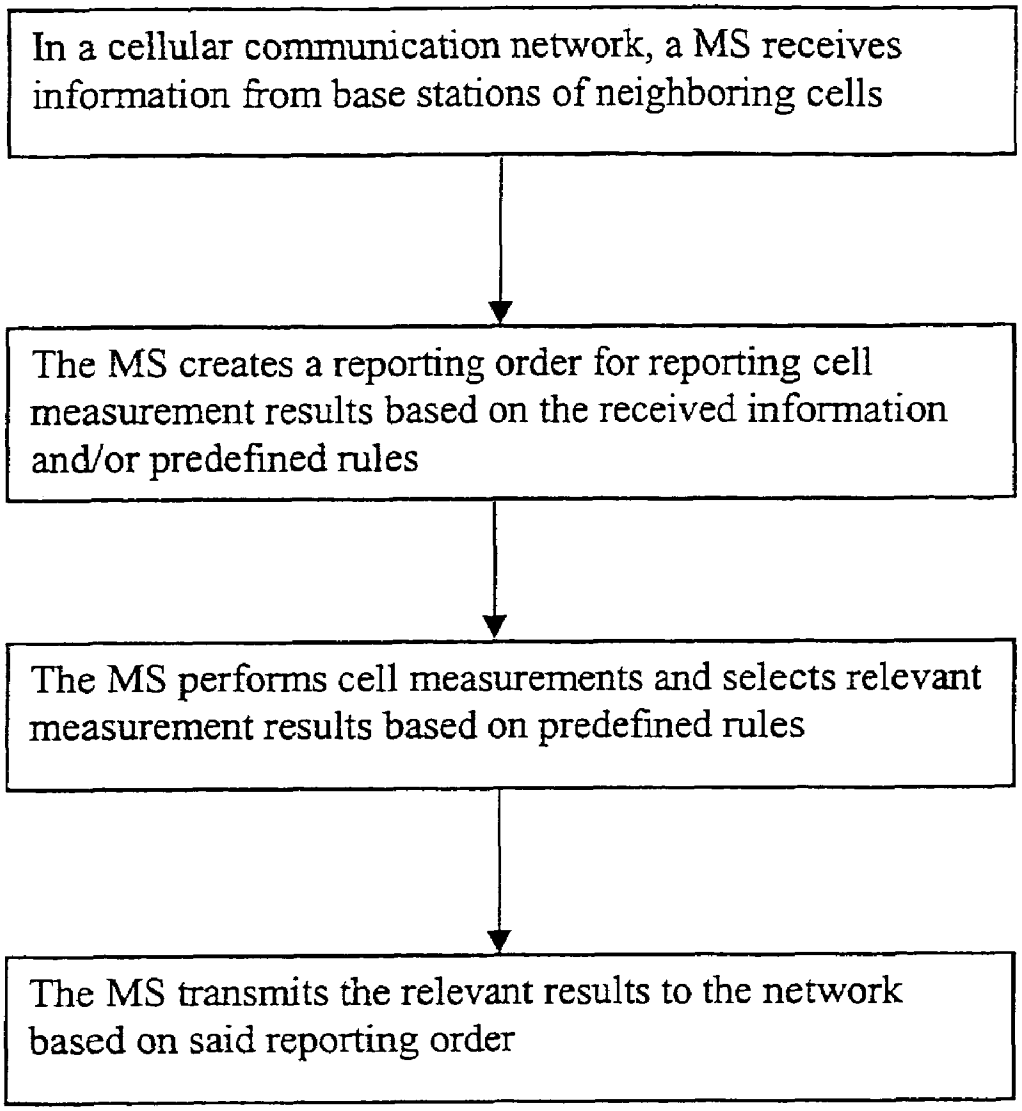

In a cellular communication network, a MS receives information from base stations of neighboring cells
The MS creates a reporting order for reporting cell measurement results based on the received information and/or predefined rules
The MS performs cell measurements and selects relevant measurement results based on predefined rules
The MS transmits the relevant results to the network based on said reporting order

FIG. 3

8	7	6	5	4	3	2	1	
Measurement Results 2 IEI								octet 1
Serving cell and other measurement results (Not relevant)								Octet 2
								Octet 3
								Octet 4
IND=1	RXLEV-NCELL 1						IND=1	Octet 5
RXLEV-NCELL 2 (low part)						IND=1	RXLEV-NCELL 3 (high part)	Octet 6
RXLEV-NCELL 3 (low part)					IND=1	RXLEV-NCELL 4 (high part)		Octet 7
RXLEV-NCELL 4 (low part)				IND=1	RXLEV-NCELL 5 (high part)			Octet 8
RXLEV-NCELL 5 (low part)			IND=0	IND=0	IND=0	IND=0	IND=0	Octet 9
IND=0	IND=0	IND=0	IND=0	IND=0	IND=0	IND=0	IND=0	Octet 10
IND=0	IND=0	IND=0	IND=0	IND=0	IND=1	RXLEV-NCELL24 (high part)		Octet 11
RXLEV-NCELL24 (low part)				IND=1	RXLEV-NCELL 25 (high part)			Octet 12
RXLEV-NCELL 25 (low part)			IND=1	RXLEV-NCELL 26 (high part)				Octet 13
RXLEV-NCELL 26 (low part)		IND=1	RXLEV-NCELL 27 (high part)					Octet 14
RXLEV-NCELL 27 (low part)	IND =1	RXLEV-NCELL 28						Octet 15
IND=1	RXLEV-NCELL 29						IND=0	Octet 16
IND=0	IND=1	RXLEV-NCELL 32						Octet 17

FIG. 4

REPORTING CELL MEASUREMENT RESULTS IN A CELLULAR COMMUNICATION SYSTEM

PRIORITY CLAIM

This is a national stage of PCT application No. PCT/EP00/09206, filed on Sep. 19, 2000. Priority is claimed on that application, and on patent application No. 9922217.6 filed in Great Britain on Sep. 20, 1999.

FIELD OF THE INVENTION

The present invention relates to reporting in a cellular communication system, and in particular, but not exclusively, to reporting of measurement results from a transceiver station to the communication system.

BACKGROUND OF THE INVENTION

A wireless communication network may comprise a cellular radio network consisting of cells. In most cases a cell can be defined as a certain area covered by one or several base transceiver stations (BTS) serving mobile stations (MS) within the cell via a radio interface. The base station may be connected to a base station subsystem (BSS). Several cells may overlap and cover together a larger area, thereby forming the coverage area of a cellular radio network. The cell (or group of cells) and thus the mobile station (MS) or similar user equipment (UE) within one of the cells of the system can be controlled by a node providing controller functionality. Examples of the network controller include a base station controller (BSC), a radio network controller (RNC) and a mobile switching center (MSC), but other control nodes may also be used. The controller can be connected further to a gateway or linking node, for example a gateway GPRS support node (GGSN) or gateway mobile switching center (GMSC), linking the cell to the other parts of the communication system and/or other communication networks, such as to a PSTN (Public Switched Telecommunications Network) or to a data network, such as to a X.25 based network or to a TCP/IP (Transmission Control Protocol/Internet Protocol) based network. The cellular telecommunication networks typically operate in accordance with a given standard (or several standards) which sets out what the elements of the network are permitted to do and how that should be achieved. Examples of the cellular telecommunications network standards include code division multiple access (CDMA) based standards (such as the Digital Advanced Mobile Phone Service (DAMPS), or Wide-band CDMA or the proposed Universal Mobile Telecommunications System (UMTS) or time division multiple access (TDMA) based standards (such as GSM: Global Standard for Mobile or the GSM based General Packet Radio Service (GPRS)) or frequency division multiple access (FDMA) based standards. In addition to basic voice and data communication services, the users of the mobile stations are provided with various other services known to the skilled person.

The mobile station and/or the base station may measure and/or define several parameters concerning the conditions in the cell, such as signal levels (power) between the receiving and transmitting stations, quality of the signal, distance between the stations, amount of transmitted data and so on. The mobile station can be provided with appropriate means for defining a value for any parameter that can be measured for the interaction between the mobile station and any of the base stations or the conditions in a cell. The measurements or definitions performed by the mobile station will be referred to in the following as cell measurements and the results obtained by the mobile station will be correspondingly referred to as cell measurement results.

During an ongoing call the mobile station may report to the network controller so called neighbouring cell measurement results associated with cells neighbouring the cell serving the mobile station at the current moment by a measurement result message. In other words, the neighbouring cells can be defined to be the other cells of the system than the cell currently serving the mobile station. For example, in the GSM based systems the reporting may be done on SACCH (Slow Associated Control Channel). In this instance the measurement result message consists of information related to the serving cell and also information concerning the six strongest neighbouring cells. In the GSM based systems the report message frame includes information bits for the measured RX-level (received signal level), BCCH-frequency (Broadcast Control Channel frequency) and the BSIC (Base Station Identity Code) for each reported neighbouring cell. At the current GSM based systems the RX-level is reported with six bits. The value range of the information is set to be from −47 dBm to −10 dBm with 1 dB steps.

In the current measurement reports it is possible to report only six neighbouring cells in maximum. Since the number of the cells with which the mobile station may interact can be greater than this it could be advantageous to have a report covering more than only the six cells. This is especially the case in multisystem or multiband networks and/or in cellular communication systems operating in a multilayer environment. In general, the multimode systems can be defined as a communication environment in which the mobile station may be in a such service area where it may be served by more than one serving network or system or standard or frequency and so on. An example of a multiband system is a dual-band GSM mobile stations served by both 900 MHz and 1800 MHz frequencies. An example of a multisystem is a dual mode telephone operating e.g. in GSM networks and in UMTS networks.

For example, in the current GSM standard a reported neighbouring cell will reserve 17 bits from the reporting message. There is no free space in the current measurement report message to include more cell measurement results for the neighbouring cells than said measurement results for six neighbouring cells.

In addition, the reporting of the RX-level with 6 bits only may cause limitations in the reporting range in some applications. Especially, the maximum value of the indicated RX-level may be insufficient for all applications. Therefore it could be advantageous to be able to indicate RX-levels that are higher than the currently possible levels, such as the −47 dBm maximum value. Reports of higher received signal levels is needed e.g. for the purposes of handover decisions in instances where the mobile station is close to a sectored base station and moving from one sector to another sector of the base station.

Furthermore, at signal levels above e.g. −47 dBm value, the current measurement report cannot indicate if the serving cell has a higher power than one of the neighbouring cells unless the serving cell is included in a list of the neighbouring cells. This approach is, however, not a desired solution since the number of the real neighbouring cells reported to the network would go down from 6 to 5.

SUMMARY OF THE INVENTION

It is an aim of the embodiments of the present invention to address one or several of the above problems.

According to one aspect of the present invention, there is provided a method in a cellular communication system for reporting cell measurement results associated with cells of the system from a transceiver station via a radio interface between the transceiver station and a cell serving the transceiver station, comprising:

defining a reporting order of the cells to be used by the transceiver station for reporting;

performing cell measurements at the transceiver station for getting cell measurement results associated with at least some of the cells;

selecting relevant cell measurement results from the performed cell measurements; and

reporting the cell measurement results from the transceiver station in the defined reporting order.

According to another aspect of the present invention there is provided a cellular communication system comprising:

a transceiver station;

a cell serving the transceiver station via a radio interface;

a plurality of further cells;

wherein the transceiver station comprises control means for performing cell measurements concerning at least some of the further cells, control means for defining a reporting order of the measurement results, control means for selecting relevant cell measurement results from the performed cell measurements, and control means for generating a report message reporting the cell measurement results in the defined reporting order.

According to another aspect of the present invention there is provided a mobile station for use in a cellular communication system comprising control means for performing cell measurements concerning cells of the system, control means for defining a reporting order of the measurement results, control means for selecting relevant cell measurement results from the performed cell measurements, and control means for generating a report message reporting the cell measurement results in the defined reporting order.

According to another aspect of the present invention there is provided a network node of a cellular communication system comprising means for receiving cell measurement results from a station communicating with one of the cells of the system, said measurement results being associated with a plurality of cells of the communication system and being reported from the station in a reporting order of the cells defined by the station, control means for defining the reporting order used by the station for the reporting and control means for attaching measurement results to cells based on the reporting order.

According to more specific embodiments, the measurement results are reported by information symbol strings containing a plurality of information symbols, wherein an indication symbol is included into the measurement report string for indicating whether the following predefined number of symbols in the string includes the cell measurement results of a subsequent cell in the reporting order of the cells or whether the subsequent cell will not be reported in the measurement report string. In addition, predefined information about the cells to the measured may be received at the mobile station, wherein the definition of the reporting order is based on said received information. The reported measurement results may be associated with respective cells at a control node of the cellular communication system.

The embodiments of the invention provide several advantages. By means of some of the embodiments it is possible to include cell measurement reports for a greater number of cells within a reporting message without increasing the length of the reporting message string. Some of the embodiments enable use of a greater number of information symbols for each of the reported cells without increasing the length of the reporting message or reducing the number of the cells reported by a single message. By means of this it is possible to increase the range of the reported measurements. In addition, in some embodiments it is not necessary to transmit an identification of the cell, such as information of the frequency of the broadcast channel and the base station identity, for each of the measured cells together with the results from the mobile station.

BRIEF DESCRIPTION OF DRAWINGS

For better understanding of the present invention, reference will now be made by way of example to the accompanying drawings in which:

FIG. **1** shows a cellular radio system with which the embodiments of the present invention can be used;

FIG. **2** is a schematic presentation of a mobile station constructed in accordance with the present invention;

FIG. **3** is a flowchart illustrating the operation of one embodiment of the present invention; and

FIG. **4** illustrates one example of coding of a report message in accordance with one embodiment of the present invention.

DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Reference is made to FIG. **1** which shows a cellular system with which the embodiments of the present invention can be used. It is noted that even though the exemplifying telecommunications network shown and described in more detail in the following uses the terminology of a circuit switched GSM (Global System for Mobile communications) public land mobile network (PLMN), the proposed solution may be used in any cellular communication system. It should also be appreciated that the embodiments of the invention may be implemented using any number of cells. The radio coverage area of a cell may consist, for example, of a relatively omnidirectional pattern or a sector of a base station may be provided with a directional or sector antenna (not shown). The sector base station may use e.g. three 120° directional antennas whereby three radio coverage areas are provided, or four 90° directional antennas providing four radio coverage areas and so on, or any combinations of different radio coverage beam widths. It should also be appreciated that base stations may sometimes be referred to as node B (e.g. in the UMTS standard).

FIG. **1** illustrates two layers or cells **1** and **2**, respectively. The arrangement may be, for example, such that the first layer of cells **1** belongs to a network based on a first standard and the second layer of cells **2** belongs to a network based on a second standard. Each of two each cell **1**,**2** is served by the respective base transceiver station BTS. Each base transceiver station BTS is arranged to transmit signals to and receive signals from the mobile station MS **7** in the cell. Likewise, the mobile station is able to transmit signals to and receive signals from the respective base transceiver station. The mobile station **7** accomplishes this via wireless or radio communication with the base stations. Typically a number of mobile stations will be communication with each base station although only one mobile station is shown in FIG. **1** for clarity.

Each of the base stations is connected to a network controller, which in one form of the exemplifying GSM system comprises a base station controller (BSC) **8** connected further to a Mobile Switching Center (MSC) **9**. In the described embodiment the BSC is providing the network controller functionality for the purposes of the described embodiments. However, it is noted that the base station controller **8** controlling one or several base stations between the network controller and the base stations may be omitted in some embodiments. Therefore any other appropriate network element may be used for providing a controller functionality than can be used for processing measurement information from the mobile station **7**. It is also noted that typically more than one network controller is provided in a network. The network controller is connected to other elements or parts of the telecommunications network system via a suitable linking or gateway apparatus, such as Gateway Mobile Switching Center (GMSC; not shown).

The implementation of the communication between the mobile station, the base station and the controller is known, and will thus not be discussed in more detail herein. It is sufficient to note that the interface may comprise channels in both uplink and downlink directions between the mobile station in the cell associated with a given base station and that the information sent to the mobile station and the data may be sent in any suitable format. The messages sent from the mobile stations may include information identifying the mobile station (for instance, MS ID and/or IMSI (mobile Station Identity and/or International Mobile Subscriber Identity, respectively)).

As disclosed by FIG. **1**, the mobile station can be simultaneously in the signaling area of several cells. The mobile station is arranged to perform measurements, for example in order to be able to provide information based on which a suitable cell can be selected for serving the mobile station. In other words, in addition to controlling the ongoing connection with the servicing base station, the mobile station may perform measurements concerning the other cells as well.

It should be appreciated that this description uses the term neighbouring cell for defining any further cell that can be reached by a mobile station in a cell of the cellular communication system. That is, the cells need not to have any “border line” therebetween but the neighbouring cells or other cells may be partially overlapping, or even covering the entire coverage area of the servicing cell. In addition, the neighbouring cells may be cells of another type of communication network (e.g. networks based on different standards) or cells of a system using another frequency. The latter is the case when, for example, so called dual-band mobile stations are used.

FIG. **3** illustrates a flow chart for an embodiment for transmitting report messages from the mobile station. In the embodiment only such measurement results that associate to relevant neighbouring cells are reported to the network controller. According to a preferred embodiment this is accomplished without including any identification parameters of the related neighbour cells. The measurement results, such as RX-levels, are reported in a specific order of which the appropriate network controller, such as the BSC or RNC, is also made aware of.

Since the controller is aware of the reporting order, it is possible for it to conclude to which neighbouring cells the reported measurement results relate. Appropriate control or

processing means **6** of the controller **8** of FIG. **1** for accomplishing this are known, and will thus not be explained in more detail. It is sufficient to note that the controller nose is arranged to receive the cell measurement results from the mobile station **7** and to define measurement result and cell pairs based on the reporting order such that a respective measurement results is associated with a respective cell.

According to one possibility the reporting order is defined in the protocols and/or standards used by the cellular communication system. According to another approach the mobile station provides the controller with information of the reporting rules for setting the cells in an order the mobile station is going to use when reporting the cell measurement results, e.g. the RX-levels of the respective base stations to the network. According to a further possibility the controller provides the mobile station with instructions concerning the reporting order to be used when reporting the cell measurement results. The mobile station may also receive an elsewhere prepared reporting order, and thereafter use the received order as such for the reporting. In this case the definition processing done by the mobile station is for defining that the received reporting order is to be used for the reporting. It is noted that the rules for setting the cells in order may be changed during the operation of the communication system. The change may be dynamic, e.g. the change may occur as response to a predefined event (e.g. a system failure, overload, peak hour conditions, night time conditions, and so on) detected or defined by the system.

This explicit reporting order of the neighbouring cells may be defined by the mobile station based on neighbouring cell BCCH (Broadcast Control Channel) frequencies (e.g. based on ARFCN: Absolute Radio Frequency Channel Number) and the BSICs (Base Transceiver Station Identity Code) of the neighbouring cells received at the mobile station from the network. As mentioned above, the appropriate controller in the radio network side is also aware of this reporting order of the cells. The mobile station proceeds the cell measurements and selects relevant neighbouring cell measurement results among the performed measurements. These selected relevant results are then transmitted to the network in the known reporting order. The controller defined based on the known reporting order those cells the respective reported results relate.

The selection of the relevant cells may be based on any appropriate predefined rule of selection. The rules may be defined in the standards the mobile station and/or the communication system is arranged to use. The rules may be stored permanently in the mobile station. According to one possibility the rules are stored in an appropriate network element and transmitted therefrom to the mobile station when ever required. As was the case with the rules for setting the cell in a predefined order, the rules for selecting relevant cells may also be changed when this is deemed necessary. The selection of the relevant cells may be based, with no limitation to the following, on the measured signaling levels, used radio frequencies, direction of the movement of the mobile station, loading conditions of the neighbouring cells and so on.

FIG. **2** illustrates schematically a sectioned mobile station **7** which may be used in the embodiments of the invention. The mobile transceiver station comprises an antenna **20** for receiving and transmitting radio signals. The mobile station **7** comprises further control means **22** for performing various cell measurements associated with several base stations. In addition, control means **24** are provided for generating the reporting order of the measurement results. Control means

26 are provided for selecting the relevant ones of the performed cell measurements results. Control means **28** are provided for generating a report message reporting the relevant cell measurement results in the generated reporting order via the radio interface with the serving base station. It should be appreciated that the functions of the controllers **22** to **28** can be implemented by a single controller, or by two or three controllers or that said functions can be distributed to more than the four control units **22** to **28** of the mobile station **7**.

A preferred embodiment for the transmission of the measurement results will now be described with reference to FIG. **4**, wherein specific indication bits are used in the report messages transmitted from the mobile station to the network. More precisely, an indication bit can be used for each neighbouring cell measurement result indicating whether the following bit is a first bit of a relevant measurement result for a cell or a bit indicating a next neighbouring cell in the predefined reporting order. The latter may be the case e.g. when no measurement information is available for the preceding neighbouring cell and therefore the cell does not have any relevancy for the operation of the mobile station. However, the division between the relevant and non-relevant cells may be based in any other criteria as well. The bit indicating a non-relevant cell can be referred to as a skip bit.

From FIG. **4** it can be seen that the measured RX-level is reported for the cells which are in the reporting order list on places **1** to **5**, **24** to **29** and **32**. No cell measurement result information is reported for the neighbouring cells being in the places **6** to **24** and **30** to **31** in the reporting order.

According to one possibility, the order of the bits for measurement results and the indication bits is such that the first bits of the measurement report string indicate only what cells are reported. The following bits will then include the information of the results. E.g. in the exemplifying system of enabling **32** neighbouring cell, the first 32 bit may be arranged such that the “1” indicates that the cell is reported. “0” would then indicate that the cell is not reported. After the first 32 bits, the following information bits or other information symbols in the string inform in the reporting order the results for those cells that were indicated by “1”.

Since the cells to which the cell measurement results relate can be identified by the reporting order used in the measurement report, no additional bits are required for the cell identification. Therefore more neighbouring cells can be added to the measurement report. For example, if the number of bits reserved for a cell to be reported is seven bits, this is ten bits less than the number of bits reserved by the current solution in the GSM for reporting one neighbour cell. As the non-relevant neighbouring cells are also included in the reporting order of the measurement results, the non-relevant cells have to be indicated in the measurement report. However, the number of bits reserved for a non-relevant neighbouring cell (i.e. not reported cell) may be only one bit, as will be explained later on in this specification.

According to a more specific example of the embodiment, the network may transmit the neighbouring cell BCCH frequencies (e.g. the ARFCN values) in System Information 5 (SI 5), System Information 5bis and System Information 5ter messages based on GSM Specification 04.18 version 8.0.0. The BSICs of the neighbouring cells are transmitted to the mobile station in a message indicating the identity of the transmitting station. This may be a new message or then a message encapsulated to another message which the mobile station may receive. According to one option the identity indication message replaces the SI 5 messages and contains both the BCCH frequencies as well as the BSICs.

According to an embodiment the mobile station sets all the neighbouring cells in an explicit reporting order based on the above described two parameters. The reporting order is also known by the network. It is noted that each BCCH frequency may have more than one associated BSIC. After the above information has been received, each of the neighbouring cells can be identified with a unique BSIC/BCCH ARFCN pair and the neighbouring cells can be put into an explicit order according to the data in the relevant system information messages.

The total number of neighbouring cells can be limited to correspond the mobile station measurement capabilities. According to an embodiment the number of cells is 32, which is the maximum number of neighbouring cells at the current network architectures. However, this is only an example, and the number of neighbouring cells can be smaller or greater than 32.

In the measurement report the RX-levels of the relevant neighbouring cells are reported using this specific order. The measurement report includes an indication bit for each neighbouring cell. By the indication bit it may be indicated whether the following bits (for example, the following 6 bits) describe the RX-level of that specific neighbouring cell or not. For example, the arrangement may be such that an indication bit value “1” means that the RX-level is included and an indication bit value “0” means that no RX-level is not included for the given cell. If no RX-level is available the bit followed the current indication bit will then be the indication bit for the next neighbouring cell in the reporting order.

The embodiments of the invention enable an arrangement where it is not necessary to associate a BSIC and an index to each individual measurement result, thereby saving a lot of space in the report message. The BSIC is not required since the BSIC/BCCH frequency information is transmitted to the mobile station and the mobile station may decide which measurements are valid i.e. relevant and such which need to be reported. In the current systems this is done at the base station controller. The index is not required and can thus be removed from the report. The mapping of the RX-level or any other measurement result to the corresponding cell is based on the order of the results instead of any indexes.

Since the embodiment makes it possible with to leave the BSIC and BCCH-frequency of each neighbour cell out from the measurement report message and thereby enables inclusion of measurement results (e.g. the received signal level) of a greater number of neighbour cells. The report includes only the RX-level of the reported neighbour cells and the indication bit, an no other parameters are required to identify the cells in the report message. In the GSM example described above this means that since 107 bits reserved for neighbour cell measurement results can be used so that only seven bits are used for a cell with measurement result and one bit is used for a cell without any (or with a non-relevant) measurement result. For example, all cells can be reported in a cell having 32 neighbours such that the report includes measurement results for seven neighbouring cells (12×7+20×1=104 bits). This leaves even 3 bits free for other reporting purposes.

According to a measurement report message that is based on the GSM standards, there can be 13 octets and 3 additional bits available for neighbouring cell reporting, thereby providing 8×13+3=107 bits long reporting string or frame. At the current systems one cell can have a maximum of 32 neighbouring cells. The RX-level reporting reserves seven bits for a relevant neighbouring cell and one bit for a non-relevant neighbouring cell. In the case all neighbouring cells can be measured, the 15 first neighbouring cells on the list can be reported. If no limitations is set to the placing of the cells in the reporting order list, the maximum number of cells would be 12. In this instance the number of the reported neighbouring cells can be doubled from the above by means of the embodiments of the present invention.

The reported signal levels may be indicated with relation to a certain predefined reference signal level. The reference signal level may be transmitted in the same measurement report message. The reference signal level is preferably set so that each of the relevant signal levels can be reported by means of the reference level. More precisely, a reference level for the signal level is transmitted e.g. with three bits, with 4 dB steps (for example, 0=−110 dBm, 1=−106 dBm, 2=−102 dBm). Each measured signal level from the serving cell and from the relevant neighbouring cells are then indicated in the report in relation to this reference signal level. The reference signal level may be chosen so that each reported signal level is explicitly stronger or weaker than the reference signal level.

The following is presented in order to further clarify the scaling of the frame. The reference signal level may be indicated with three bits, thereby offering eight different values. Six bits are reserved for the indication of the relation between the measured result and the reference value. This makes it possible to have up to 63 dB dynamics in the signal level reporting. If the difference from the reference level is indicated with five bits, then dynamic would be up to 31 dB, which may also be sufficient for several applications. The five bit indication would save one further bit per reported neighbouring cell when compared to the received signal level reporting used in some of the current cellular systems.

Using reference level and indicating the difference from this reference level it is possible to widen the reporting range from −48 dBm to stronger signal levels. The stronger (i.e higher or greater) signal levels are levels >−48 dBm, such as −47 dBm, −40 dBm or −30 dBm.

The enhanced cell measurement reporting discussed above can be readily supported by "new" mobiles stations comprising the required control hardware and/or software, as illustrated by FIG. **2**. It is, however, preferred that the embodiment are used under control of an appropriate network element or elements. This guarantees compatibility between the "new" mobiles stations supporting the embodiments of the invention and "old" network implementations that cannot handle the described new reporting mode. If the neighbouring cell frequencies are sent with current system information messages while the BSIC information is sent in separate messages, the mobile station may send measurement reports with the "old" report after a handover until the mobile station is ordered to use the new report mode, e.g. as a result of receiving the message indicating the BSICs. By means of this it is possible to minimize the gap in neighbouring cell reporting after a handover, since the information of neighbouring cell frequencies can be received before the full information required for the new reporting format. The old reporting format needs to be used until it is known that the new cell supports the new reporting format. Alternatively the reporting mode after the handover is controlled by a corresponding new indicator in the handover command.

It should be appreciated that whilst embodiments of the present invention have been described in relation to mobile stations, embodiments of the present invention are applicable to any other suitable type of user equipment. In addition, while a message containing information bits and an indication bit are discussed above, the embodiments may be implemented by using any appropriate information symbols.

It is also noted herein that while the above describes exemplifying embodiments of the invention, there are several variations and modifications which may be made to the disclosed solution without departing from the scope of the present invention as defined in the appended claims.

What is claimed is:

1. A method in a cellular communication system for reporting cell measurement results associated with cells of the system from a transceiver station via a radio interface between the transceiver station and a cell serving the transceiver station, comprising:

defining a reporting sequence of the cells to be used by the transceiver station for reporting;

performing cell measurements at the transceiver station for getting cell measurement results associated with at least some of the cells;

selecting relevant cell measurement results from the performed cell measurements; and

reporting the cell measurement results from the transceiver station in the defined reporting sequence without including any identification parameters of the cells.

2. A method according to claim **1**, wherein the measurement results are reported by information symbol strings containing a plurality of information symbols, the method further comprising a step of including an indication symbol into the measurement report string for indicating whether the following predefined number of symbols in the string includes the cell measurement results of a subsequent cell in the reporting sequence of the cells or whether the subsequent cell will not be reported in the measurement report string.

3. A method according to claim **2**, wherein, in the event that the cell measurement indication symbol indicates that it will not be followed by symbols reporting the measurement results, the following symbol included in the measurement report string is a further indication symbol designated for a cell following the subsequent cell in the reporting sequence of the cells.

4. A method according to claim **1**, comprising further steps of receiving predefined information about the cells to be measured at the mobile station, and defining the reporting sequence based on said received information.

5. A method according to claim **4**, wherein said information comprises frequency of a broadcasting control channel and the identity of a transmitting base station of the cell to be measured.

6. A method according to claim **4**, wherein at least part of the information is transmitted in a separate message via the broadcasting control channel.

7. A method according to claim **1**, further comprising a step of associating each of the reported measurement results with respective cells at a control node of the cellular communication system.

8. A method according to claim **1**, wherein the reported cell measurement result for a cell comprises signal level of a radio signal received at the transceiver station.

9. A method according to claim **1**, wherein the reporting sequence is defined and the cell measurements are performed at the transceiver station for cells other than the serving cell.

10. A method according to claim **1**, wherein the reporting sequence is based on the information received from the serving cell.

11. A method according to claim **1**, wherein rules for defining the reporting sequence are stored at the transceiver station.

12. A method according to claim **1**, comprising a step of transmitting rules for the reporting sequence to the transceiver station via the radio interface.

13. A method according to claim **1**, comprising a step of changing rules for defining the reporting sequence.

14. A method according to claim **1**, wherein rules for selecting the relevant other cells are stored at the transceiver station.

15. A method according to claim **1**, comprising a step of transmitting rules for the selection of relevant cells to the transceiver station via the radio interface.

16. A method according to claim **1**, comprising a step of changing the rules for the selection of the relevant cells.

17. A method according to claim **1**, wherein the transceiver station sends the communication system information of the rules used for generating the cell measurement report.

18. A method according to claim **1**, wherein the reported information of the cell measurement results is based on reference values.

19. A method according to claim **18** in conjunction with claim **8**, wherein the reported information indicates if the measured signal level is stronger or weaker than the reference value.

20. A cellular communication system comprising:

a transceiver station;

a cell serving the transceiver station via a radio interface;

a plurality of further cells;

wherein the transceiver station comprises control means for performing cell measurements concerning at least some of the further cells, control means for defining a reporting sequence of the measurement results, control means for selecting relevant cell measurement results from the performed cell measurements, and control means for generating a report message reporting the cell measurement results in the defined reporting sequence without including any identification parameters of the cells.

21. A cellular communication system according to claim **20**, comprising at least two different cellular network arrangements.

22. A cellular communication system according to claim **20**, wherein the report message contains information symbols and at least one indication symbol in a string, said indication symbol indicating whether the following predefined number of symbols in the string define the cell measurement results of a subsequent cell in the reporting sequence of the cells or whether the subsequent cell will not be reported in the string.

23. A cellular communication system according to claim **22**, wherein, in the event that the cell measurement indication symbol is for indicating that it will not be followed by symbols reporting the measurement results, the following symbol in the measurement report string is a further indication symbol designated for a cell following the subsequent cell in the reporting sequence of the cells.

24. A cellular communication system according to claim **20**, wherein the transceiver station is arranged to receive predefined information associated with at least some of the further cells for use in defining the reporting sequence of the further cells.

25. A cellular communication system according to claim **24**, wherein the information comprises the frequency of a broadcasting control channel and the identity of a transmitting base station of the cell to be measured.

26. A cellular communication system according to claim **20**, further comprising a control node including means for associating measurement results with corresponding cells based on the reporting sequence.

27. A mobile station for use in a cellular communication system comprising control means for performing cell measurements concerning cells of the system, control means for defining a reporting sequence of the measurement results, control means for selecting relevant cell measurement results from the performed cell measurements, and control means for generating a report message reporting the cell measurement results in the defined reporting sequence without including any identification parameters of the cells.

28. A mobile station according to claim **27**, said mobile station being arranged to operate in at least two different cellular network systems.

29. A mobile station according to claim **27** being further arranged to receive predefined information associated with at least some of the further cells for use in defining the reporting sequence of the further cells.

30. A network node of a cellular communication system comprising means for receiving cell measurement results from a station communicating with one of the cells of the system, said measurement results being associated with a plurality of cells of the communication system and being reported from the station in a reporting sequence of the cells defined by the station, control means for defining the reporting order used by the station for the reporting and control means for attaching measurement results to cells based on the reporting sequence without including any identification parameters of the cells.

* * * * *

EXHIBIT F

US005862178A

United States Patent [19]

Järvinen et al.

[11] **Patent Number: 5,862,178**

[45] **Date of Patent: Jan. 19, 1999**

[54] **METHOD AND APPARATUS FOR SPEECH TRANSMISSION IN A MOBILE COMMUNICATIONS SYSTEM**

[75] Inventors: **Kari Järvinen**; **Janne Vainio**; **Petri Haavisto**, all of Tampere, Finland

[73] Assignee: **Nokia Telecommunications OY**, Espoo, Finland

[21] Appl. No.: **612,934**

[22] PCT Filed: **Jul. 5, 1995**

[86] PCT No.: **PCT/FI95/00390**

§ 371 Date: **Jun. 20, 1996**

§ 102(e) Date: **Jun. 20, 1996**

[87] PCT Pub. No.: **WO96/02091**

PCT Pub. Date: **Jan. 25, 1996**

[30] **Foreign Application Priority Data**

Jul. 11, 1994 [FI] Finland 943302

[51] **Int. Cl.**^{6} **H04B 1/66**

[52] **U.S. Cl.** **375/240**; 375/262; 704/201; 704/501

[58] **Field of Search** 375/240, 262, 375/341, 265; 371/37.4; 704/201, 227, 228, 500, 501

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,115,469	5/1992	Taniguchi et al. .	
5,271,089	12/1993	Ozawa .	
5,511,096	4/1996	Huang et al.	375/265
5,657,333	8/1997	Ikekawa	371/37.4
5,684,893	11/1997	Shikakura	371/37.4

FOREIGN PATENT DOCUMENTS

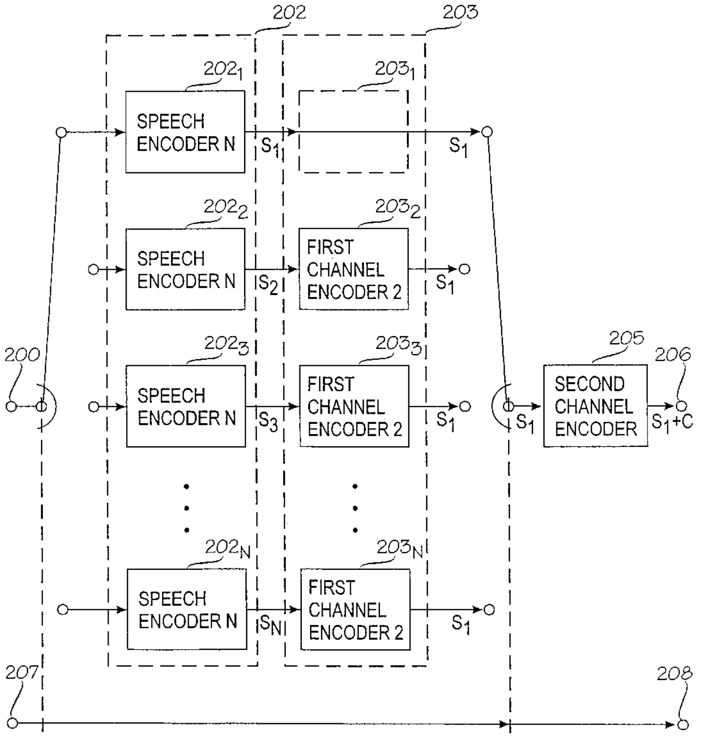
0 570 171	11/1993	European Pat. Off. .
0 588 307	3/1994	European Pat. Off. .
0 634 840	1/1995	European Pat. Off. .

Primary Examiner—Don N. Vo
Attorney, Agent, or Firm—Pillsbury Madison & Sutro LLP

[57] **ABSTRACT**

A method and apparatus for speech transmission in a telecommunications system in which a speech signal is compressed to a small number of speech coding bits by a speech coding method, and the speech coding bits are subjected to channel coding. Several different speech coding methods, which may all operate at different transmission rates, are involved in the speech transmission. The method is based on the use of two-stage channel coding. The first channel coding is dependent on the speech coding method, and it is performed in connection with the speech coding in such a manner that the total transmission rate provided by the speech coding and the first channel coding is always constant irrespective of the speech coding method. The second channel coding performed thereafter is always exactly the same regardless of the speech coding method and the first channel coding method, and it is used with all speech coding methods. The second channel coding may be, for example, the original channel coding in an existing telecommunications system.

14 Claims, 2 Drawing Sheets



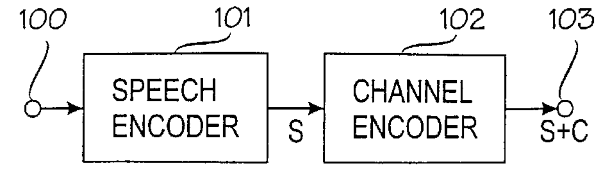


FIG. 1A

PRIOR ART

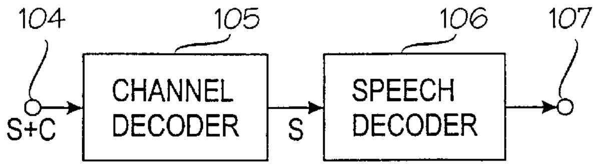


FIG. 1B

PRIOR ART

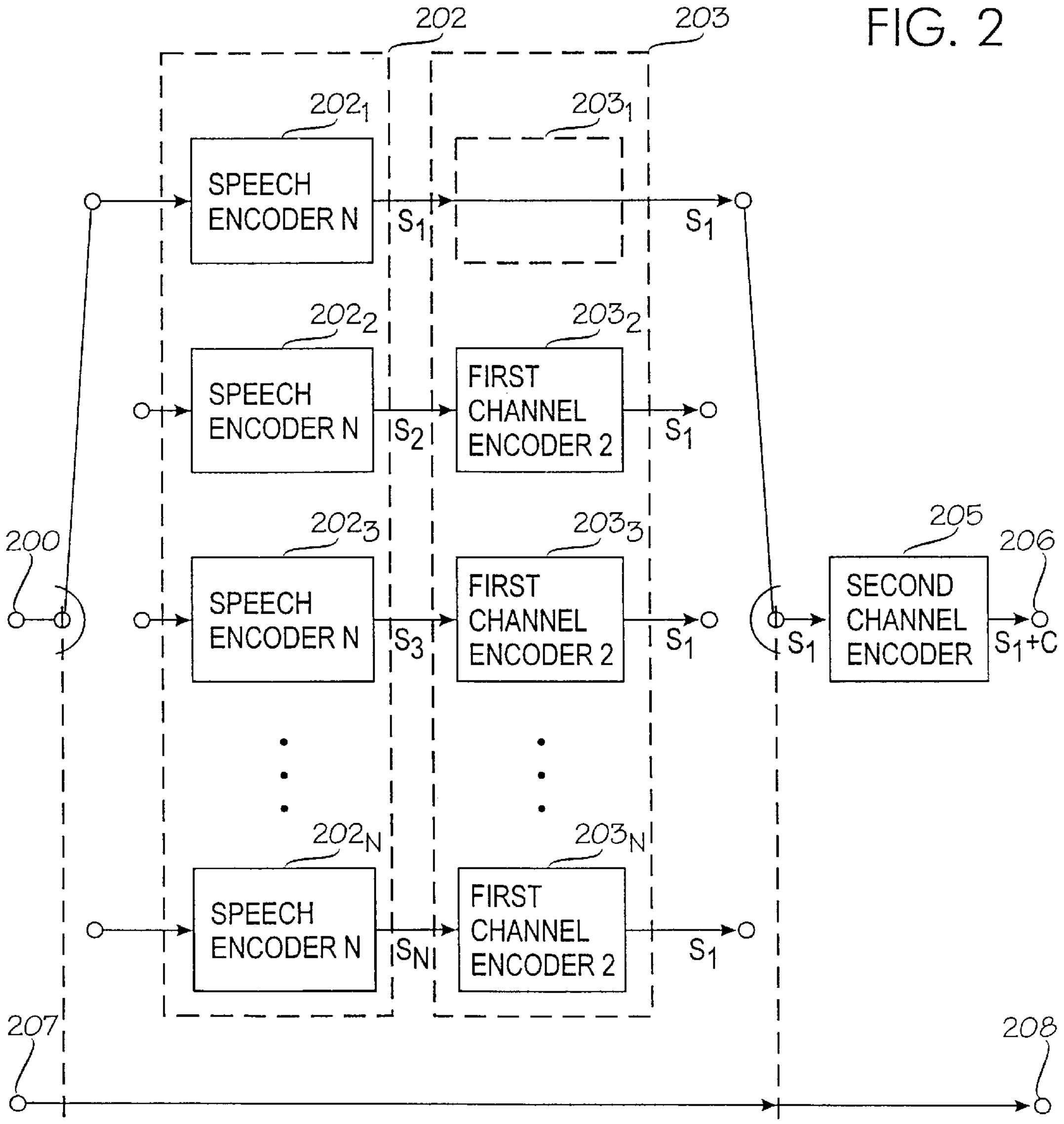
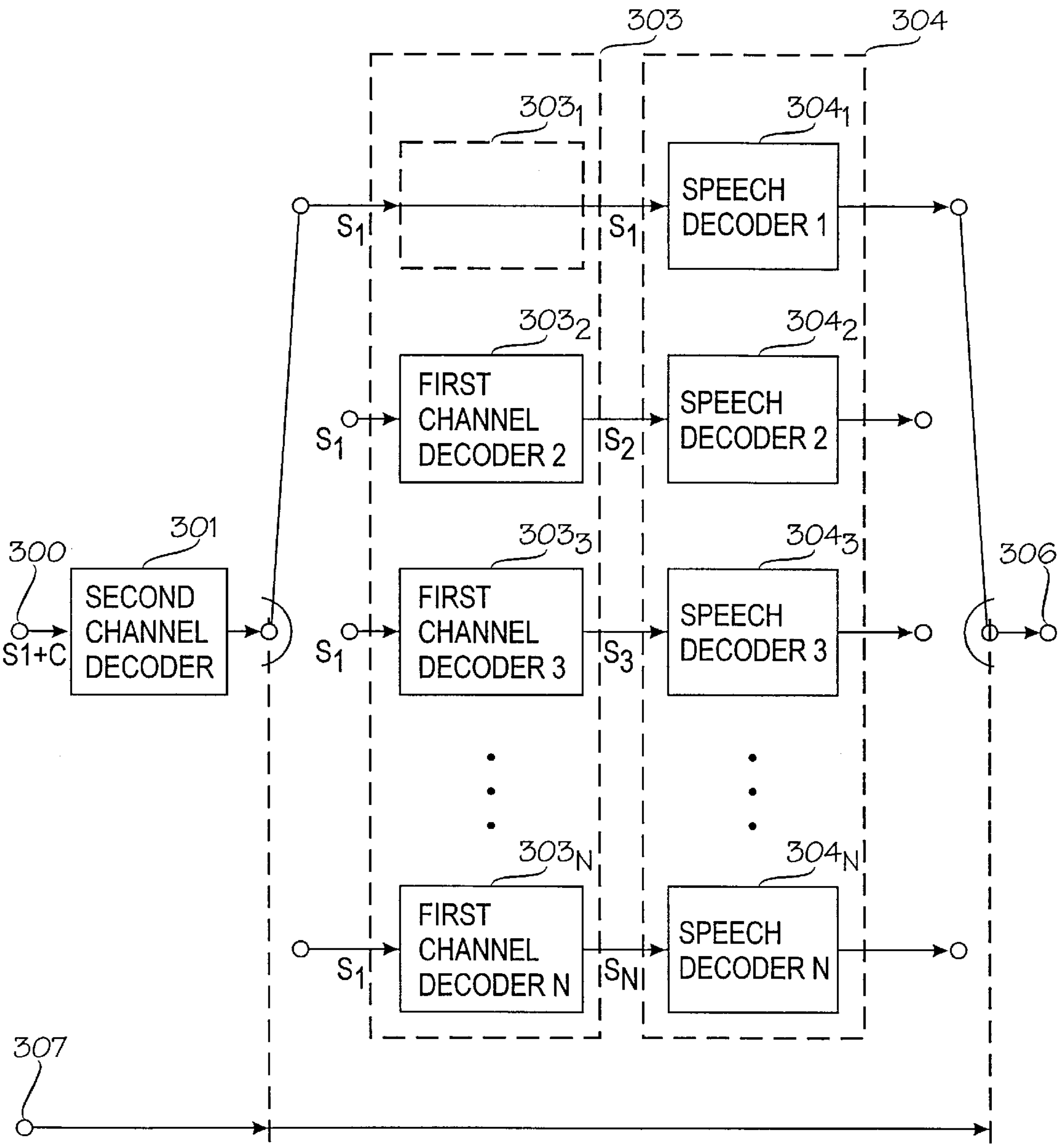


FIG. 2

FIG. 3


303
304
303$_1$
304$_1$
S$_1$
S$_1$
SPEECH DECODER 1
303$_2$
304$_2$
S$_1$
FIRST CHANNEL DECODER 2
S$_2$
SPEECH DECODER 2
300
301
S1+C
SECOND CHANNEL DECODER
303$_3$
304$_3$
S$_1$
FIRST CHANNEL DECODER 3
S$_3$
SPEECH DECODER 3
306
303$_N$
304$_N$
S$_1$
FIRST CHANNEL DECODER N
S$_N$
SPEECH DECODER N
307

METHOD AND APPARATUS FOR SPEECH TRANSMISSION IN A MOBILE COMMUNICATIONS SYSTEM

This application claims benefit of international application PCT/ Fl 95/00390 filed Jul. 5, 1995.

FIELD OF THE INVENTION

The invention relates to a method for speech transmission in a mobile communications system, the method comprising compressing a speech signal to a small number of speech coding bits by a speech coding method, and channel encoding the speech coding bits.

BACKGROUND OF THE INVENTION

In telecommunications systems transmitting digital speech, a speech signal is usually subjected to two coding operations: speech coding and channel coding.

Speech coding comprises speech encoding performed in the transmitter by a speech encoder and speech decoding performed in the receiver by a speech decoder. The speech encoder in the transmitter compresses a speech signal so that the number of bits used for representing the speech signal per a unit of time is reduced, whereby less transmission capacity is required for transmitting the speech signal. The speech decoder in the receiver performs a reverse operation and synthesizes the speech signal from the bits generated by the speech encoder. However, the speech synthesized in the receiver is not identical with the original speech compressed by the speech encoder; the original speech has changed more or less as a result of the speech coding. In general, the more the speech is compressed in the speech coding, the more its quality deteriorates during the coding. In the pan-European GSM mobile communication system (Global System for Mobile Communication), for example, the speech encoder of a full-rate traffic channel compresses a speech signal to a transmission rate of 13 kbit/s. The speech synthesized by the corresponding speech decoder is clearly of a poorer quality than the speech transmitted by, for instance, a public switched telephone network (PSTN).

Thus, when a speech coding method is selected, a compromise must be made between the quality offered by the method and the transmission capacity required by it. Another factor to be considered in the selection is the complexity of the implementation of the speech coding method: the quality of speech can usually be improved without increasing the transmission rate if higher requirements for the method as regards calculation capacity and thereby also higher costs of the implementation are allowed. On account of the continuous development of speech coding methods and the implementation techniques, more and more advanced methods are available for speech transmission in the existing telecommunications systems. After the development of the method employed in the GSM, speech coding technology has advanced to such an extent that, as compared with the above-mentioned 13 kbit/s speech coding method, a higher quality of speech can now be achieved at a much lower transmission rate, e.g. 8 kbit/s.

Channel coding comprises channel encoding performed in the transmitter by a channel encoder, and channel decoding performed in the receiver by a channel decoder. The purpose of channel coding is to protect speech coding bits to be transmitted against errors occurring in the transmission channel. Channel coding can either be used for merely detecting whether the transmission has caused any errors in the speech coding bits without any possibility of correcting them, or it may be capable of correcting errors caused by the transmission, provided that the number of errors does not exceed a given maximum, which is dependent on the channel coding method.

The selection of the channel coding method employed depends on the quality of the transmission channel. In fixed transmission networks the probability of errors is often very low, wherefore not much channel coding is required, whereas in wireless networks such as mobile telephone networks the probability of errors in the transmission channels is often very high, and the channel coding method employed has a significant effect on the resulting quality of speech. Mobile telephone networks usually employ both error-detecting and error-correcting channel coding methods concurrently.

Channel coding is based on the use of error check bits, also called channel coding bits, added to the speech encoding bits. Bits produced by the speech encoder of the transmitter are supplied to a channel encoder, which adds a number of error check bits to them. In the above-mentioned GSM full-rate transmission channel, for example, error check bits with a transmission rate of 9.8 kbit/s are added to speech coding bits of 13 kbit/s on the transmission channel, whereby the total transmission rate of the speech signal on the channel will be 22.8 kbit/s. The channel decoder decodes the channel encoding in the receiver in such a way that only the 13 kbit/s bit stream produced by the speech encoder is applied to the speech decoder. During channel decoding, the channel decoder detects and/or corrects errors that have occurred on the channel as far as such error correction is possible.

Speech coding and channel coding are closely connected with each other in telecommunications systems transmitting speech. The significance of the bits produced by the speech encoder for the quality of speech generally varies so that in some cases one error in an important bit may cause audible noise in the synthesized voice, whereas a larger number of errors in less important bits may be almost imperceptible. How big the differences between the importance of speech coding bits are depends essentially on the speech coding method employed; however, at least small differences can be found in most methods. When a speech transmission method is developed for a telecommunications system, channel coding is therefore usually designed together with speech coding in such a manner that the bits that are the most important for the quality of speech are protected more carefully than less important bits. On a full-rate channel of the GSM system, for instance, the bits produced by the speech encoder are divided into three different categories according to their importance. The most important category is protected in channel coding with both an error-detecting and an error-correcting code; the second most important category is protected only with an error-detecting code; the least important category is not protected at all in channel coding.

Although the speech coding and channel coding are closely connected, there are often considerable differences in their implementation in digital mobile telephone networks. The GSM system may once again be used as an example. Speech encoding and speech decoding are typically carried out by means of software, using a digital signal processor. This applies both to terminal equipment (telephones) and to network elements. Channel coding may also be performed by means of software, but often a separate integrated circuit is designed for this purpose, especially at the network end. Thus, changing of the speech coding method requires often merely a new signal processing program, whereas changing of the channel coding method may require equipment changes.

In addition to the way they are implemented, these two codings, speech coding and channel coding, may differ in their physical locations at the network end of a mobile telephone system. In the GSM system, for example, channel coding in the network is performed in a base station, while speech coding is performed in a separate transcoder unit, which may be remote from the base station, and even if it is located at the base station, it is a completely separate unit. Because of the separate locations, any changes in the transmission rates of the channel coding and speech coding will also entail changes in the connections between the different network elements.

In view of the different ways in which speech and channel coding are performed and their separate locations, it would be clearly more advantageous if the quality of speech could be improved in an existing system merely by changing the speech coding. As the channel coding is, however, usually designed particularly for the speech coding of the existing system, and as the new speech coding method should use exactly the same transmission rate as the original speech coding method of the system, methods for adapting new speech coding methods for existing telecommunications systems have not been disclosed previously.

FIG. **1A** and **1B** are block diagrams illustrating a transmitter and a receiver of a prior art telecommunications system. In the transmitter shown in FIG. **1A**, a speech signal **100** is supplied to a speech encoder **101**, which on the basis of the signal generates compressed speech coding bits having a transmission rate of S kbit/s. These speech coding bits are supplied to a channel encoder **102**, where error check bits are added to them, which results in a total transmission rate of S+C kbit/s. This bit stream **103** is transmitted over the transmission channel to the receiver shown in FIG. **1B**. In the receiver of FIG. **1B**, the bit stream **104** received from the transmitter is at first supplied to a channel decoder **105**, which decodes the channel encoding and transmits the speech coding bits thus obtained to a speech decoder **106**; the transmission rate of the speech coding bits is again S kbit/s. The speech decoder synthesizes a digital speech signal **107**. The telecommunications systems of the prior art thus employ only one speech encoding method and a corresponding channel coding method. Such telecommunications systems include, for example, all the commonest digital mobile telephone systems.

The prior art systems also include systems in which two different speech coding methods are used in such a manner that a separate channel coding method corresponds to each speech coding method, and in which the total transmission rate obtained as a result of the speech and channel coding is different in these two methods. An example of such a system is the GSM mobile telephone system, in which full-rate and half-rate traffic channels are specified.

There are also known solutions in which transmitters and receivers according to FIG. **1A** and **1B** are connected in parallel so that the system that is formed comprises several different speech encoding methods, each of which has a corresponding channel coding method. The speech coding methods used in such a system can operate at different transmission rates, wherefore the channel coding methods corresponding to them are also mutually independent and operate at different transmission rates.

SUMMARY OF THE INVENTION

The object of the present invention is to provide a digital telecommunications system in which several different

speech coding methods operating at different transmission rates are used for transmitting speech.

An object of the invention is a method and apparatus which allow the transmission of speech in a digital telecommunications system by the use of several different speech coding methods operating at different transmission rates.

Another object of the invention is a method for adapting more advanced speech coding methods operating at lower transmission rates for an existing digital telecommunications system using a certain speech coding method.

Still another object of the invention is a method for allowing addition of new speech coding methods to a digital telecommunications system without changing the channel coding method originally used.

Yet a further object of the invention is a method for allowing addition of new speech coding methods to an existing digital telecommunications system in such a manner that the addition causes as small changes as possible in the telecommunications system.

This is achieved with a method of the type described in the foregoing BACKGROUND section, which according to the invention is characterized by

using in the transmission of the speech N different speech coding methods, all of which operate at different transmission rates **S1**, **S2**, . . . , and SN kbit/s, respectively, where N≧2 and S1≧S2≧. . . ≧SN,

employing with each speech coding method a first channel encoding method specific for the respective speech coding method, the first channel encoding method comprising adding error-detecting and error-correcting first channel coding bits to the speech coding bits, and producing a constant transmission rate **S1** independent of the speech coding method employed so that the transmission rate of the first channel coding bits added to the speech coding bits during the first channel encoding is, depending on the speech coding method employed, **0**, S1–S2, . . . , S1–SN kbit/s, respectively,

after the first channel encoding, performing a second channel encoding, in which error-detecting and error-correcting second channel coding bits are added to the signal generated by the first channel encoding, the transmission rate of the second channel coding bits being C kbit/s, whereby after the second channel encoding the total transmission rate is a constant **S1**+C kbit/s irrespective of the selected speech encoding method.

The invention also relates to a transmitter apparatus for a telecommunications system transmitting digital speech, the apparatus comprising

speech encoding means for coding a speech signal by a speech coding method,

channel encoding means for channel-encoding the speech-encoded signal to a signal whose transmission rate is equal to the total transmission rate on the transmission channel. The transmitter apparatus is characterized according to the invention in that

the speech encoding means employ two or more speech coding methods, which provide speech-encoded signals having mutually different transmission rates,

the channel encoding performed by the channel encoding means consists of two steps comprising

first channel encodings which are specific for each speech encoding method and which, from the encoded speech signals having different transmission rates, generate first channel-encoded signals having the same constant transmission rate which is independent of the speech coding method, and

a second channel encoding which is independent of the speech coding method and which, from a selected first channel-encoded signal, generates a second channel-encoded signal having a constant transmission rate which is independent of the speech coding method and which is the same as said total transmission rate.

The invention further relates to a receiver apparatus in a telecommunications system transmitting digital speech, comprising

channel decoding means for decoding a received channel-encoded speech signal,

speech decoding means for speech-decoding a channel-decoded speech signal by a speech coding method. The receiver apparatus is characterized according to the invention in that

the speech decoding means employ two or more speech decoding methods for decoding speech-encoded speech signals produced by two or more speech encoding methods and having mutually different transmission rates,

the channel decoding performed by the channel decoding means consists of two steps comprising

a second channel decoding which is independent of the speech coding method and which, from the received channel-encoded speech signal whose constant transmission rate, which is independent of the speech coding method, is the same as the total transmission rate used in the telecommunications channel, produces a first signal having a lower constant transmission rate which is independent of the speech coding method,

first channel decodings which are specific for each speech coding method and which channel-decode the first signal, producing encoded speech signals which are specific for each speech coding method and which have mutually different transmission rates.

According to the invention, speech transmission in a digital telecommunications system employs several different speech coding methods, which may all operate at different transmission rates in such a manner that the total transmission rate obtained as a result of speech coding and channel coding remains the same irrespective of the transmission rate of the speech coding method employed. The method is based on the use of two-part channel coding. The first channel coding is dependent on the speech encoding method and is performed in connection with speech coding in such a way that the total transmission rate provided by the speech encoding and the first channel encoding is always constant irrespective of the speech coding method used. The second channel encoding, subsequently performed, is always exactly the same regardless of the speech encoding method and the first channel encoding method, and it is used with all speech encoding methods. The second channel coding may be, for example, the channel coding originally used in an existing telecommunications system, e.g. channel coding according to the recommendations of the GSM system. In this case, the first channel coding is not used in connection with the speech coding method originally employed in the telecommunications system; in other words, the transmission rate of the first channel coding bits, provided by the first channel encoding, is 0. The first channel coding methods used in connection with speech encoding methods that have been added later and operate at a lower rate provide the same total transmission rate as the original speech encoding method. The new speech encoding methods can thus be added to an existing telecommunications system without changing the channel coding method originally employed. The invention thus allows the quality of voice in an existing system to be improved with as small changes as possible.

The invention differs essentially from, e.g., the GSM system, in which full-rate and half-rate channels are specified, since the invention allows the use of several speech encoding methods in a telecommunications system in such a manner that the total transmission rate used by the speech and channel coding is constant irrespective of the speech encoding method employed. As regards the present invention, the known full-rate and half-rate transmission channels form separate systems, and the invention can be implemented independently in both transmission channels.

The speech coding method employed on each connection and the first channel coding method associated with it can be selected in many different ways, e.g. manually by the user, automatically on the basis of the erroneousness of the transmission path or on the basis of signalling between the transmitter and the receiver.

The method of the invention is thus based on the use of first channel coding in such a manner that a constant transmission rate is obtained as a result of speech encoding and the first channel encoding; a new speech coding method can be adapted for an existing system without changing the originally used second channel coding method. It is particularly characteristic of the invention that, when it is applied to an existing system, all speech coding methods have a common second channel encoder, whereas a separate first channel coding method is associated with each speech coding method in such a way that one speech encoder is not provided with any kind of first channel encoder.

The invention can be implemented in such a way that the first channel encoding is performed in connection with speech encoding, whereby the originally used channel coding unit, which performs the second channel coding, can be retained unchanged. In the GSM mobile telephone network, for example, the first channel coding can be carried out by means of software in a transcoder unit together with the new speech coding method, in which case no other changes are required at the fixed network end. In a terminal equipment (telephone), the new speech coding method and the corresponding first channel coding method can be implemented using the signal processor of the telephone in the same way as in the originally used speech coding.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the invention will be described in greater detail by means of preferred embodiments with reference to the accompanying drawings, in which:

FIG. **1**A and FIG. **1**B illustrate a transmitter and a receiver of the prior art, respectively,

FIG. **2** is a block diagram of a transmitter in a telecommunications system according to the invention,

FIG. **3** is block diagram of a receiver in a telecommunications system according to the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

The present invention is particularly suitable for telecommunications systems in which channel coding is particularly significant. The main field of application of the invention is wireless speech transmission, e.g. in digital mobile telephone systems. A particularly important field of application for the invention is the GSM mobile telephone system and its derivatives which are similar to the GSM as regards speech coding and channel coding but which may differ from the GSM for instance in their operating frequency ranges, such as the DCS-1800 and DCS-1900 systems.

As stated above, speech transmission in a digital telecommunications system of the invention employs several different speech coding methods which do not all operate at the same transmission rate. A first channel coding method is assigned to each speech coding method in such a way that the total transmission rate obtained as a result of speech coding and channel coding is kept constant regardless of the transmission rate of the speech coding method employed. The second part of channel coding is always exactly the same irrespective of which speech coding method and first channel coding method are used.

FIG. **2** is a block diagram of a transmitter in a telecommunications system according to the invention. The transmitter comprises N parallel speech encoders **202**$_1$ –**202**$_N$; the transmission rates of the compressed speech signals generated by these encoders, i.e. of the speech coding bits, are S_1, S_2. . . , S_N kbit/s, respectively (for reasons of clarity, the unit kbit/s for the transmission rate will be omitted below). A digital speech signal **200** to be transmitted is supplied to an input switch **201**, which is used to select one of these N speech encoders **202** for each speech connection. In the embodiment illustrated in FIG. **2**, the invention is applied in such a way that new, more advanced speech coding methods are added to an existing system. Therefore the speech encoder **202**$_1$ in Figure **1**A employs a speech coding method that has originally been used in the existing telecommunications system and that provides a transmission rate of S_1 for the speech coding bits, which is the same as the transmission rate of speech coding bits used originally in the existing telecommunications system. In the transmitter, it is thus also possible to select N−1 other speech encoders **202**$_2$–**202**$_N$, which provide transmission rates of S_2, S_3 ,. . . S_N, respectively, where the total number of speech encoders is $N \geqq 2$. The transmission rates of the speech encoders have the following relationship: $S_1 \geqq S_2 \geqq S_3 \geqq . . . \geqq S_N$, where $S_1 \geqq S_N$ must be true. The transmission rates of speech coding bits used by the speech encoders added to the telecommunications system may thus be, for some of the speech encoders **202**$_2$–**202**$_N$ the same as the transmission rate S_1, originally used for speech coding bits in the telecommunications system; but at least for one speech encoder this transmission rate is lower than the transmission rate S_1 originally used. Each speech encoder **202**$_1$–**202**$_N$ is used with a channel encoder **203**$_1$–**203**$_N$ specific for the respective speech coding method; however, in the case of those speech encoders which provide a transmission rate of S_1 for the speech coding bits, the first channel encoder **203** does not affect the speech coding bits in any way but forwards them as such to the second channel encoder **205**. In this case, the transmission rate provided by the first channel encoder for the channel coding bits, is thus 0, and the transmission rate to the second channel encoder **205** is S_1. In other words, the first channel encoder **203** is, in fact, omitted from this embodiment, like the first speech encoder **202**$_1$ in FIG. **2**, corresponding to the speech coder **202** originally used. A first channel coding bit rate equal to that of the first channel encoder **203**$_2$–**203**$_N$ may also be provided by another speech encoder **202**$_2$–**202**$_N$, if the speech coding bit rate of the respective speech encoder is S_1. In other cases, the first channel encoder **203**$_2$–**203**$_N$ adds error correction bits to the bit stream generated by the corresponding speech encoder **202**$_2$–**202**$_N$ so that the total transmission rate provided by the speech encoding and the first channel encoding is S_1 irrespective of the speech encoding method used. The channel coding bit rate provided by the first channel encoders **203**$_1$–**203**$_N$ is thus correspondingly **0**, S_1–S_2, S_1–S_3, . . . , S_1–S_N, depending on the speech encoding method employed by the speech encoder **202**$_1$–**202**$_N$ connected in series before them. It is characteristic of the invention that there is at least one speech encoding method whose respective first channel encoder **203** provides a first channel coding bit rate higher than 0. From the first channel encoder **203**$_1$–**203**$_N$ selected for the speech connection, the speech coding bits and the first channel coding bits are supplied via a switch **204** to a second channel encoder **205**. In the transmitter according to the invention, the transmission rate of the bit stream to be transmitted to the second channel encoder **205** is thus a constant S_1 kbit/s. The second channel encoder adds error correction bits to the bit stream produced by the selected speech encoder **202** and the first channel encoder **203** so that, at the output **206** of the second channel encoder, the total transmission rate is a constant S_1+C kbit/s. The switches **201** and **204** are controlled synchronically by a control signal **207** so that they will select the series connection of the speech encoder **202** which implements the desired speech encoding method, and the respective first channel encoder **203**. Information on the selected speech coding method is also sent to the transmission channel in a signal **208** to enable the receiver to select the correct first channel decoding and speech decoding methods corresponding to the speech encoding and first channel encoding methods used.

FIG. **3** is a block diagram of a receiver in a telecommunications system according to the invention. The receiver comprises a second channel decoder **301**, a selection switch **302**, N parallel first channel decoders **303**$_1$–**303**$_N$, N parallel speech decoders **304**$_1$–**304**$_N$, and a selection switch **305**. The receiver receives the speech coding bits and the first and second channel coding bits from the transmitter through the transmission channel at the input **300** of the second channel decoder **301**. The second channel decoder **301** decodes the second channel encoding performed by the second channel encoder **205** of the transmitter shown in FIG. **2**; as a result of this, the transmission rate of the bit stream received at the input **300** decreases from the constant S_1+C to the constant S_1. The second channel decoder **301** is thus independent of the speech coding method used and always performs the same channel decoding. The bit stream from the output of the second channel decoder **301**, having the transmission rate of S_1, is supplied to the selection switch **302**. The selection switch **302** switches the output of the second channel decoder **301** to one of N first channel decoders **303**$_1$–**303**$_N$, depending on the speech coding method used. The receiver also receives a signal **307** from the transmitter, through the transmission channel. Signal **307** corresponds to signal **208** of FIG. **2** and gives information on the speech coding method employed on the speech connection; the state of switch **302** and also that of switch **305** are determined on the basis of this information. The first channel decoder **303** is always dependent on the speech coding method employed, and it is connected in series with the speech decoder **304** assigned to it. The first channel decoder **303** decodes the first channel encoding performed by the first channel encoder **203** of the transmitter shown in FIG. **2** and provides the transmission rate used by the selected speech coding method. If the transmission rate of the channel coding bits added by the first channel encoding is 0, as in the case of channel encoder **203**$_1$ in FIG. **2**, the respective first channel decoder feeds the bits received from the second channel decoder **301**, the transmission rate of said bits being S_1, directly to the associated speech decoder; thus, in fact, there is no first channel decoder for such a speech coding method. In FIG. **3**, first channel decoder **303**$_1$—corresponding to the missing first channel encoder **203**$_1$ of FIG. **2** —is omitted. Naturally only one of the channel decoders is in use at a time. The other first channel decoders **303**$_2$–**303**$_N$ of FIG. **3** decode the channel encoding associated with the speech encoders **202**$_2$–**202**$_N$ of FIG. **2** and thus decrease the constant transmission rate S_1 of the bit stream received from the second channel decoder **301** by the transmission rate **0**, S_1–S_2, S_1–S_3, . . . , S_1–S_N, providing the transmission rates S_1, S_2, . . . , S_N kbit/s, which are dependent on the speech coding methods. The bit stream generated by the first channel decoder **303**$_1$–**303**$_N$ is supplied to the corresponding speech decoder **304**$_1$–**304**$_4$, which by means of the received speech coding bits generates a synthesized speech signal. The output signal of the speech decoder of the selected speech coding method is switched by selection switch **305** to the output **306** of the receiver. The position of the selection switch **305** is determined on the basis of signal **307** received from the transmitter through the transmission channel.

In the embodiment of the invention illustrated in FIGS. **2** and **3**, information on the speech coding method employed is forwarded through the transmission channel from the transmitter to the receiver. This information transfer may be based on any suitable method, e.g. a signalling method known per se. The speech coding method may also be permanent at each receiver or transmitter. It is, however, essential that both the transmitter and the receiver have information on the speech coding method employed so that the positions of the switches **201**, **204**, **302** and **305** can be determined correctly, and the same speech coding method can be selected both in the transmitter and in the receiver.

There are several ways of selecting the speech coding method according to the invention for each speech connection. Some factors influencing the selection and a few selection method will be described in the following; however, the invention is not limited to these examples.

If the transmission rate used for transmitting the speech coding bits is as low as possible in the selected speech coding method, more bits are left for the first channel coding. In this case, the performance of the system will be improved in an erroneous channel, but, on the other hand, it may be decreased in an error-free channel, where it would be advantageous to use as much capacity as possible for speech coding. To classify speech coding methods as error-tolerant methods and methods suitable for a high-quality transmission channel according to the transmission rate is a very coarse simplification, because transmission rate is not the only significant factor. In this connection, however, such a classification will clarify the selection of the speech coding method. According to one embodiment of the invention, the speech coding method is selected according to the erroneousness of the transmission channel: in the case of a high quality transmission channel, a speech coding method is selected in which a major part of the transmission channel capacity is used for speech coding, i.e. the speech coding has a high transmission rate; in the case of a poor quality transmission channel, a speech coding method is selected in which the first channel coding is emphasized more, i.e. the speech coding method has a low transmission rate. The selection can be made by monitoring the quality/erroneousness of the transmission channel when the connection is established. Since the quality of a transmission channel may vary to a great extent during a speech connection, the quality/erroneousness can also be monitored during the speech connection, and if necessary, the speech coding method can be changed.

One of the most significant advantages of the present invention is that it allows new speech coding methods to be added to an existing telecommunications system. In such a case, it is essential that the transmitters and receivers using the new speech coding methods still operate together with the transmitters and receivers which have originally been used in the telecommunications system and in which these new speech coding methods have not been implemented. A telecommunications system of this kind typically comprises various transmitters and receivers which do not employ a uniform group of speech coding methods. However, all transmitters and receivers must be able to use at least one speech coding method which is common to all of them. If, for example, the new system of the invention is provided by planning and realizing a new speech coding method for use on a full-rate GSM transmission channel, the new GSM system will comprise telephones and network elements provided with both the new speech coding method and the method currently in use in the GSM system (i.e. new equipments). In addition, the system will also comprise equipments which have already been used previously and which are provided only with the current speech coding method according to the GSM system (i.e. old equipments). When a new and an old equipment communicate with each other, the speech coding method selected must be the current GSM method, which can be selected in both equipments. Another factor influencing the selection is thus a heterogeneous group of equipments: the speech coding method selected at the beginning of a connection is the most suitable speech coding method which can be selected both in the transmitter and in the receiver. Even in this case, it may be necessary to change the speech coding method during the connection, as the transmitter and receiver may also be changed during one speech connection.

In the description of the invention, it has been stated that the channel encoder **203**, **205** adds error check bits to the speech coding bits. The channel encoder **203**, **205** can, in fact, operate in practice so that the error check bits are added to the speech coding bits generated by the speech encoder in such a manner that the speech coding bits are still visible and unchanged in the resulting bit error which now also includes the channel coding bits. Depending on the channel coding method, the channel encoder **203**, **205** may also operate so that even the speech coding bits are changed when error check bits are added. In this case, the channel decoder **301**, **303** restores the speech coding bits at channel decoding if the number of errors received from the channel does not exceed the error correction capability of the channel coding. In view of the present invention, there is no difference between these two methods, and the expression “the channel encoder adds error check bits to the speech coding bits” refers to both these cases, since, from the point of view of speech coding and the transmission rate, this is exactly what happens.

In a telecommunications system, a speech signal is often also subjected to other operations, such as encryption, interleaving of the bits to be transmitted (closely connected with channel coding), a possible precoding associated with the modulation method, or bit interleaving in association with spectral shaping of the signal; however, these methods are irrelevant to the present invention. In the present invention, channel coding refers particularly to the use of error-detecting and error-correcting codes. Depending on how the channel coding is implemented, the channel decoder may have available data on the results of demodulation so that it may utilize data on the error probabilities of individual bits, i.e. the so-called soft decisions of the demodulator. It is not relevant to the invention whether soft decisions are available or not, and the channel decoder of the invention covers both cases. In typical implementations, the second channel decoder **301** of the invention has the results of soft decisions available, whereas the first channel decoder **303** does not, but the system of the invention may also be implemented in some other way.

The following is a simple general example of how a new speech coding method is added to a full-rate transmission channel of the GSM mobile telephone system for use in conjunction with the RPE-LTP speech coding method presently in use. The example is given merely to illustrate the invention; it is thus only one possible embodiment, and the invention is not limited to it. In an RPE-LTP speech coding method, a speech signal is divided into frames of 20 ms, of each of which an RPE-LTP speech encoder forms 260 speech coding bits, whereby the transmission rate of the speech coding bits is 13 kbit/s. The channel encoder used on a full-rate GSM speech channel, i.e. the second channel encoder in the system of the invention, adds 196 error coding bits to 260 speech coding bits; the total bit number in one 20 ms frame is thus 456 bits, which corresponds to a total transmission rate of 22.8 kbit/s. In this example, a technically highly advanced speech coding method in which the transmission rate of speech coding bits is 8 kbit/s and the speech signal is divided into frames of 10 ms, each containing 80 bits, is added to a full-rate GSM speech channel. To implement the invention, a first channel coding method must be designed for this speech coding method. A simple exemplary solution for a first channel coding method consists of the following operations, which are described from the point of view of the first channel encoder:

(a) Two speech frames of 80 bits are combined in the first channel encoder into one frame of 160 bits.

(b) 100 error-correcting bits are added to these 160 bits by an error-correcting code known per se. The selection of the code is influenced by both the 8 kbit/s speech coding method employed and the channel coding method of the full-rate GSM channel. This results in a 260-bit speech frame according to a full-rate GSM channel.

(c) The 260 bits generated are classified into three groups according to their importance in view of the channel coding of the full-rate GSM channel.

Thereafter the speech coding bits and the first channel coding bits are supplied to the second channel encoder, which is identical with the channel encoder used in connection with the RPE-LTP. In the receiver, the first channel decoder decodes the first channel encoding.

The figures and the description associated with them are intended merely to illustrate the present invention. In their details, the method, receiver and transmitter of the invention may vary within the scope of the appended claims.

We claim:

1. A method for speech transmission of a speech in a telecommunications system, said method comprising the steps of:

compressing a speech signal of the speech to a small number of speech coding bits by speech coding method,

channel encoding the speech coding bits, and

using, in transmitting the speech as a transmitted signal by a transmitter, N different speech coding methods, all of which operate at different transmission rates **S1**, **S2**, . . . , and SN kbit/s, respectively, where N≧2 and **S1** ≧**S2**≧. . . ≧SN, including:

employing with each speech coding method a first channel encoding method specific for the respective said speech coding method, said first channel encoding method comprising adding error-detecting and error-correcting first channel coding bits to the speech coding bits, and producing a constant transmission rate **S1** which is independent of the speech coding method employed, so that the transmission rate of the first channel coding bits added to the speech coding bits during the first channel encoding its, depending on the speech coding method employed, **0** **S1**–**S2**, . . . , **S1**–SN kbit/s, respectively, and

after the first channel encoding, performing a second channel encoding, in which error-detecting and error-correcting second channel coding bits are added to the signal generated by the first channel encoding, the transmission rate of said second channel coding bits being C kbit/s, whereby, after the second channel encoding, the total transmission rate is a constant **S1**+C kbit/s irrespective of the selected speech encoding method.

2. The method according to claim **1**, further including:

receiving the transmitted signal, including:

performing a second channel decoding for removing the second channel coding bits, which were added by the second channel encoding and the transmission rate of which is C kbit/s, and

performing, after the second channel decoding, a first channel decoding for removing the first channel coding bits added by the first channel encoding, in such a manner that, depending on the speech coding method employed, a transmission rate of **S1**, **S2**, . . . , SN kbit/s, respectively, is provided for the speech coding bits to be supplied to the speech decoding.

3. The method according to claim **1** or **2**, further comprising:

classifying the bits supplied to the second channel coding into several groups according to their importance for error protection in the speech coding method employed, in such a manner that the error correction capability of the second channel coding is directed to the bits that are the most important for each speech coding method and the first channel coding method employed in conjunction with the respective speech coding method.

4. The method according to claim **1** or **2**, wherein:

when a speech connection is established, the speech coding method employed is selected according to the erroneousness of the transmission path in such a way that the more there are transmission errors on the transmission channel, the lower is the transmission rate of the speech coding bits to the first channel encoding from the selected speech coding method, and the higher is the transmission rate of the first channel coding bits.

5. The method according to claim **4**, further comprising:

changing the speech coding method during the speech connection when the erroneousness of the transmission path changes in such a way that the more there are transmission errors on the transmission path, the lower is the transmission rate of the speech coding bits supplied to the first channel encoding from the selected speech coding method.

6. The method according to claim **1** or **2**, in an instance wherein:

a corresponding speech decoding method cannot be selected in all receivers of a plurality of receivers for all the speech coding methods that can be selected in the transmitter, and

a corresponding speech coding method cannot be selected in all transmitters of a plurality of transmitters for all the speech decoding methods that can be selected in the different receivers, and

said method further comprising:

when a speech connection is established, the speech coding method employed is selected by means of signalling between the respective transmitter and the respective receiver so that the speech coding method selected is a speech coding method which can be selected both in the respective transmitter and in the respective receiver.

7. The method according to claim **1** or **2**, in an instance wherein:

a corresponding speech decoding method cannot be selected in all receivers of a plurality of receivers for all the speech coding method which can be selected in all transmitters of a plurality of transmitters, and

a corresponding speech coding method cannot be selected in all of the transmitters for all the speech decoding methods which can be selected in all of the receivers, and

said method further comprising:

manually selecting the speech coding method employed before a speech connection is established in such a way that the speech coding method selected is a speech coding method which can be selected both in the respective transmitter and in the respective receiver.

8. The method according to claim **1**, further comprising:

carrying out the first channel encoding in more than one step, and

the second channel encoding being the same in the case of all speech coding methods.

9. A transmitter apparatus for a telecommunications system transmitting digital speech on a transmission channel, said apparatus comprising:

speech means for coding a speech signal by a speech coding method to provide a speech encoded signal,

channel encoding means for channel-encoding the speech-encoded signal to a signal whose transmission rate is equal to a total transmission rate on the transmission channel,

the speech encoding means employing two or more speech coding methods, which provide speech-encoded signals have mutually different transmission rates (**S1**, **S2**, . . . , SN),

the channel encoding means being arranged to provide the channel encoding in two steps comprising

first channel encodings which are specific for each speech encoding method and which, from the encoded speech signals having different transmission rates, generate first channel-encoded signals having a same constant transmission rate (**S1**) which is independent of the speech coding method, and

a second channel encoding which is independent of the speech coding method and which, from a selected first channel-encoded signal, generates a second channel-encoded signal having a constant transmission rate (**S1**+C) which is independent of the speech coding method and which is the same as said total transmission rate.

10. The transmitter apparatus according to claim **9**, comprising:

means for selecting the speech encoding method and the first channel encoding, and for switching the signal produced by the selected speech encoding method and first channel encoding to the second channel encoding.

11. The method according to claim **10**, wherein:

said means for selecting are arranged to be controlled on the basis of the erroneousness of the transmission path, or on the basis of signalling between the transmitter apparatus and a receiver apparatus, or manually.

12. A receiver apparatus in a telecommunications system transmitting digital speech on a telecommunications channel at a total transmission rate, comprising:

channel decoding means for decoding a received channel-coded speech signal,

speech decoding means for speech-decoding a channel-decoded speech signal by a speech decoding method,

the channel decoding means being arranged to provide channel decoding two steps comprising:

a second channel decoding which is independent of the speech coding method and which, from said received channel-encoded speech signal, sharing a constant transmission rate (**S1**+C), which is independent of the speech coding method and is the same as the total transmission rate used in the telecommunications channel, produces a first signal having a lower constant transmission rate (**S1**) which is independent of the speech coding method, and

first channel decodings which are specific for each speech coding method and which channel-decode said first signal, producing encoded speech signals which are specific for each speech coding method and which have mutually different transmission rates (**S1**, **S2**, . . . , **S3**), and

the speech decoding means employ two or more speech decoding methods for decoding said speech-coded speech signals produced by two or more speech encoding methods and having mutually different transmission rates (**S1**, **S2**, . . . , SN).

13. The receiver apparatus according to claim **12**, comprising:

means for selecting the speech decoding method employed and the first channel decoding specific for the selected speech decoding method, and for switching the signal produced by the second channel decoding (**301**) to the selected speech decoding method and selected first channel decoding method.

14. The receiver apparatus according to claim **13**, wherein:

the selection means are arranged to be controlled on the basis of the erroneousness of the transmission path, or on the basis of signalling between a transmitter apparatus and the receiver apparatus, or manually.

* * * * *

EXHIBIT G

US005946651A

United States Patent [19]

Jarvinen et al.

[11] **Patent Number: 5,946,651**

[45] **Date of Patent: Aug. 31, 1999**

[54] **SPEECH SYNTHESIZER EMPLOYING POST-PROCESSING FOR ENHANCING THE QUALITY OF THE SYNTHESIZED SPEECH**

[75] Inventors: **Kari Jarvinen**; **Tero Honkanen**, both of Tampere, Finland

[73] Assignee: **Nokia Mobile Phones**, Salo, Finland

[21] Appl. No.: **09/135,936**

[22] Filed: **Aug. 18, 1998**

Related U.S. Application Data

[63] Continuation of application No. 08/662,991, Jun. 13, 1996.

[51] **Int. Cl.**^{6} **G10L 9/14**

[52] **U.S. Cl.** **704/223**; 704/208; 704/219; 704/220; 704/222

[58] **Field of Search** 704/200, 207, 704/223, 219, 221, 222, 220, 208

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,815,135	3/1989	Taguchi	381/37
4,969,192	11/1990	Chen et al.	381/31
5,029,211	7/1991	Ozawa	704/207
5,241,650	8/1993	Gerson et al.	704/200
5,247,357	9/1993	Israelsen	358/133
5,327,520	7/1994	Chen	704/219
5,327,521	7/1994	Savic et al.	704/272
5,414,796	5/1995	Jacobs et al.	704/221
5,444,816	8/1995	Adoul et al.	395/2.28
5,483,668	1/1996	Malkamaki et al.	455/33.2
5,495,555	2/1996	Swamiathan	704/207
5,506,934	4/1996	Kawama	395/267
5,651,091	7/1997	Chen	395/2.32
5,664,055	9/1997	Kroon	704/223

FOREIGN PATENT DOCUMENTS

0 030 390A1	6/1981	European Pat. Off. .
0 333 425A2	9/1989	European Pat. Off. .
0 459 358A2	12/1991	European Pat. Off. .
WO 91/06091	5/1991	WIPO .

Primary Examiner—David R. Hudspeth
Assistant Examiner—Vijay B. Chawan
Attorney, Agent, or Firm—Perman & Green, LLP

[57] **ABSTRACT**

A post-processor **317** and method substantially for enhancing synthesised speech is disclosed. The post-processor **317** operates on a signal ex(n) derived from an excitation generator **211** typically comprising a fixed code book **203** and an adaptive code book **204**, the signal ex(n) being formed from the addition of scaled outputs from the fixed code book **203** and adaptive code book **204**. The post-processor operates on ex(n) by adding to it a scaled signal pv(n) derived from the adaptive code book **204**. A gain or scale factor p is determined by the speech coefficients input to the excitation generator **211**. The combined signal ex(n)+pv(n) is normalised by unit **316** and input to an LPC or speech synthesis filter **208**, prior to being input to an audio processing unit **209**.

46 Claims, 7 Drawing Sheets

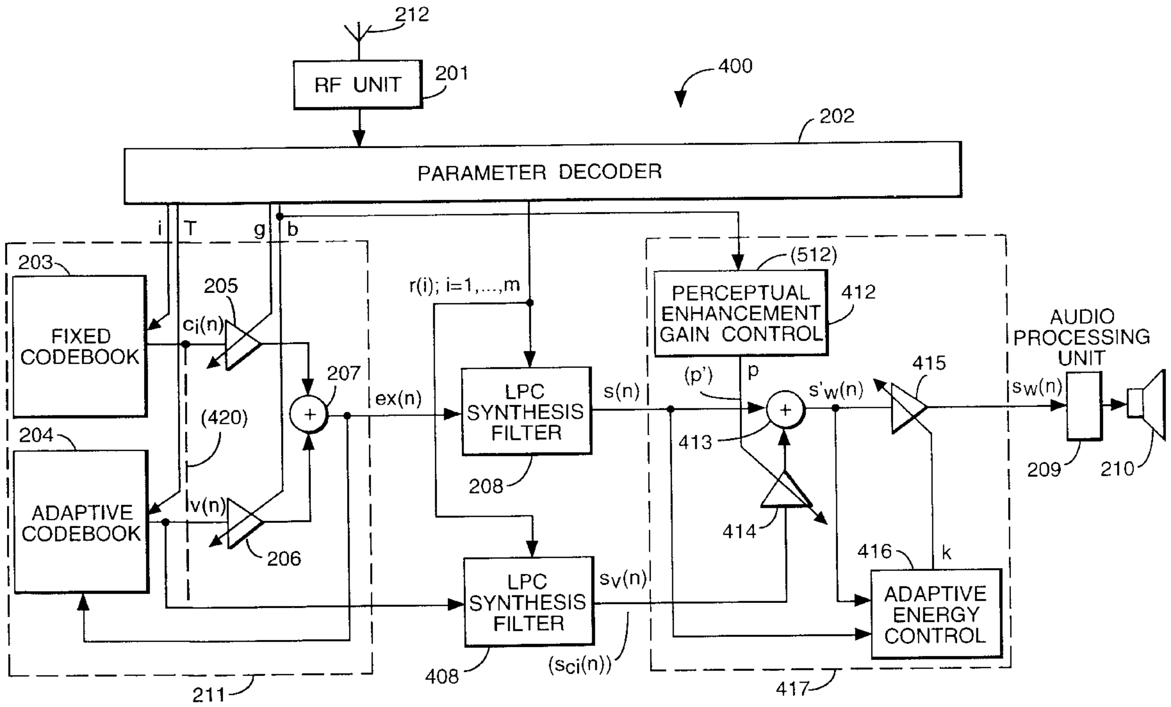


Fig. 1.
PRIOR ART

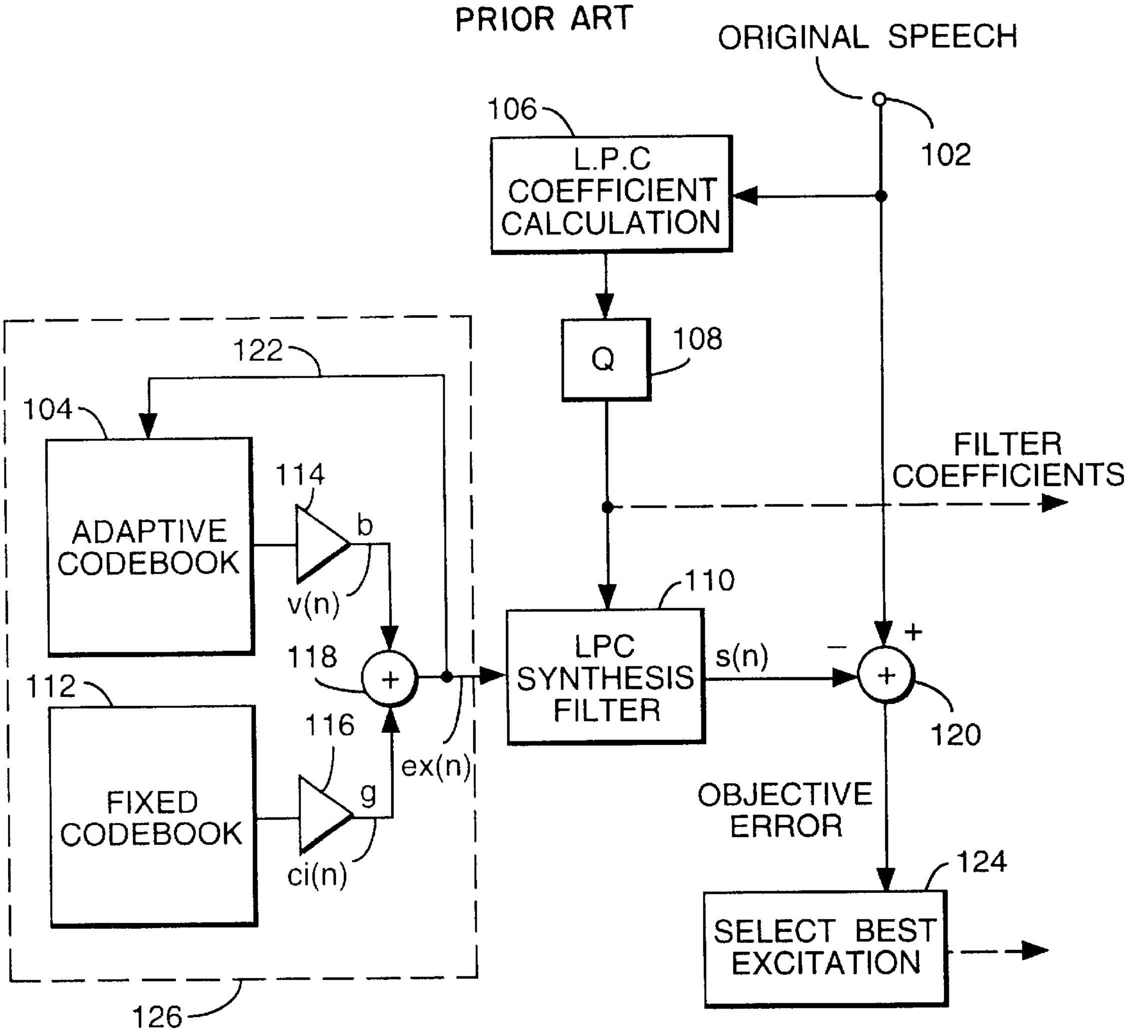


Fig.2. PRIOR ART

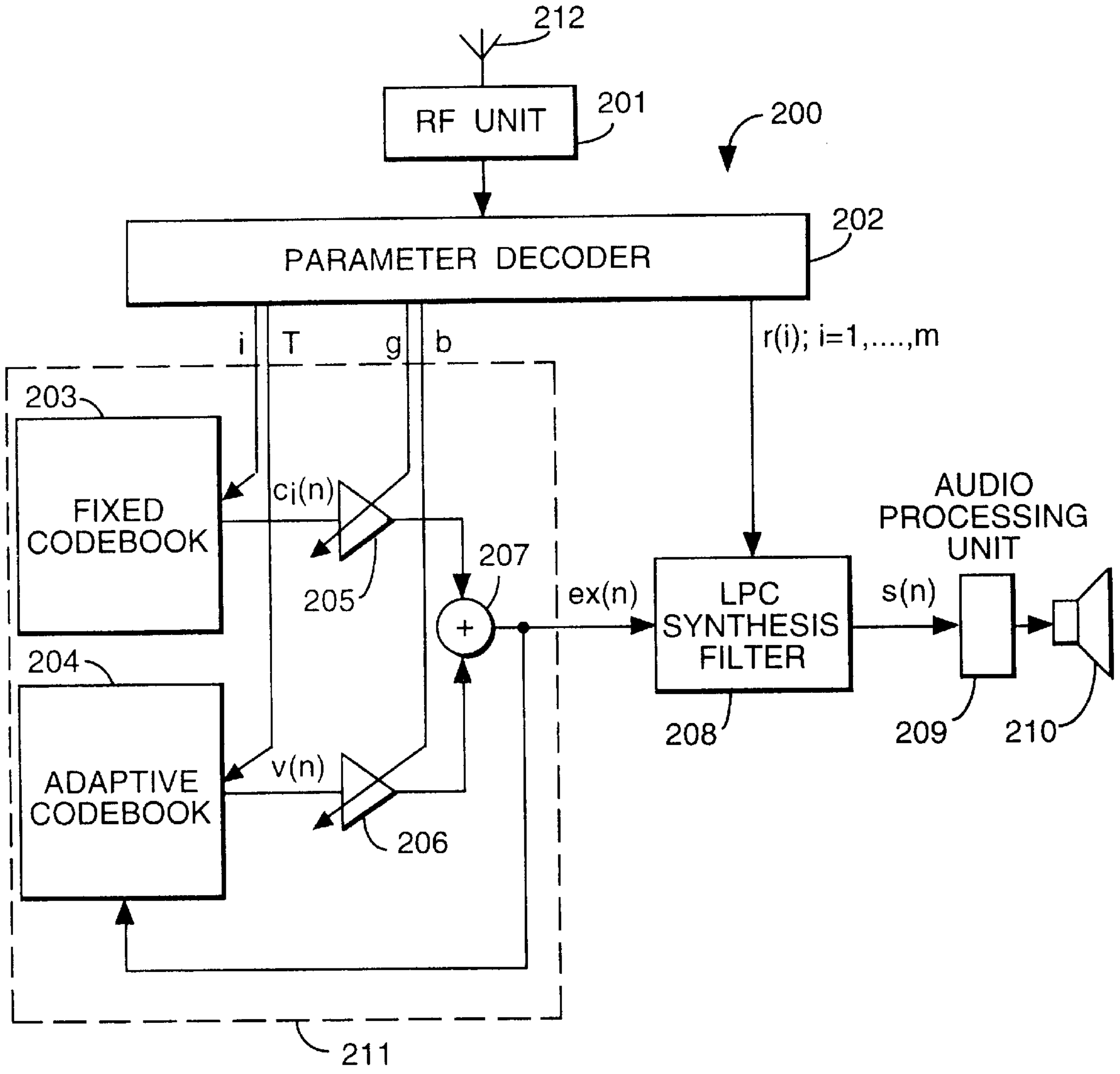


Fig.3.

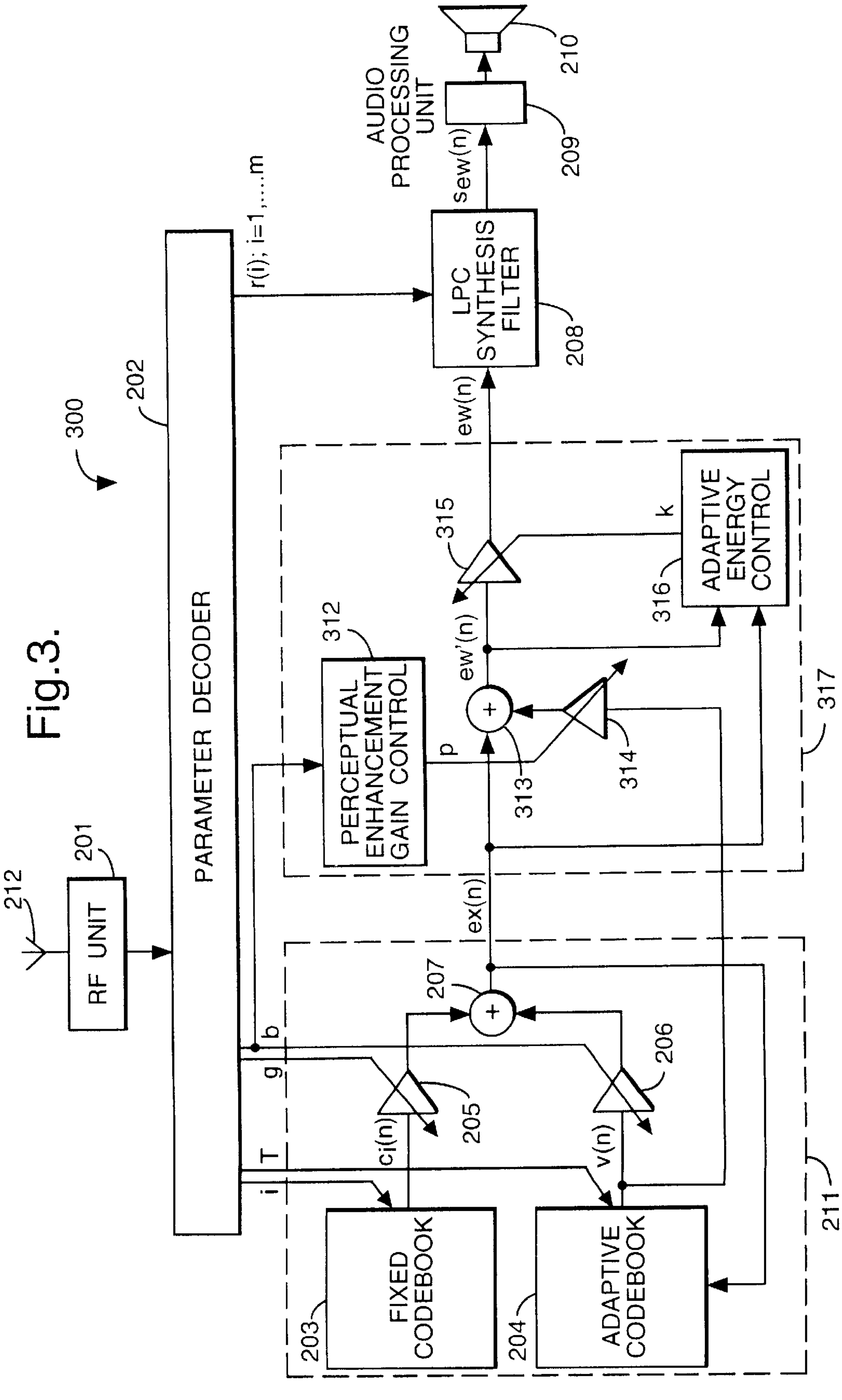

300
212
201
RF UNIT
202
PARAMETER DECODER
r(i); i=1,...,m
LPC SYNTHESIS FILTER
208
sew(n)
AUDIO PROCESSING UNIT
209
210
ew(n)
315
k
ADAPTIVE ENERGY CONTROL
316
ew'(n)
312
PERCEPTUAL ENHANCEMENT GAIN CONTROL
p
313
314
317
ex(n)
207
b
g
T
i
205
206
ci(n)
v(n)
FIXED CODEBOOK
203
ADAPTIVE CODEBOOK
204
211

Fig.4.

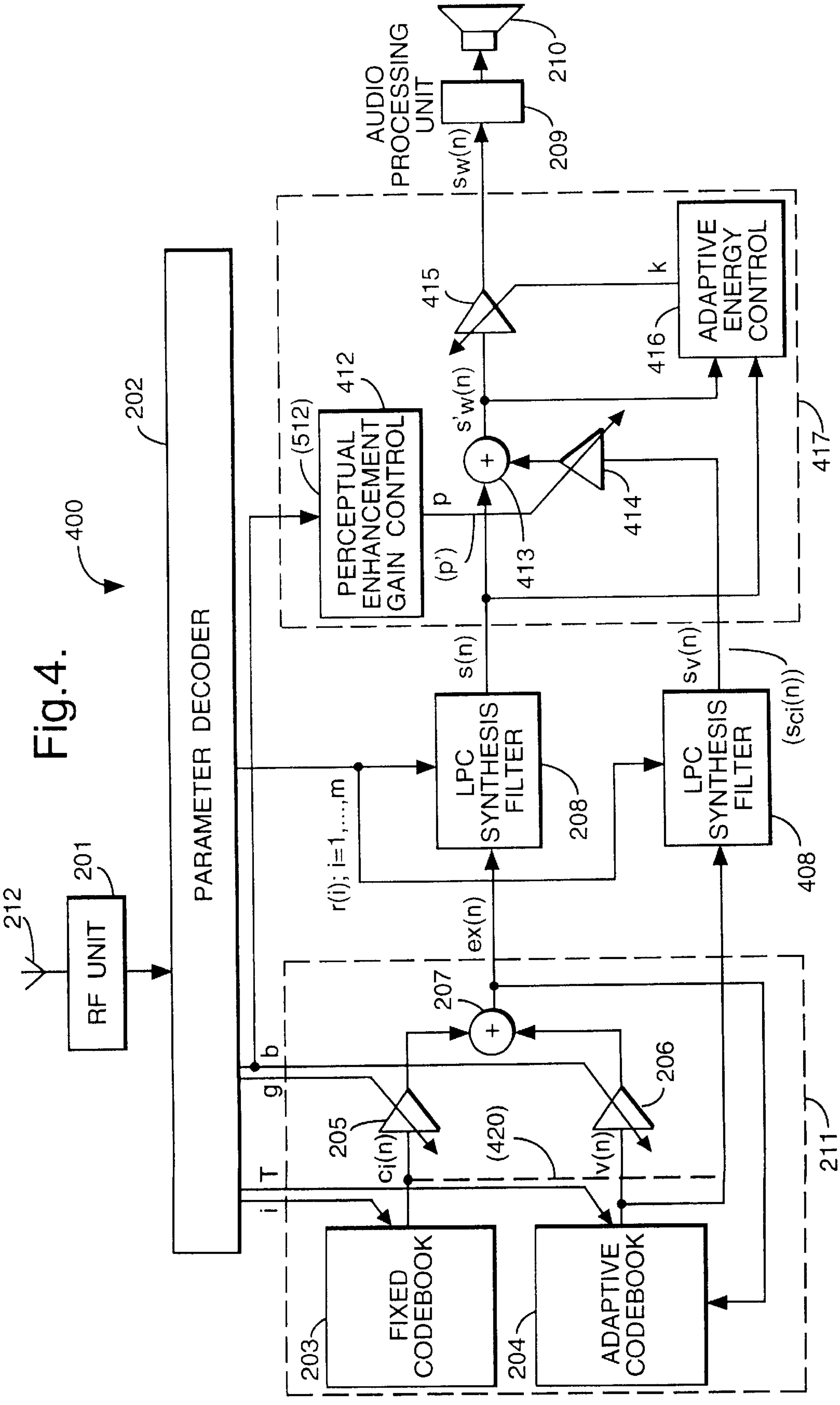

400
212
RF UNIT
201
PARAMETER DECODER
202
i
T
g
b
FIXED CODEBOOK
203
ADAPTIVE CODEBOOK
204
ci(n)
205
lv(n)
206
(420)
207
211
ex(n)
r(i); i=1,...,m
LPC SYNTHESIS FILTER
208
LPC SYNTHESIS FILTER
408
s(n)
sv(n)
(sci(n))
PERCEPTUAL ENHANCEMENT GAIN CONTROL
412
(512)
p
(p')
413
414
s'w(n)
415
k
ADAPTIVE ENERGY CONTROL
416
417
sw(n)
AUDIO PROCESSING UNIT
209
210

Fig.5.

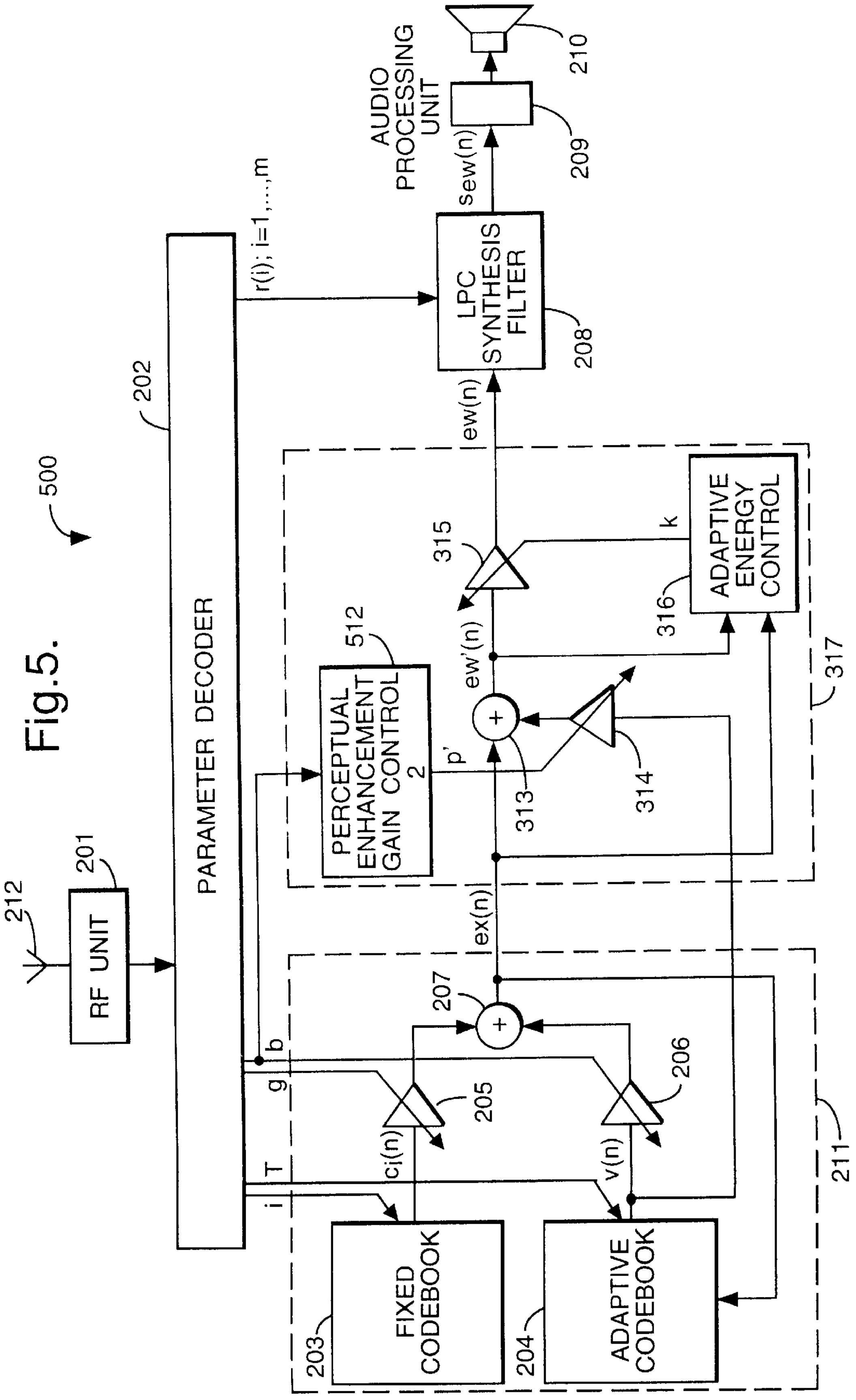

500
212
RF UNIT
201
PARAMETER DECODER
202
r(i); i=1,...,m
LPC SYNTHESIS FILTER
208
sew(n)
AUDIO PROCESSING UNIT
209
210
ew(n)
315
k
ADAPTIVE ENERGY CONTROL
316
317
ew'(n)
512
PERCEPTUAL ENHANCEMENT GAIN CONTROL 2
p'
313
314
ex(n)
207
b
g
T
i
205
206
ci(n)
v(n)
FIXED CODEBOOK
203
ADAPTIVE CODEBOOK
204
211

Fig.6.

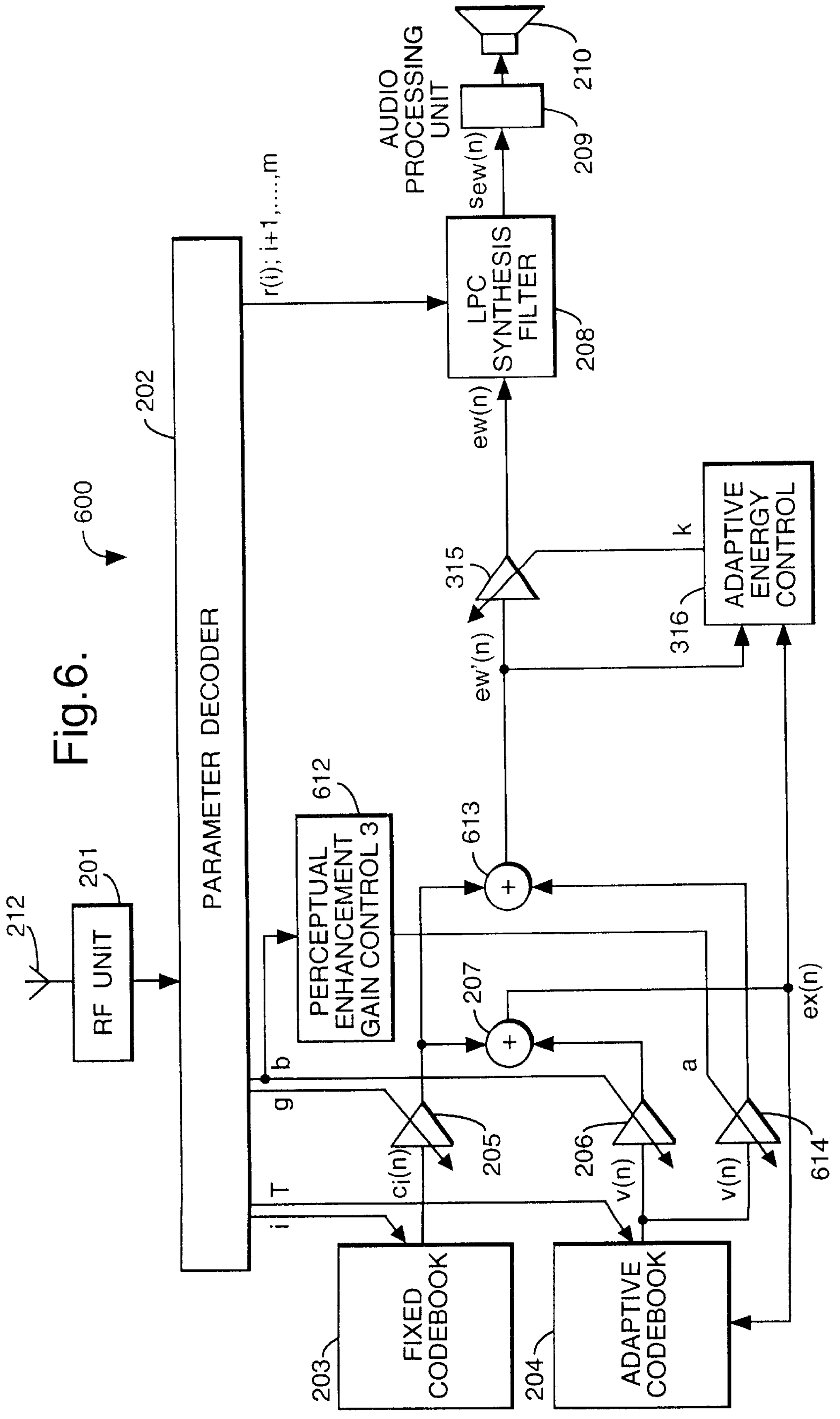
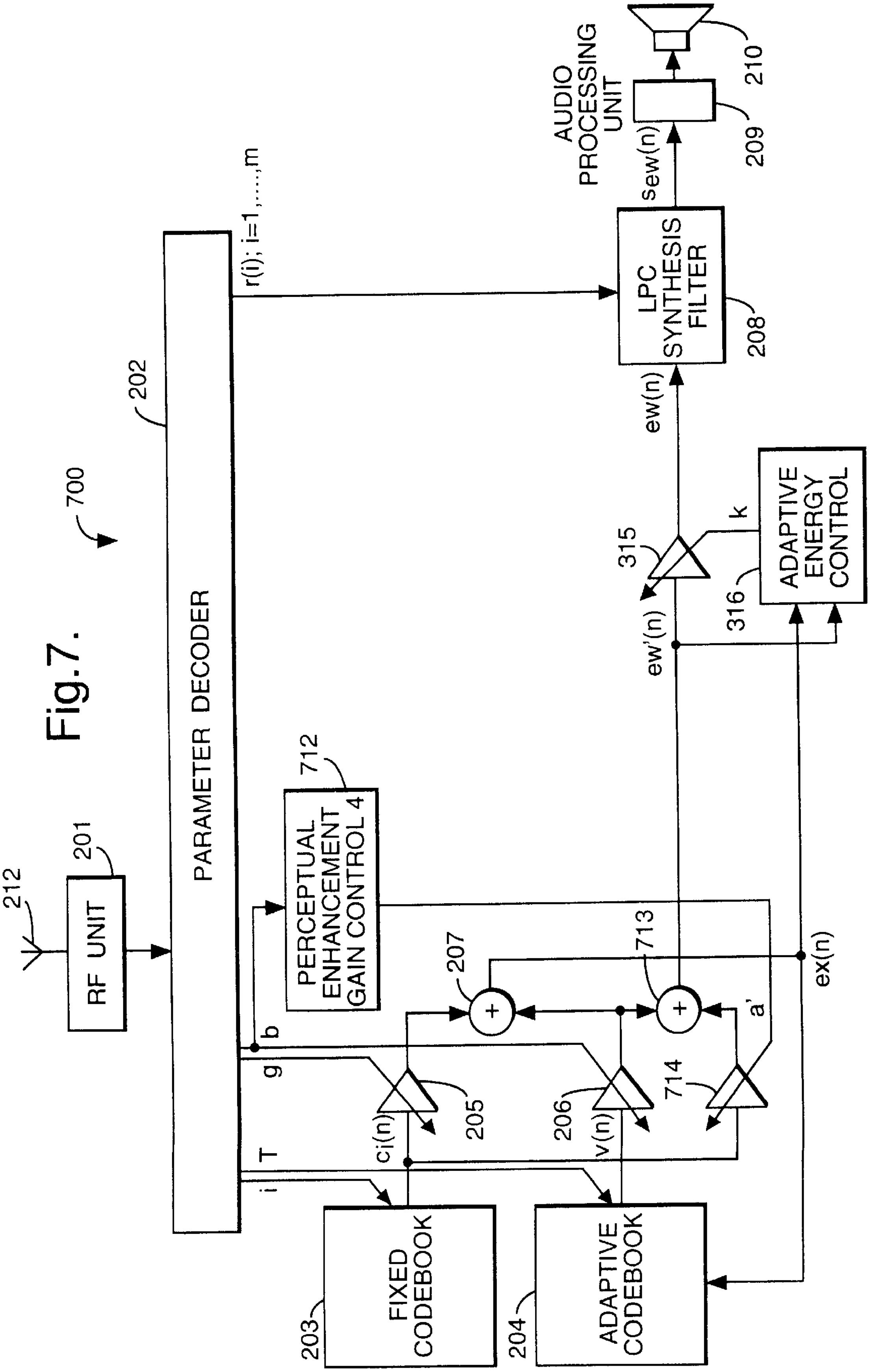

600
212
RF UNIT
201
PARAMETER DECODER
202
r(i); i+1,....,m
LPC SYNTHESIS FILTER
208
sew(n)
AUDIO PROCESSING UNIT
209
210
ew(n)
315
k
ADAPTIVE ENERGY CONTROL
316
ew'(n)
613
+
612
PERCEPTUAL ENHANCEMENT GAIN CONTROL 3
207
+
ex(n)
b
g
T
i
a
205
206
614
$c_i(n)$
v(n)
v(n)
FIXED CODEBOOK
203
ADAPTIVE CODEBOOK
204

Fig.7.


700
212
RF UNIT
201
PARAMETER DECODER
202
r(i); i=1,....,m
LPC SYNTHESIS FILTER
208
sew(n)
AUDIO PROCESSING UNIT
209
210
ew(n)
315
k
ADAPTIVE ENERGY CONTROL
316
ew'(n)
PERCEPTUAL ENHANCEMENT GAIN CONTROL 4
712
207
713
+
+
a'
ex(n)
b
g
T
i
205
206
714
c(n)
v(n)
FIXED CODEBOOK
203
ADAPTIVE CODEBOOK
204

SPEECH SYNTHESIZER EMPLOYING POST-PROCESSING FOR ENHANCING THE QUALITY OF THE SYNTHESIZED SPEECH

This application is a continuation of copending U.S. patent application Ser. No. 08/662,991, filed Jun. 13, 1996, which in turn claims priority from U.K. Patent Application No.: 9512284, filed on Jun. 15, 1995 (as does this continuation application).

FIELD OF INVENTION

The present invention relates to an audio or speech synthesiser for use with compressed digitally encoded audio or speech signals. In particular, to a post-processor for processing signals derived from an excitation code book and adaptive code book of a LPC type speech decoder.

BACKGROUND TO INVENTION

In digital radio telephone systems the information, i.e. speech, is digitally encoded prior to being transmitted over the air. The encoded speech is then decoded at the receiver. First, an analogue speech signal is digitally encoded using Pulse Code Modulation (PCM) for example. Then speech coding and decoding of the PCM speech (or original speech) is implemented by speech coders and decoders. Due to the increase in use of radio telephone systems the radio spectrum available for such systems is becoming crowded. In order to make the best possible use of the available radio spectrum, radio telephone systems utilise speech coding techniques which require low numbers of bits to encode the speech in order to reduce the bandwidth required for the transmission. Efforts are continually being made to reduce the number of bits required for speech coding to further reduce the bandwidth required for speech transmission.

A known speech coding/decoding method is based on linear predictive coding (LPC) techniques, and utilises analysis-by-synthesis excitation coding. In an encoder utilising such a method, a speech sample is first analysed to derive parameters which represent characteristics such as wave form information (LPC) of the speech sample. These parameters are used as inputs to short-term synthesis filter. The short-term synthesis filter is excited by signals which are derived from a code book of signals. The excitation signals may be random, e.g. a stochastic code book, or may be adaptive or specifically optimised for use in speech coding. Typically, the code book comprises two parts, a fixed code book and the adaptive code book. The excitation outputs of respective code books are combined and the total excitation input to the short term synthesis filter. Each total excitation signal. is filtered and the result compared with the original speech sample (PCM coded) to derive an "error" or difference between the synthesised speech sample and the original speech sample. The total excitation which results in the lowest error is selected as the excitation for representing the speech sample. The code book indices, or addresses, of the location of respective partial optimal excitation signals in the fixed and adaptive code book are transmitted to a receiver, together with the LPC parameters or coefficients. A composite code book identical to that at the transmitter is also located at the receiver, and the transmitted code book indices and parameters are used to generate the appropriate total excitation signal from the receiver's code book. This total excitation signal is then fed to a short-term synthesis filter identical to that in the transmitter, and having the transmitted LPC coefficients as respective inputs. The output from the short-term synthesis filter is a synthesised speech frame which is the same as that generated in the transmitter by the analysis-by-synthesis method.

Due to the nature of digital coding, although the synthesised speech is objectively accurate it sounds artificial. Also, degradations, distortions and artifacts are introduced into the synthesised speech due to quantisation effects and other anomalies due to the electronic processing. Such artifacts particularly occur in low bit-rate coding since there is insufficient information to reproduce the original speech signal exactly. Hence there have been attempts to improve the perceptual quality of synthesised speech. This has been attempted by the use of post-filters which operate on the synthesised speech sample to enhance its perceived quality. Known post-filters are located at the output of the decoder and process the synthesised speech signal to emphasise or attenuate what are generally considered to be the most important frequency regions in speech. The importance of respective regions of speech frequencies has been analysed primarily using subjective tests on the quality of the resulting speech signal to the human ear. Speech can be split into two basic parts, the spectral envelope (formant structure) or the spectral harmonic structure (line structure), and typically post-filtering emphasises one or other, or both of these parts of a speech signal. The filter coefficients of the post-filter are adapted depending on the characteristics of the speech signal to match the speech sounds. A filter emphasising or attenuating the harmonic structure is typically referred to as a long-term, or pitch or long delay post filter, and a filter emphasising the spectral envelope structure is typically referred to as a short delay post filter or short-term post filter. A further known filtering technique for improving the perceptual quality of synthesised speech is disclosed in International Patent Application WO 91/06091. A pitch prefilter is disclosed in WO 91/06091 comprising a pitch enhancement filter, normally disposed at a position after a speech synthesis or LPC filter, moved to a position before the speech synthesis or LPC filter where it filters pitch information contained in the excitation signals input to the speech synthesis or LPC filter. However, there is still a desire to produce synthesised speech which has even better perceptual quality.

SUMMARY OF INVENTION

According to a first aspect of the present invention there is provided a synthesiser for speech synthesis, comprising a post-processing means for operating on a first signal including speech periodicity information and derived from an excitation source, wherein the post-processing means is adapted to modify the speech periodicity information content of the first signal in accordance with a second signal derivable from the excitation source.

According to a second aspect of the present invention there is provided a method for enhancing synthesised speech, comprising

deriving a first signal including speech periodicity information from an excitation source,

deriving a second signal from the excitation source, and

modifying the speech periodicity information content of the first signal in accordance with the second signal.

An advantage of the present invention is that the first signal is modified by a second signal originating from the same source as the first signal, and thus no additional sources of distortion or artifacts such as extra filters are introduced. Only the signals generated in the excitation source are utilised. The relative contributions of the signals inherent to the excitation generator in a speech synthesiser are being modified, with no artificial added signals, to re-scale the synthesiser signals.

Good speech enhancement may be obtained if post-processing of the excitation is based on modifying the relative contributions of the excitation components derived within the excitation generator of the speech synthesiser itself.

Processing the excitation by filtering the total excitation ex(n) without considering or modifying the relative contributions of the signals inherent to the excitation generator, i.e. v(n) and c_i(n) typically does not give the best possible enhancement. Modifying the first signal in accordance with the second signal from the same excitation source increases waveform continuity within the excitation and in the resulting synthesised speech signal, thereby improving its perceptual quality.

In a preferred embodiment the excitation source comprises a fixed code book and an adaptive code book, the first signal being derivable from a combination of first and second partial excitation signals respectively selectable from the fixed and adaptive code books, which is a particularly convenient excitation source for a speech synthesiser.

Preferably, there is a gain element for scaling the second signal in accordance with a scaling factor (p) derivable from pitch information associated with the first signal from the excitation source, which has the advantage that the first signal speech periodicity information content is modified which has greater effect on perceived speech quality than other modifications.

Suitably, the scaling factor (p) is derivable from an adaptive code book scaling factor (b), and the scaling factor (p) is derivable in accordance with the following equation,

$$\text{if}\quad\begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \le b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \vdots \\ TH_{N-1} \le b \le TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, b is the adaptive code book gain factor, p is the post-processor means scale factor, a_{snh} is a linear scaler and f(b) is a function of gain b

In a specific embodiment the scaling factor (p) is derivable in accordance with

$$\mathit{if}\quad\begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b \le TH_{upper} & \text{then } p = a_{enh} b^2 \\ b > TH_{upper} & \text{then } p = a_{enh} b \end{array}$$

where a_{enh} is a constant that controls the strength of the enhancement operation, b is adaptive code book gain, TH are threshold values and p is the post-processor scale factor which utilises the insight that speech enhancement is most effective for voiced speech where b typically has a high value, whereas for unvoiced sounds where b has a low value a not so strong enhancement is required.

The second signal may originate from the adaptive code book, and may also be substantially the same as the second partial excitation signal. Alternatively, the second signal may originate from the fixed code book, and may also be substantially the same as the first partial excitation signal.

For the second signal originating from the fixed code book, the gain control means is adapted to scale the second signal in accordance with a second scaling factor (p')

where,

$$p' = -\frac{gp}{(p+b)}$$

and g is a fixed code book scaling factor, b is an adaptive code book scaling factor and p is the first scaling factor.

The first signal may be a first excitation signal suitable for inputting to a speech synthesis filter, and the second signal may be a second excitation signal suitable for inputting to a speech synthesis filter. The second excitation signal may be substantially the same as the second partial excitation signal.

Optionally, the first signal may be a first synthesised speech signal output from a first speech synthesis filter and derivable from the first excitation signal, and the second signal may be the output from a second speech synthesis filter and derivable from the second excitatiori signal. An advantage of this is that speech enhancement is carried out on the actual synthesised speech and thus there are less electronic components to introduce distortion to the signal before it is rendered audible.

Advantageously, there is provided an adaptive energy control means adapted to scale a modified first signal in accordance with the following relationship,

$$k = \sqrt{\frac{\sum_{n=0}^{N-1} ex^2(n)}{\sum_{n=0}^{N-1} ew'^2(n)}}$$

where N is a suitably chosen adaption period, ex(n) is the first signal, ew'(n) is the modified first signal and k is an energy scale factor. which normalises the resulting enhanced signal to the power input to the speech synthesiser.

In a third aspect according to the invention there is provided, a radio device, comprising

a radio frequency means for receiving a radio signal and recovering coded information included in the radio signal, and

an excitation source coupled to the radio frequency means for generating a first signal including speech periodicity information in accordance with the coded information, wherein the radio device further comprises a post-processing means operably coupled to the excitation source to receive the first signal and adapted to modify the speech periodicity information content of the first signal in accordance with a second signal derived from the excitation source and a speech synthesis filter coupled to receive the modified first signal from the post-processing means and for generating synthesised speech in response thereto.

In a fourth aspect of the invention there is provided a synthesiser for speech synthesis, comprising first and second excitation sources for respectively generating first and second excitation signals, and modifying means for modifying the first excitation signal in accordance with a scaling factor derivable from pitch information associated with the first excitation signal.

In a fifth aspect of the invention there is provided a synthesiser for speech synthesis, comprising first and second excitation sources for respectively generating first and second excitation signals, and modifying means for modifying the second excitation signal in accordance with a scaling factor derivable from pitch information associated with the first excitation signal.

The fourth and fifth aspects of the invention advantageously integrate scaling of excitation signals within the excitation generator itself.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows a schematic diagram of a known Code Excitation Linear Prediction (CELP) encoder;

FIG. **2** shows a schematic diagram of a known CELP decoder;

FIG. **3** shows a schematic diagram of a CELP decoder in accordance with a first embodiment of the invention;

FIG. **4** shows a second embodiment in accordance with the invention;

FIG. **5** shows a third embodiment in accordance with the invention;

FIG. **6** shows a fourth embodiment in accordance with the invention; and

FIG. **7** shows a fifth embodiment in accordance with the invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

Embodiments in accordance with the invention will now be described, by way of example only, and with reference to the accompanying drawings.

A known CELP encoder **100** is shown in FIG. **1**. Original speech signals are input to the encoder at **102** and Long Term Prediction (LTP) coefficients T,b are determined using adaptive code book **104**. The LTP prediction coefficients are determined for segments of speech typically comprising 40 samples and are 5 ms in length. The LTP coefficients relate to periodic characteristics of the original speech. This includes any periodicity in the original speech and not just to periodicity which corresponds to the pitch of the original speech due to vibrations in the vocal cords of a person uttering the original speech.

Long Term Prediction is performed using adaptive code book **104** and gain element **114**, which comprise a part of excitation signal (ex(n)) generator **126** shown dotted in FIG. **1**. Previous excitation signals ex(n) are stored in the adaptive code book **104** by virtue of feedback loop **122**. During the LTP process the adaptive code book is searched by varying an address T, known as a delay or lag, pointing to previous excitation signals ex(n). These signals are sequentially output and amplified at gain element **114** with a scaling factor b to form signals v(n) prior to being added at **118** to an excitation signal $c_i(n)$ derived from the fixed code book **112** and scaled by a factor g at gain element **116**. Linear Prediction Coefficients (LPC) for the speech sample are calculated at **106**. The LPC coefficients are then quantised at **108**. The quantised LPC coefficients are then available for transmission over the air and to be input to short term filter **110**. The LPC coefficients (r(i), i=1 . . . , m where m is prediction order) are calculated for segments of speech comprising 160 samples over 20 ms. All further processing is typically performed in segments of 40 samples, that is to say an excitation frame length of 5 ms. The LPC coefficients relate to the spectral envelope of the original speech signal.

Excitation generator **126** effectively comprises a composite code book **104, 112** comprising sets of codes for exciting short term synthesis filter **110**. The codes comprise sequences of voltage amplitudes, each corresponding to a speech sample in the speech frame.

Each total excitation signal ex(n) is input to short term or LPC synthesis filter **110** to form a synthesised speech sample s(n). The synthesised speech sample s(n) is input to a negative input of adder **120**, having an original speech sample as a positive input. The adder **120** outputs the difference between the original speech sample and the synthesised speech sample, this difference being known as an objective error. The objective error is input to a best excitation selection element **124**, which selects the total excitation ex(n) resulting in a synthesised speech frame s(n) having the least objective error. During the selection the objective error is typically further spectrally weighted to emphasise those spectral regions of the speech signal important for human perception. The respective adaptive and fixed code book parameters (gain b and delay T, and gain g and index i) giving the best excitation signal ex(n) are then transmitted, together with the LPC filter coefficients r(i), to a receiver to be used in synthesising the speech frame to reconstruct the original speech signal.

A decoder suitable for decoding speech parameters generated by an encoder as described with reference to FIG. **1** is shown in FIG. **2**. Radio frequency unit **201** receives a coded speech signal via an antenna **212**. The received radio frequency signal is down converted to a baseband frequency and demodulated in the RF unit **201** to recover speech information. Generally, coded speech is further encoded prior to being transmitted to comprise channel coding and error correction coding. This channel coding and error correction coding has to be decoded at the receiver before the speech coding can be accessed or recovered. Speech coding parameters are recovered by parameter decoder **202**.

The speech coding parameters in LPC speech coding are the set of LPC synthesis filter coefficients r(i); i=1 . . . ,m, (where m is the order of the prediction), fixed code book index i and gain g. The adaptive code book speech coding parameters delay T and gain b are also recovered.

The speech decoder **200** utilises the above mentioned speech coding parameters to create from the excitation generator **211** an excitation signal ex(n) for inputting to the LPC synthesis filter **208** which provides a synthesised speech frame signal s(n) at its output as a response to the excitation signal ex(n). The synthesised speech frame signal s(n) is further processed in audio processing unit **209** and rendered audible through an appropriate audio transducer **210**.

In typical linear predictive speech decoders, the excitation signal ex(n) for the LPC synthesis filter **208** is formed in excitation generator **211** comprising a fixed code book **203** generating excitation sequence $c_i(n)$ and adaptive code book **204**. The location of the code book excitation sequence ex(n) in the respective code books **203**, **204** is indicated by the speech coding parameter i and delay T. The fixed code book excitation sequence $c_i(n)$ partially used to form the excitation signal ex(n) is taken from the fixed excitation code book **203** from a location indicated by index i and is then suitably scaled by the transmitted gain factor g in the scaling unit **205**. Similarly, the adaptive code book excitation sequence v(n) also partially used to form excitation signal ex(n) is taken from the adaptive code book **204** from a location indicated by delay T using selection logic inherent to the adaptive code book and is then suitably scaled by the transmitted gain factor b in scaling unit **206**.

The adaptive code book **204** operates on the fixed code book excitation sequence $c_i(n)$ by adding a second partial excitation component v(n) to the code book excitation sequence g $c_i(n)$. The second component is derived from past excitation signals in a manner already described with reference to FIG. **1**, and is selected from the adaptive code book **204** using selection logic suitably included in the adaptive code book. The component v(n) is suitably scaled in the scaling unit **206** by the transmitted adaptive code book gain b and then added to g $c_i(n)$ in the adder **207** to form the total excitation signal ex(n), where

$$\text{ex(n)}=g\ c_i(n)+b\ v(n). \tag{1}$$

The adaptive code book **204** is then updated by using the total excitation signal ex(n).

The location of the second partial excitation component v(n) in the adaptive code book **204** is indicated by the speech coding parameter T. The adaptive excitation component is selected from the adaptive code book using speech coding parameter T and selection logic included in the adaptive code book.

An LPC speech synthesis decoder **300** in accordance with the invention is shown in FIG. **3**. The operation of speech synthesis according to FIG. **3** is the same as for FIG. **2** except that the total excitation signal ex(n) is, prior to being used as the excitation for the LPC synthesis filter **208**, processed in excitation post-processing unit **317**. The operation of circuit elements **201** to **212** in FIG. **3** are similar to those in FIG. **2** with the same numerals.

In accordance with an aspect of the invention, a post-processing unit **317** for the total excitation ex(n) is used in the speech decoder **300**. The post-processing unit **317** comprises an adder **313** for adding a third component to the total excitation ex(n). A gain unit **315** then appropriately scales the resulting signal ew'(n) to form signal ew(n) which is then used to excite the LPC synthesis filter **208** to produce synthesised speech signal $s_{ew}(n)$. The speech synthesised according to the invention has improved perceptual quality compared to the speech signal s(n) synthesised by the prior art speech synthesis decoder shown in FIG. **2**.

The post-processing unit **317** has the total excitation ex(n) input to it, and outputs a perceptually enhanced total excitation ew(n). The post-processing unit **317** also has. the adaptive code book gain b, and an unscaled partial excitation component v(n) taken from the adaptive code book **204** at a location indicated by the speech coding parameters as further inputs. Partial excitation component v(n) is suitably the same component which is employed inside the excitation generator **211** to form the second excitation component bv(n) which is added to the scaled code book excitation $gc_i(n)$ to form the total excitation ex(n). By using an excitation sequence which is derived from the adaptive code book **204**, no further sources of artifacts are added to the speech processing electronics, as is the case with the known post or pre-filter techniques which use extra filters. The excitation post-processing unit **317** also comprises scaling unit **314** which scales the partial excitation component v(n) by a scale factor p, and the scaled component pv(n) is added by adder **313** to the total excitation component ex(n). The output of adder **313** is an intermediate total excitation signal ew'(n). it is of the form,

$$ew'(n)=gc_i(n)+bv(n)+pv(n)=gc_i(n)+(b+p)\ v(n). \tag{2}$$

The scaling factor p for scaling unit **314** is determined in the perceptual enhancement gain control unit **312** using the adaptive code book gain b. The scaling factor pre-scales the contribution of the two excitation components from the fixed and adaptive code book, $c_i(n)$ and v(n), respectively. The scaling factor p is adjusted so that during synthesised speech frame samples that have high adaptive code book gain value b the scale factor p is increased, and during speech that has low adaptive code book gain value b the scaling factor p is reduced. Furthermore, when b is less than a threshold value ($b<TH_{low}$) the scaling factor p is set to zero. The perceptual enhancement gain control unit **312** operates in accordance with equation (3) given below,

$$\text{if}\ \begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b \le TH_{upper} & \text{then } p = a_{enh}b^2 \\ b > TH_{upper} & \text{then } p = a_{enh}b \end{array} \tag{3}$$

where a_{enh} is a constant that controls the strength of the enhancement operation. The applicant has found that a good value for a_{enh} is 0.25, and good values for TH_{low} and TH_{upper} are 0.5 and 1.0, respectively.

Equation 3 can be of a more general form, and a general formulation of the enhancement function is shown below in equation (4). In the general case, there could be more than 2 thresholds for the enhancement gain b. Also, the gain could be defined as a more general function of b.

$$\text{if}\ \begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b < TH_2 & \text{then } p = a_{enh1}f_1(b) \\ TH_2 \le b < TH_3 & \text{then } p = a_{enh2}f_2(b) \\ \vdots & \quad\vdots \\ TH_{N-1} \le b \le TH_{upper} & \text{then } p = a_{enhN-1}f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN}f_N(b) \end{array} \tag{4}$$

In the preferred embodiment previously described N=2, TH_{low}=0.5, TH_2=1.0, TH3= , a_{enh1}=0.25, and a_{enh2}=0.25, $f_1(b)=b^2$, and $f^2(b)=b$.

The threshold values (TH), enhancement values (a_{enh}) and the gain functions (f(b)) are arrived at empirically. Since the only realistic measure of perceptual speech quality can be obtained by human beings listening to the speech and giving their subjective opinions on the speech quality, the values used in equations (3) and (4) are determined experimentally. Various values for the enhancement thresholds and gain functions are tried, and those resulting in the best sounding speech are selected. The applicant has utilised the insight that the enhancement to the speech quality using this method is particularly effective for voiced speech where b typically has a high value, whereas for less voiced sounds which have a lower value of b not so strong an enhancement is required. Thus, gain value p is controlled such that for voiced sounds, where the distortions are most audible, the effect is strong and for unvoiced sounds the effect is weaker or not used at all. Thus, as a general rule, the gain functions (f_n) should be chosen so that there is a greater effect for higher values of b, than for lower values of b. This increases the difference between the pitch components of the speech and the other components.

In the preferred embodiment, operating in accordance with equation (3), the functions operating on gain value b are a squared dependency for mid-range values of b and a linear dependency for high-range values of b. it is the applicant's present understanding that this gives good speech quality since for high values of b, i.e. highly voiced speech, there is greater effect and for lower values of b there is less effect. This is because b typically lies in the range $-1<b<1$ and therefore $b^2<b$.

To ensure unity power gain between the input signal ex(n), and the output signal ew(n) of the excitation post-processing unit **317**, a scale factor is computed and is used to scale the intermediate excitation signal ew'(n) in the scaling unit **315** to form the post-processed excitation signal ew(n). The scale factor k is given as

$$k = \sqrt{\frac{\sum_{n=0}^{N-1} ex^2(n)}{\sum_{n=0}^{N-1} ew'^2(n)}} \tag{5}$$

where N is a suitably chosen adaption period. Typically, N is set equal to the excitation frame length of the LPC speech codec.

In the adaptive code book of the encoder, for values of T which are less than the frame length or excitation length a part of the excitation sequence is unknown. For these unknown portions a replacement sequence is locally generated within the adaptive code book by using suitable selection logic. Several adaptive code book techniques to generate this replacement sequence are known from the state of the art. Typically, a copy of a portion of the known excitation is copied to where the unknown portion is located thereby creating a complete excitation sequence. The copied portion may be adapted in some manner to improve the quality of the resulting speech signal. When doing such copying, the delay value Tis not used since it would point to the unknown portion. Instead, a particular selection logic resulting in a modified value for T is used (for example, using T multiplied by an integer factor so that it always points to the known signal portion). So that the decoder is synchronised with the encoder, similar modifications are employed in the adaptive code book of the decoder. By using such a selection logic to generate a replacement sequence within the adaptive code book, the adaptive code book is able to adapt for high pitch voices such as female and child voices resulting in efficient excitation generation and improved speech quality for these voices.

For obtaining good perceptual enhancement, all modifications inherent to the adaptive code book e.g. for values of T less than the frame length are taken into account in the enhancement post-processing. This is obtained in accordance with the invention by the use of the partial excitation sequence from the adaptive code book v(n) and the re-scaling of the excitation components, inherent to the excitation generator of the speech synthesiser.

In summary, the method enhances the perceptual quality of the synthesised speech and reduces audible artifacts by adaptively scaling the contribution of the partial excitation components taken from the code book **203** and from the adaptive code book **204**, in accordance with equations (2), (3), (4) and (5).

FIG. **4** shows a second embodiment in accordance with the invention, wherein the excitation post-processing unit **417** is located after the LPC synthesis filter **208** as illustrated. In this embodiment an additional LPC synthesis filter **408** is required for the third excitation component derived from the adaptive code book **204**. In FIG. **4**, elements which have the same function as in FIGS. **2** and **3**, also have the same reference numerals.

In the second embodiment shown in FIG. **4**, the LPC synthesised speech is perceptually enhanced by post-processor 4l7. The total excitation signal ex(n) derived from the code book **203** and adaptive code book **204** is input to LPC synthesis filter **208** and processed in a conventional manner in accordance with the LPC coefficients r(i). The additional or third partial excitation component v(n) derived from the adaptive code book **204** in the manner described in relation to FIG. **3** is input unscaled to a second LPC synthesis filter **408** and processed in accordance with the LPC coefficients r(i). The outputs s(n) and $s_v(n)$ of respective LPC filters **208**, **408** are input to post-processor **417** and added together in adder **413**. Prior to being input to adder **413**, signal $s_v(n)$ is scaled by scale factor p. As described with reference to FIG. **3**, the values for processing scale factor or gain p can be arrived at empirically. Additionally, the third partial excitation component may be derived from the fixed code book **203** and the scaled speech signal p's$_v$(n) subtracted from speech signal s(n).

The resulting perceptually enhanced output $s_w(n)$ is then input to the audio processing unit **209**.

Optionally, a further modification of the enhancement system can be formed by moving the scaling unit **414** of FIG. **4** to be in front of the LPC synthesis filter **408**. Locating the post-processor **417** after the LPC or short term synthesis filters **208**, **408** can give better control of the emphasis of the speech signal since it is carried out directly on the speech signal, not on the excitation signal. Thus, less distortions are likely to occur.

Optionally, enhancement can be achieved by modifying the embodiments described with reference to FIGS. **3** and **4** respectively, such that the additional (third) excitation component is derived from the fixed code book **203** instead of the adaptive code book **204**. Then, a negative scaling factor should be used instead of the original positive gain factor p, to decrease the gain for excitation sequence $c_i(n)$ from the fixed code book. This results in a similar modification of the relative contributions of the partial excitation signals $c_i(n)$ and v(n), to speech synthesis as achieved with the embodiments of FIGS. **3** and **4**.

FIG. **5** shows an embodiment in accordance with the invention in which the same result as obtained by using scaling factor p and the additional excitation component from the adaptive code book may be achieved. In this embodiment, the fixed code book excitation sequence $c_i(n)$ is input to scaling unit **314** which operates in accordance with scale factor p' output from perceptual enhancement gain control **2 512**. The scaled fixed code book excitation, p' $c_i(n)$, output from scaling unit **314** is input to adder **313** where it is added to total excitation sequence ex(n) comprising components $c_i(n)$ and v(n) from the fixed code book **203** and adaptive code book **204** respectively.

When increasing the gain for the excitation sequence signal v(n) from the adaptive code book **204** the total excitation (before adaptive energy control **316**) is given by equation (2), viz.

$$ew'(n)=g\ c_i(n)+(b+p)\ v(n) \tag{2}$$

When decreasing the gain for an excitation sequence $c_i(n)$ from the fixed code book **203**, the total excitation (before adaptive energy control **316**) is given as

$$ew'(n)=(g+p')\ c_i(n)+bv(n) \qquad (6),$$

where p' is the scaling factor derived by perceptual enhancement gain control **2 512** shown in FIG. **5**. Taking equation (2) and reformulating it into a form similar to equation (6) gives:

$$\begin{aligned} ew'\ (n) &= g\ c_i(n)+(b+p)\ v(n) \\ &= \frac{p+b}{b}\left[\left(\frac{gb}{p+b}\right)c_i(n)+bv(n)\right] \\ &= \frac{p+b}{b}\left[\left(g-\frac{gp}{p+b}\right)c_i(n)+bv(n)\right] \end{aligned}$$

Thus, selecting

$$p' = -\frac{gp}{(p+b)}$$

In the embodiment of FIG. **5** a similar enhancement as obtained with the embodiment of FIG. **3** will be achieved. When the intermediate total excitation signal ew'(n) is scaled by adaptive energy control **316** to the same energy content as ex(n), then both embodiments, FIG. **3** and FIG. **5**, result in the same total excitation signal ew(n).

Perceptual enhancement gain control **2 512** can therefore utillse the same processing as employed in relation to the embodiments of FIGS. **3** and **4** to generate "p", and then utilise equation (8) to get p'.

The intermediate total excitation signal ew'(n) output from adder **313**. is scaled in scaling unit **315** under control of adaptive energy control **316** in a similar manner as described above in relation to the first and second embodiments.

Referring now to FIG. **4**, LPC synthesised speech may be perceptually enhanced by post-processor **417** by synthesised speech derived from additional excitation signals from the fixed code book.

The dotted line **420** in FIG. **4** shows an embodiment wherein the fixed code book excitation signals $c_i(n)$ are coupled to LPC synthesis filter **408**. The output of the LPC synthesis filter **408** ($sc_i(n)$) is then scaled in unit **414** in accordance with scaling factor p' derived from perceptual enhancement gain control **512**, and added to the synthesised signal s(n) in adder **413** to produce intermediate synthesis signal $s'_w(n)$. After normalisation in scaling unit **415** the resulting synthesis signal $s_w(n)$ is forwarded to the audio processing unit **209**.

The foregoing embodiments comprise adding a component derived from the adaptive code book **204** or fixed code book **203** to an excitation ex(n) or synthesised s(n), to form an intermediate excitation ew'(n) or synthesised signal s'_w (n).

Optionally, post-processing may be dispensed with and the adaptive code book v(n) or fixed code book c(n) excitation signals may be scaled and directly combined together. Thereby obviating the addition of components to unscaled combined fixed and adaptive code book signals.

FIG. **6** shows an embodiment in accordance with an aspect of the invention having the adaptive code book excitation signals v(n) scaled and then combined with the fixed code book excitation signals $c_i(n)$ to directly form an intermediate signal ew(n). Perceptual enhancement gain control **612** outputs parameter "a" to control scaling unit **614**. Scaling unit **614** operates on adaptive code book excitation signal v(n) to scale-up or amplify excitation signal v(n) over the gain factor b used to get the normal excitation. Normal excitation ex(n) is also formed and coupled to the adaptive code book **204** and adaptive energy control **316**. Adder **613** combines up-scaled excitation signal av(n) and fixed code book excitation $c_i(n)$ to form an intermediate signal;

$$ew'(n)=g\ c_i(n)+av(n) \tag{9}$$

If a=b+p, then the same processing as given by equation (2) may be achieved.

FIG. **7** shows an embodiment operable in a manner similar to that shown in FIG. **6**, but down-scaling or attenuating the fixed code book excitation signal $c_i(n)$. For this embodiment the intermediate excitation sign ew'(n) is given by:

$$ew'(n)=(g+p')\ c_i(n)+bv(n)=a'c_i(n)+bv(n) \tag{10}$$

where,

$$a' = g - \frac{gp}{p+b} = \frac{gb}{p+b}. \tag{11}$$

Perceptual enhancement gain control **712** outputs a control signal a' in accordance with equation (11), to obtain a similar result as obtained with equation (6) in accordance with equation (8). The down-scaled fixed code book excitation signal $a'c_i(n)$ is combined with adaptive code book excitation signal v(n) in adder **713** to form intermediate excitation signal ew'(n). The remaining processing is carried out as described before, to normalise the excitation signal and formed synthesised signal $s_{ew}(n)$.

The embodiments described with reference to FIGS. **6** and **7** perform scaling of the excitation signals within the excitation generator, and directly from the code books.

The determination of scaling factor "p" for the embodiments described with reference to FIGS. **5**, **6** and **7** may be made in accordance with equations (3) or (4) described above.

Various methods of control of the enhancement level (a_{enh}) may be employed. In addition to the adaptive code book gain b, the amount of enhancement could be a function of the lag or delay value T for the adaptive code book **204**. For example, the post processing could be turned on (or emphasised) when operating in a high pitch range or when the adaptive code book parameter T is shorter than the excitation block length (virtual lag range). As a result, female and child voices, forwhich the invention is most beneficial, would be highly post processed.

The post processing control could also be based on voiced/unvoiced speech decisions. For example, the enhancement could be stronger for voiced speech, and it could be totally turned off when the speech is classified as unvoiced. This can be derived from the adaptive code book gain value b which is itself a simple measure of voiced/unvoiced speech, that is to say the higher b, the more voiced speech present in the original speech signal.

Embodiments in accordance with the present invention may be modified, such that the third partial excitation sequence is not the same partial excitation sequence derived from the adaptive code book or fixed code book in accordance with conventional speech synthesis, but is selectable via selection logic typically included in respective code books to choose another third partial excitation sequence. The third partial excitation sequence may be chosen to be the immediately previously used excitation sequence or to be always a same excitation sequence stored in the fixed code book. This would act to reduce the difference between speech frames and thereby enhance the continuity of the speech. Optionally, b and/or T can be recalculated in the decoder from the synthesised speech and used to derive a third partial excitation sequence. Further, a fixed gain p and/or fixed excitation sequence can be added or subtracted as appropriate to the total excitation sequence ex(n) or speech signal s(n) depending on the location of the post-processor.

In view of the foregoing description it will be evident to a person skilled in the art that various modifications may be made within the scope of the invention. For example, variable-frame-rate coding, fast code book searching, reversal of the order of pitch prediction and LPC prediction may be utilised in the codec. Additionally, post-processing in accordance with the present invention could also be included in the encoder, not just the decoder. Furthermore, aspects of respective embodiments described with reference to the drawings may be combined to provide further embodiments in accordance with the invention.

The scope of the present disclosure includes any novel feature or combination of features disclosed therein either explicitly or implicitly or any generalisatlon thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed by the present invention. The applicant hereby gives notice that new claims may be formulated to such features during prosecution of this application or of any such further application derived therefrom.

What we claim is:

1. A Linear Predictive Coding (LPC) synthesiser for speech synthesis, comprising:

an excitation source; and

a LPC decoder comprising post-processing means coupled to an output of said excitation source for operating on a first signal including speech periodicity information derived from said excitation source, wherein the post-processing means modifies the speech periodicity information content of the first signal in accordance with a second signal derivable from said excitation source in order to produce an enhanced synthesised speech signal.

2. A synthesiser according to claim **1**, wherein the post-processing means comprises gain control means for scaling the second signal in accordance with a first scaling factor (p) derivable from pitch information associated with the first signal.

3. A synthesiser according to claim **2**, wherein the excitation source comprises a fixed code book and an adaptive code book, the first signal comprising a combination of first and second partial excitation signals respectively originating from the fixed and adaptive code books.

4. A synthesiser according to claim **3**, wherein the first scaling factor (p) is derivable from an adaptive code book gain factor (b).

5. A synthesiser according to claim **4**, wherein the first scaling factor (p) is derivable in accordance with the following relationship,

$$\text{if}\quad \begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \le b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \quad\vdots \\ TH_{N-1} \le b \le TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, b is the adaptive code book gain factor, p is the first post-processing means scale factor, a_{enh} is a linear scaler and f(b) is a function of the adaptive code book gain factor b.

6. A synthesiser according to claim **4**, wherein the scaling factor (p) is derivable in accordance with

$$\text{if}\quad \begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b \le TH_{upper} & \text{then } p = a_{enh} b^2 \\ b > TH_{upper} & \text{then } p = a_{enh} b \end{array}$$

where a_{enh} is a constant that controls the strength of the enhancement operation, b is the adaptive code book gain factor, TH are threshold values and p is the first post-processing means scale factor.

7. A synthesiser according to claim **3**, wherein the second signal originates from the adaptive code book.

8. A synthesiser according to claim **7**, wherein the second signal is substantially the same as the second partial excitation signal.

9. A synthesiser according to claim **7**, wherein the first signal is a first excitation signal suitable for inputting to a speech synthesis filter, and the second signal is a second excitation signal suitable for inputting to a speech synthesis filter.

10. A synthesiser according to claim **3**, wherein the second signal originates from the fixed code book.

11. A synthesiser according to claim **10**, wherein the second signal is substantially the same as the first partial excitation signal.

12. A synthesiser according to claim **10**, wherein the gain control means scales the second signal in accordance with a second scaling factor (p') where,

$$p' = -\frac{gp}{(p+b)}$$

and where g is a fixed code book scaling factor, b is an adaptive code book gain factor and p is the first scaling factor.

13. A synthesiser according to claim **12**, wherein the first signal is a first synthesised speech signal output from a first speech synthesis filter, the second signal is the output from a second speech synthesis filter, and the gain control means operates on signals input to the second speech synthesis filter.

14. A synthesiser according to claim **10**, wherein the first signal is a first synthesised speech signal output from a first speech synthesis filter, the second signal is the output from a second speech synthesis filter, and the gain control means operates on signals input to the second speech synthesis filter.

15. A synthesiser according to claim **2**, wherein the excitation source comprises a fixed code book and an adaptive code book, the first signal comprising a combination of first and second partial excitation signals respectively originating from the fixed and adaptive code books, the second signal being substantially the same as the second partial excitation signal and originating from the adaptive code book, the first signal being modified by combining the second signal with the first signal, and the first scaling factor (p) being derivable from an adaptive code book gain factor (b) in accordance with the following relationship,

$$\text{if}\quad \begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \le b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \quad\vdots \\ TH_{N-1} \le b \le TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, b is the adaptive code book gain factor, p is the first post-processing means scale factor, a_{enh} is a linear scaler and f(b) is a function of the adaptive code book gain factor b.

16. A synthesiser according to claim **2**, wherein the excitation source comprises a fixed code book and an adaptive code book, the first signal comprising a combination of first and second partial excitation signals respectively originating from the fixed and adaptive code books, the second signal being substantially the same as the first partial excitation signal and originating from the fixed code book, the first signal being modified by combining the second signal with the first signal, and the first scaling factor (p) being derivable from an adaptive code book gain factor (b) in accordance with the following relationship,

$$\text{if}\quad \begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \leq b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \leq b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \qquad \vdots \\ TH_{N-1} \leq b \leq TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, b is the adaptive code book gain factor, p is the first post-processing means scale factor, a_{enh} is a linear scaler and f(b) is a function of the adaptive code book gain factor b.

17. A method for use with Linear Predictive Coding (LPC) for enhancing synthesised speech, comprising steps of:

deriving a first signal including speech periodicity information from an excitation source,

deriving a second signal from the excitation source, and

modifying in a LPC decoder the speech periodicity information content of the first signal in accordance with the second signal in order to produce an enhanced synthesised speech signal.

18. A method according to claim **17**, further comprising scaling the second signal in accordance with a first scaling factor (p) derived from pitch information associated with the first signal.

19. A method according to claim **18**, wherein the excitation source comprises a fixed code book and an adaptive code book, the first signal comprising a combination of first and second partial excitation signals respectively originating from the fixed and adaptive code books.

20. A method according to claim **19**, wherein the first scaling factor (p) is derivable from a gain factor (b) for the pitch information of the first signal.

21. A method according to claim **20**, wherein the first scaling factor (p) is derivable in accordance with the following relationships,

$$\text{if}\quad \begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \leq b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \leq b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \qquad \vdots \\ TH_{N-1} \leq b \leq TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, b is the gain factor for the pitch information of the first signal, p is the first scaling factor, a_{enh} is a linear scaler and f(b) is a function of b.

22. A method according to claim **19**, wherein the second signal originates from the adaptive code book.

23. A method according to claim **22**, wherein the second signal is substantially the same as the second partial excitation signal.

24. A method according to claim **22**, wherein the first signal is a first synthesised speech signal output from a first speech synthesis filter and the second signal is the output of a second speech synthesis filter.

25. A method according to claim **19**, wherein the second signal originates from the fixed code book.

26. A method according to claim **25**, wherein the second signal is substantially the same as the first partial excitation signal.

27. A method according to claim **25**, wherein the second signal is scaled in accordance with a second scaling factor (p') where,

$$p' = -\frac{gp}{(p+b)}$$

g is a fixed code book scaling factor, b is an adaptive code book scaling factor and p is the first scaling factor.

28. A method according to claim **25**, wherein the first signal is a first synthesised speech signal output from a first speech synthesis filter and the second signal is the output of a second speech synthesis filter.

29. A method according to claim **17**, wherein the first signal is a first excitation signal suitable for inputting to a first speech synthesis filter, and the second signal is a second excitation signal suitable for inputting to a second speech synthesis filter.

30. A method for use with Linear Predictive Coding (LPC) for enhancing synthesised speech, comprising steps of:

deriving a first signal including speech periodicity information from an excitation source, comprising a fixed code book and an adaptive code book,

the first signal comprising a combination of first and second partial excitation signals respectively originating from the fixed and adaptive code books,

deriving a second signal from the excitation source, and

modifying in a LPC decoder the speech periodicity information content of the first signal in accordance with the second signal in order to produce an enhanced synthesised speech signal,

the second signal being substantially the same as the second partial excitation signal and originating from the adaptive code book, the first signal being modified by combining the second signal with the first signal, and a first scaling factor (p) being derivable from an adaptive code book scaling factor (b) in accordance with the following relationship,

$$\text{if}\quad \begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \leq b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \leq b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \qquad \vdots \\ TH_{N-1} \leq b \leq TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, a_{enh} is a linear scaler and f(b) is a function of b.

31. A method for use with Linear Predictive Coding (LPC) for enhancing synthesised speech, comprising steps of:

deriving a first signal including speech periodicity information from an excitation source, comprising a fixed code book and an adaptive code book,

the first signal comprising a combination of first and second partial excitation signals respectively originating from the fixed and adaptive code books,

deriving a second signal from the excitation source, and

modifying in a LPC decoder the speech periodicity information content of the first signal in accordance with the second signal in order to produce an enhanced synthesised speech signal,

the second signal being substantially the same as the first partial excitation signal and originating from the fixed code book, the first signal being modified by combining the second signal with the first signal, and a first scaling factor (p) being derivable from an adaptive code book scaling factor (b) in accordance with the following relationship,

$$\text{if}\quad\begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \le b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \vdots \\ TH_{N-1} \le b \le TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, a_{enh} is a linear scaler and f(b) is a function of b.

32. A Linear Predictive Coding (LPC) synthesiser for speech synthesis, comprising first and second excitation sources for respectively generating first and second excitation signals, and a LPC decoder comprising modifying means for modifying the first excitation signal in accordance with a scaling factor derivable from pitch information associated with the first excitation signal in order to produce an enhanced synthesised speech signal.

33. A synthesiser according to claim **32**, wherein the modifying means scales the first excitation signal in accordance with a scaling factor (a) derivable from pitch information associated with the first signal.

34. A synthesiser according to claim **33**, wherein the first excitation source is an adaptive code book and the second excitation source is a fixed code book.

35. A synthesiser according to claim **34**, wherein the scaling factor (a) is of the form a=b+p, where b is an adaptive code book gain and p is a perceptual enhancement gain factor derivable in accordance with the following relationships;

$$\text{if}\quad\begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \le b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \vdots \\ TH_{N-1} \le b \le TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, a_{enh} is a linear scaler and f(b) is a function of gain b.

36. A synthesiser according to claim **35**, wherein the first and second excitation signals are combined after modification.

37. A synthesiser according to claim **34**, wherein the scaling factor (a) is of the form a=b+p, where b is an adaptive code book gain and p is a perceptual enhancement gain factor, and wherein the perceptual enhancement gain factor p is derivable in accordance with;

$$\text{if}\quad\begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b \le TH_{upper} & \text{then } p = a_{enh} b^2 \\ b > TH_{upper} & \text{then } p = a_{enh} b \end{array}$$

where a_{enh} is a constant that controls the strength of the enhancement operation and TH are threshold values.

38. A Linear Predictive Coding (LPC) synthesiser for speech synthesis, comprising first and second excitation sources for respectively generating first and second excitation signals, and a LPC decoder comprising modifying means for modifying the second excitation signal in accordance with a scaling factor derivable from pitch information associated with the first excitation signal in order to produce an enhanced synthesised speech signal.

39. A synthesiser according to claim **38**, wherein the modifying means scales the second excitation signal in accordance with a scaling factor (a') derivable from pitch information associated with the first signal.

40. A synthesiser according to claim **39**, wherein the first excitation source is an adaptive code book and the second excitation source is a fixed code book.

41. A synthesiser according to claim **40**, wherein the scaling factor (a') satisfies the following relationship;

$$a' = -\frac{gp}{(p+b)}$$

where g is a fixed code book gain factor, b is an adaptive code gain factor and p is a perceptual enhancement gain factor derivable in accordance with;

$$\text{if}\quad\begin{array}{ll} b < TH_{low} & \text{then } p = 0.0 \\ TH_{low} \le b < TH_2 & \text{then } p = a_{enh1} f_1(b) \\ TH_2 \le b < TH_3 & \text{then } p = a_{enh2} f_2(b) \\ \vdots & \vdots \\ TH_{N-1} \le b \le TH_{upper} & \text{then } p = a_{enhN-1} f_{N-1}(b) \\ b > TH_{upper} & \text{then } p = a_{enhN} f_N(b) \end{array}$$

where TH represents threshold values, a_{enh} is a linear scaler and f(b) is a function of gain b.

42. A method for use with Linear Predictive Coding (LPC) for speech synthesis, comprising steps of:

generating first and second excitation signals,

modifying in a LPC decoder the first excitation signal in accordance with a gain factor associated therewith, and

further modifying in the LPC decoder the first excitation signal in accordance with a scaling factor derivable from pitch information associated with the first excitation signal in order to produce an enhanced synthesised speech signal.

43. A method for use with Linear Predictive Coding (LPC) for speech synthesis, comprising steps of:

generating first and second excitation signals,

modifying in a LPC decoder the first excitation signal in accordance with a gain factor associated therewith, and

modifying in the LPC decoder the second excitation signal in accordance with a scaling factor derivable from pitch information associated with the first excitation signal in order to produce an enhanced synthesised speech signal.

44. A time domain speech synthesiser, comprising:

an excitation source providing first and second partial excitation signals having a speech periodicity information content; and

a speech quality enhancement post-processor coupled to said excitation source for operating on one of said first and second partial excitation signals, said post-processor modifying the speech periodicity information content of the operated on partial excitation signal in accordance with a signal derivable from at least one of said first and second partial excitation signals.

45. A synthesiser for speech synthesis, comprising:

an input unit for inputting a signal and for extracting coded information from said signal, the coded information comprising fixed codebook and adaptive codebook parameters, including an adaptive codebook gain factor;

an excitation source comprising a fixed codebook and an adaptive codebook and having inputs coupled to outputs of said input unit for receiving extracted coded information therefrom, said excitation source being responsive to the received extracted coded information for outputting a first partial excitation signal from said fixed codebook and a second partial excitation signal from said adaptive codebook, said excitation source further comprising means for combining said first and second partial excitation signals into a composite excitation signal; and

a perceptual enhancement post-processor coupled to said excitation source for operating on said composite excitation signal by combining said composite excitation signal with a scaled version of said second partial excitation signal, wherein an amount of scaling of said second partial excitation signal is controlled by a scaling factor having a value that is function of a value of said adaptive codebook gain factor.

46. A synthesiser as in claim **45**, wherein said input unit inputs said signal from a radio channel.

* * * * *

EXHIBIT H

US006882727B1

(12) **United States Patent**
Vialen et al.

(10) **Patent No.: US 6,882,727 B1**
(45) **Date of Patent: Apr. 19, 2005**

(54) **METHOD OF CIPHERING DATA TRANSMISSION IN A RADIO SYSTEM**

(75) Inventors: **Jukka Vialen**, Espoo (FI); **Fabio Longoni**, Espoo (FI)

(73) Assignee: **Nokia Mobile Phones Ltd.**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/519,184**

(22) Filed: **Mar. 6, 2000**

(30) **Foreign Application Priority Data**

Mar. 8, 1999 (FI) 990500

(51) **Int. Cl.**^{7} **H04K 9/08**
(52) **U.S. Cl.** **380/33**; 380/270; 380/259
(58) **Field of Search** 380/259, 33; 280/270

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,418,425	A	*	11/1983	Fennel et al.	380/33
4,484,025	A	*	11/1984	Ostermann et al.	380/279
4,797,921	A	*	1/1989	Shiraishi	380/28
5,185,796	A	*	2/1993	Wilson	380/277
5,278,906	A	*	1/1994	Boly et al.	380/268
5,285,497	A	*	2/1994	Thatcher, Jr.	380/217
5,319,712	A	*	6/1994	Finkelstein et al.	380/44
5,412,730	A	*	5/1995	Jones	380/46
5,455,863	A		10/1995	Brown et al.	380/23
5,500,650	A	*	3/1996	Snodgrass et al.	342/42
5,600,722	A		2/1997	Yamaguchi et al.	380/21
5,675,581	A	*	10/1997	Soliman	370/252
5,696,828	A	*	12/1997	Koopman, Jr.	380/46
6,373,946	B1	*	4/2002	Johnston	380/211
6,535,979	B1	*	3/2003	Vialen et al.	713/163

FOREIGN PATENT DOCUMENTS

WO	WO 97/12461	4/1997
WO	WO 99/39525	8/1999

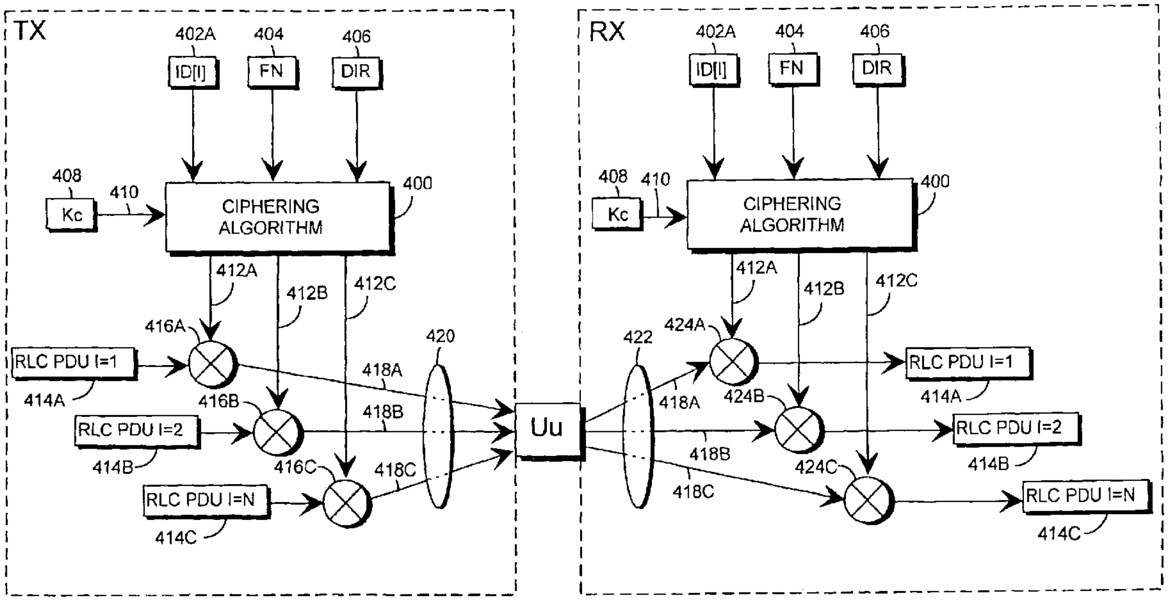
* cited by examiner

Primary Examiner—Gregory Morse
Assistant Examiner—Ellen Tran
(74) *Attorney, Agent, or Firm*—Perma & Green, LLP

(57) **ABSTRACT**

The invention relates to a method of ciphering data transmission in a radio system, and to a user equipment using the method, and to a radio network subsystem using the method. The method includes the steps of: **(602)** generating a ciphering key; **(604**A**)** producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter; **(604**B**)** using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm; and **(606)** producing ciphered data by applying the ciphering mask to plain data.

25 Claims, 13 Drawing Sheets



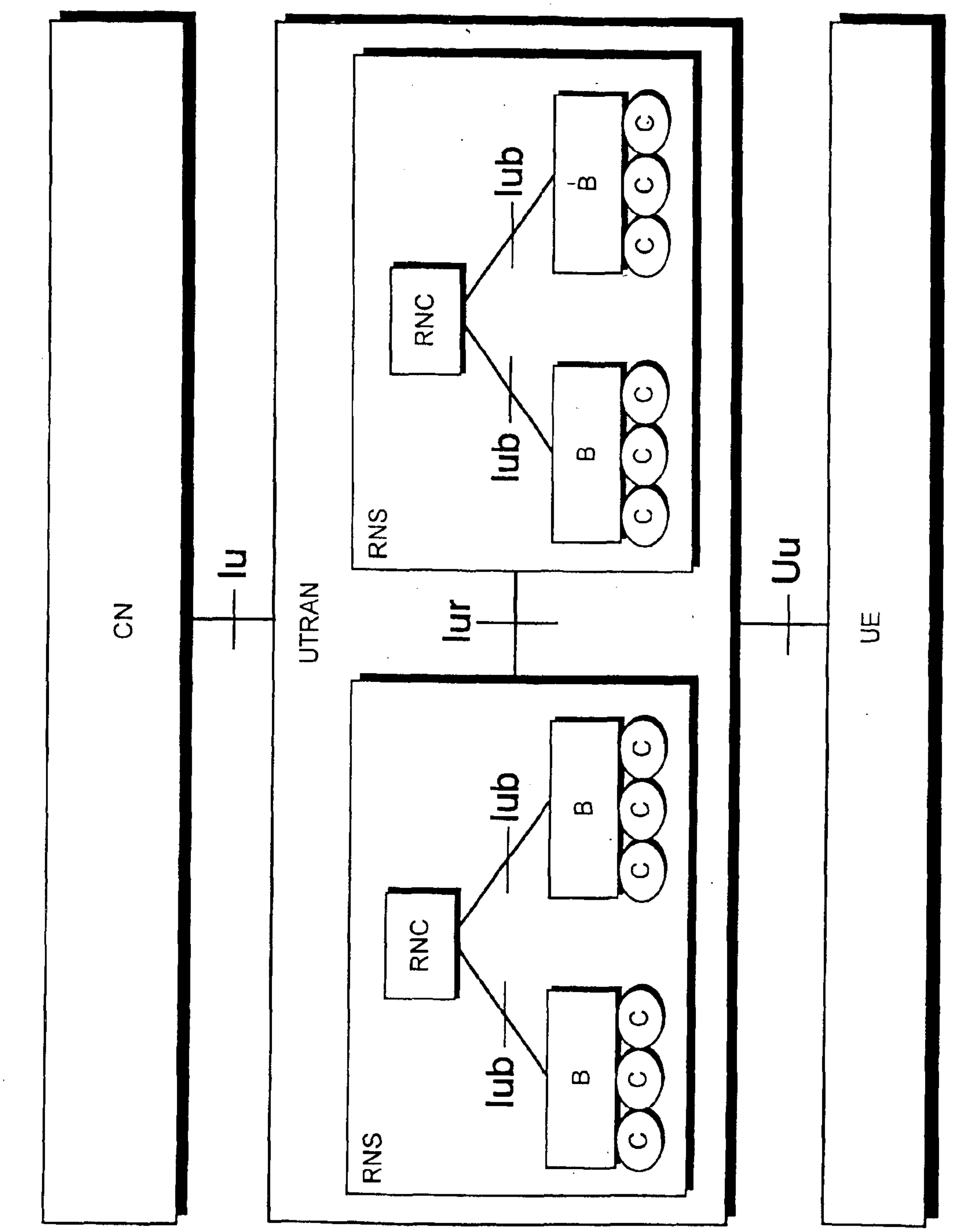

CN
Iu
UTRAN
RNS
RNC
Iub
Iub
B
B
C
C
C
C
C
C
Iur
RNS
RNC
Iub
Iub
B
B
C
C
C
C
C
C
Uu
UE

Fig 1A

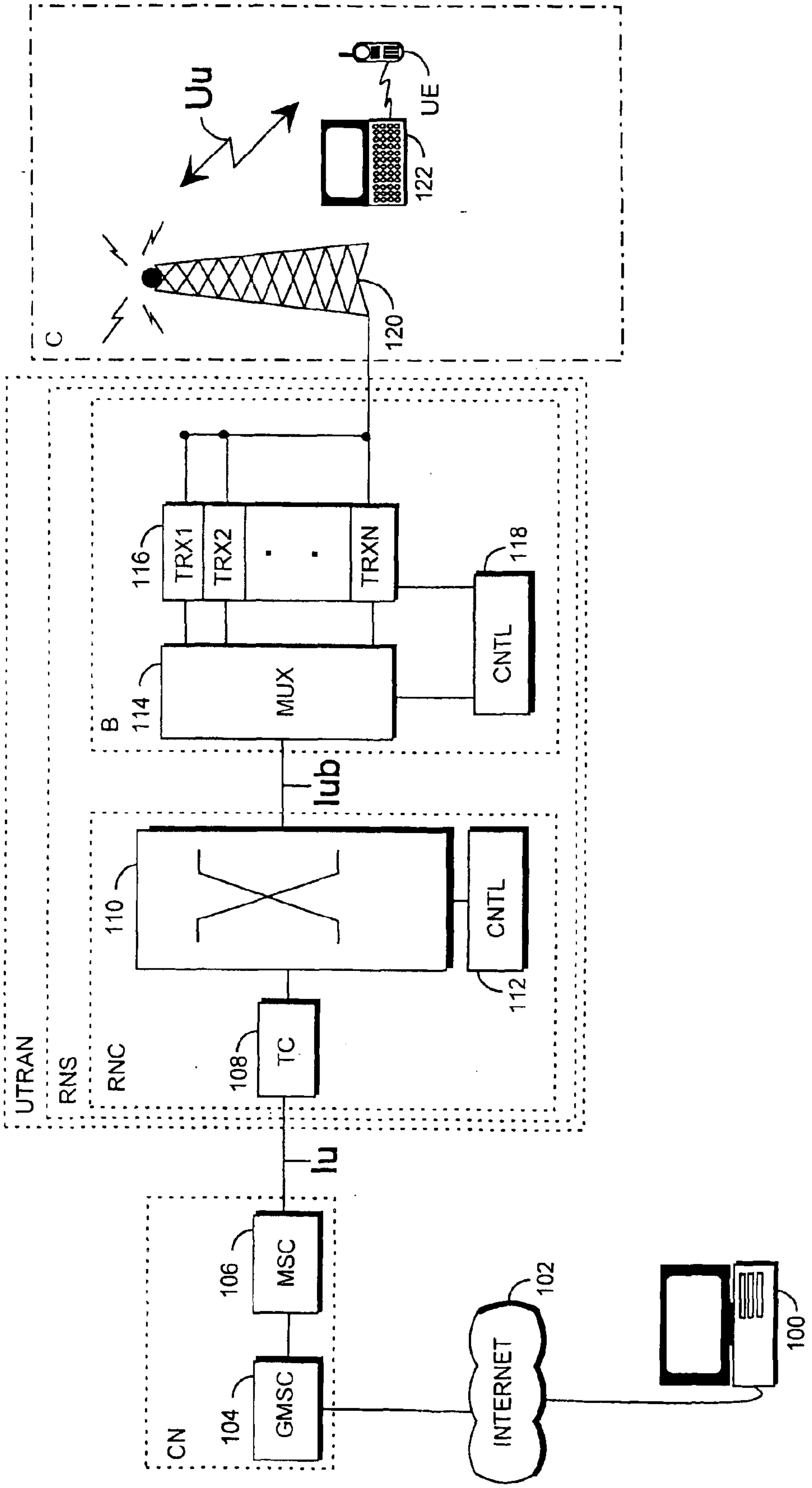

C
120
Uu
UE
122
UTRAN
RNS
RNC
B
114
MUX
116
TRX1
TRX2
TRXN
118
CNTL
Iub
110
CNTL
112
TC
108
Iu
CN
106
MSC
104
GMSC
INTERNET
102
100

Fig 1B

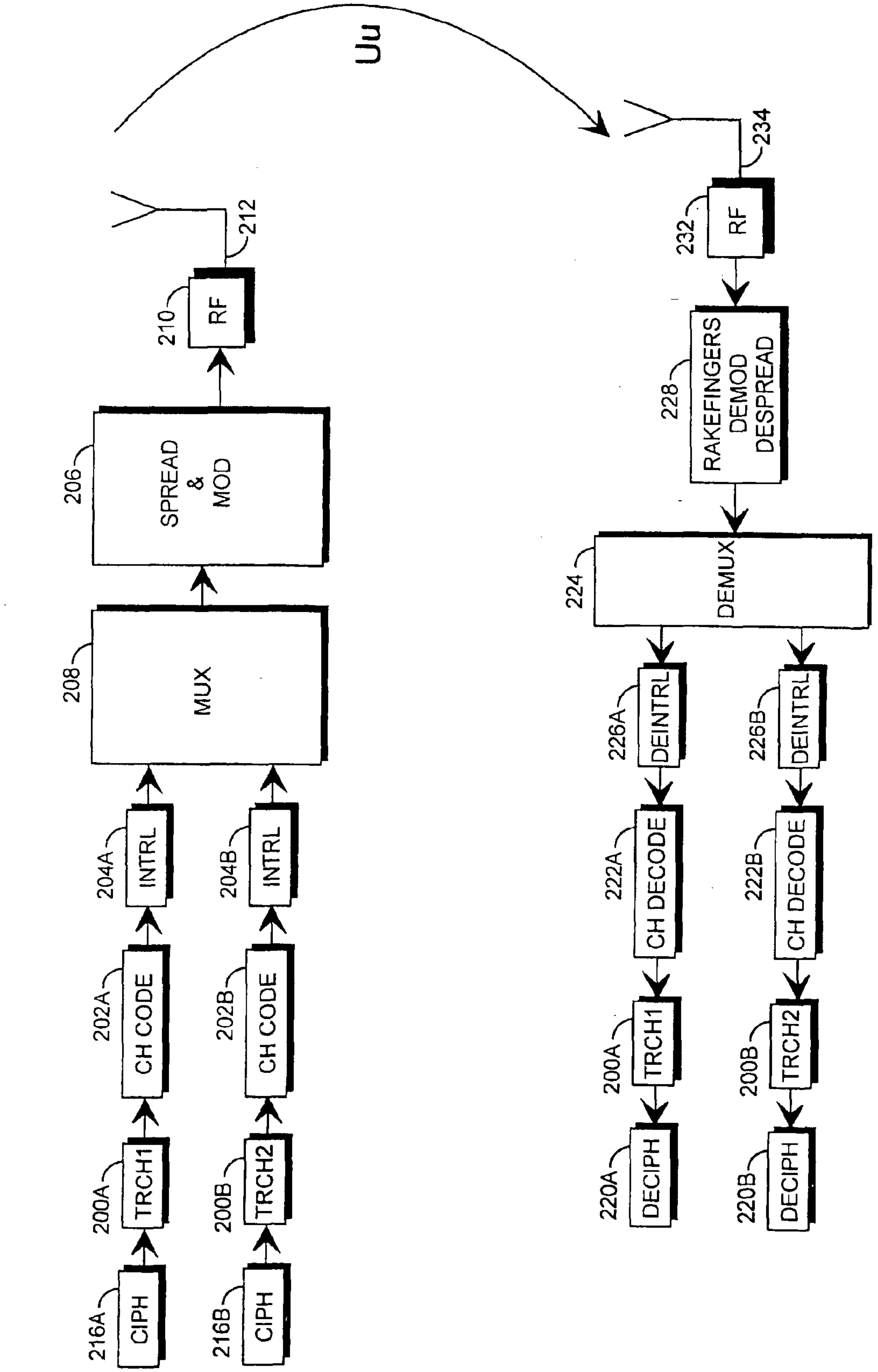

Uu
212
210
RF
206
SPREAD
&
MOD
208
MUX
204A
INTRL
204B
INTRL
202A
CH CODE
202B
CH CODE
200A
TRCH1
200B
TRCH2
216A
CIPH
216B
CIPH
234
232
RF
228
RAKEFINGERS
DEMOD
DESPREAD
224
DEMUX
226A
DEINTRL
226B
DEINTRL
222A
CH DECODE
222B
CH DECODE
200A
TRCH1
200B
TRCH2
220A
DECIPH
220B
DECIPH

Fig 2A

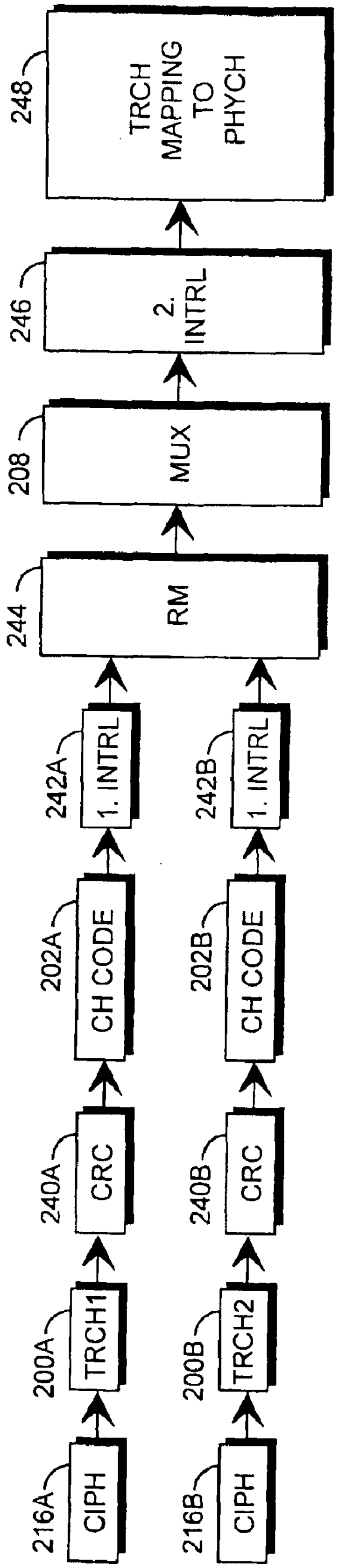

216A
CIPH
200A
TRCH1
240A
CRC
202A
CH CODE
242A
1. INTRL
216B
CIPH
200B
TRCH2
240B
CRC
202B
CH CODE
242B
1. INTRL
244
RM
208
MUX
246
2. INTRL
248
TRCH MAPPING TO PHYCH

Fig 2B

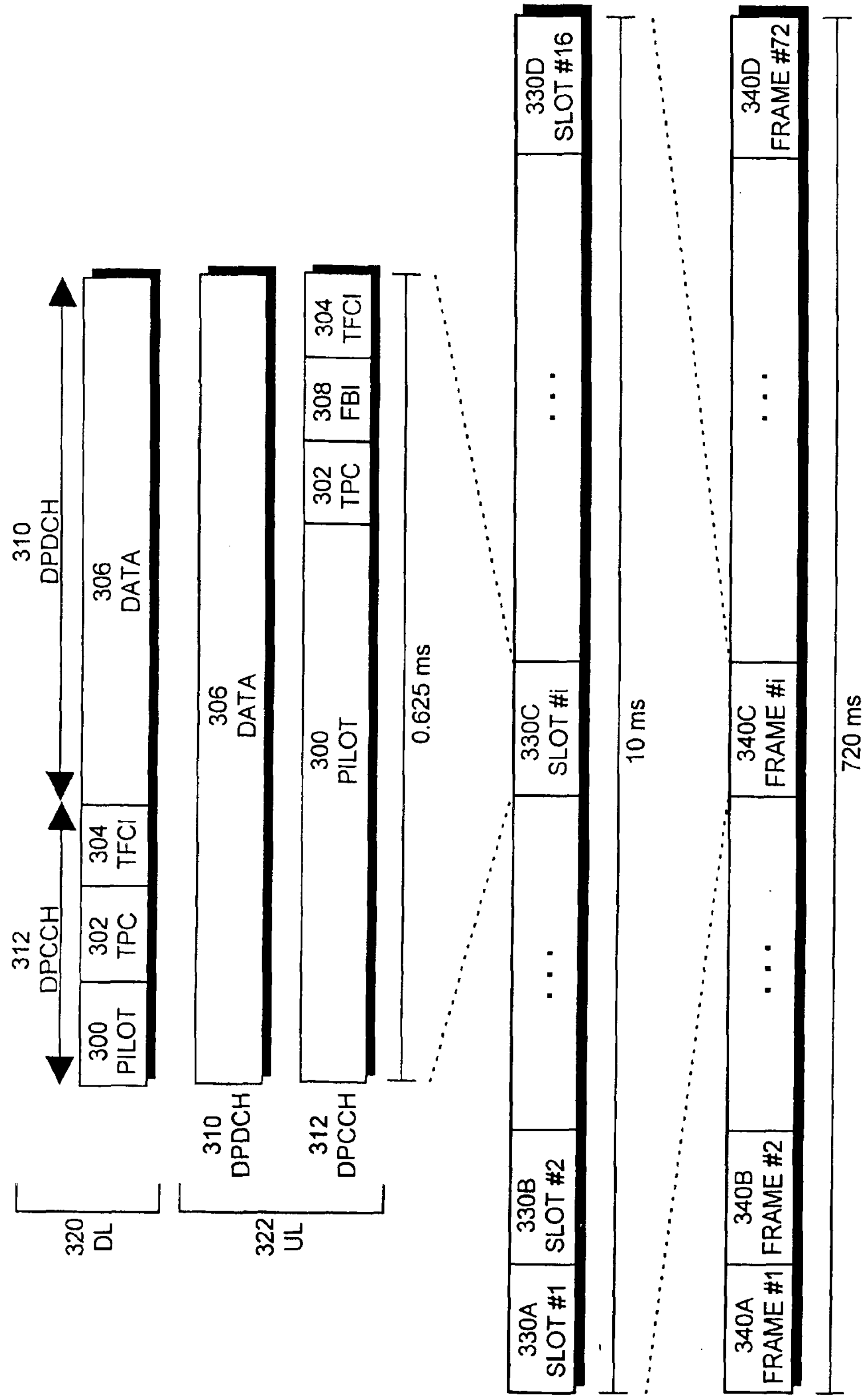

320
DL
322
UL
312
DPCCH
310
DPDCH
300
PILOT
302
TPC
304
TFCI
306
DATA
310
DPDCH
306
DATA
312
DPCCH
300
PILOT
302
TPC
308
FBI
304
TFCI
0.625 ms
330A
SLOT #1
330B
SLOT #2
330C
SLOT #i
330D
SLOT #16
. . .
. . .
10 ms
340A
FRAME #1
340B
FRAME #2
340C
FRAME #i
340D
FRAME #72
. . .
. . .
720 ms

Fig 3

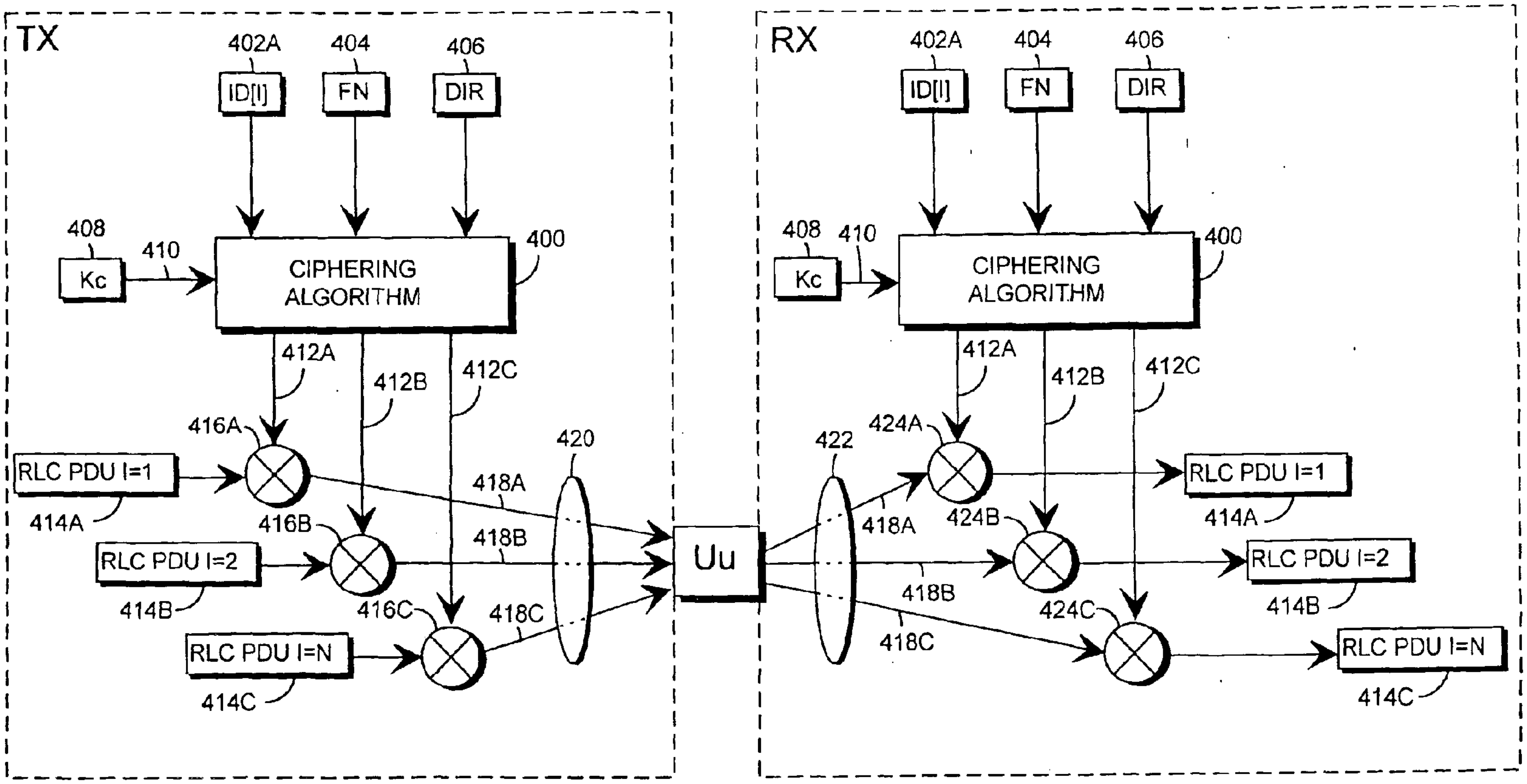

TX
402A
ID[I]
404
FN
406
DIR
408
Kc
410
CIPHERING ALGORITHM
400
412A
412B
412C
416A
RLC PDU I=1
414A
416B
RLC PDU I=2
414B
416C
RLC PDU I=N
414C
418A
418B
418C
420
Uu
RX
402A
ID[I]
404
FN
406
DIR
408
410
Kc
CIPHERING ALGORITHM
400
412A
412B
412C
422
424A
418A
424B
418B
418C
424C
RLC PDU I=1
414A
RLC PDU I=2
414B
RLC PDU I=N
414C

Fig 4A

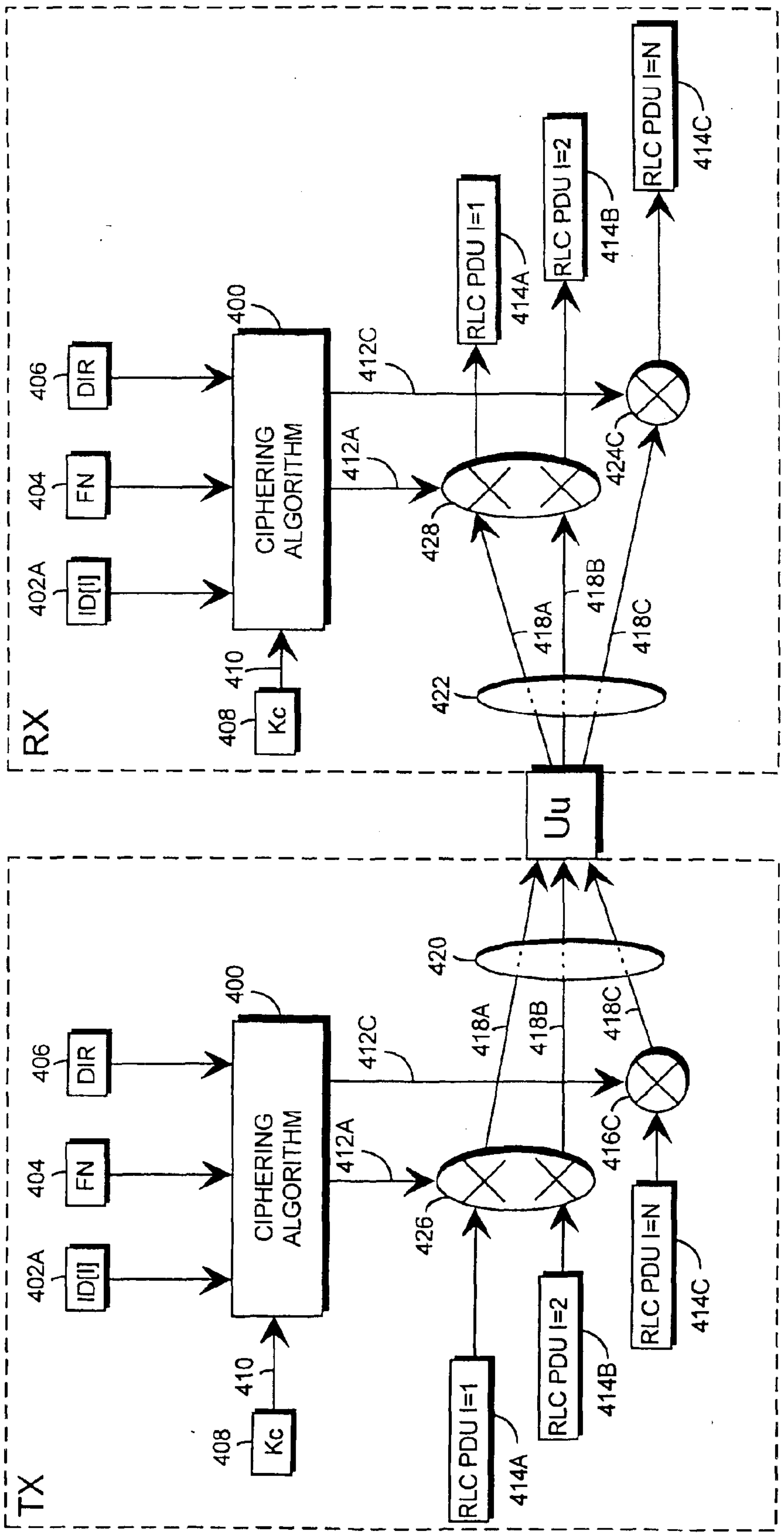

RX
TX
408
Kc
410
402A
ID[I]
404
FN
406
DIR
CIPHERING ALGORITHM
400
412A
412C
428
426
424C
416C
422
420
418A
418B
418C
RLC PDU I=1
RLC PDU I=2
RLC PDU I=N
414A
414B
414C
Uu

Fig 4B

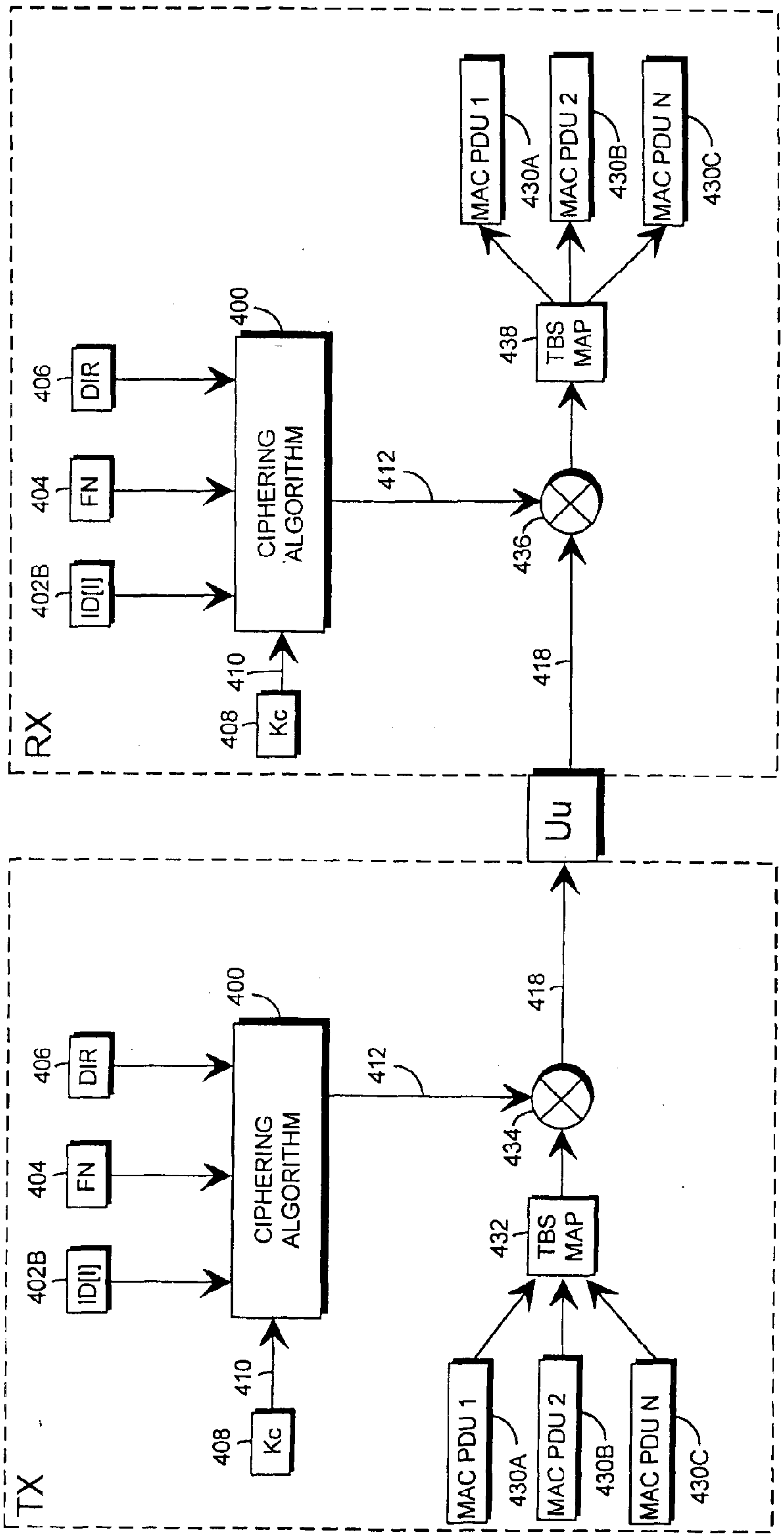

RX
408
Kc
410
402B
ID[I]
404
FN
406
DIR
400
CIPHERING ALGORITHM
412
436
418
438
TBS MAP
MAC PDU 1
430A
MAC PDU 2
430B
MAC PDU N
430C
Uu
TX
408
Kc
410
402B
ID[I]
404
FN
406
DIR
400
CIPHERING ALGORITHM
412
434
418
432
TBS MAP
MAC PDU 1
430A
MAC PDU 2
430B
MAC PDU N
430C

Fig 4C

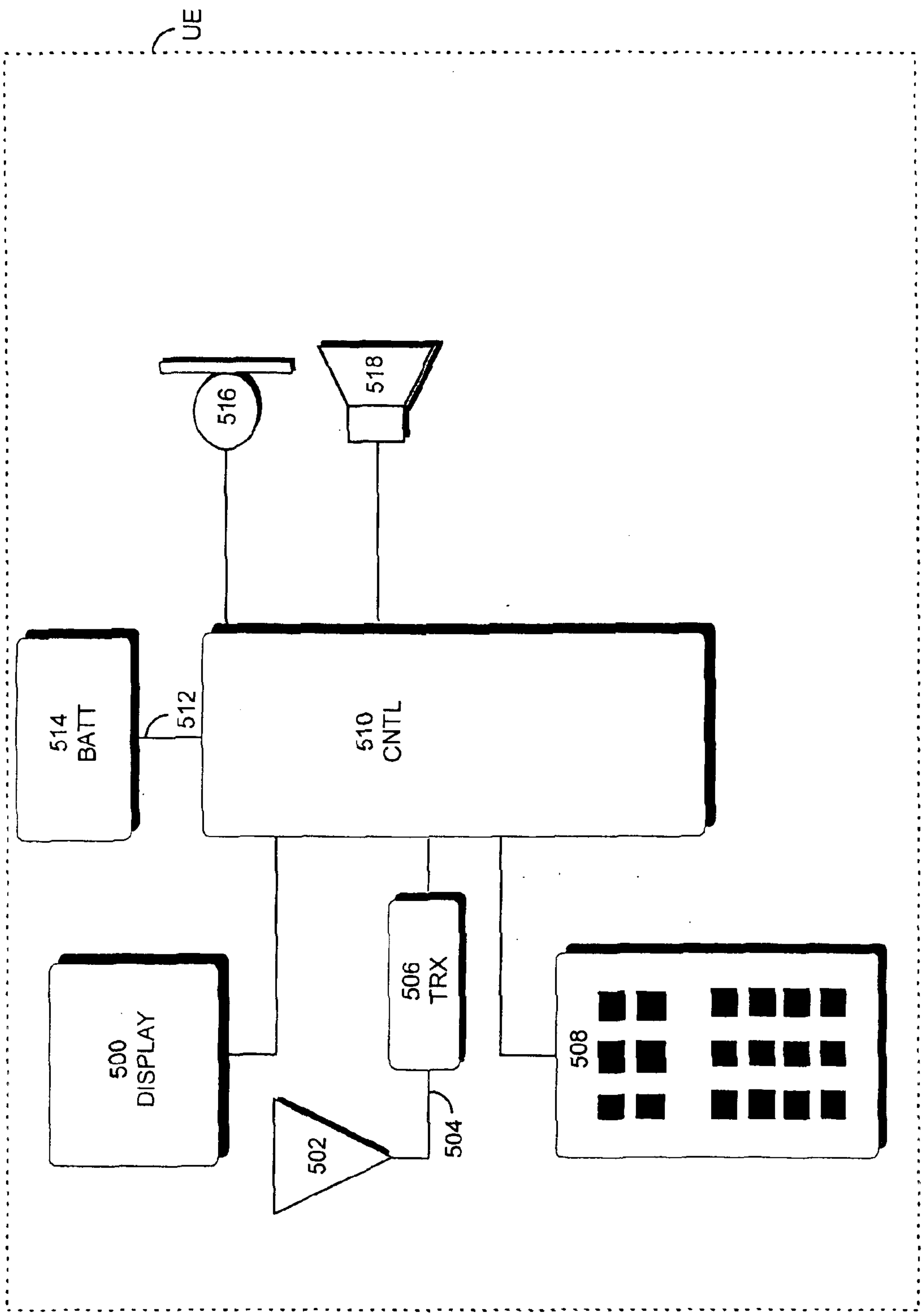

UE
516
518
514
BATT
512
510
CNTL
500
DISPLAY
506
TRX
502
504
508

Fig 5

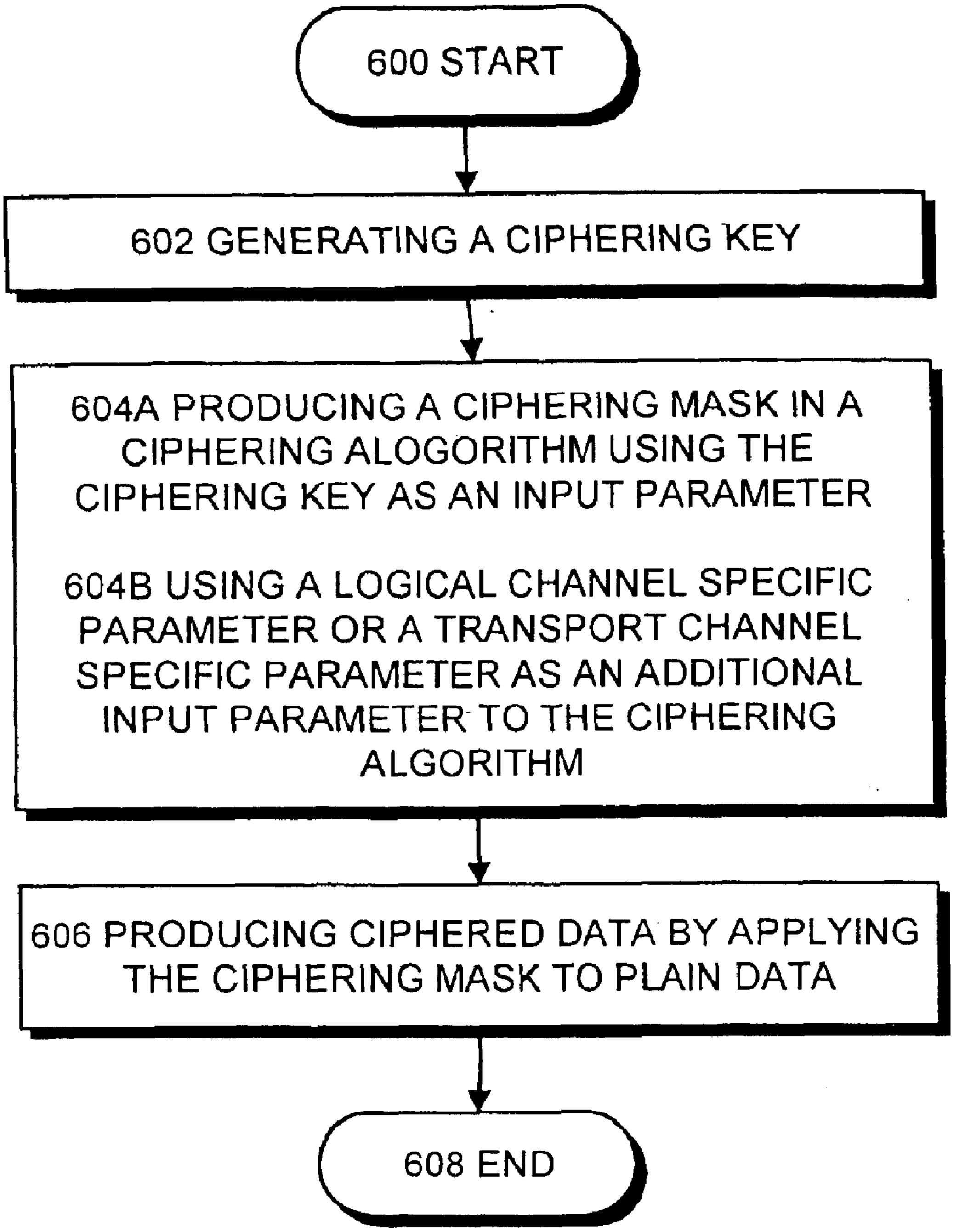

600 START
602 GENERATING A CIPHERING KEY
604A PRODUCING A CIPHERING MASK IN A CIPHERING ALOGORITHM USING THE CIPHERING KEY AS AN INPUT PARAMETER
604B USING A LOGICAL CHANNEL SPECIFIC PARAMETER OR A TRANSPORT CHANNEL SPECIFIC PARAMETER AS AN ADDITIONAL INPUT PARAMETER TO THE CIPHERING ALGORITHM
606 PRODUCING CIPHERED DATA BY APPLYING THE CIPHERING MASK TO PLAIN DATA
608 END

Fig 6

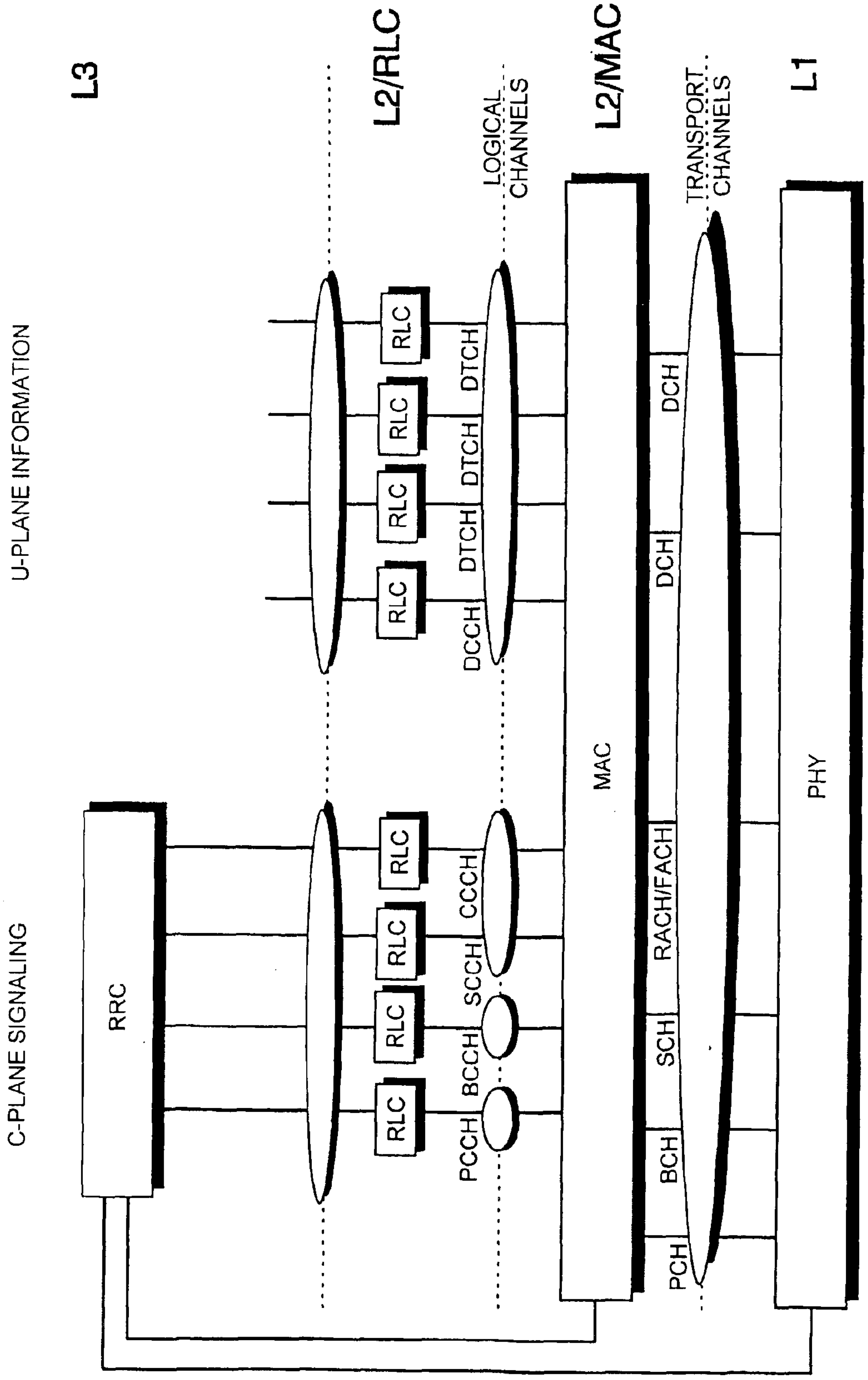

L3
L2/RLC
LOGICAL CHANNELS
L2/MAC
TRANSPORT CHANNELS
L1
U-PLANE INFORMATION
C-PLANE SIGNALING
RRC
RLC
RLC
RLC
RLC
RLC
RLC
RLC
RLC
DCCH
DTCH
DTCH
DTCH
PCCH
BCCH
SCCH
CCCH
MAC
DCH
DCH
RACH/FACH
SCH
BCH
PCH
PHY

Fig 7A

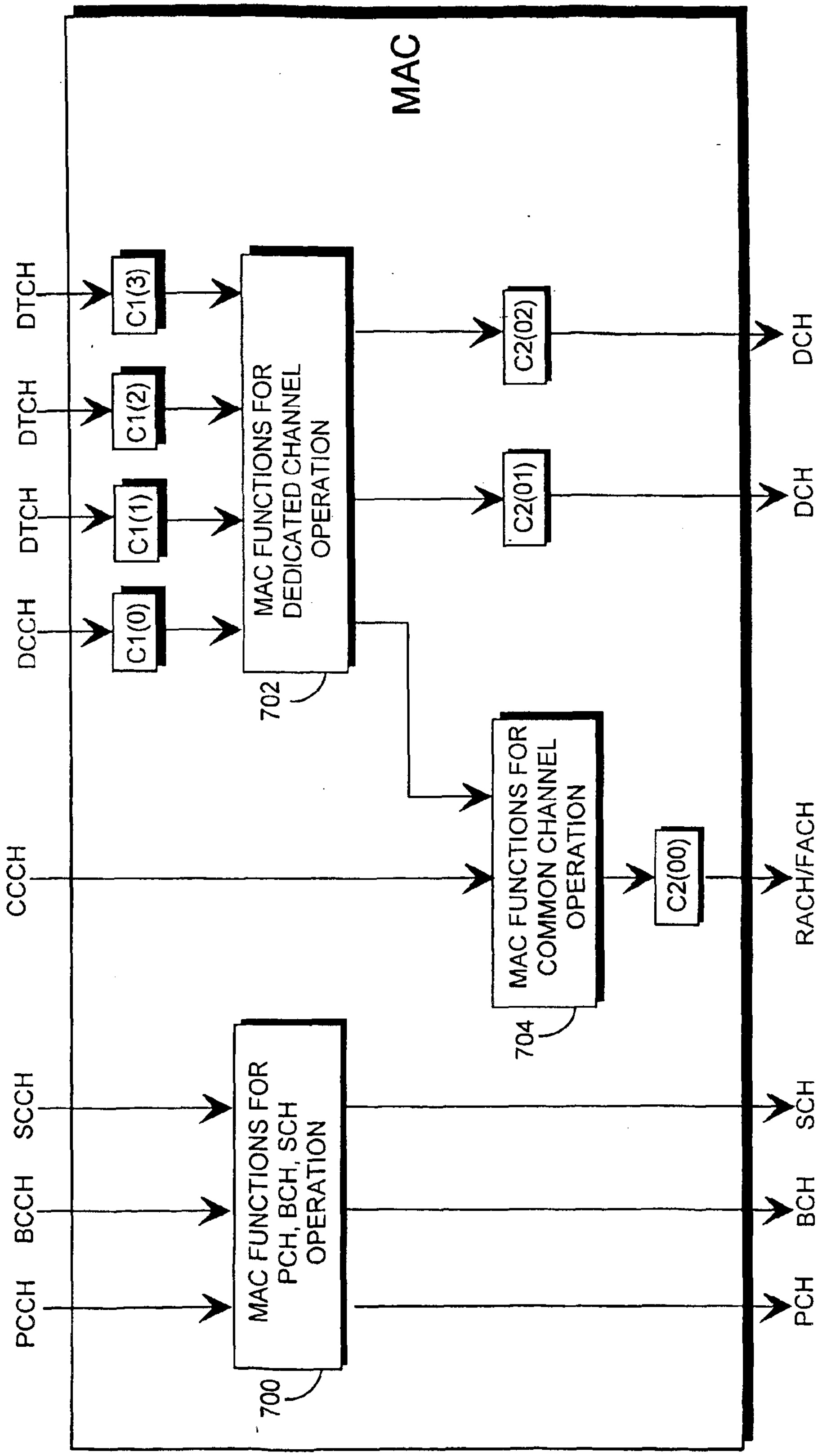

MAC
DTCH
DTCH
DTCH
DCCH
C1(3)
C1(2)
C1(1)
C1(0)
MAC FUNCTIONS FOR DEDICATED CHANNEL OPERATION
702
C2(02)
C2(01)
DCH
DCH
CCCH
MAC FUNCTIONS FOR COMMON CHANNEL OPERATION
704
C2(00)
RACH/FACH
SCCH
BCCH
PCCH
MAC FUNCTIONS FOR PCH, BCH, SCH OPERATION
700
SCH
BCH
PCH

Fig 7B

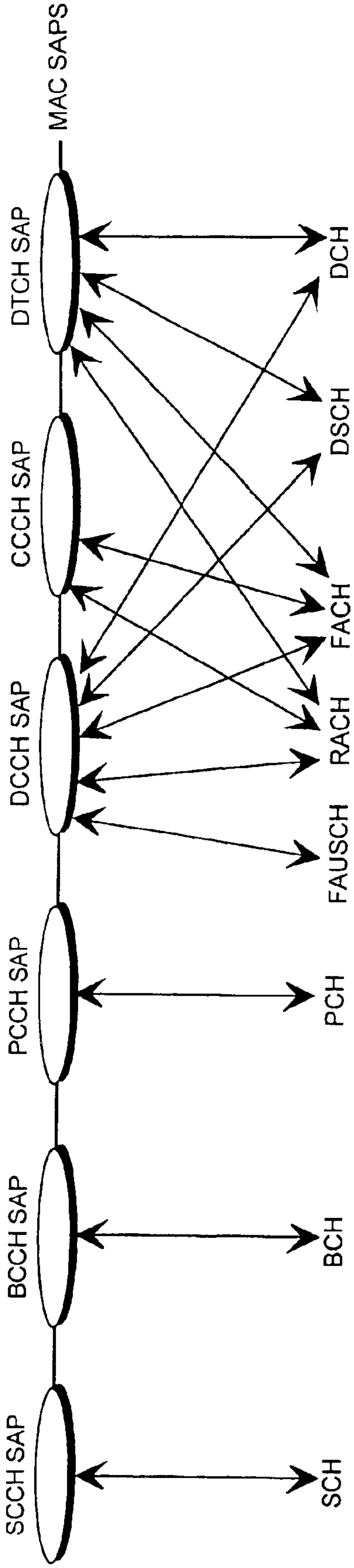

MAC SAPS
DTCH SAP
CCCH SAP
DCCH SAP
PCCH SAP
BCCH SAP
SCCH SAP
DCH
DSCH
FACH
RACH
FAUSCH
PCH
BCH
SCH

Fig 7C

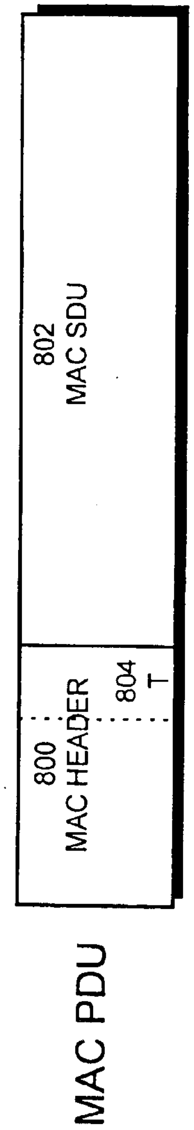

MAC PDU
800
MAC HEADER
804
T
802
MAC SDU

Fig 8

METHOD OF CIPHERING DATA TRANSMISSION IN A RADIO SYSTEM

FIELD OF INVENTION

The invention relates to a method of ciphering data transmission in a radio system.

BACKGROUND OF INVENTION

Ciphering is today used in many data transmission systems to prevent the data transmitted from falling into the hands of an unauthorized user. The ciphering has grown in significance in the past few years, particularly as wireless telecommunication has become more common.

The ciphering can be performed, for example, by encrypting the information to be transmitted in a transmitter, and by decrypting the information in a receiver. In the encryption means the information to be transmitted, for example a bit stream, is multiplied by a certain number of encryption bit patterns, whereby it is difficult to find out what the original bit stream was if the encryption bit pattern used is unknown.

In a digital GSM system, for example, ciphering is performed on the radio path: a ciphered bit stream to be transmitted onto the radio path is formed by XORing data bits with ciphering bits, the ciphering bits being formed by an algorithm known per se (the A5 algorithm), using a ciphering key Kc. The A5 algorithm encrypts the information transmitted on the traffic channel and the DCCH control channel.

The ciphering key Kc is set when the network has authenticated the terminal but the traffic on the channel has not yet been ciphered. In the GSM system the terminal is identified on the basis of the International Mobile Subscriber Identity IMSI, which is stored in the terminal, or the Temporary Mobile Subscriber Identity TMSI, which is formed on the basis of the subscriber identity. A subscriber identification key Ki is also stored in the terminal. A terminal identification key is also known to the system.

In order that the ciphering would be reliable, information on the ciphering key Kc must be kept secret. The cipher key is therefore transmitted from the network to the terminal indirectly. A Random Access Number RAND is formed in the network, and the number is then transmitted to the terminal via the base station system. The ciphering key Kc is formed by a known algorithm (the A5 algorithm) from the random access number RAND and the subscriber identification key Ki. The ciphering key Kc is computed in the same way both in the terminal and in the network part of the system.

In the beginning, data transmission on a connection between the terminal and the base station is thus not ciphered. The ciphering does not start until the base station system sends the terminal a cipher mode command. When the terminal has received the command, it starts to cipher data to be sent and to decipher received data. Correspondingly, the base station system starts to decipher the received data after sending the cipher mode command and to cipher the sent data after the reception and successful decoding of the first ciphered message from the terminal. In the GSM system the cipher mode command comprises a command to start ciphering, and information on the algorithm to be used.

The problem in the known methods is that they have been designed for the present systems, wherefore they are inflexible and not suited for the ciphering of data transmission in new systems, where several parallel services for one mobile station are possible. If we use the same ciphering mask twice for two or more parallel protocol data units that will be sent using the same air interface frame, then an eavesdropper may deduce a lot of information from the data streams. The amount of information that can be deduced depends on the structure of the data streams. From random data that has no structure one cannot obtain any information, but usually there is a structure in the data, especially in the signaling data.

BRIEF DESCRIPTION OF INVENTION

It is an object of the invention to provide a method, and a user equipment and a radio network subsystem implementing the method, solving the above problems. This is achieved with a method of ciphering data transmission in a radio system, comprising: generating a ciphering key; producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter; producing ciphered data by applying the ciphering mask to plain data. Using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm.

The invention also relates to a user equipment, comprising: generating means for generating a ciphering key; a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter; ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data. The ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter.

The invention further relates to a radio network subsystem, comprising: generating means for generating a ciphering key; a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter; ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data. The ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter.

The preferred embodiments of the invention are claimed in the dependent claims.

Several advantages are achieved with the invention. In the solution of the present invention, ciphering and its properties can be flexibly controlled. The present invention enhances user security in new radio systems. This solution is also better than the known technique, which uses a long enough ciphering mask only once for each air interface frame, because it allows distributed implementation of the needed functionality in the protocol stack.

BRIEF DESCRIPTION OF FIGURES

In the following the invention will be described in greater detail by means of preferred embodiments and with reference to the attached drawings, in which

FIGS. **1**A and **1**B illustrate an example of a mobile telephone system;

FIG. **2**A illustrates a transmitter and a receiver;

FIG. **2**B illustrates transport channel coding and multiplexing;

FIG. **3** illustrates a frame structure;

FIGS. **4**A, **4**B and **4**C show a block diagram of a ciphering environment according to the invention;

FIG. **5** illustrates a mobile station

FIG. **6** is a flow diagram illustrating a method according to the invention;

FIG. **7**A illustrates an example of a protocol stack;

FIG. **7**B illustrates an example of a protocol stack according to the invention;

FIG. **7**C illustrates mapping between logical channels and transport channels;

FIG. **8** illustrates the structure of a Medium Access Control Layer Protocol Data Unit.

DETAILED DESCRIPTION OF INVENTION

The present invention can be used in different mobile telephone systems. In the following examples, the use of the invention is described in the Universal Mobile Telephone System (UMTS) without restricting the invention to it. The examples illustrate the FDD (Frequency Division Duplex) operation of the UMTS, but do not restrict the invention to it.

With reference to FIGS. **1**A and **1**B, a typical mobile telephone system structure will be described. FIG. **1**B only comprises the blocks that are essential for the description of the invention, although it is apparent to a person skilled in the art that a common mobile telephone system also comprises other functions and structures, which need not be discussed in greater detail here. The main parts of the mobile telephone system are: a core network CN, a UMTS terrestrial radio access network UTRAN, and a user equipment UE. The interface between the CN and the UTRAN is called the Iu interface, and the interface between the UTRAN and the UE is called the Uu interface.

The UTRAN is composed of radio network subsystems RNS. The interface between two RNSs is called the Iur interface. The RNS is composed of a radio network controller RNC and one or more node Bs B. The interface between the RNC and the node B is called the Iub interface. The reception area of the node B, i.e. cell, is denoted in FIG. **1**A by C.

As the presentation in FIG. **1**A is very abstract, it is clarified in FIG. **1**B by setting forth the parts of the GSM system that correspond to the parts of the UMTS. It is clear that the presented mapping is by no means a binding one but an approximation, because the responsibilities and functions of the parts of the UMTS are still being planned.

FIG. **1**B illustrates a packet switched transmission via Internet **102** from a computer **100** connected with the mobile telephone system to a portable computer **122** connected with a user equipment UE. The user equipment UE may be a fixedly mounted wireless local loop terminal, a vehicle-mounted terminal or a hand-held portable terminal, for example.

The infrastructure of the radio network UTRAN is composed of radio network subsystems RNS, i.e. base station subsystems. The radio network subsystem RNS is composed of a radio network controller RNC, i.e. a base station controller, and at least one node B, i.e. a base station, under the control of the RNC.

The node B comprises a multiplexer **114**, transceivers **116**, and a control unit **118** which controls the operation of the transceivers **116** and the multiplexer **114**. The multiplexer **114** arranges the traffic and control channels used by a plurality of transceivers **116** on a single transmission connection Iub.

The transceivers **116** of the node B have a connection to an antenna unit **120** which is used for providing a bi-directional (or sometimes one-way) radio connection Uu to a user equipment UE. The structure of the frames transmitted on the radio connection Uu is determined in detail and the connection is referred to as an air interface.

The radio network controller RNC comprises a group switching field **110** and a control unit **112**. The group switching field **110** is used for switching speech and data and for connecting signaling circuits. The node B and the radio network controller RNC form a base station subsystem, which additionally comprises a transcoder, also known as a speech codec, or TRAU (Transcoder and Rate Adapter Unit) **108**.

The division of the functions and the physical structures of the radio network controller RNC and the node B may differ according to the actual realization of the radio network subsystem. Typically, the node B implements the radio connection. The radio network controller RNC typically manages the following: radio resource control, inter-cell handover control, power control, timing and synchronization, and paging for user equipment.

The transcoder **108** is usually located as close to a mobile switching center **106** as possible because this allows speech to be transmitted between the transcoder **108** and the radio network controller RNC in a cellular radio network form, which saves transmission capacity.

The transcoder **108** converts different digital speech coding modes used between a public switched telephone network and a cellular radio network to make them compatible, for instance from the 64 kbit/s fixed network form to another form (such as 13 kbit/s) of the cellular radio network, and vice versa. Naturally, the transcoding is carried out only for speech. The control unit **112** carries out call control, mobility management, collection of statistical data and signaling.

The core network CN is composed of the infrastructure belonging to the mobile telephone system which is not part of the UTRAN. FIG. **1**B illustrates two equipments, which are part of the core network CN, namely a mobile switching center **106**, and a gateway mobile switching center **104**, which handles mobile telephone system interfaces towards the outside world, in this example towards the Internet **102**.

FIG. **5** illustrates an exemplary structure of the user equipment UE. The essential parts of the user equipment UE are: an interface **504** to the antenna **502** of the user equipment UE, a transceiver **506**, a control part **510** of the user equipment UE, an interface **512** to the battery **514**, and a user interface comprising a display **500**, a keyboard **508**, a microphone **516** and a speaker **518**.

FIG. **2**A illustrates the functioning of a radio transmitter/radio receiver pair. The radio transmitter may be located in the node B or in the user equipment. Correspondingly the radio receiver may be located in the user equipment or in the node B.

The upper portion of FIG. **2**A illustrates the essential functionality of the radio transmitter. Different services placed in a physical channel are, for example, speech, data, moving or still video picture, and the control channels of the system that are processed in the control part **214** of the radio transmitter. The control part **214** is related to the control of the equipment itself and to the control of the connection. FIG. **2**A illustrates manipulation of two different transport channels **200**A, **200**B. Different services call for different source encoding equipment: speech for example calls for a speech codec. For the sake of clarity, source encoding equipment is not, however, presented in FIG. **2**A.

First the logical channels are ciphered in blocks **216**A, **216**B. In the ciphering, ciphered data is produced by applying a ciphering mask to plain data. Then the ciphered data is placed in the transport channel in blocks **200**A, **200**B. As later will be explained with reference to FIGS. **4**A, **4**C and **7**B the ciphering can be performed either for a logical channel or for a transport channel. Different channels are then channel encoded in blocks **202**A and **202**B. One form of channel coding is different block codes, one example of which is a cyclic redundancy check, or CRC. Another typical way of performing channel coding is convolutional coding and its different variations, such as punctured convolutional coding and turbo coding.

Having been channel encoded, the channels are interleaved in an interleaver **204**A, **204**B. The object of the interleaving is to make error correction easier. In the interleaving, the bits are mixed with each other in a predetermined fashion, so that transitory fading on the radio path does not necessarily make the transferred information unidentifiable.

Different signals are multiplexed in block **208** so that they can be sent using the same transmitter.

The interleaved encrypted bits are then spread with a spreading code, scrambled with a scrambling code, and modulated in block **206**, whose operation is described in detail in FIG. **2**B.

Finally, the combined signal is conveyed to the radio frequency parts **210**, which may comprise power amplifiers and bandwidth restricting filters. An analog radio signal is then transmitted through an antenna **212** to the radio path Uu.

The lower portion of FIG. **2**A illustrates the typical functionality of a radio receiver. The radio receiver is typically a Rake receiver. The analog radio signal is received from the radio path Uu by an antenna **234**. The received signal is conveyed to radio frequency parts **232**, which comprise a filter that blocks the frequencies outside the desired frequency band. A signal is then converted in a demodulator **228** into an intermediate frequency or directly into baseband, and in this form the signal is sampled and quantized.

Because the signal in question is a multipath propagated signal, efforts are made to combine the signal components propagated on different multipaths in block **228**, which comprises several Rake fingers.

de-interleaved. After that the physical channels are processed in a specific channel decoder **222**A, **222**B, where the channel coding used in the transmission is decoded. Convolutional coding is advantageously decoded with a Viterbi decoder. After this the transport channels are mapped to the logical channels in blocks **200**A, **200**B, or the other possibility is that the deciphering is performed for the transport channels. The channel decoded channels (logical or transport) are deciphered in blocks **220**A, **220**B by applying a ciphering mask to the received data. Each received logical channel can be further processed, for example, by transferring the data to the computer **122** connected with the user equipment UE. The control channels of the system are conveyed to the control unit **236** of the radio receiver.

FIG. **2**B illustrates how the transport channels are coded and multiplexed. In principle, FIG. **2**B is in part the same as FIG. **2**A but seen from another perspective. In blocks **240**A, **240**B a Cyclic Redundancy Check is added to each Transport Block. Interleaving is performed in two stages, in blocks **242**A, **242**B and **246**. When two or more services having different quality of service requirements are multiplexed into one or more physical channels, then service specific rate matching **244** is used. In rate matching the channel symbol rates are adjusted to an optimum level, where the minimum quality of service requirement of each service is fulfilled with the same channel symbol energy. Mapping of the transport channels to physical channels is performed in block **248**.

As the ciphering is the key issue in the current invention, its principle will be next described in more detail. In Table 1 the first row represents the plain data bits that have to be transmitted to the recipient. The bits on the second row constitute a ciphering mask. The ciphering mask is applied to the plain data, usually by using the exclusive-or operation, i.e. XOR. The resulting ciphered data is on the third row. This ciphered data is sent through the air interface to the recipient. The recipient then performs deciphering by applying the same ciphering mask that has been used in the transmitter to the received data. The fourth row is a ciphering mask that is summed with the third row by using the XOR operation. The resulting recovered data is presented on the fifth row. As we will see, the recovered data is the same as the plain data.

TABLE 1

Plain data	0	1	1	1	0	1	0	0	1	1	1	0	0	1	1	1	0	0	0
Ciphering mask	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	1	1	1	1
Ciphered data	0	1	0	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1
Ciphering mask	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	1	1	1	1
Recovered data	0	1	1	1	0	1	0	0	1	1	1	0	0	1	1	1	0	0	0

In a so-called rowing Rake finger, delays for the different multipath propagated signal components are searched. After the delays have been found, different Rake fingers are allocated for receiving each of the multipath propagated signals by correlating the received signal with the used spreading code delayed with the found delay of that particular multipath. The different demodulated and despread multipaths of the same signal are then combined in order to obtain a stronger signal.

The received physical channel is then demultiplexed in a demultiplexer **224** into data streams of different channels. The channels are then directed each to a de-interleaver **226**A, **226**B, where the received physical channel is then

FIG. **3** shows an example of a frame structure used on a physical channel. Frames **340**A, **340**B, **340**C, **340**D are given a running number from one to seventy-two, and they form a 720-millisecond long super frame. The length of one frame **340**C is ten milliseconds. The frame **340**C is divided into sixteen slots **330**A, **330**B, **330**C, **330**D. The length of slot **330**C is 0.625 milliseconds. One slot **330**C corresponds typically to one power control period, during which the power is adjusted for example by one decibel up or down.

The physical channels are divided into different types, including common physical channels and dedicated physical channels.

The common physical channels are used to carry the following transport channels: PCH, BCH, RACH and FACH.

The dedicated physical channels consist of dedicated physical data channels (DPDCH) **310** and dedicated physical control channels (DPCCH) **312**. The DPDCHs **310** are used to carry data **306** generated in layer two of the OSI (Open Systems Interconnection) model and layers above it, i.e. dedicated control channels (DCH). The DPCCHs **312** carry the control information generated in layer one of the OSI model. Control information comprises: pilot bits **300** used in channel estimation, feedback information (FBI) **308** transmit power-control commands (TPC) **302**, and optionally a transport format combination indicator (TFCI) **304**. The TFCI **304** tells the receiver the transport formats of different transport channels, i.e. Transport Format Combination, used in the current frame.

As can be seen from FIG. **3**, the down-link DPDCHs **310** and DPCCHs **312** are time multiplexed into the same slot **330**C. In the up-link the channels are sent in parallel so that they are IQ/code multiplexed (I=in-phase, Q=quadrature) into each frame **340**C.

The channels in the radio interface Uu are processed according to a protocol architecture comprising, according to the ISO (International Standardization Organization) OSI (Open Systems Interconnection) model, three protocol layers: a physical layer (=layer one), a data link layer (=layer two), and a network layer (=layer three). The protocol stacks are located both in the radio network subsystem RNS and in the user equipment UE. Each unit (e.g. user equipment, or radio network subsystem) has a layer which is in logical communication with a layer of another unit. Only the lowest, physical layers communicate with each other directly. The other layers always use the services offered by the next, lower layer. The message must thus physically pass in the vertical direction between the layers, and only in the lowermost layer the message passes horizontally between the layers. FIG. **7**A illustrates the layers of the protocol architecture. The ovals between different sub-layers indicate service access points (SAP).

The physical layer L**1** offers different transport channels to the MAC sub-layer MAC and higher layers. The physical layer transport services are described by how and with what characteristics data is transferred over the radio interface. The transport channels include a Paging Channel PCH, Broadcast Channel BCH, Synchronization Channel SCH, Random Access Channel RACH, Forward Access Channel FACH, Down-link Shared Channel DSCH, Fast Up-link Signaling Channel FAUSCH, and Dedicated Channel DCH. The physical layer L**1** maps transport channels with physical channels. In the FDD (Frequency Division Duplex) mode a physical channel is characterized by the code, frequency and, in the up-link, the relative phase (I/Q). In the TDD (Time Division Duplex) mode the physical channel is also characterized by the time slot.

The transport channels may be divided into common channels (where there is a need for in-band identification of the UEs when particular UEs are addressed) and dedicated channels (where the UEs are identified by the physical channel, i.e. code and frequency for the FDD and code, time slot and frequency for the TDD).

The common transport channel types are as follows. The RACH is a contention based up-link channel used for transmission of a relatively small amount of data, for example of initial access or non-real-time dedicated control or traffic data. The FACH is a common down-link channel without closed-loop power control used for transmission of a relatively small amount of data. The DSCH is a down-link channel shared by several UEs carrying dedicated control or traffic data. The BCH is a down-link channel used for broadcasting system information to an entire cell. The SCH is a down-link channel used for broadcasting synchronization information to an entire cell in the TDD mode. The PCH is a down-link channel used for broadcasting control information to an entire cell allowing efficient UE sleep mode procedures.

The dedicated transport channel types, in turn, are as follows. The DCH is a channel dedicated to one UE used in up-link or down-link. The FAUSCH is an up-link channel used to allocate dedicated channels in conjunction with the FACH. The data link layer is divided into two sub-layers: a MAC sub-layer (Medium Access Control) and a RLC sub-layer (Radio Link Control). The MAC sub-layer L**2**/MAC offers different logical channels to the RLC sub-layer L**2**/RLC. The logical channel is characterized by the type of information that is transferred. The logical channels include a Paging Control Channel PCCH, Broadcast Control Channel BCCH, Synchronization Control Channel SCCH, Common Control Channel, Dedicated Control Channel DCCH and Dedicated Traffic Channel DTCH.

The control channels are used for transfer of control plane information only. The SCCH is a down-link channel for broadcasting synchronization information in case of TDD (Time Division Duplex) operation. The BCCH is a down-link channel for broadcasting system control information. The PCCH is a down-link channel that transfers paging information. The CCCH is a bi-directional channel for transmitting control information between the network and the UEs. This channel is commonly used by the UEs having no RRC connection with the network. The DCCH is a point-to-point bi-directional channel that transmits dedicated control information between the UE and the network. This channel is established through an RRC connection setup procedure.

The traffic channels are used for the transfer of user plane information only. The DTCH is a point-to-point channel, dedicated to one UE, for the transfer of user information. A DTCH can exist in both up-link and down-link.

The MAC layer maps logical channels with transport channels. One of the functions of the MAC sub-layer is to select the appropriate transport format for each transport channel depending on the momentary source bit rate.

FIG. **7**C illustrates mapping between logical channels and transport channels. An SCCH is connected to an SCH. A BCCH is connected to a BCH. A PCCH is connected to a PCH. A CCCH is connected to a RACH and a FACH. A DTCH can be connected to either a RACH and a FACH, to a RACH and a DSCH, to a DCH and a DSCH, or to a DCH. A DCCH can be connected to either a RACH and a FACH, to a RACH and a DSCH, to a DCH and a DSCH, to a DCH, or to a FAUSCH.

The third layer L**3** has a RRC sub-layer (Radio Resource Control) that handles the control plane signaling of layer three between the user equipment and the network. Among the functions carried out by the RRC sub-layer are assignment, reconfiguration and release of radio resources for the RRC connection. So the RRC sub-layer handles the assignment of the radio resources required for the RRC connection, including the requirements of both the control and the user plane. The RRC layer may reconfigure radio resources during an established RRC connection.

In the present invention we are interested in the encryption of the different services' data flows of one user. According-ing to the known techniques, all data flows would be encrypted using the same ciphering mask.

The method according to the invention for ciphering data transmission in a radio system is presented in FIG. **6**. The performance of the method begins in block **600**.

In block **602** a ciphering key is generated according to a known technique, for example as described in the Background of the Invention section.

In block **604**A a ciphering mask is produced in a ciphering algorithm using the ciphering key as an input parameter. Also a logical channel specific parameter or a transport channel specific parameter is used as an additional input parameter to the ciphering algorithm. The logical channel specific parameter can be one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier, or some other parameter identifying the logical channel used. The transport channel specific parameter can be, for example, the Dedicated Channel Identifier, or some other parameter identifying the transport channel used.

The term 'bearer' is a high-level name for transmission of information used in connection with a network service. Depending on the services, information in the UMTS can usually be transmitted using one or more bearers. The services include, for example, speech transmission, data services and video service. A radio bearer, on the other hand, represents that part of the bearer which extends over the air interface. One logical channel normally carries one radio bearer. A logical channel defines the service offered by the MAC layer. A logical channel can be mapped to different types of transport channels depending on the existing service mode (either to a dedicated transport channel or common transport channels). The transport channels define the services offered by the physical layer. It is also possible to multiplex several logical channels into one transport channel in the MAC layer. The transport channels are further mapped to physical channels in the physical layer. Several transport channels can be multiplexed into one physical channel by layer **1**. It is also possible that after transport channel multiplexing the data stream is divided between several physical channels.

The invention can thus be applied to a radio system whose terminals can communicate with other transceivers using one or more parallel radio bearers. Typically, when a call is established between a terminal and a network, a physical channel is first established for a Signaling Radio Bearer SRB between the terminal and the radio network subsystem, and once this channel has been established, the actual traffic bearer(s) can be established. The SRB can also be called a signaling link.

The direction of transmission (up-link/down-link) can be used as an additional input parameter to the ciphering algorithm.

Yet another parameter exists: a radio frame specific parameter can be used as an additional input parameter to the ciphering algorithm. The radio frame specific parameter can be, for example, the User Equipment Frame Number (UEFN), or some other parameter identifying the used radio frame. The radio frame specific parameter depends on the protocol layer where the ciphering function is implemented. If it is implemented in the protocol layer that is terminated in the UE and the CN, then a mechanism for conveying the used frame number to the receiving entity has to be defined. If the ciphering function is located in the MAC layer or layer **1** (or some other layer terminated in the UE and the node B or the RNC), a frame number at least partly consisting of the physical frame number can be used, which means that the used frame number need not be signaled with the data.

In block **606** ciphered data is produced by applying the ciphering mask to plain data, using for example the XOR operation as described in Table 1.

Next, an elaborated example illustrating the implementation of the ciphering method in the transmitter and in the receiver is explained in connection with FIGS. **4**A, **4**B and **4**C. Only the relevant points will be illustrated, but it will be clear for a person skilled in the art how ciphering can be performed in various situations for example with different numbers of PDUs.

FIG. **4**A describes a block diagram defining the basic ciphering environment defined in this invention. Generating means **408** are used for generating a ciphering key **410** according to a known technique. Connected with the generating means **408** there is a ciphering algorithm **400** for producing ciphering masks **412**A, **412**B, **412**C. The ciphering algorithm uses the generated ciphering key **410** as an input parameter. The ciphering algorithm **400** uses a logical channel specific parameter **402**A as an additional input parameter.

In the receiver end, the logical channel specific parameter needed for deciphering can be read from an unciphered MAC header, for example from the C/T-field of the MAC header. The structure of the MAC PDU is illustrated in FIG. **8**. The MAC PDU consists of an optional MAC header **800** and a MAC Service Data Unit (MAC SDU) **802**. Both the MAC header and the MAC SDU are of variable size. The content and the size of the MAC header **800** depend on the type of the logical channel, and in some cases none of the parameters in the MAC header **800** are needed. The size of the MAC-SDU **802** depends on the size of the RLC PDU, which is defined during the set-up procedure. The MAC header **800** comprises a C/T-field **804**. This option allows efficient MAC multiplexing of different logical channels (or different instances of the same logical channel type) into one transport channel, both into dedicated transport channels and common transport channels. When this method is used, the MAC header is not ciphered, which allows separating the different MAC PDUs in the receiver end and which in the common channel mode allows reading the RNTI (Radio Network Temporary Identity) field that is needed for routing messages to the correct entity in the UTRAN.

Connected with the ciphering algorithm **400** there are ciphering means **416**A, **416**B, **416**C for producing ciphered data **418**A, **418**B, **418**C by applying the ciphering mask **412**A, **412**B, **412**C to the plain data **414**A, **414**B, **414**C. As can be seen from FIG. **4**A, the plain data includes Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and for each logical channel an individual ciphering mask is produced. So in FIG. **4**A the ciphering masks **412**A, **412**B and **412**C are all different from each other.

In block **420** the ciphered RLC-PDUs are processed through the MAC layer and mapped into one Transport Block Set, i.e. MAC PDU Set.

Another possible solution is one in which the plain data includes one Radio Link Control Layer Protocol Data Unit **414**A from only one logical channel, and for said logical channel an individual ciphering mask **412**A is produced. So the invention also works for the individual logical channel.

Normally a new ciphering mask is produced for each radio frame of the physical layer of the protocol stack. If interleaving is used, then a new ciphering mask can be produced for each interleaving period of the physical layer of the protocol stack. Typically one interleaving period consists of several radio frames.

The left-hand side of FIG. **4**A represents the operations carried out in the transmitter. The corresponding operations will also be carried out in the receiver, as illustrated on the right-hand side of FIG. **4**A. The only differences are that block **422** is used to derive RLC-PDUs out of the received Transport Block Set, and that the deciphering means **424**A, **424**B, **424**C are used to decipher the received data.

In one embodiment of the invention, a Radio Link Control Layer Protocol Data Unit of at least one logical channel is already ciphered, and the step of producing ciphered data is not repeated for said already ciphered Radio Link Control Layer Protocol Data Unit. It is thus avoided that the data would be ciphered twice. Of course, if for example such end-to-end ciphering is used, the data can be ciphered twice: first by the application using the service, and then by the MAC layer according to the invention. This will cause no loss of transmission capacity, as the XOR operation does not add any extra bits, even if it is performed twice.

FIG. **4**B illustrates a solution to a situation where the plain data includes at least two successive Radio Link Control Layer Protocol Data Units of one logical channel. If we assume, for example, that the first RLC PDU **414**A and the second RLC PDU **414**B are from one logical channel, then the problem can be solved in such a way that only one ciphering mask **412**A is produced for these PDUs **414**A, **414**B. Different parts of this ciphering mask **412**A are then used for ciphering the first PDU **414**A and the second PDU **414**B. The length of the required ciphering mask **412**A in this case is naturally the sum of the lengths of the first and the second PDU **414**A, **414**B. Because the PDUs **414**A, **414**B are from the same logical channel (same Radio Access Bearer), the maximum length required can be calculated as being two times the maximum RLC PDU size of that bearer.

FIG. **4**C illustrates a situation where the plain data includes one Transport Block Set (TBS) including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and for each Transport Block Set one ciphering mask **412** is used in producing the ciphered data. In this option, the basic unit to be ciphered is a Transport Block Set. This defines the required length of the ciphering mask **412** produced by the algorithm **400**. Layer **1** still adds Transport Block specific CRCs (Cyclic Redundancy Check), but because the XOR operation does not change the length of data, it should be possible to cipher the whole TBS as one unit. The length of each transport block in the TBS has to be told to L**1** anyway. This option has the disadvantage that the MAC header is also ciphered, and so the MAC PDUs cannot be routed anywhere on the network side before the TBS is deciphered. This is a problem if common channels over Iur are possible. The length of the required ciphering mask **412** is equal to the maximum Transport Block Set size for the transport channel in question.

Another possible solution is one in which the plain data includes one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

The solution of the invention is implemented in the radio system preferably by software, whereby the invention requires certain functions in the protocol processing software located in the transmitter and in the receiver, especially in blocks **204**A, **204**B and **226**A, **226**B of FIG. **2**A. Thus the generating means **408**, the ciphering algorithm **400**, and the ciphering means **416**A, **416**B, **416**C can be software modules of the protocol stack residing in the user equipment UE and in the radio network subsystem RNS. The solution can also be implemented with hardware, for example using ASIC (Application Specific Integrated Circuit) or discrete components.

The method of the invention can be implemented, for example, in the Medium Access Control Layer of the protocol stack. This is illustrated in FIG. **7**B, which shows a high-level overview of the MAC layer depicted in FIG. **7**A with ciphering functions included. C**1**( ) and C**2**( ) are two alternatives for the location of ciphering. C**1**(**0**), C**1**(**1**), C**1**(**2**) and C**1**(**3**) refer to the use of logical channel specific ciphering parameters as explained above with reference to FIGS. **4**A and **4**B, whereas C**2**(**00**), C**2**(**01**) and C**2**(**02**) refer to the use of transport channel specific ciphering parameters. Some MAC functions may be needed below C**2**(**00**), C**2**(**01**) and C**2**(**02**) blocks, but for the sake of clarity they are not illustrated here. Basically the RLC PDUs come to the MAC layer from each logical channel. In the MAC layer the RLC-PDUs are then mapped to the MAC PDUs in the functional blocks **700**, **702**, **704**, which include the operations for the PCH, BCH, SCH, Dedicated Channel and Common Channel operations. Normally one RLC PDU is mapped to one MAC PDU (=Transport Block). This mapping realizes the mapping from a logical channel to a transport channel. The mapping rules have been explained above in connection with FIG. **7**C. If ciphering is used for the CCCH then a ciphering block, for example C**1**(**4**), should be in FIG. **7**B in the line between the ‘CCCH’ and the functional block **704**.

Even though the invention is described above with reference to an example shown in the attached drawings, it is apparent that the invention is not restricted to it, but can vary in many ways within the inventive idea disclosed in the attached claims.

What is claimed is:

1. A method of ciphering data transmission in a radio system, comprising:

generating a ciphering key;

producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter;

producing ciphering data by applying the ciphering mask to plain data;

using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm,

wherein the logical channel specific parameter is one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

2. The method as claimed in claim **1**, further comprising:

using the direction of transmission as an additional input parameter to the ciphering algorithm.

3. A method of ciphering data transmission in a radio system, comprising:

generating a ciphering key;

producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter;

producing ciphered data by applying the ciphering mask to plain data;

using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm,

wherein the transport channel specific parameter is a Dedicated Channel Identifier.

4. A method of ciphering data transmission in a radio system, comprising:

generating a ciphering key;

producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter;

producing ciphered data by applying the ciphering mask to plain data;

using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm;

using a radio frame specific parameter as an additional input parameter to the ciphering algorithm;

wherein the radio frame specific parameter is a User Equipment Frame Number.

5. A method of ciphering data transmission in a radio system, comprising:

generating a ciphering key;

producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter;

producing ciphered data by applying the ciphering mask to plain data;

using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm,

wherein the plain data includes Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and for each logical channel an individual ciphering mask is produced.

6. The method as claimed in claim **5**, wherein a Radio Link Control Layer Protocol Data Unit of at least one logical channel is already ciphered, and the step of producing ciphered data is not repeated for said already ciphered Radio Link Control Layer Protocol Data Unit.

7. A method of ciphering data transmission in a radio system, comprising:

generating a ciphering key;

producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter;

producing ciphered data by applying the ciphering mask to plain data;

using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm,

wherein the plain data includes at least two successive Radio Link Control Layer Protocol Data Units of one logical channel, and for each Radio Link Control Layer Protocol Data Unit a different part of the ciphering mask is used in producing the ciphered data.

8. A method of ciphering data transmission in a radio system, comprising:

generating a ciphering key;

producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter;

producing ciphered data by applying the ciphering mask to plain data;

using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm,

wherein the plain data includes one Transport Block Set including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

9. A method of ciphering data transmission in a radio system, comprising:

generating a ciphering key;

producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter,

producing ciphered data by applying the ciphering mask to plain data;

using a logical channel specific paramter or a transport channel specific parpmeter as an additional input parameter to the ciphering algorithm,

wherein the plain data includes one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

10. A user equipment, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or transport channel specific parameter as an additional input parameter,

wherein the logical channel specific parameter is one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

11. A user equipment, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the transport channel specific parameter is a Dedicated Channel Identifier.

12. A user equipment, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter;

wherein the ciphering algorithm uses a radio frame specific parameter as an additional input parameter, and

the radio frame specific parameter is a User Equipment Frame Number.

13. A user equipment, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transpoirt channel specific parameter as an additional input parameter;

wherein the ciphering means accept plain data including Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and the ciphering algorithm produces for each logical channel an individual ciphering mask, and the ciphering means use for each logical channel the ciphering mask of said channel.

14. The user equipment as claimed in claim **13**, wherein a Radio Link Control Layer Protocol Data Unit of at least one logical channel is already ciphered, and the ciphering means do not cipher said already ciphered Radio Link Control Layer Protocol Data Unit.

15. A user equipment, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the ciphering means accept plain data including at least two successive Radio Link Control Layer Protocol Data Units on one logical channel, and the ciphering algorithm produces for said logical channel an individual ciphering mask, and the ciphering means use for each Radio Link Control Layer Protocol Data Unit different part of the ciphering mask.

16. A user equipment, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the ciphering means accept plain data including one Transport Block Set including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and the ciphering algorithm produces for each Transport Block Set an individual ciphering mask, and the ciphering means use for each Transport Block Set one ciphering mask.

17. A user equipment, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the ciphering means accept plain data including one Transport Block Set including a Medium Access Control Layer Protocol Data Unit on one logical channel, and the ciphering algorithm produces for each Transport Block Set an individual ciphering mask, and the ciphering means use for each Transport Block Set one ciphering mask.

18. A radio network subsystem, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter;

wherein the logical channel specific parameter is one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

19. A radio network subsystem, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the transport channel specific parameter is a Dedicated Channel Identifier.

20. A radio network subsystem, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the ciphering algorithm uses a radio frame specific parameter as an additional input parameter, and

the radio frame specific parameter is a User Equipment Frame Number.

21. A radio network subsystem, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional parameter,

wherein the ciphering means accept plain data including Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and the ciphering algorithm produces for each logical channel an individual ciphering mask, and the ciphering means use for each logical channel the ciphering mask of said channel.

22. The radio network subsystem as claimed in claim **21**, wherein a Radio Link Control Layer Protocol Data Unit of at least one logical channel is already ciphered, and the ciphering means do not cipher said already ciphered Radio Link Control Layer Protocol Data Unit.

23. A radio network subsystem, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key an an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the ciphering means accept plain data including at least two successive Radio Link Control Layer Protocol Data Units of one logical channel, and the ciphering algorithm produces for said logical channel an individual ciphering mask, and the ciphering means use for each Radio Link Control Layer Protocol Data Unit a different part of the ciphering mask.

24. A radio network subsystem, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the ciphering means accept plain data including one Transport Block Set including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and the ciphering algorithm produces for each Transport Block Set an individual ciphering mask, and the ciphering means use for each Transport Block Set one ciphering mask.

25. A radio network subsystem, comprising:

generating means for generating a ciphering key;

a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter;

ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data;

the ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter,

wherein the ciphering means accept plain data including one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and the ciphering algorithm produces for each Transport Block Set an individual ciphering mask, and the ciphering means use for each Transport Block set one ciphering mask.

* * * * *

EXHIBIT I

US007009940B2

(12) United States Patent
Vialen et al.

(10) **Patent No.: US 7,009,940 B2**
(45) **Date of Patent: Mar. 7, 2006**

(54) **INTEGRITY CHECK IN A COMMUNICATION SYSTEM**

(75) Inventors: **Jukka Vialen**, Espoo (FI); **Valtteri Niemi**, Helsinki (FI)

(73) Assignee: **Nokia Corporation**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 710 days.

(21) Appl. No.: **09/975,410**

(22) Filed: **Oct. 10, 2001**

(65) **Prior Publication Data**

US 2002/0044552 A1 Apr. 18, 2002

Related U.S. Application Data

(63) Continuation of application No. PCT/EP01/00735, filed on Jan. 23, 2001.

(30) **Foreign Application Priority Data**

Feb. 22, 2000 (GB) 0004178

(51) **Int. Cl.**
H04J 1/16 (2006.01)

(52) **U.S. Cl.** **370/252**; 370/278; 370/386; 713/200; 709/222

(58) **Field of Classification Search** 370/328, 370/338, 410, 252, 329, 278, 384, 386; 380/247, 380/270; 455/411; 713/181, 200; 705/75, 705/18; 709/203, 220–222
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,393,269	A		7/1983	Konheim et al.	
5,970,143	A	*	10/1999	Schneier et al.	713/181
6,081,601	A	*	6/2000	Raivisto	380/270
6,108,424	A	*	8/2000	Pitiot	380/270
6,671,507	B1	*	12/2003	Vinck	455/411
6,728,529	B1	*	4/2004	Kuo et al.	455/411
6,751,227	B1	*	6/2004	Ahmavaara et al.	370/410
6,763,112	B1	*	7/2004	Haumont	380/247

FOREIGN PATENT DOCUMENTS

WO	WO 99/39525	8/1999

OTHER PUBLICATIONS

3GPP TS 33.102 V3.9.0 (Jun. 2001)□□3rd Generation Partnership Project; □□Technical Specification Group Services and System Aspects;□□3G Security;□□Security Architecture (Release 1999), pp. 28-35.*

3GPP TS 33.102 V3.3.1 (Jan. 2000), 3rd Generation Partnership Project; Technical Specification Group Services and Aspects; 3G Security Architecture (Release 1999), Sec. 6.4-6.6 (pp. 28-34).*

3GPP TS 33.102 V3.9.0 (2001-06)□□3rd Generation Partnership Project □□Technical Specification Group Services and System Aspects; □□3G Security; □□Security Architecture (Release 1999), pp. 28-35.*

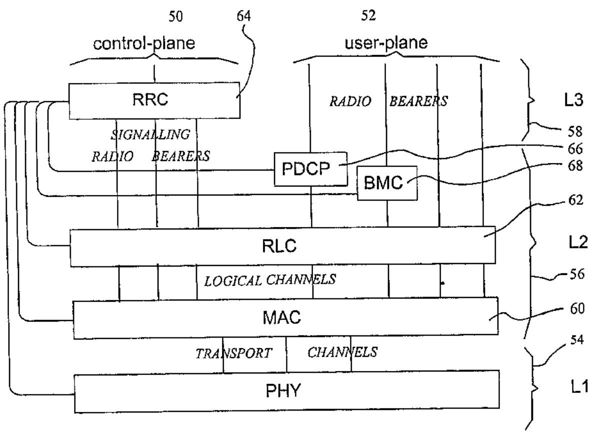
(Continued)

Primary Examiner—John Pezzlo
(74) *Attorney, Agent, or Firm*—Squire, Sanders & Dempsey L.L.P.

(57) **ABSTRACT**

A method of communication between a first node and a second node for a system where a plurality of different channels is provided between said first and second node. The method comprises the step of calculating an integrity output. The integrity output is calculated from a plurality of values, some of said values being the same for said different channels. At least one of said values is arranged to comprise information relating to the identity of said channel, each channel having a different identity. After the integrity output has been calculated, Information relating to the integrity output is transmitted from one of said nodes to the other.

21 Claims, 7 Drawing Sheets



OTHER PUBLICATIONS

3G TS 33.102 V3.3.1 (Jan. 2000), 3rd Generation Partnership; Technical Specification Group Services and System Aspects: 3G Security; Security; Architecture (3G TS 33.102 version 3.3.1 Release 1999), Jan. 2000, pp. 1-64.*

PCT International Search Report.

State of the Art Document: 3G TS 33.102 V3.2.1 (Oct. 1999), 3rd Generation Partnership; Technical Specification Group Services and System Aspects: 3G Security; Security; Architecture pp. 1-64.

Krayem-Nevoux R et al: "Payphone Service For Third Generation Mobile Systems," Proceedings of the Global Telecommunications Conference, vol.-, Nov. 29, 1993, pp. 1708-1712.

Von Bernd Friedrichs: Authentische Und Zuverlassige Mobilkommunikation fur sicherheitsrelevante Anwendungen. Teil II: Systemarchitektur Und Einbettung in GSM; vol. 49, No. 3/04, Mar. 1, 1995, pp. 48-57.

* cited by examiner

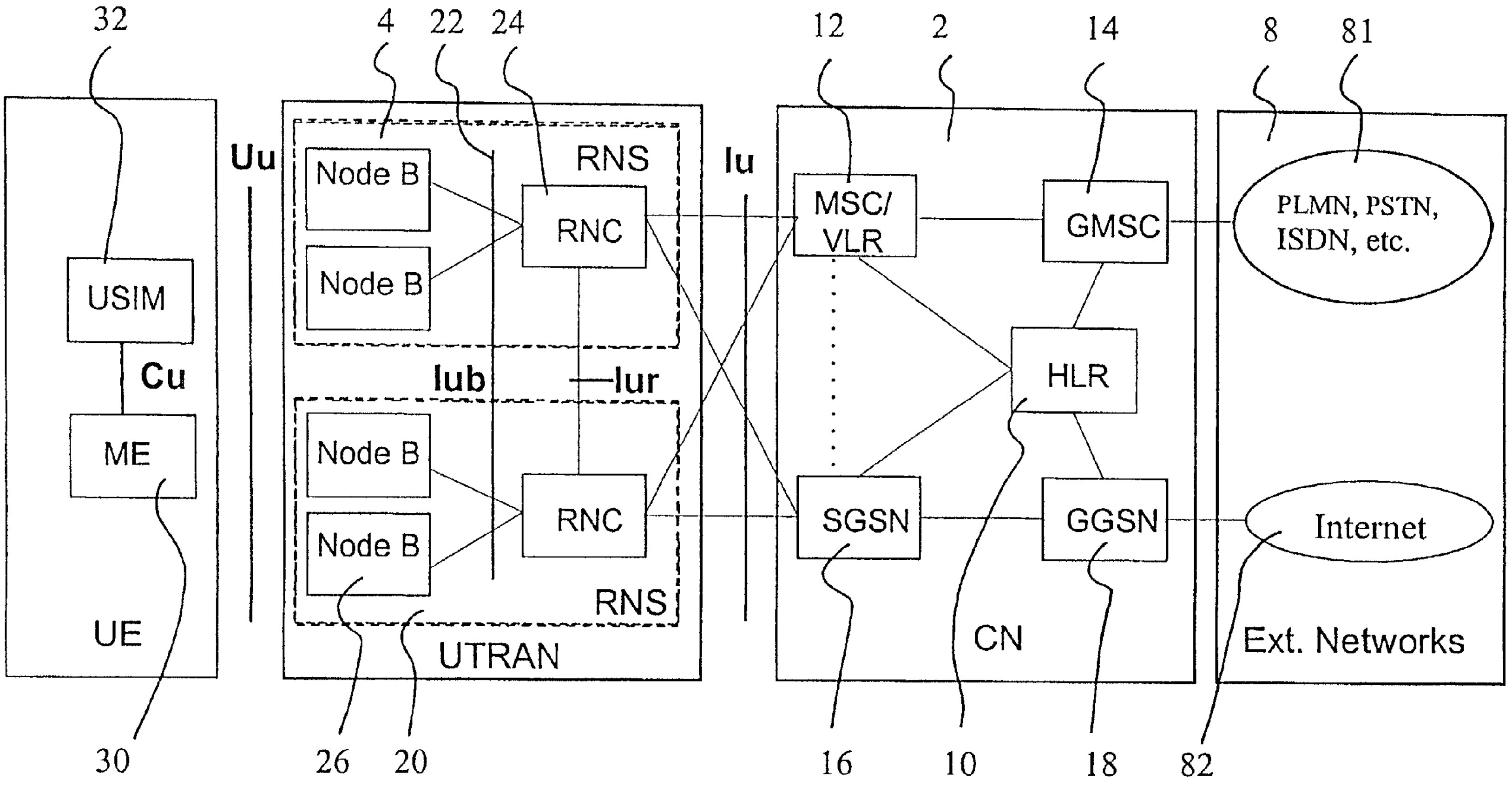

32
4
22
24
12
2
14
8
81
Uu
RNS
Iu
Node B
RNC
MSC/
VLR
GMSC
PLMN, PSTN,
ISDN, etc.
USIM
Node B
HLR
Cu
Iub
—Iur
ME
Node B
RNC
SGSN
GGSN
Internet
Node B
RNS
UE
UTRAN
CN
Ext. Networks
30
26
20
16
10
18
82

Fig. 1

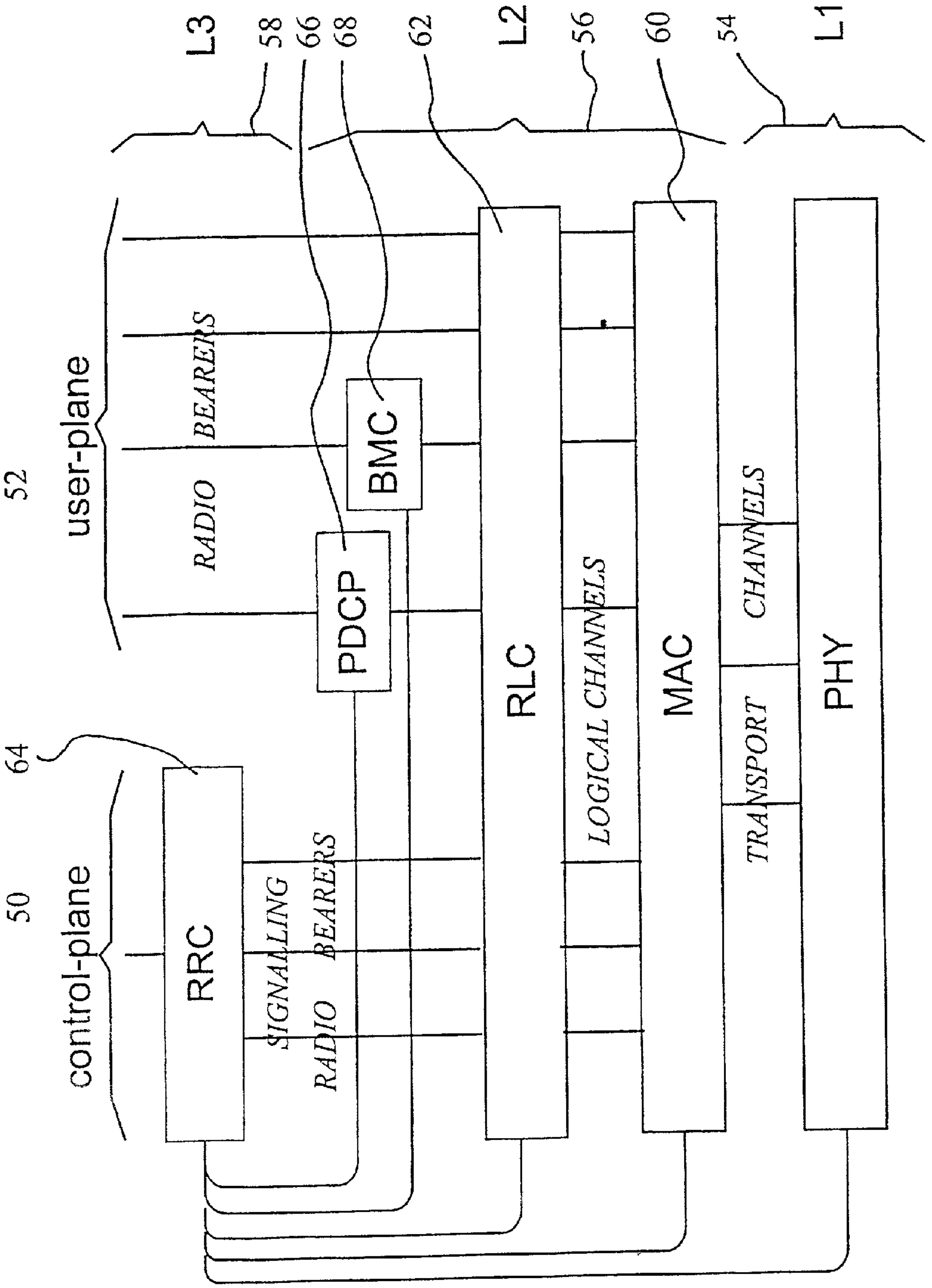

L3
58
66
68
62
L2
56
60
54
L1
52
user-plane
RADIO BEARERS
BMC
PDCP
RLC
LOGICAL CHANNELS
MAC
TRANSPORT CHANNELS
PHY
64
50
control-plane
RRC
SIGNALLING RADIO BEARERS

Fig. 2

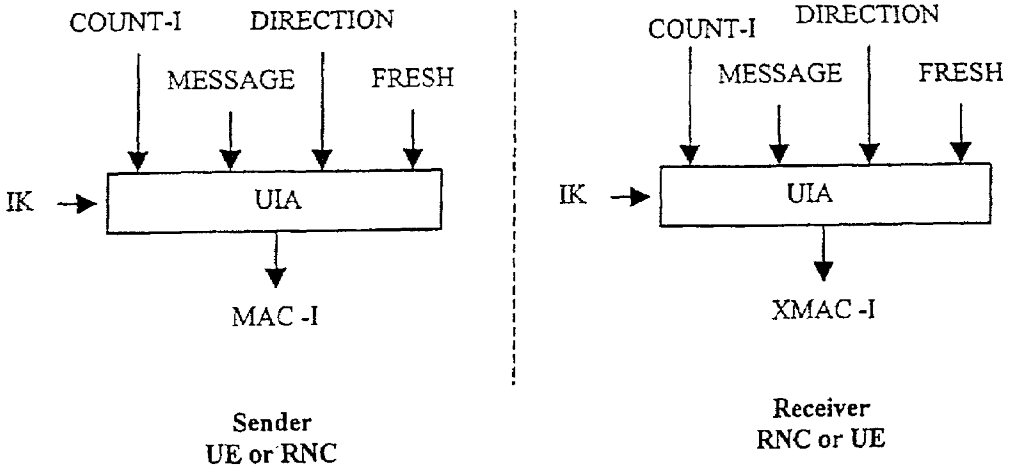

COUNT-I
DIRECTION
MESSAGE
FRESH
IK
UIA
MAC -I
Sender
UE or RNC
COUNT-I
DIRECTION
MESSAGE
FRESH
IK
UIA
XMAC -I
Receiver
RNC or UE

Fig. 3

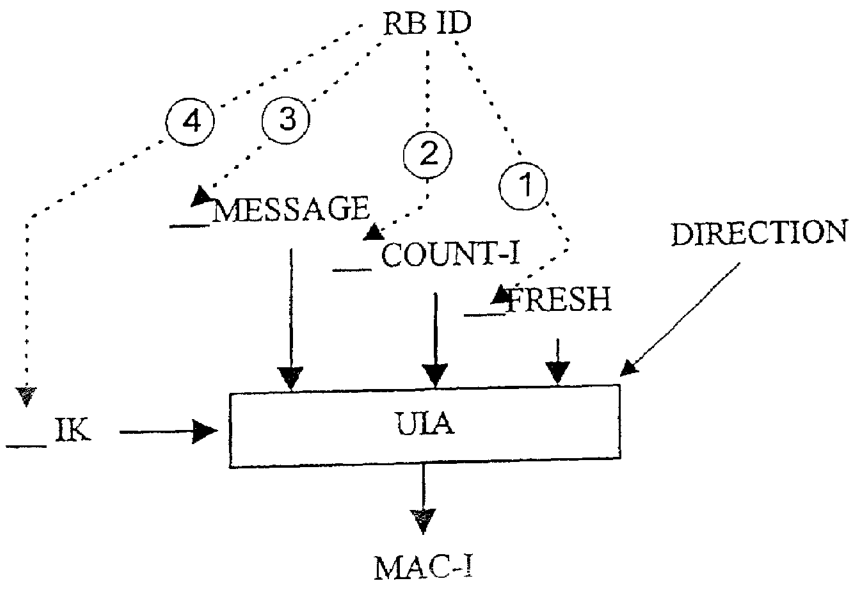

RB ID
4
3
2
1
MESSAGE
COUNT-I
FRESH
DIRECTION
IK
UIA
MAC-I

Fig. 4

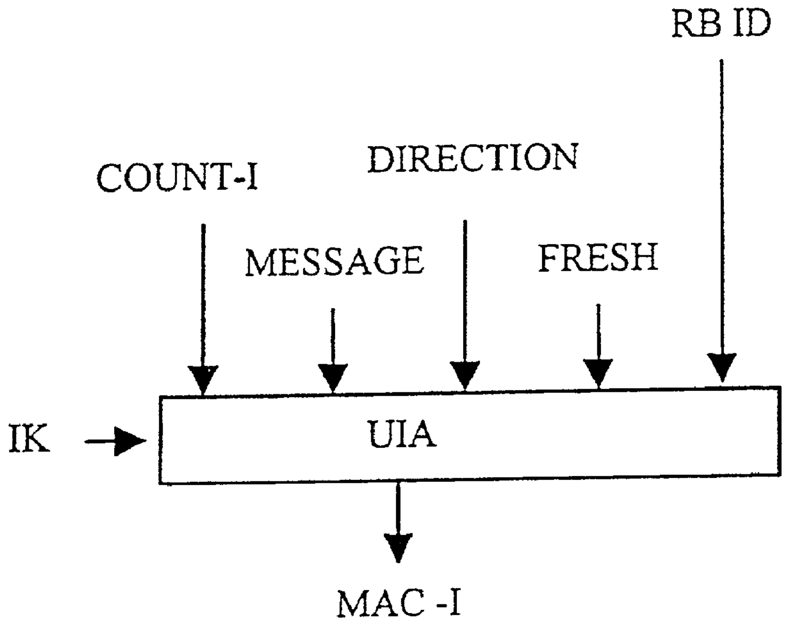

RB ID
COUNT-I
DIRECTION
MESSAGE
FRESH
IK
UIA
MAC -I

Fig. 5

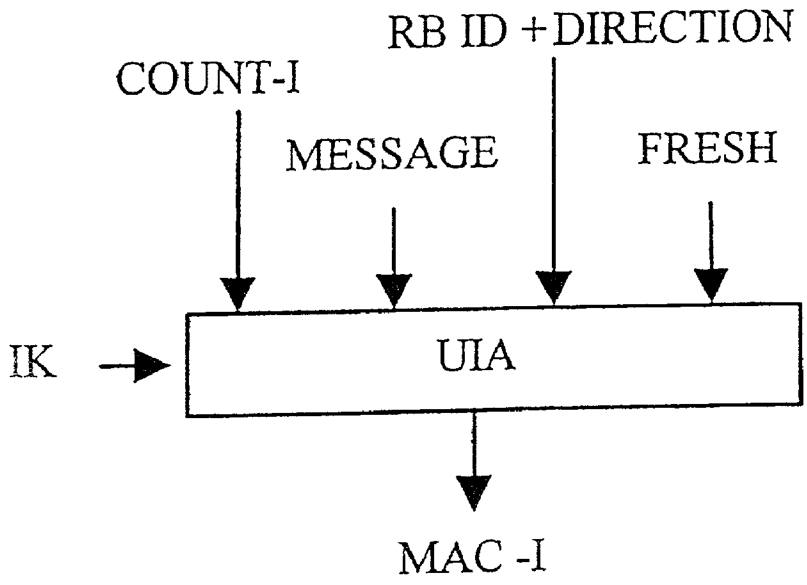

RB ID +DIRECTION
COUNT-I
MESSAGE
FRESH
IK
UIA
MAC -I

Fig. 6

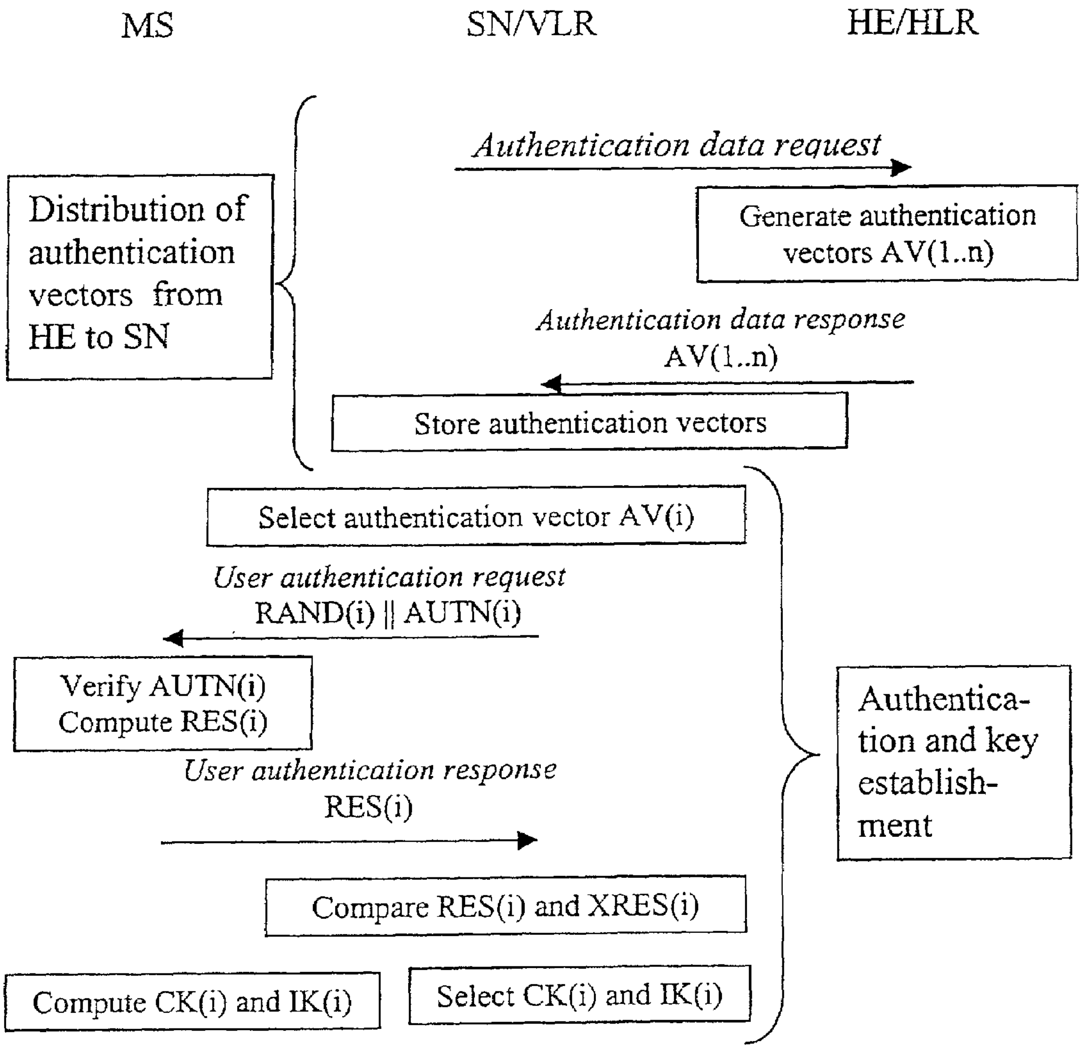

MS
SN/VLR
HE/HLR
Distribution of authentication vectors from HE to SN
Authentication data request
Generate authentication vectors AV(1..n)
Authentication data response AV(1..n)
Store authentication vectors
Select authentication vector AV(i)
User authentication request RAND(i) || AUTN(i)
Verify AUTN(i) Compute RES(i)
User authentication response RES(i)
Compare RES(i) and XRES(i)
Compute CK(i) and IK(i)
Select CK(i) and IK(i)
Authentication and key establishment

Fig. 7

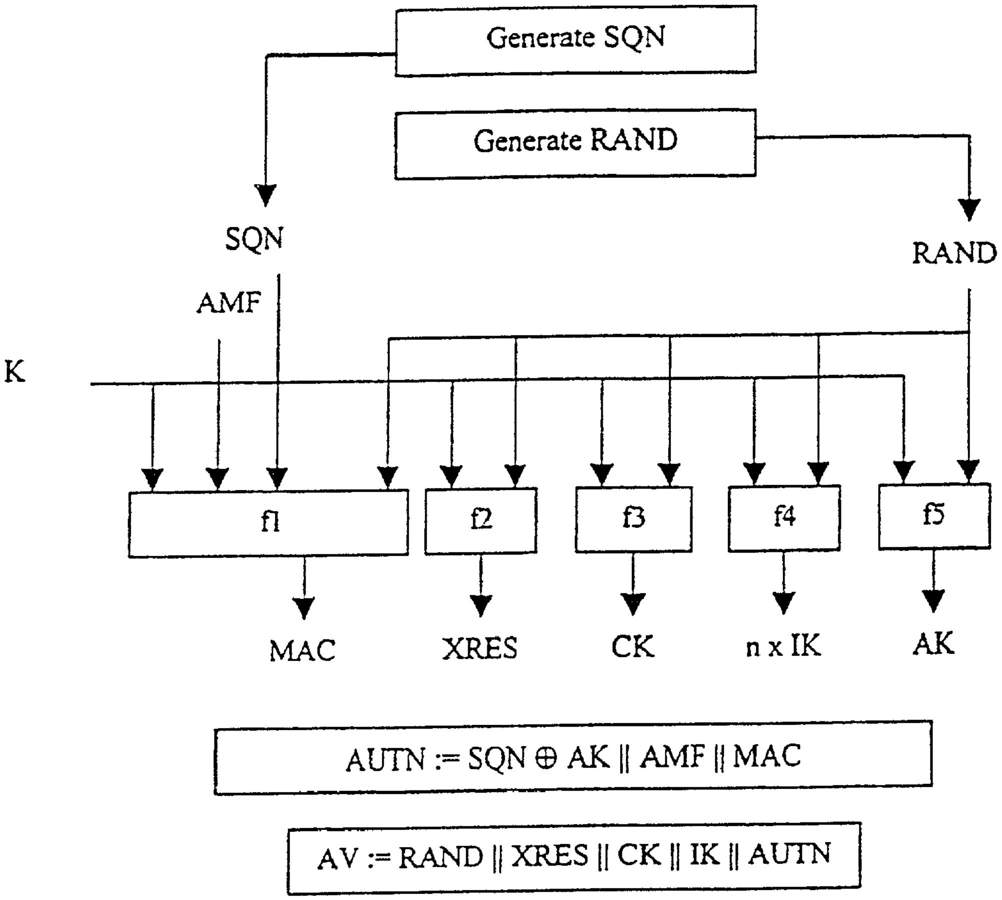

Generate SQN
Generate RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
n x IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Fig. 8

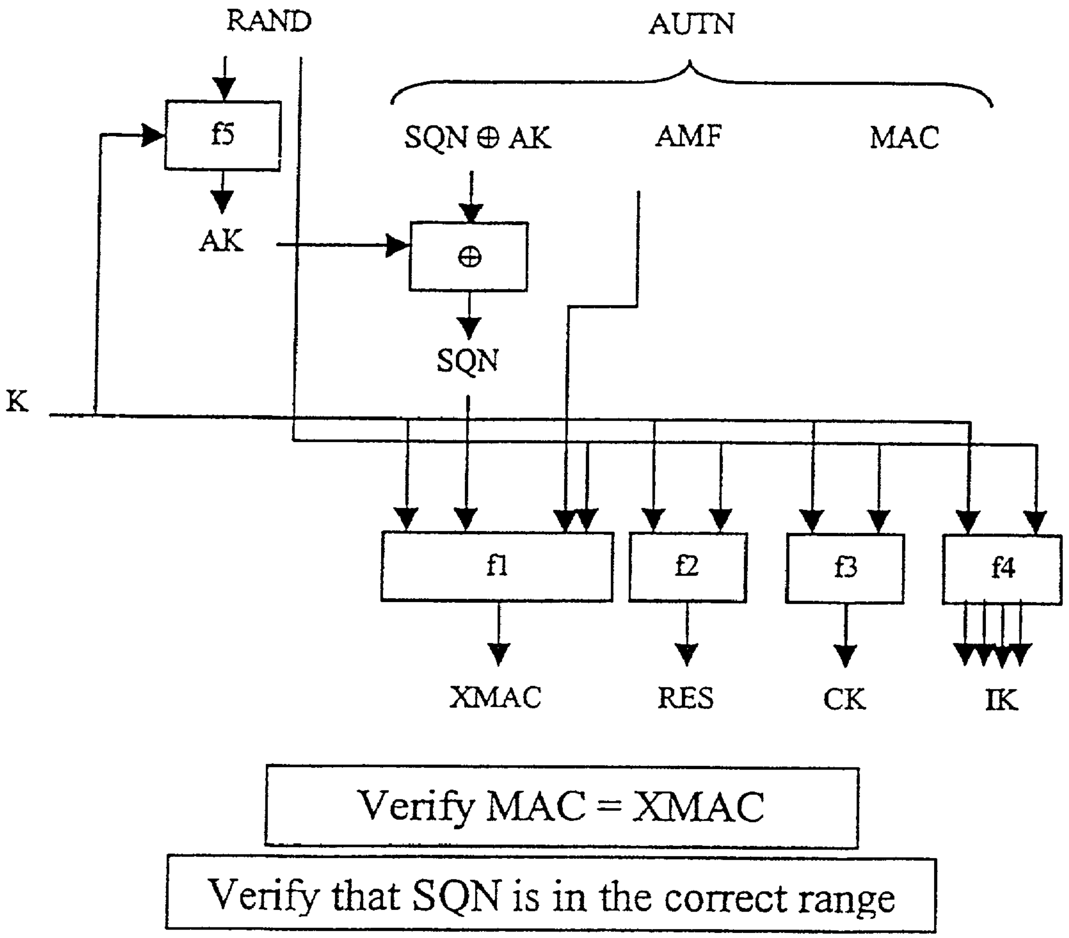

RAND
AUTN
f5
SQN ⊕ AK
AMF
MAC
AK
⊕
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
Verify MAC = XMAC
Verify that SQN is in the correct range

Fig. 9

INTEGRITY CHECK IN A COMMUNICATION SYSTEM

This application is a continuation of PCT/EP01/00735 filed Jan. 23, 2001.

FIELD OF THE INVENTION

The present invention relates to a method for checking the integrity of communications between a first node and a second node. In particular, but not exclusively, the invention relates to a method for checking the integrity of communications between a mobile station and a cellular network.

BACKGROUND TO THE INVENTION

Various different telecommunication networks are known. A telecommunication network is a cellular telecommunication network, wherein the area covered by the network is divided into a plurality of cells. Each cell is provided with a base station, which serves mobile stations in the cell associated with the base station. User equipment, such as mobile stations, thus receive signals from and transmit signals to the base station, and thereby may communicate through the base stations. The cellular system also typically comprises a base station controller controlling the operation of one or more base stations. At least some of the user equipment in the system may be able to communicate simultaneously on one or more communication channels.

Telecommunications are subject to the problem of ensuring that the received information is sent by an authorised sender and not by an unauthorised party who is trying to masquerade as the sender. The problem is especially relevant to cellular telecommunication systems, where the air interface presents an potential opportunity for an unauthorised party to eavesdrop and replace the contents of a transmission.

One solution to this problem is authentication of the communicating parties. An authentication process aims to discover and check the identity of both communicating parties, so that each party receives information about the identity of the other party, and can trust the identity. Authentication is typically performed in a specific procedure at the beginning of a connection. However, this procedure leaves room for the unauthorized manipulation, insertion, and deletion of subsequent messages. There is a need for separate authentication of each transmitted message. This can be done by appending a message authentication code (MAC-I) to the message at the transmitting end, and checking the message authentication code MAC-I value at the receiving end.

A message authentication code MAC-I is typically a relatively short string of bits, which is dependent on the message it protects and on a secret key known both by the sender and by the recipient of the message. The secret key is generated and agreed during the authentication procedure at the beginning of the connection. In some cases the algorithm (that is used to calculate the message authentication code MAC-I based on the secret key and the message) is also secret but this is not usually the case.

The process of authentication of single messages is often called integrity protection. To protect the integrity of a message, the transmitting party computes a message authentication value based on the message to be sent and the secret key using the specified algoritm, and sends the message with the message authentication code MAC-I value. The receiving party recomputes a message authentication code MAC-I value based on the message and the secret key according to the specified algorithm, and compares the received message authentication code MAC-I and the calculated message authentication code MAC-I. If the two message authentication code MAC-I values match, the recipient can trust that the message is intact and sent by the supposed party.

Integrity protection schemes can be attacked. There are two methods that an unauthorised party can use to forge a message authentication code MAC-I value for a modified or a new messages. The first method involves the obtaining of the secret key and the second method involves providing modified or new message without knowledge of the secret key.

The secret key can be obtained by a third party in two ways:

by computing all possible keys until a key is found, which matches with data of observed message authentication code MAC-I pairs, or by otherwise breaking the algorithm for producing message authentication code MAC-I values; or

by directly capturing a stored or transmitted secret key.

The original communicating parties can prevent a third party from obtaining the secret key by using an algorithm that is cryptographically strong, by using a long enough secret key to prevent the exhaustive search of all keys, and by using a secure method for the transmission and storage of secret keys.

A third party can try to disrupt messaging between the two parties without a secret key by guessing the correct message authentication code MAC-I value, or by replaying some earlier message transmitted between the two parties. In the latter case, the correct message authentication code MAC-I for the message is known from the original transmission. This attack can be very useful for an unauthorised third party. For instance, it may multiply the number of further actions that are favorable to the intruder. Even money transactions may be repeated this way.

Correct guessing of the message authentication code MAC-I value can be prevented by using long message authentication code MAC-I values. The message authentication MAC-I value should be long enough to reduce the probability of guessing right to a sufficiently low level compared to the benefit gained by one successful forgery. For example, using a 32 bit message authentication code MAC-I value reduces the probability of a correct guess to 1/4294967296. This is small enough for most applications.

Obtaining a correct message authentication code MAC-I value using the replay attack i.e. by replaying an earlier message, can be prevented by introducing a time varying parameter to the calculation of the message authentication MAC-I values. For example, a time stamp value or a sequence number can be used as a further input to the message authentication code MAC-I algorithm in addition to the secret integrity key and the message.

In the case where a sequence of numbers are used as time varying parameters, a mechanism is used which prevents the possibility of using the same sequence number more than once with the same secret key. Typically, both communicating parties keep track of the used sequence numbers.

If there are several communication channels in use which all use the same secret key the following problem arises. A message in one communication channel associated with a given sequence number, for example n, can be repeated on another communicating channel at a suitable time, that is whenever the sequence number n is acceptable on the other channel.

It has been proposed to apply ciphering and integrity protection in the UMTS system for the third generation standard. However the method, which has been proposed, permits the identical message to be sent on two different signalling radio bearers at different times. This makes the system vulnerable to man-in-the-middle attacks. In particular, such a system may be vulnerable to the "replay attack" described above.

Typically, one single repeated signalling message does not give a significant advantage to the unauthorised third party but it is possible that the third party could try to repeat a longer dialogue in order to, for example, set-up an additional call and, thus steal parts of a connection.

SUMMARY OF THE INVENTION

It is an aim of embodiments of the present invention to address one or more of the problems discussed previously.

According to one aspect of the present invention, there is provided a method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity, and transmitting information relating to the integrity output from one of said nodes to the other.

A separate input may be provided for said information relating to the identity of the channel. Said information relating to the identity of the channel may be combined with at least one other input value. Said input values may comprise one or more of the following values: an integrity key; a direction value; a fresh value; a message value and a count value. The output of the integrity algorithm may be sent from one node to another. Said communication channels may comprise a radio bearer. Said input values may be input to an algorithm for calculation of said output.

According to another aspect of the present invention, there is provided a method for carrying out an integrity check for a system comprising a first node and a second node, a plurality of communication channels being provided between said first node and said second node, said method comprising calculating an integrity output using a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity.

According to another aspect of the present invention, there is provided a method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of: calculating an integrity output using a plurality of values, one of said values being an integrity key, each of said channels having a different integrity key; and transmitting information relating to the output of said integrity algorithms from one of said nodes to the other.

According to another aspect of the present invention, there is provided a method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising: triggering an authentication procedure; and calculating a desired number of integrity parameters by the authentication procedure.

According to another aspect of the present invention, there is provided a node, said node for use in a system comprising a said node and a further node, a plurality of different channels being provided between said nodes, said node comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity; and means for transmitting information relating to the integrity output from said node to said further node.

According to another aspect of the present invention there is provided a node, said node for use in a system comprising said node and a further node, a plurality of different channels being provided between said nodes, said node comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity; and means for comparing information relating to the integrity output calculated by said node with a value calculated by the further node.

According to another aspect of the present invention, there is provided an algorithm for calculating an integrity output for use in a system comprising a node and a further node, a plurality of different channels being provided between said nodes, said algorithm comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity.

Several advantages may be achieved by the embodiments of the invention. In the solution of the present invention, the replay attack may be prevented also in the case when several parallel communication channels are used. An advantage is that the embodiments may be flexibly applied to any system utilising parallel communication channels within one connection. The embodiment of the present invention may enhance user security in communication systems, especially in wireless communication systems. The embodiments may ensure that parallel communication channels within a connection will never use same set of input parameters for calculating the message authentication code MAC-I.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention and as to how the same may be carried into effect, reference will now be made by way of example to the accompanying drawings in which:

FIG. **1** shows elements of a cellular network with which embodiments of the present invention can be used;

FIG. **2** shows the radio interface Uu protocol architecture between the user equipment UE and Node B and between the user equipment UE and radio network controller RNC of FIG. **1**;

FIG. **3** illustrates schematically the integrity protection function;

FIG. **4** shows the integrity protection function as modified in accordance with embodiments of the present invention;

FIG. **5** shows the integrity protection function as modified in accordance with a further embodiment of the invention;

FIG. **6** shows a further embodiment of the present invention;

FIG. **7** shows an authentication and key agreement procedure;

FIG. **8** shows generation of authentication vectors; and

FIG. **9** shows an example of user authentication function in USIM in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

With reference to FIG. **1**, a typical mobile telephone system structure will be described. The main parts of the mobile telephone system are: a core network CN **2**, a UMTS terrestrial radio access network UTRAN **4**, and user equipment UE **6**. The core network CN **2** can be connected to external networks **8**, which can be either Circuit Switched (CS) networks **81** (e.g. PLMN, PSTN, ISDN) or Packet Switched (PS) networks **82** (e.g. the internet). The interface between the core network CN **2** and the UMTS terrestrial radio access network UTRAN **4** is called the lu interface, and the interface between the UMTS terrestrial radio access network UTRAN **4** and the user equipment UE **6** is called the Uu interface. As shown in FIG. **1**, the RNC is connected to two CN nodes (MSC/VLR and SGSN). In some network topologies it may be possible that one RNC is connected to one CN node or to more than two CN nodes.

The core network CN **2** is composed of a Home Location Register HLR **10**, a Mobile Services Switching Centre/Visitor Location Register MSC/VLR**12**, a Gateway MSC GMSC **14**, a Serving GPRS (General Packet Radio Service) Support Node SGSN **16** and a Gateway GPRS Support Node GGSN **18**.

The UTRAN **4** is composed of radio network subsystems RNS **20** and **22**. The interface between two radio network subsystems RNSs is called the lur interface. The radio network subsystems RNS **20** and **22** are composed of a radio network controller RNC **24** and one or more node Bs **26**. The interface between the radio network controller RNC **24** and node B **26** is called the lub interface.

The Radio Network Controller RNC **24** is the network element responsible for the control of the radio resources of UTRAN **4**. The RNC **24** interfaces the core network CN **2** (normally to one MSC **12** and one SGSN **16**) and also terminates the Radio Resource Control RRC protocol that defines the messages and procedures between the user equipment UE **6** and UTRAN **4**. The RNC **24** logically corresponds to the base station controller of the GSM (global system for mobile communications) standard.

The main function of the Node B **26** is to perform the air interface L**1** processing (channel coding and interleaving, rate adaptation, spreading, etc) It also performs some basic Radio Resource Management operation such as the inner loop power control. It logically corresponds to the Base Transceiver Station of the GSM standard.

The user equipment UE **6** consists of two parts: the Mobile Equipment ME **30** and the UMTS Subscriber Identity Module USIM **32**. The mobile equipment ME is the radio terminal used for radio communication over the Uu interface between the user equipment UE **6** and the UTRAN **4**. The USIM **32** is a smart card that holds the subscriber identity, performs authentication algorithms, and stores authentication and encryption keys and some subscription information that is needed at the terminal.

With reference to FIG. **2**, the radio interface protocol architecture according to the 3GPP specifications will be described. The protocol entities described operate between:

the user equipment UE **6**, and NodeB **26** and/or

the user equipment UE **6**, and the RNC **24**.

The division of protocol layers between NodeB **26** and RNC **24** is not described here further.

The radio interface protocols can be divided into a control plane **50** and a user plane **52**. The control plane **50** is used for all signaling between the UE **6**, and the RNC **24**, and also between the user equipment UE **6**, and the core network CN **2**. The user plane, carries the actual user data. Some of the radio interface protocols operate only in one plane whilst some protocols operate in both planes.

The radio interface protocols can be divided into layers, which are layer **1** L**1** **54** (also called the physical layer), layer **2** L**2** **56** (also called the data link layer) and layer **3** L**3** **58** (also called the network layer). Some layers contain only one protocol whilst some layers contain several different protocols.

The physical layer L**1** **54** offers services to the Medium Access Control (MAC) layer **60** via transport channels that are characterised by how and with what characteristics the data is transferred.

The Medium Access Control (MAC) layer **60**, in turn, offers services to the radio link control RLC layer **62** by means of logical channels. The logical channels are characterized by what type of data is transmitted. In the medium access control MAC layer **60** the logical channels are mapped to the transport channels.

The Radio Link Control RLC **62** layer offers services to higher layers via service access points SAP, which describe how the radio link control RLC layer **62** handles the data packets and if for example an automatic repeat request (ARQ) function is used. On the control plane **50**, the radio link control RLC services are used by the radio resource control RRC layer **64** for signalling transport. Normally a minimum of three radio link control RLC **62** entities are engaged to signalling transport—one transparent, one unacknowledged and one acknowledged mode entity. On the user plane **52**, the RLC services are used either by the service specific protocol layers—packet data convergence protocol PDCP **66** or broadcast multicast control BMC **68**—or by other higher layer user plane functions (e.g. speech codec). The RLC services are called Signalling Radio Bearers in the control plane and Radio Bearers in the user plane for services not utilizing the PDCP or BMC protocols.

The Packet Data Convergence Protocol (PDCP) exists only for the packet switched PS domain services (services routed via the SGSN) and its main function is header compression, which means compression of redundant protocol control information (e.g., TCP/IP and RTP/UDP/IP headers) at the transmitting entity and decompression at the receiving entity. The services offered by PDCP are called Radio Bearers.

The Broadcast Multicast Control protocol (BMC) exists only for the short message service SMS Cell Broadcast service, which is derived from GSM. The service offered by the BMC protocol is also called a Radio Bearer.

The RRC layer **64** offers services to higher layers (to the Non Access Stratum) via service access points. All higher layer signalling between the user equipment UE **6** and the core network CN **2** (mobility management, call control, session management, etc.) is encapsulated into RRC messages for transmission over the radio interface.

The control interfaces between the RRC **64** and all the lower layer protocols are used by the RRC layer **64** to configure characteristics of the lower layer protocol entities including parameters for the physical, transport and logical channels. The same control interfaces are used by the RRC layer **64** e.g. to command the lower layers to perform certain types of measurements and by the lower layers to report measurement results and errors to the RRC.

The embodiment of the invention is described in the context of a UMTS (Universal Mobile Telecommunications System). The present invention is applicable to all types of communication e.g. signalling, real-time services and non-real-time services. However, it should be appreciated that embodiments of the present invention are applicable to any other system.

In the proposal for the UMTS standard for the third generation, the SGSN **16** and the user equipment UE **6**, for example a mobile station have an upper layer **L3** which supports mobility management MM (sometimes called GMM) and session management SM. This upper layer also supports the short message service SMS. These upper layer **L3** protocols are derived from the second generation GPRS system. The SMS supports the mobile-originated and mobile-terminated short message service described in the third generation specification 3GPP TS 23.040. The mobility management function manages the location of the mobile station, that is attachment of the mobile station to the network and authentication. Thus MM supports mobility management functionality such as attach, detach, security (e.g. authentication) and routing updates. In accordance with an embodiment integrity keys may be calculated during authentication procedure of the MM. An exemplifying embodiment of this aspect of the present invention will be explained in more detail later.

The SGSN **16** and RNS **20** have a Radio Access Network Application Protocol (RANAP) layer. This protocol is used to control the lu-interface bearers, but it also encapsulates and carries higher-layer signalling. RANAP handles the signalling between the SGSN **16** and the. RNS **20**. RANAP is specified in the third generation specification 3GPP TS 25.413. The mobile station **6** and the RNS **20** both have a radio resource control protocol RRC which provides radio bearer control over the radio interface, for example for the transmission of higher layer signalling messages and SMS messages. This layer handles major part of the communication between the mobile station **6** and the RNC**24**. A RRC is specified, for example, in the third generation specification 3GPP TS 25.331

MM, SM and SMS messages are sent from the SGSN **16** to the RNS **20** encapsulated into a RANAP protocol message (the message is called Direct Transfer in the 3GPP specifications). The packet is forwarded by the RANAP layer of the RNC **24** to the RRC layer of the RNC **24**. The relay function in the RNS **20** effectively strips the RANAP headers off and forwards the payload into the RRC protocol by using an appropriate primitive so that the RRC layer knows that this is an upper layer message that must be forwarded to the mobile station **6**. The RNC **24** inserts an integrity checksum to the (RRC) message carrying the higher layer message in payload (the RRC message is called Direct Transfer in the 3GPP specifications). The RNC **24** may also cipher the message. This will be described in more detail hereinafter. The RNS **20** forwards the packet via the air interface to the mobile station **6**.

In the mobile originated direction, the RRC layer of the mobile station **6** receives the higher layer message, encapsulates it into a RRC Direct Transfer message and adds a message authentication code to it before sending it to the RNS **20**. The message is relayed from the RRC layer to the RANAP layer of the RNS **20**. The RNS **20** checks associated information with the message to see if the packet has been integrity checked.

The integrity check procedure will now be described. Most radio resource control RRC, mobility management MM and session management SM (as well as other higher layer **3** protocol) information elements are considered sensitive and must be integrity protected. Due to this, an integrity function may be applied on most RRC signalling messages transmitted between the mobile station and the RNS **20**. However, those RRC messages which are sent before the integrity key is known may be ignored. This integrity function uses an integrity algorithm with the integrity key IK to compute a message authentication code for a given message. This is carried out in the mobile station and the RNS which both have integrity key IK and the integrity algorithm.

Reference is made to FIG. **3** which illustrates the use of the integrity algorithm to calculate the message authentication code MAC-I.

The input parameters to the algorithm are the integrity key IK, a time or message number dependent input COUNT-I, a random value generated by the network FRESH, the direction bit DIRECTION and the signalling data MESSAGE. The latter input is the message or data packet. Based on these input parameters, a message authentication code for data integrity (MAC-I) is calculated by the integrity algorithm UIA. This code MAC-I is then appended to the message before sending over the air interface, either to or from the mobile station.

The receiver of that code and message also computes a message authentication code for data integrity XMAC-I on the message received using the same algorithm UIA. The algorithm UIA has the same inputs as at the sending end of the message. The codes calculated by the algorithm at the sending end (MAC-I) and at the receiving end (XMAC-I) should be the same if the data integrity of the message is to be verified.

The input parameter COUNT-I is a value incremented by one for each integrity protected message. COUNT-I consists of two parts: the hyperframe number (HFN) as the most significant part and a message sequence number as the least significant part. The initial value of the hyperframe number is sent by the mobile station to the network during a connection set-up. At connection release, the mobile station stores the greatest used hyperframe number from the connection and increments it by one. This value is then used as the initial HFN value for next connection. In this way the user is assured that no COUNT-I value is re-used (by the network) with the same integrity key for different connections. After an (re-) authentication procedure, when a new IK is generated and taken into use, the HFN value can be reset back to zero.

The input parameter FRESH protects the network against replay of signalling messages by the mobile station. At connection set-up the network generates a random value FRESH and sends it to the user. The value FRESH is subsequently used by both the network and the mobile station throughout the duration of a single connection. This mechanism assures the network that the mobile station is not replaying any old message authentication code MAC-I from previous connection.

The setting of the integrity key IK is as described herein. The key may be changed as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber is known. The key IK is stored in the visitor location register and transferred to the RNC, when it is needed. The key IK is also stored in the mobile station until it is updated at the next authentication.

A key set identifier KSI is a number which is associated with the cipher and integrity keys derived during authentication procedure. It is stored together with the cipher and integrity keys in the MS and in the network. The key set identifier is used to allow key re-use during subsequent connection set-ups. The KSI is used to verify whether the MS and the network are to use the same cipher key and integrity key.

A mechanism is provided to ensure that a particular integrity key is not used for an unlimited period of time, to avoid attacks using compromised keys.

Authentication which generates integrity keys is not mandatory at connection setup.

The mobile station is arranged to trigger the generation of a new cipher key and an integrity key if the counter reaches a maximum value set by the operator and stored in the mobile station at the next RRC connection request message sent out. This mechanism will ensure that an integrity key and cipher key cannot be reused more times than the limit set by the operator.

It should be appreciated that there may be more than one integrity algorithm and information is exchanged between the mobile station and the radio network controllers defining the algorithm. It should be noted that the same algorithm should be used by the sender and receiver of messages.

When a mobile station wishes to establish a connection with the network, the mobile station shall indicate to the network which version or versions of the algorithm the MS supports. This message itself must be integrity protected and is transmitted to the RNC after the authentication procedure is complete.

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the mobile station with those indicated by the mobile station and act according to the following rules:

1) If the mobile station and the network have no versions of the algorithm in common, then the connection shall be released.

2) If the mobile station and the network have at least one version of the algorithm in common, then the network shall select one of the mutually acceptable versions of the algorithm for use on that connection.

Integrity protection is performed by appending the message authentication code MAC-I to the message that is to be integrity protected. The mobile station can append the MAC-I to messages as soon as it has received a connection specific FRESH value from the RNC.

If the value of the hyper-frame number HFN is larger or equal to the maximum value stored in the mobile station, the mobile station indicates to the network in the RRC connection set-up that it is required to initialise a new authentication and key agreement.

The RNC may be arranged to detect that new security parameters are needed. This may be triggered by (repeated) failure of integrity checks (e.g. COUNT-I went out of synchronisation), or handover to a new RNC does not support an algorithm selected by the old RNC, etc.

A new cipher key CK is established each time an authentication procedure is executed between the mobile station and the SGSN.

The integrity key IK may be changed if there is handoff of the mobile station from one base station to a different base station

It should be appreciated that embodiments of the invention, the integrity check may only be commenced at any point after the connection has been set up as well as at attach.

It should be appreciated that with data connections, the connection may be open for relatively long periods of time or may even be permanently open.

It has been agreed that more than one signalling radio bearer, that is a radio bearer on the control plane that is a service offered by RLC, can be established between a mobile station or other user equipment **6** and the RNS **20**. The current 3GPP specification proposes that up to four signalling radio bearers can be provided.

In the current 3GPP specification, two or more of the signalling radio bearers SRB may have the same input parameters to the integrity algorithm illustrated in FIG. **3**. If all input parameters to the integrity algorithm are the same then the output is the same.

This current proposal, as mentioned previously, leaves open the possibility for an intruder or a 'man-in-the-middle' to repeat a signalling message from one signalling radio bearer on another signalling radio bearer. The COUNT-I value is specific to each signalling radio bearer and may be different on different signalling bearers. Consider the following scenario. A message has been sent on a first signalling radio bearer SRB**1** with a COUNT value of 77. When the count value for a second signalling radio bearer SRB**2** reaches 77, the unauthorised party can simply repeat the message sent earlier on SRB**1** by using SRB**2**.

Typically, one single signalling message from a signalling radio bearer repeated in the second signalling radio bearer does not give a significant advantage to the 'man-in-the-middle' but it may be possible for the unauthorised party to repeat also a longer dialogue in order, for example, to set-up an additional call which the 'man-in-the-middle' can utilize and, thus, steal parts of the connection. A simpler 'repeat-attack'**0** case would be that the unauthorised party could e.g. repeat a dialogue carried via SMS, the dialogue being e.g. money transaction.

With the current third generation proposals, this problem may only arise in a limited number of circumstances. This is due to the fact that the usage of the four signalling radio bearers (SRB) is limited. Only certain RRC messages can be sent on certain signalling radio bearers. The "repeat attack" scenario would be possible for a Non Access Stratum (NAS) message (CM/MM/SMS etc. messages carried in RRC Direct Transfer) or a NAS message dialogue between UE and SGSN/MSC. RRC Direct Transfer is a RRC message, which carries in payload all the NAS messages over the air interface. However, this problem could harm a mobile user as for example SMS messages could be adversely affected.

There are two basic solutions to the 'replay attack' problem. Firstly, different communication channels using the same secret key can coordinate the use of sequence numbers COUNT-I in such way that each sequence number is used at most once in any of the channels. This coordination may be very cumbersome or even impossible in some situations. It should be appreaciated that when the embodiments are applied to the radio interface of the 3rd generation cellular network UMTS, the communication channels may be called radio bearers.

As will be discussed in more detail, embodiments of the present invention use a solution where an additional parameter is used as an input to the calculation of the message authentication code MAC-I. The value of this parameter is unique at least to each communication channel which uses the same secret key. The value may be unique also to all communication channels within one connection between the user equipment UE **6** and RNS **20**.

In a further embodiment of the present invention, the problem is avoided by ensuring that same integrity key is never used for different parallel communication channels.

With reference to FIG. **4**, the modifications to the known integrity protection function embodying the present invention are described. These modifications do not cause any changes to the actual integrity algorithm UIA.

A communication channel specific parameter is added as input to the integrity protection algorithm. In the 3GPP specifications, this communication channel specific parameter is the radio bearer identification (RB ID). In one example of an application of the present invention, the radio bearer identification represents the identity of the signalling radio bearer in the proposed WCDMA third generation system and can be a number between 0 and 3. It should be noted that the used communication channel specific parameter depends on the protocol layer where the message authentication code is calculated. Still using 3GPP specification as an example, if the message authentication code would be added in the RLC protocol, the parameter would be a logical channel (see FIG. **2**) identity. As another possible example, if the integrity protection would be performed in the PDCP protocol layer or in the RRC protocol layer, the additional parameter would be a radio bearer (see FIG. **2**) identity. It should be appreciated that when discussing the control plane part of the protocol stack, the terms signalling radio bearer identity and radio bearer identity are equivalent.

Since the identity of the signaling radio bearer is known by both the sender and the receiver, that is the user equipment UE **6** and the RNS **20**, it is not necessary to send the identity information explicitly over the radio interface.

FIG. **4** illustrates the possible places where the new parameter can be included without modifying the integrity algorithm UIA. Since the sender and receiver are similar when looking from the input parameter viewpoint (see FIG. **3**), only one side in shown in FIG. **4**. It should be appreciated that the receive and the transmit parts will perform the same algorithm. As can be seen from FIG. **4**, the preferred embodiments include the new parameter by appending it (as a string) to one or more of the existing algorithm input parameters.

In one embodiment the signalling radio bearer identification RB IB is made part of the input parameters FRESH or COUNT-I. This is illustrated with numbers '**1**' and '**2**' in FIG. **4**, respectively. In practice, the FRESH and COUNT-I parameters would incorporate both FRESH or COUNT-I information and the identification information. For example if the FRESH value has n bits the FRESH information would be represented by a bits and the identification information by b bits where a+b=n. This would mean in effect shortening the FRESH parameter. The same modification may be made to the COUNT-I parameter. In one modification, part of the signalling radio bearer identification may be provided by the COUNT-I parameter and part by the FRESH parameter. However, if the COUNT-I is made shorter it may take shorter time for it to 'wrap around' i.e. to reach the maximum value and come back to zero. If the FRESH parameter is shortened, it may be that the probability of repeating the value by accident (it is randomly chosen) increases.

In a further embodiment the signalling radio bearer id is made part of the integrity key IK. This is illustrated with number '**4**' in FIG. **4**. For example if the IK value has n bits the IK information would be represent by a bits and the identification information by b bits where a+b=n. However, if the key IK is shorter there is increased probability to simply guess the key.

In a further embodiment of the present invention, the identity of the signaling radio bearer may be incorporated into the MESSAGE that is fed into the integrity algorithm. This is illustrated with number '**3**' in FIG. **4**. Since the identity of the signaling radio bearer is known by both the sender and the receiver, that is the mobile station and the RNS **20**, it is not necessary to send the identity information over the radio interface with the actual MESSAGE. For example, if the MESSAGE has n bits and the identity RB ID, has i bits, the actual 'MESSAGE' that would be fed into the integrity algorithm would have n+i bits. Thus, instead of just the MESSAGE alone being input to the integrity algorithm, the bit string fed into the integrity algorithm would become signaling radio bearer identity and the MESSAGE. This solution has no impact on the security issues (e.g. counter lengths) related to the integrity algorithm. This means that no parameter that is fed to the algorithm is made shorter:

In some embodiments, it is possible to divide the identification information between more than one input.

FIG. **5** illustrates a further embodiment of the invention, this embodiment having effect to the actual integrity algorithm UIA. In this embodiment the integrity algorithm is provided with an additional parameter, as shown in FIG. **5**. In this example, when integrity protection is performed in the RRC protocol layer, the additional parameter is a (signalling) radio bearer identification RB ID, which is unique to the (signalling) radio bearer. This parameter is input separately and is used in the calculation performed by the integrity algorithm UIA.

FIG. **6** illustrates a further embodiment of the invention, this embodiment having effect to the actual integrity algorithm UIA. In this embodiment the new parameter bearer id (RB ID) is combined with the parameter DIRECTION. This embodiment would effectively make the existing i.e. 'old' DIRECTION parameter longer and thus have effect on the actual integrity algorithm UIA.

In an alternative embodiment, a unique integrity key IK is produced for each radio bearer. This may be achieved by modifying the authentication procedure of an upper layer L**3** which supports mobility management MM and session management SM in the proposed UMTS specifications. As was briefly explained above, the mobility management function manages the location of the mobile station, that is attachment of the mobile station to the network and authentication. The integrity algorithm performed on each of the signalling radio bearers during a modified authentication procedure may provide unique results, preventing the type of attack outlined previously.

Reference will now be made to FIGS. **7** to **9** showing possible authentication and key agreement procedures. The described mechanisms achieve mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the User Services Identity Module USIM and the Authentication Centre AuC in the user's Home Environment HE. In addition, the USIM and the HE keep track of counters SEQ_{Ms} and SEQ_{HE} respectively to support network authentication.

The procedure may be designed such that it is compatible with e.g. the current GSM security architecture and facilitate migration from the GSM to the UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from the ISO standard ISO/IEC 9798-4. Before explaining the formation of the integrity keys, an authentication and key agreement mechanism will be discussed. An overview of a possible authentication and key agreement mechanism is shown in FIG. **7**. FIG. **8** shows a possible procedure for the generation of authentication vectors.

Upon receipt of a request from the VLR/SGSN, the HE/AuC sends an ordered array of n authentication vectors (the equivalent of a GSM "triplet") to the VLR/SGSN. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the VLR/SGSN and the USIM.

When the VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the array and sends the parameters RAND and AUTN to the user. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the VLR/SGSN. The USIM also computes CK and IK. The VLR/SGSN compares the received RES with XRES. If they match the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the VLR/SGSN to the entities which perform ciphering and integrity functions. In the proposed UMTS system, these entities may preferably be some of the radio interface protocols described in FIG. **2**. The entities are located preferably in the User Equipment UE and in the Radio Network Controller RNC.

VLR/SGSNs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipner and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages.

The authenticating parties shall be the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The mechanism may consist of the following procedures:

Distribution of authentication information from the HE/AuC to the VLR/SGSN. The VLR/SGSN is assumed to be trusted by the user's HE to handle authentication information securely. It is also assumed that the intra-system links between the VLR/SGSN to the HE/AuC are adequately secure. It is further assumed that the user trusts the HE.

Mutual authentication and establishment of new cipher and integrity keys between the VLR/SGSN and the MS.

Distribution of authentication data from a previously visited VLR to the newly visited VLR. It is assumed that the links between VLR/SGSNs are adequately secure.

The purpose of the distribution of authentication data from HE to SN is to provide the VLR/SGSN with an array of fresh authentication vectors from the user's HE to perform a number of user authentications. The VLR/SGSN invokes the procedures by requesting authentication vectors to the HE/AuC. The authentication data request shall include a user identity. If the user is known in the VLR/SGSN by means of the IMUI, the authentication data request shall include the IMUI. If the user is identified by means of an encrypted permanent identity, the HLR-message from which the HE can derive the IMUI may be included instead. In that case, this procedure and the procedure user identity request to the HLR are preferably integrated.

Upon the receipt of the authentication data request from the VLR/SGSN, the HE may have pre-computed the required number of authentication vectors and retrieve them from the HLR database or may compute them on demand. The HE/AuC sends an authentication response back to the VLR/SGSN that contains an ordered array of n authentication vectors AV(1 . . . n). The HE/AuC generates a fresh sequence number SQN and an unpredictable challenge RAND. For each user the HE/AuC keeps also track of a counter that is SQN_{HE}.

The mechanisms for verifying the freshness of sequence numbers in the USIM shall to some extent allow the out-of-order use of sequence numbers. This is to ensure that the authentication failure rate due to synchronisation failures is sufficiently low. This requires the capability of the USIM to store information on past successful authentication events (e.g. sequence numbers or relevant parts thereof). The mechanism shall ensure that a sequence number can still be accepted if it is among the last x=50 sequence numbers generated. This shall not preclude that a sequence number is rejected for other reasons such as a limit on the age for time-based sequence numbers.

The same minimum number x needs to be used across the systems to guarantee that the synchronisation failure rate is sufficiently low under various usage scenarios, in particular simultaneous registration in the CS- and the PS-service domains, user movement between VLRs/SGSNs which do not exchange authentication information, super-charged networks.

The use of SEQHE may be specific to the method of generation sequence numbers. An authentication and key management field AMF may be included in the authentication token of each authentication vector.

Subsequently the following values can be computed:

a message authentication code MAC=$\mathbf{f1}_K$(SQN||RAND||AMF) where f**1** is a message authentication function;

an expected response XRES=$\mathbf{f2}_K$(RAND) where f**2** is a (possibly truncated) message authentication function;

a cipher key CK=$\mathbf{f3}_K$ (RAND) where f**3** is a key generating function;

an integrity key IK=$\mathbf{f4}_K$(RAND) where f**4** is a key generating function;

an anonymity key AK=$\mathbf{f5}_K$(RAND) where f**5** is a key generating function or f**5≡0**.

According to the embodiments of the present invention, more than one IK is generated. This can be achieved, for example, by modifying the f**4** function such that it produces the desired number of IKs (e.g. 4: see FIG. **9**). A possibility is to specify that the f**4** function must be triggered several times during the generation of an authentication vector. This can be implemented e.g. by feeding in the second round the first produced IK[**1**] as input to the f**4** function instead of a new RAND. In the third 'round' the IK[**2**] produced in the second round would be fed into f**4** function to obtain third integrity key IK[**3**]. A possibility is also to input a desired number of RANDS to the function f**4**. Thus it is possible to produce as many IK:s as necessary for the system in question. For example, in the UMTS system according to 3GPP Release'99 specifications, four integrity keys would be needed.

The authentication token AUTN=SQN⊕AK||AMF||MAC may then be constructed. The AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only. If no concealment is needed, then f**5≡0**.

The purpose of the authentication and key agreement procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the MS. During the authentication, the user verifies the freshness of the authentication vector that is used. The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR database. The VLR/SGSN sends to the user the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector. Upon receipt the user proceeds as shown in FIG. **9**.

Upon receipt of RAND and AUTN the user first computes the anonymity key AK=f**5**$_K$ (RAND) and retrieves the sequence number SQN=(SQN⊕AK)⊕AK. Next the user computes XMAC=f**1**$_K$ (SQN||RAND||AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends user authentication reject back to the VLR/SGSN with an indication of the cause and the user abandons the procedure. Next the USIM verifies that the received sequence number SQN is in the correct range.

According to an embodiment of the present invention, the USIM generates more than one IK instead of generating only one IK. As explained above. This can be achieved, for example, by modifying the f**4** function, by specifying that the f**4** function must be triggered several times during the generation of an authentication vector or by input of a desired number of RANDs into the f**4** function. This may require that the network (SN/VLR) sends the required number of RANDs and AUTNs to the UE and that the UE may need to produce also a RES for each RAND and return all the produced RESs to the network, as was described above for the case of one RAND+AUTN.

Embodiments of the present invention may be used in any system enabling nonciphered signalling and utilising integrity checksums in at least two parallel radio bearers.

The embodiments of the present invention have been described in the context of a wireless cellular telecommunications network. However, alternative embodiments of the present invention may be used with any other type of communications network wireless or otherwise. Embodiments of the present invention may be used any form or communication where integrity checks or the like are provided with a plurality of radio bearers or the like in parallel.

What is claimed is:

1. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of:

calculating an integrity output, said integrity output being calculated from a plurality of input values, some of said input values being the same for said different channels, at least one of said input values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said input values are identical for said different channels; and

transmitting information relating to the integrity output from one of said nodes to the other,

wherein said information relating to the identity of the channel is combined with only one other input value.

2. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of:

calculating an integrity output, said integrity output being calculated from a plurality of input values, some of said input values being the same for said different channels, at least one of said input values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said input values are identical for said different channels;

and transmitting information relating to the integrity output from one of said nodes to the other,

wherein said information relating to the identity of the channel is combined with at least one other input value, and

wherein said combined input value input comprises a first part allocated to the identity of the bearer and a second part allocated to the other information provided by said value.

3. A method as claimed in claim **1**, wherein said values input to an algorithm comprise one or more of the following values:

an integrity key; a direction value, a fresh value, a message value and a count value.

4. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of:

calculating an integrity output, said integrity output being calculated from a plurality of input values, some of said input values being the same for said different channels, at least one of said input values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said input values are identical for said different channels; and

transmitting information relating to the integrity output from one of said nodes to the other,

wherein said information relating to the identity of the channel is combined with at least one other input value, and

wherein said information relating to the identity of the channel is combined with one or more of the following values input to an algorithm: a fresh value; a count value; and integrity key; a direction value and a message value.

5. A method as claimed in claim **4**, wherein said message value is sent from one node to another without the channel identification information.

6. A method as claimed in claim **1**, wherein the output of an integrity algorithm is sent from one node to another.

7. A method as claimed in claim **1**, wherein communication between said first and second nodes is via a wireless connection.

8. A method as claimed in claim **7**, wherein one of said first and second nodes is user equipment.

9. A method as claimed in claim **8**, wherein said user equipment is a mobile station.

10. A method as claimed in claim **7**, wherein one of said first and second nodes is a radio network controller.

11. A method as claimed in claim **7**, wherein one of said first and second nodes is a node B.

12. A method as claimed in claim **1**, wherein said communication channels comprise a radio bearer.

13. A method as claimed in claim **12**, wherein said radio bearer is a signaling radio bearer.

14. A method as claimed in claim **1**, wherein said input values are input to an algorithm for calculation said output.

15. A method as claimed in claim **3**, wherein the same integrity key is used for the different channels.

16. A method for carrying out an integrity check for system comprising a first node and a second node, a plurality of communication channels being provided between said first node and said second node, said method comprising the step of calculating an integrity output using a plurality of values, at least one of said values being arranged to comprise information relating to the identity of said channel, each having a different identity and at least one of said values being identical for said different channels; and transmitting information relating to the integrity output from one of said nodes to the other node,

wherein said information relating to the identity of the channel is combined with only one other input value.

17. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of:

calculating an integrity output using a plurality of values, one of said values being an integrity key, each of said channels having a different integrity key; and

transmitting information relating to the output of an integrity algorithm from one of said nodes to the other, wherein said information relating to the identity of the channel is combined with only one other input value.

18. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising:

triggering an authentication procedure;

calculating a desired number of integrity parameters by the authentication procedure; and transmitting said integrity parameters from one of said nodes to the other node,

wherein information relating to the identity of the channel is combined with only one other input value.

19. A node, said node for use in a system comprising a said node and a further node, a plurality of different channels being provided between said nodes, said node comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, at least one of said values being arranged to comprise information relating to the identity of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said values being identical for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity,

wherein said information relating to the identity of the channel is combined with only one other input value.

20. A node, said node for use in a system comprising said node and a further node, a plurality of different channels being provide between said nodes, said node comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said values being identical for said different channels means for transmitting information relating to the integrity output from one of said nodes to the other node; and means for comparing information relating to the integrity output calculated by said node with a value calculated by the further node,

wherein said information relating to the identity of the channel is combined with only one other input value.

21. An algorithm for calculating an integrity output for use in a system comprising a node and a further node, a plurality of different channels being provided between said nodes, said algorithm comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, at least on of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said values being identical for said different channels,

wherein said information relating to the identity of the channel is combined with at least one other input value.

* * * * *

EXHIBIT J

US007403621B2

(12) **United States Patent**
Vialèn et al.

(10) **Patent No.: US 7,403,621 B2**
(45) **Date of Patent: Jul. 22, 2008**

(54) **SYSTEM FOR ENSURING ENCRYPTED COMMUNICATION AFTER HANDOVER**

(75) Inventors: **Jukka Vialèn**, Espoo (FI); **Valtteri Niemi**, Helsinki (FI)

(73) Assignee: **Nokia Corporation**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1306 days.

(21) Appl. No.: **10/013,257**

(22) Filed: **Nov. 6, 2001**

(65) **Prior Publication Data**

US 2002/0066011 A1 May 30, 2002

(30) **Foreign Application Priority Data**

Nov. 28, 2000	(FI)	 20002613
Feb. 14, 2001	(FI)	 20010282

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **380/272**

(58) **Field of Classification Search** 380/270, 380/272, 37, 42, 283, 29, 28, 47, 46, 44
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,926,549	A	7/1999	Pinkas	
6,119,228	A	9/2000	Angelo et al.	
6,374,112	B1 *	4/2002	Widegren et al.	455/452.2
6,466,556	B1 *	10/2002	Boudreaux	370/331
6,587,680	B1 *	7/2003	Ala-Laurila et al.	455/411
6,763,112	B1 *	7/2004	Haumont	380/247
6,785,352	B1 *	8/2004	Ranta	375/354
6,876,747	B1 *	4/2005	Faccin et al.	380/247
7,113,600	B1 *	9/2006	Rosenhed	380/272
2002/0035682	A1 *	3/2002	Niemi et al.	713/151
2002/0044552	A1 *	4/2002	Vialen et al.	370/389
2002/0071480	A1 *	6/2002	Marjelund et al.	375/141
2002/0174332	A1 *	11/2002	Vialen et al.	713/152
2003/0144003	A1 *	7/2003	Ranta et al.	455/450

FOREIGN PATENT DOCUMENTS

EP	1111952		6/2001
JP	55-34532	A	3/1980
JP	11-175202	A	7/1999
JP	2000-184452		6/2000
WO	WO 98/37721		8/1998
WO	WO 99/26420		5/1999

(Continued)

OTHER PUBLICATIONS

International Search Report for PCT/FI01/00870.

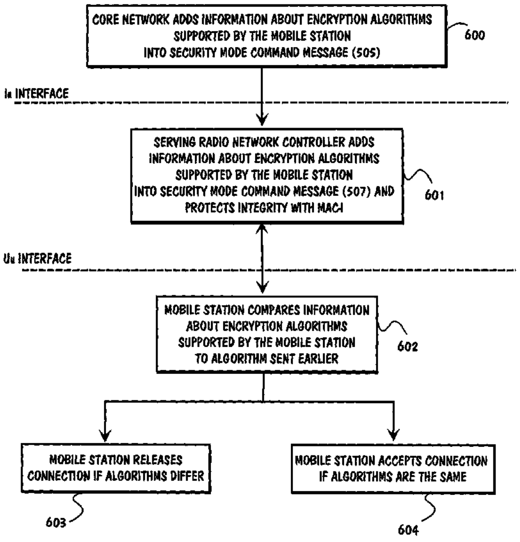
(Continued)

Primary Examiner—Matthew B Smithers
(74) *Attorney, Agent, or Firm*—Squire, Sanders & Dempsey, L.L.P.

(57) **ABSTRACT**

During connection setup with a first radio access network, a multimode mobile station sends an unprotected initial signaling message that includes information about those encryption algorithms that the multimode mobile station supports when it communicates in a second radio access network. The first radio access network saves some or all the information. Then it composes and sends an integrity-protected message that includes information about the encryption algorithms supported by the multimode mobile station in the second radio access network.

47 Claims, 10 Drawing Sheets


CORE NETWORK ADDS INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION INTO SECURITY MODE COMMAND MESSAGE (505)
600
Iu INTERFACE
SERVING RADIO NETWORK CONTROLLER ADDS INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION INTO SECURITY MODE COMMAND MESSAGE (507) AND PROTECTS INTEGRITY WITH MACI
601
Uu INTERFACE
MOBILE STATION COMPARES INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION TO ALGORITHM SENT EARLIER
602
MOBILE STATION RELEASES CONNECTION IF ALGORITHMS DIFFER
603
MOBILE STATION ACCEPTS CONNECTION IF ALGORITHMS ARE THE SAME
604

SOLUTION 1

FOREIGN PATENT DOCUMENTS

WO	WO 00/36860	6/2000
WO	WO 00/69206	11/2000

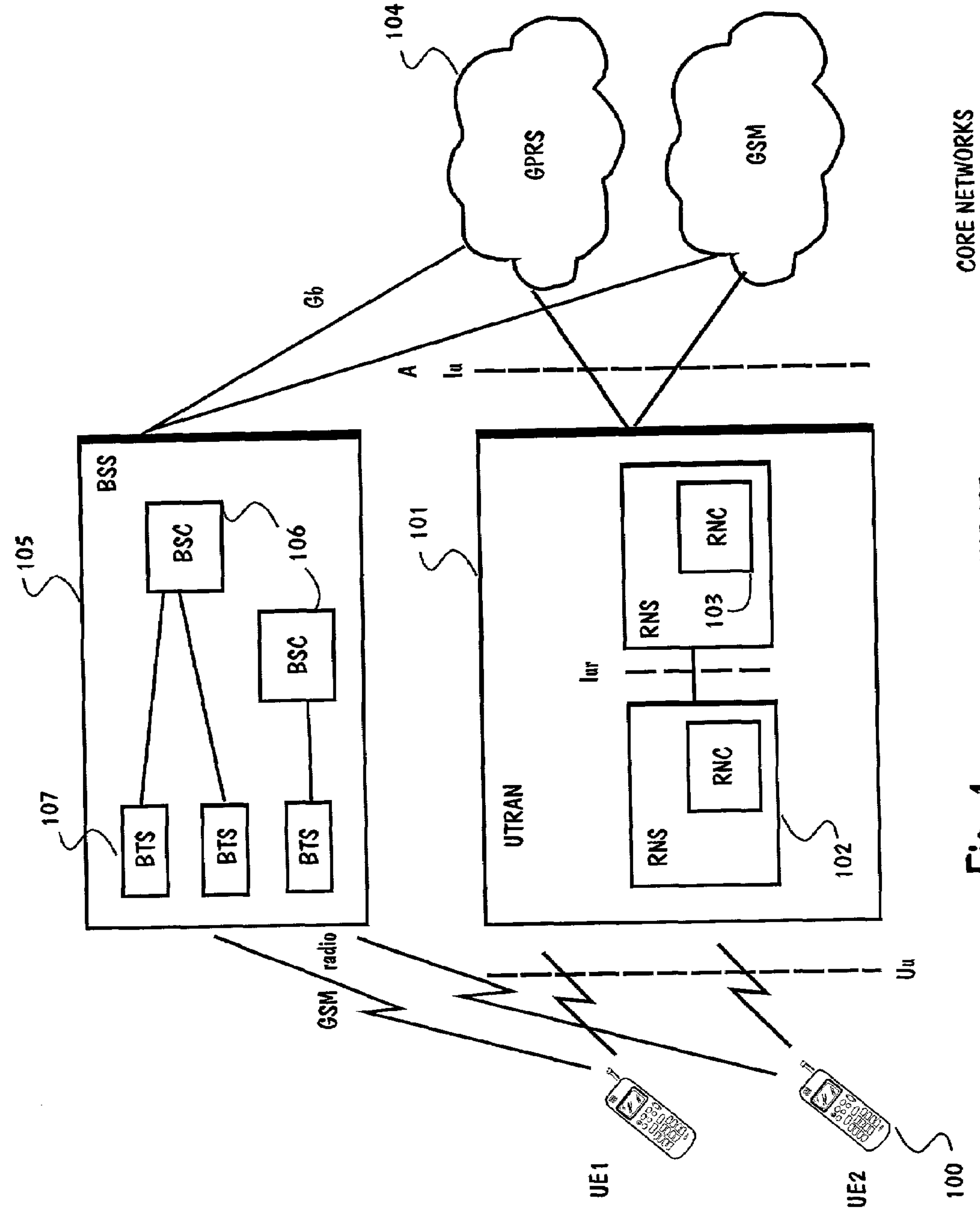
OTHER PUBLICATIONS

3 GPP TS 35.201, V4.0.0(Aug. 2001), 3RD Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1;f8 and f9 Specification (Release 4), 2001, Valbonne, France.

3G TS 33.102, v 3.2.0(Oct. 1999), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (3G TS 33.102 version 3.2.0); 1999, Valbonne, France.

3G TS 33.102, (v3.3.1) "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture", version 3.3.1 Release 1999, Jan. 2000, Valbonne, France.

* cited by examiner



PRIOR ART

Fig. 1

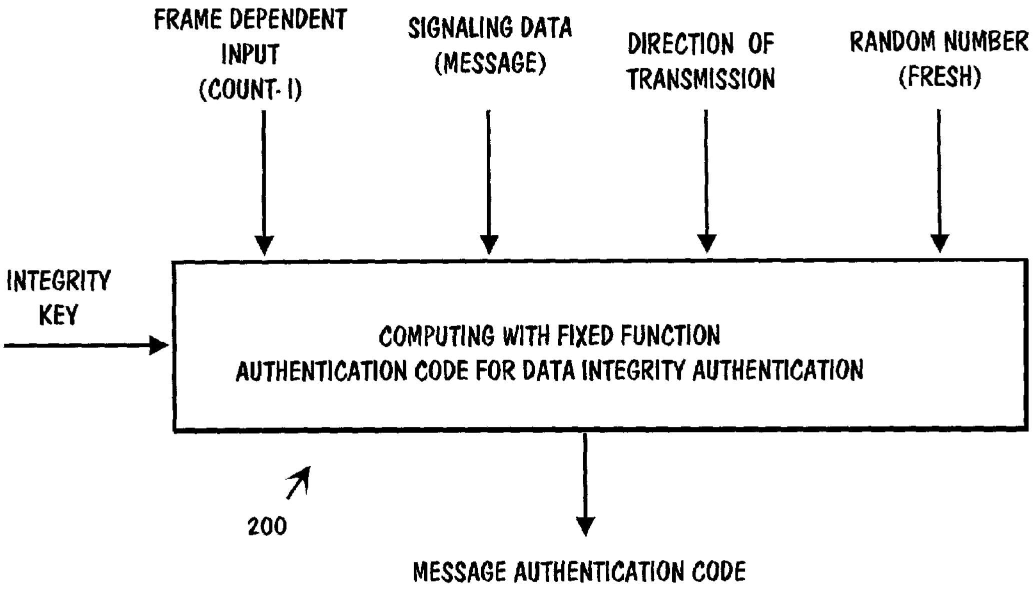
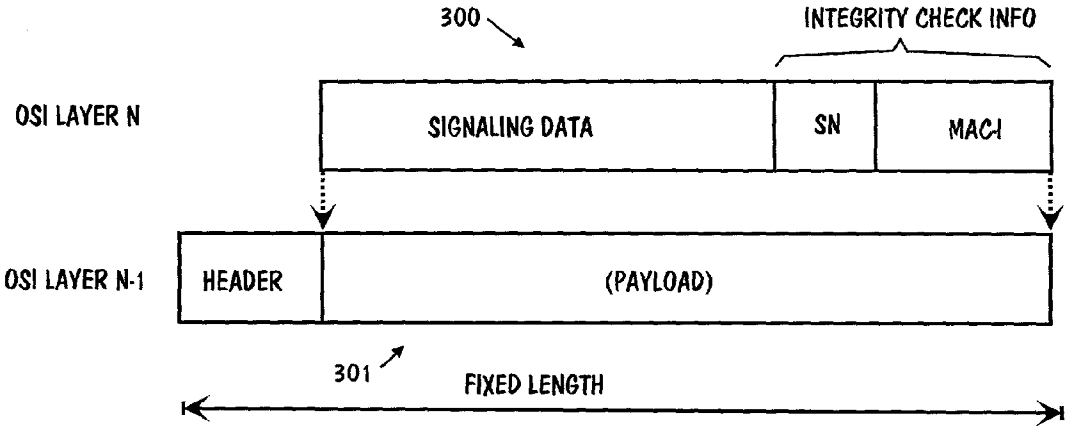

FRAME DEPENDENT INPUT (COUNT- I)
SIGNALING DATA (MESSAGE)
DIRECTION OF TRANSMISSION
RANDOM NUMBER (FRESH)
INTEGRITY KEY
COMPUTING WITH FIXED FUNCTION AUTHENTICATION CODE FOR DATA INTEGRITY AUTHENTICATION
200
MESSAGE AUTHENTICATION CODE

Fig. 2

PRIOR ART



PRIOR ART

Fig. 3

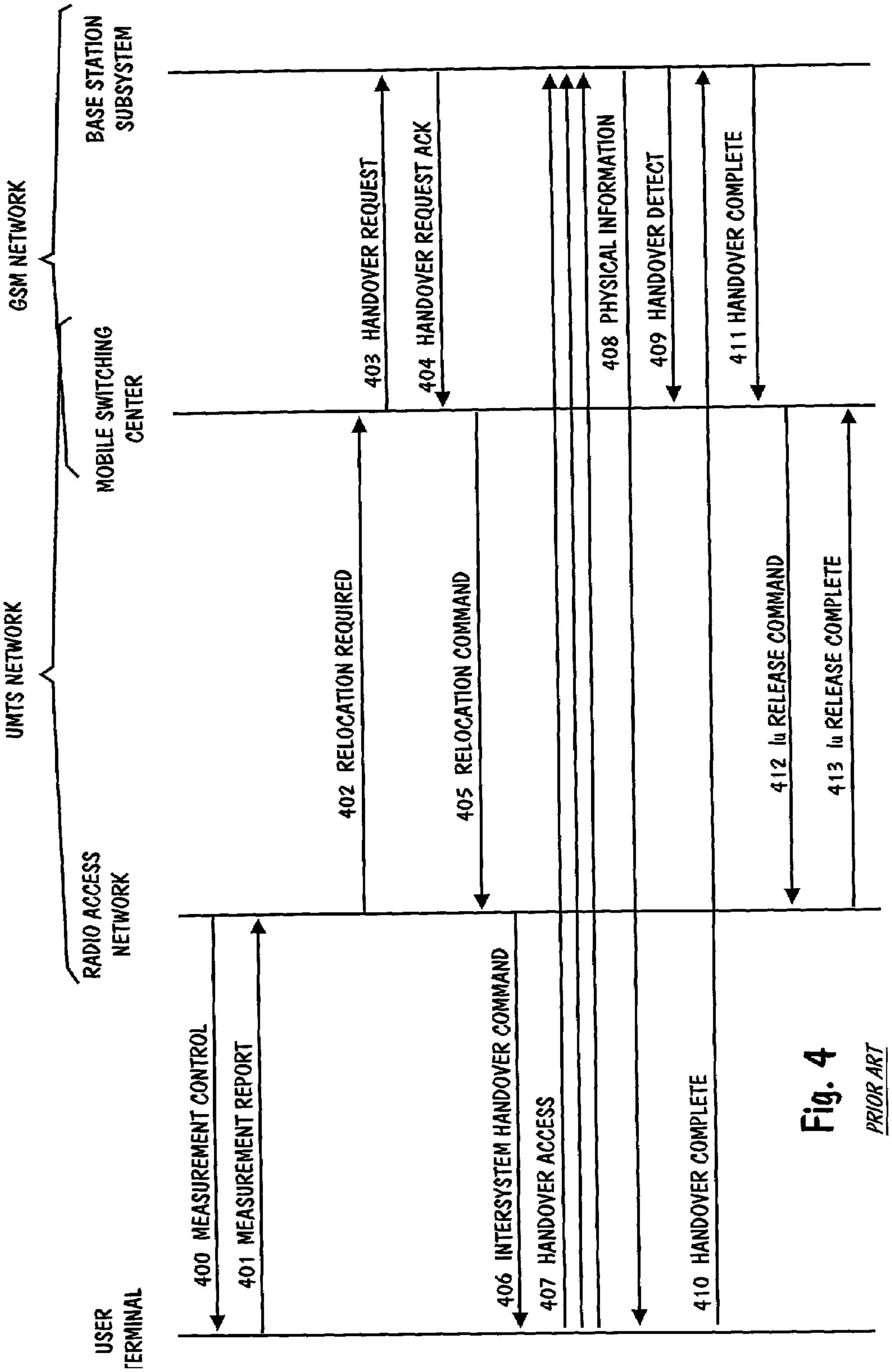


Fig. 4

PRIOR ART

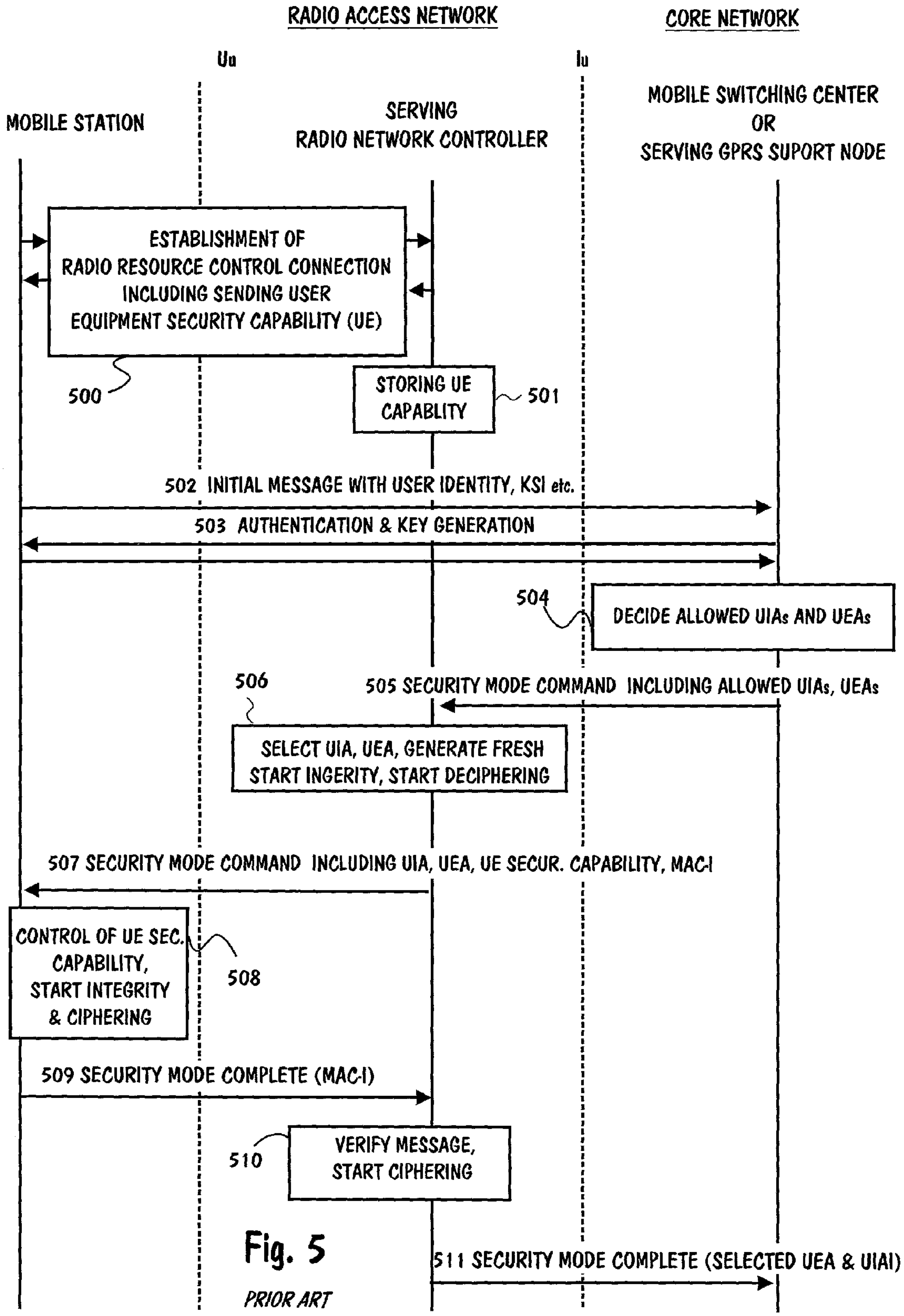

RADIO ACCESS NETWORK
CORE NETWORK
Uu
Iu
MOBILE STATION
SERVING
RADIO NETWORK CONTROLLER
MOBILE SWITCHING CENTER
OR
SERVING GPRS SUPORT NODE
ESTABLISHMENT OF
RADIO RESOURCE CONTROL CONNECTION
INCLUDING SENDING USER
EQUIPMENT SECURITY CAPABILITY (UE)
500
STORING UE
CAPABLITY
501
502 INITIAL MESSAGE WITH USER IDENTITY, KSI etc.
503 AUTHENTICATION & KEY GENERATION
504
DECIDE ALLOWED UIAs AND UEAs
506
505 SECURITY MODE COMMAND INCLUDING ALLOWED UIAs, UEAs
SELECT UIA, UEA, GENERATE FRESH
START INGERITY, START DECIPHERING
507 SECURITY MODE COMMAND INCLUDING UIA, UEA, UE SECUR. CAPABILITY, MAC-I
CONTROL OF UE SEC.
CAPABILITY,
START INTEGRITY
& CIPHERING
508
509 SECURITY MODE COMPLETE (MAC-I)
510
VERIFY MESSAGE,
START CIPHERING
511 SECURITY MODE COMPLETE (SELECTED UEA & UIAI)

Fig. 5

PRIOR ART

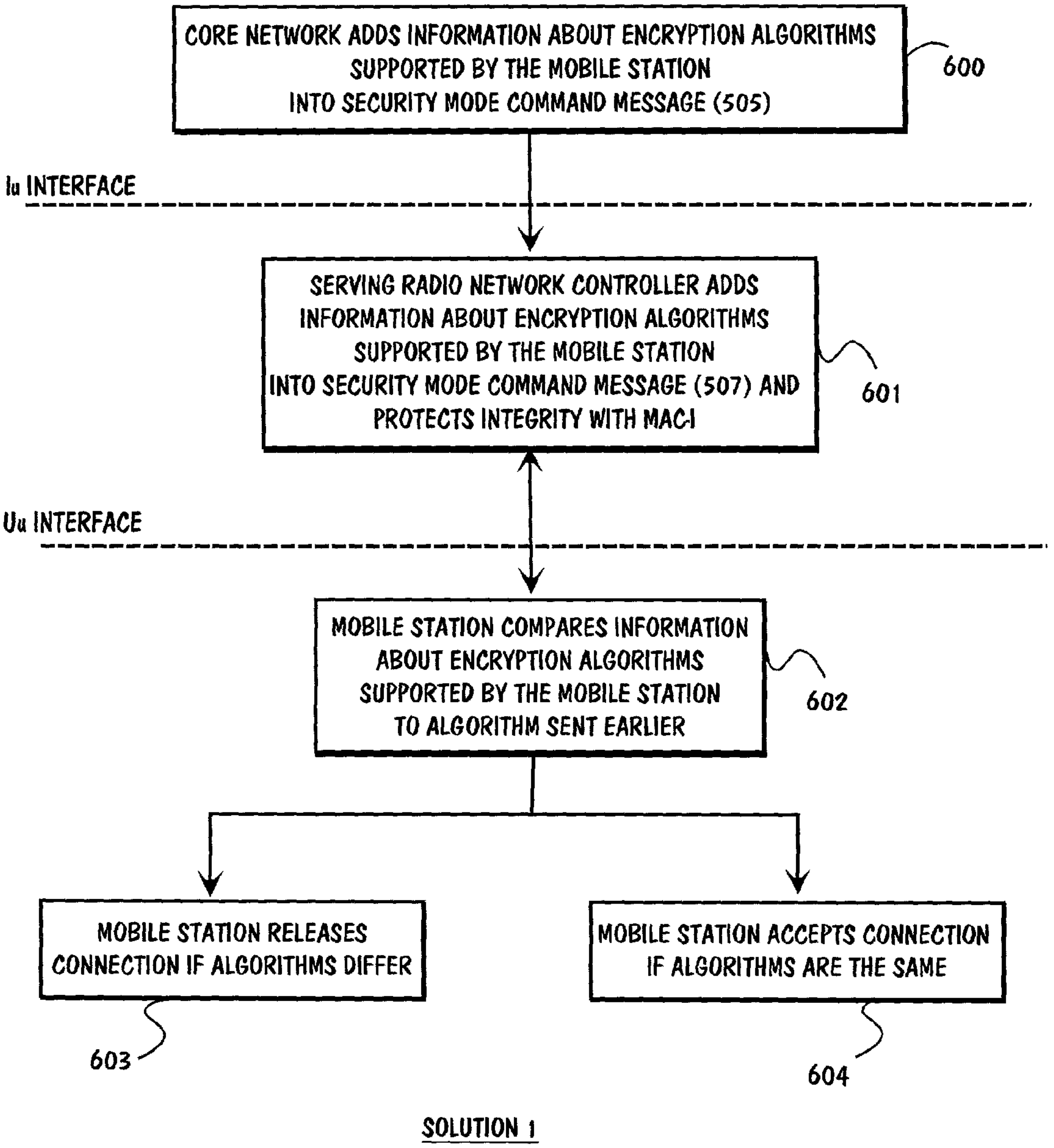

CORE NETWORK ADDS INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION INTO SECURITY MODE COMMAND MESSAGE (505)
600
Iu INTERFACE
SERVING RADIO NETWORK CONTROLLER ADDS INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION INTO SECURITY MODE COMMAND MESSAGE (507) AND PROTECTS INTEGRITY WITH MAC-I
601
Uu INTERFACE
MOBILE STATION COMPARES INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION TO ALGORITHM SENT EARLIER
602
MOBILE STATION RELEASES CONNECTION IF ALGORITHMS DIFFER
603
MOBILE STATION ACCEPTS CONNECTION IF ALGORITHMS ARE THE SAME
604
SOLUTION 1

Fig. 6

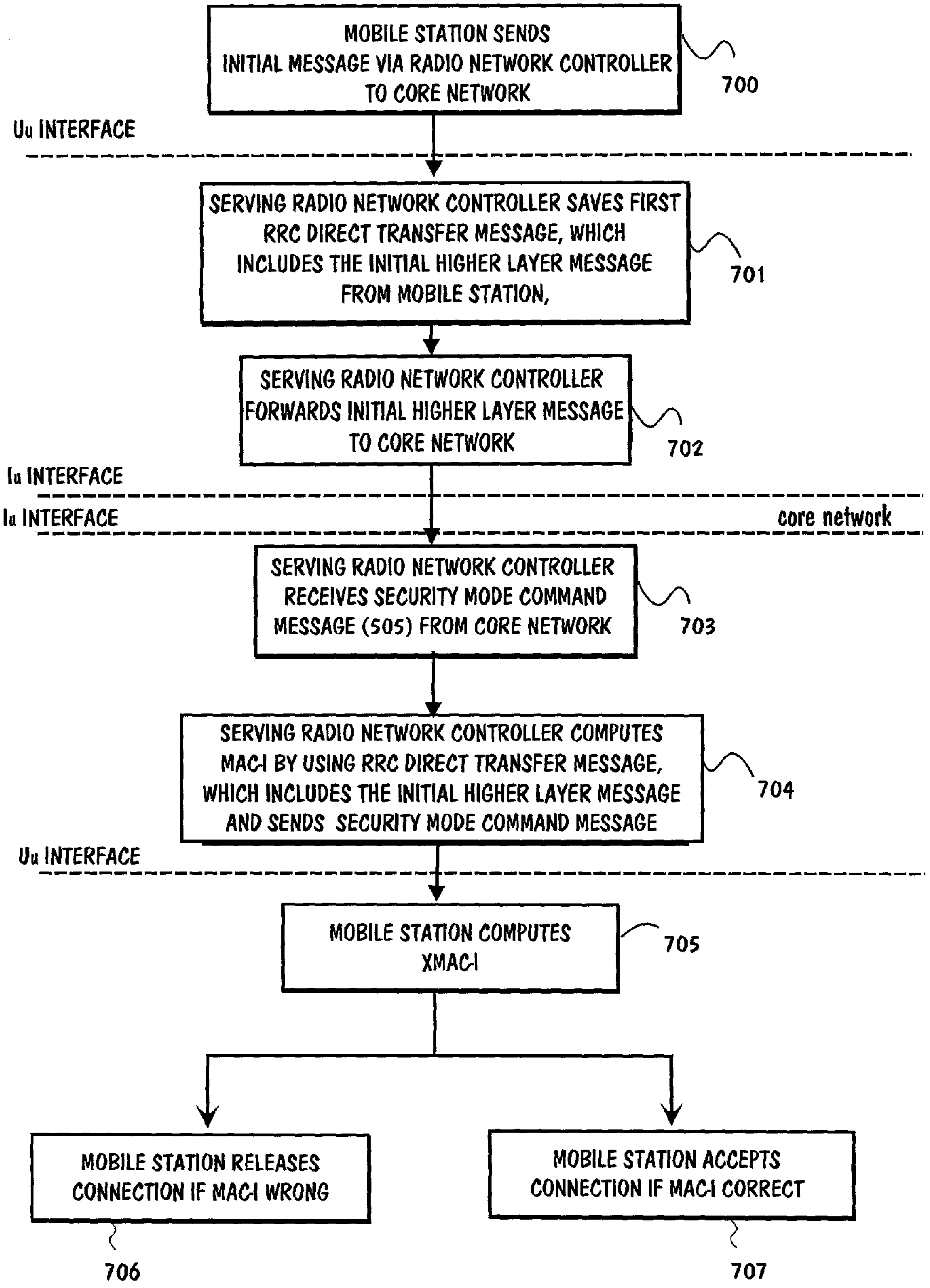
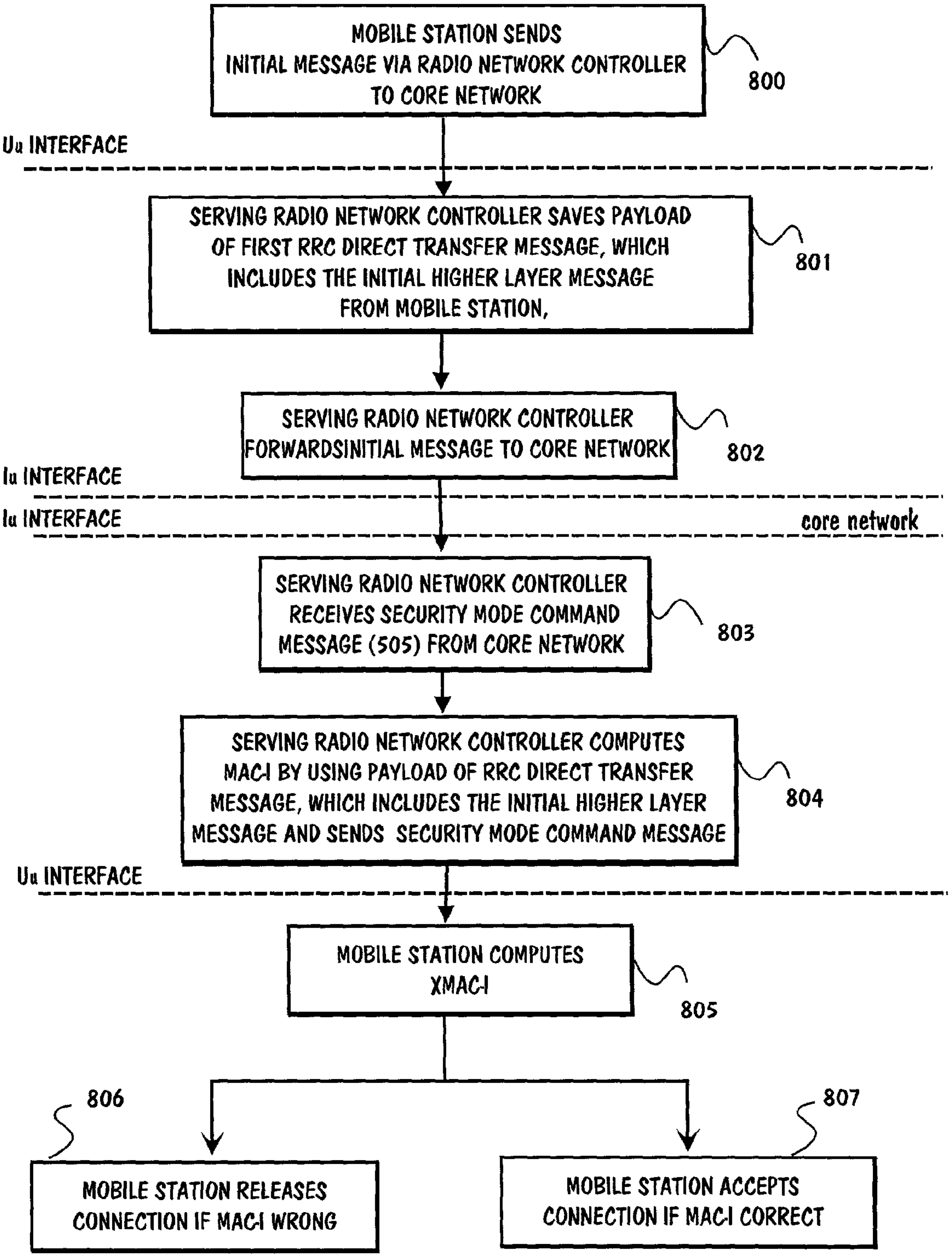

MOBILE STATION SENDS INITIAL MESSAGE VIA RADIO NETWORK CONTROLLER TO CORE NETWORK
700
Uu INTERFACE
SERVING RADIO NETWORK CONTROLLER SAVES FIRST RRC DIRECT TRANSFER MESSAGE, WHICH INCLUDES THE INITIAL HIGHER LAYER MESSAGE FROM MOBILE STATION,
701
SERVING RADIO NETWORK CONTROLLER FORWARDS INITIAL HIGHER LAYER MESSAGE TO CORE NETWORK
702
Iu INTERFACE
Iu INTERFACE
core network
SERVING RADIO NETWORK CONTROLLER RECEIVES SECURITY MODE COMMAND MESSAGE (505) FROM CORE NETWORK
703
SERVING RADIO NETWORK CONTROLLER COMPUTES MAC-I BY USING RRC DIRECT TRANSFER MESSAGE, WHICH INCLUDES THE INITIAL HIGHER LAYER MESSAGE AND SENDS SECURITY MODE COMMAND MESSAGE
704
Uu INTERFACE
MOBILE STATION COMPUTES XMAC-I
705
MOBILE STATION RELEASES CONNECTION IF MAC-I WRONG
706
MOBILE STATION ACCEPTS CONNECTION IF MAC-I CORRECT
707

Fig. 7

SOLUTION 2


MOBILE STATION SENDS
INITIAL MESSAGE VIA RADIO NETWORK CONTROLLER
TO CORE NETWORK
800
Uu INTERFACE
SERVING RADIO NETWORK CONTROLLER SAVES PAYLOAD
OF FIRST RRC DIRECT TRANSFER MESSAGE, WHICH
INCLUDES THE INITIAL HIGHER LAYER MESSAGE
FROM MOBILE STATION,
801
SERVING RADIO NETWORK CONTROLLER
FORWARDSINITIAL MESSAGE TO CORE NETWORK
802
Iu INTERFACE
Iu INTERFACE
core network
SERVING RADIO NETWORK CONTROLLER
RECEIVES SECURITY MODE COMMAND
MESSAGE (505) FROM CORE NETWORK
803
SERVING RADIO NETWORK CONTROLLER COMPUTES
MAC-I BY USING PAYLOAD OF RRC DIRECT TRANSFER
MESSAGE, WHICH INCLUDES THE INITIAL HIGHER LAYER
MESSAGE AND SENDS SECURITY MODE COMMAND MESSAGE
804
Uu INTERFACE
MOBILE STATION COMPUTES
XMAC-I
805
806
807
MOBILE STATION RELEASES
CONNECTION IF MAC-I WRONG
MOBILE STATION ACCEPTS
CONNECTION IF MAC-I CORRECT

SOLUTION 3

Fig. 8

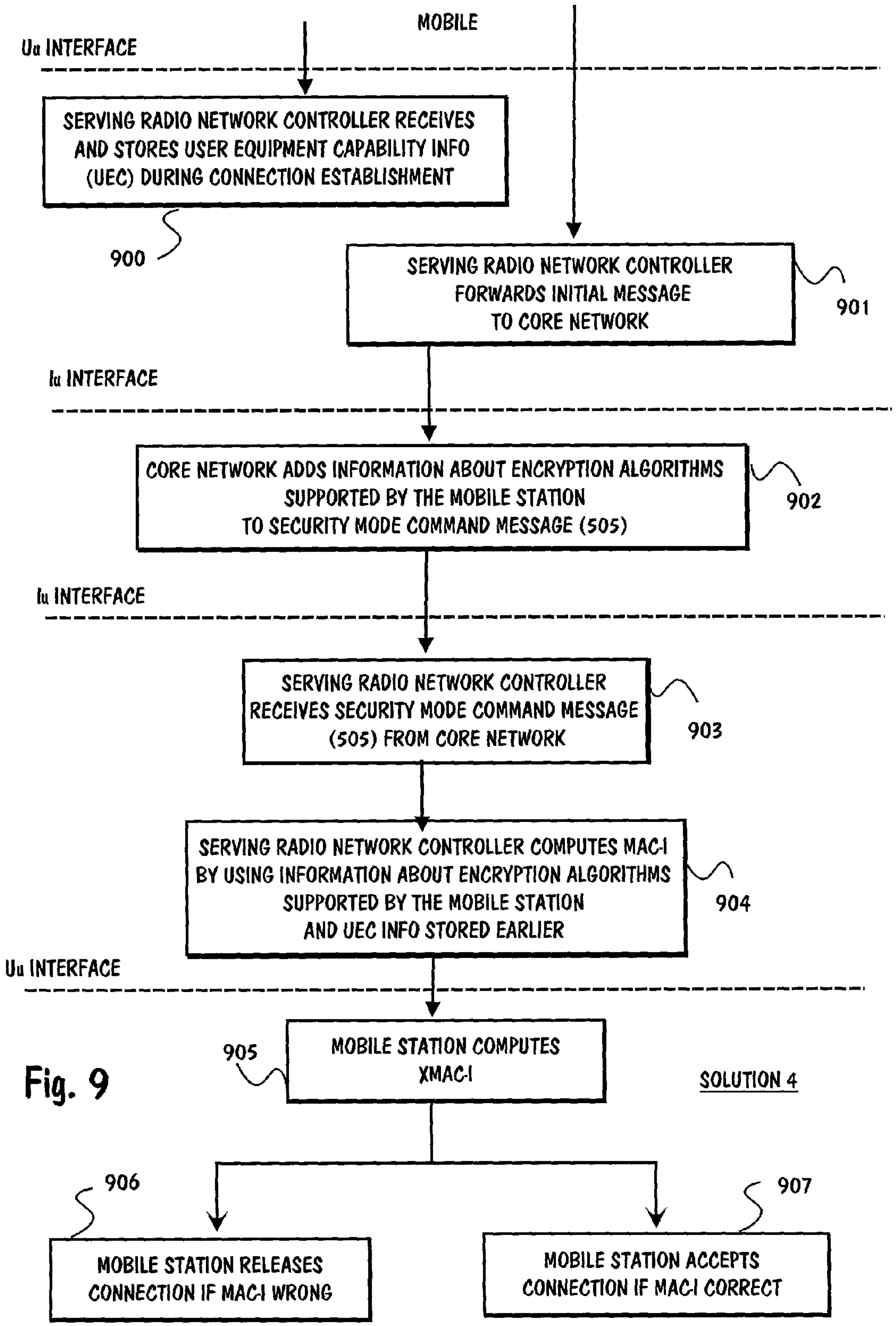

MOBILE
Uu INTERFACE
SERVING RADIO NETWORK CONTROLLER RECEIVES AND STORES USER EQUIPMENT CAPABILITY INFO (UEC) DURING CONNECTION ESTABLISHMENT
900
SERVING RADIO NETWORK CONTROLLER FORWARDS INITIAL MESSAGE TO CORE NETWORK
901
Iu INTERFACE
CORE NETWORK ADDS INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION TO SECURITY MODE COMMAND MESSAGE (505)
902
Iu INTERFACE
SERVING RADIO NETWORK CONTROLLER RECEIVES SECURITY MODE COMMAND MESSAGE (505) FROM CORE NETWORK
903
SERVING RADIO NETWORK CONTROLLER COMPUTES MAC-I BY USING INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION AND UEC INFO STORED EARLIER
904
Uu INTERFACE
905
MOBILE STATION COMPUTES XMAC-I
SOLUTION 4
906
907
MOBILE STATION RELEASES CONNECTION IF MAC-I WRONG
MOBILE STATION ACCEPTS CONNECTION IF MAC-I CORRECT

Fig. 9

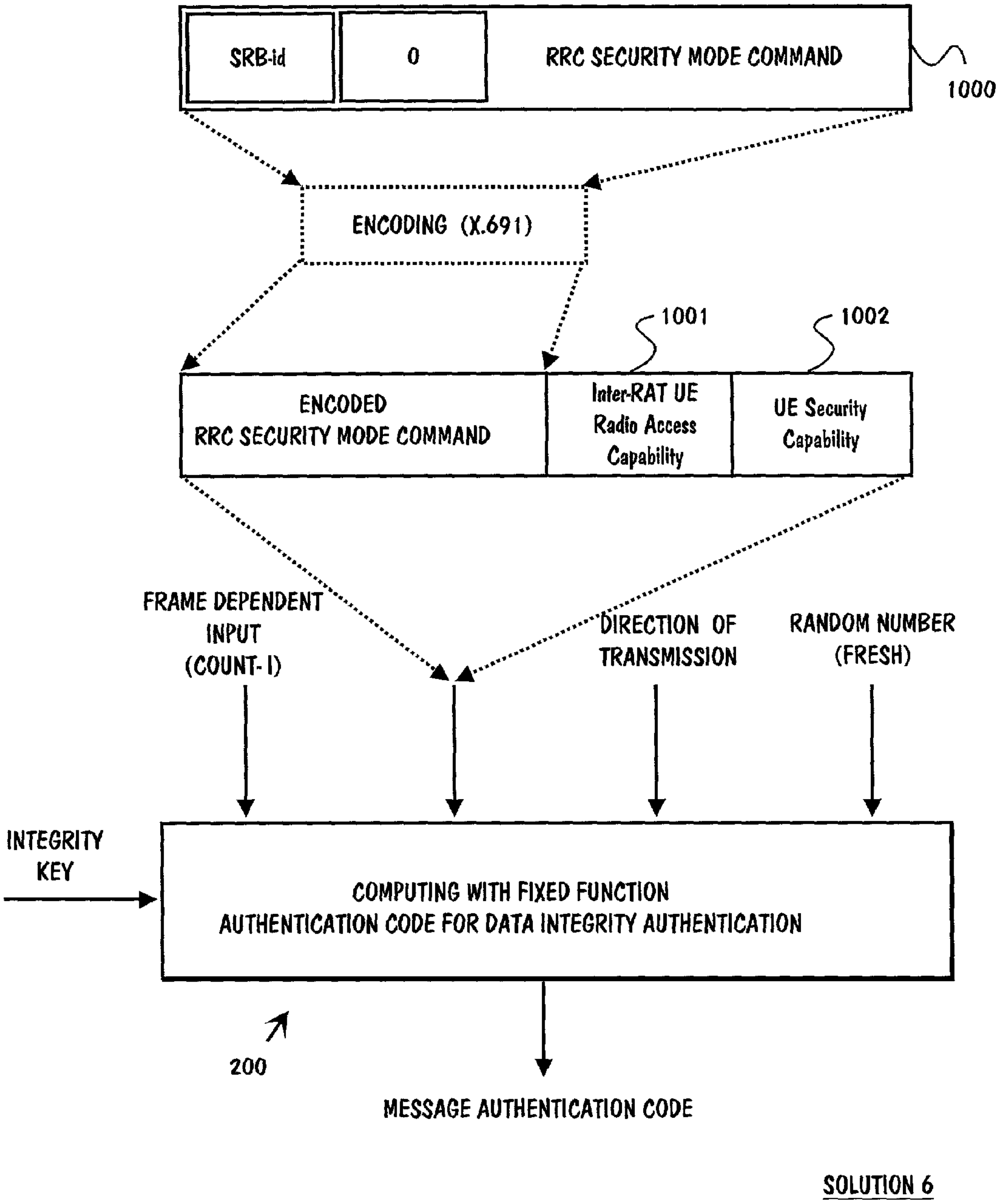

SRB-id
0
RRC SECURITY MODE COMMAND
1000
ENCODING (X.691)
1001
1002
ENCODED
RRC SECURITY MODE COMMAND
Inter-RAT UE
Radio Access
Capability
UE Security
Capability
FRAME DEPENDENT
INPUT
(COUNT- I)
DIRECTION OF
TRANSMISSION
RANDOM NUMBER
(FRESH)
INTEGRITY
KEY
COMPUTING WITH FIXED FUNCTION
AUTHENTICATION CODE FOR DATA INTEGRITY AUTHENTICATION
200
MESSAGE AUTHENTICATION CODE
SOLUTION 6

Fig. 10

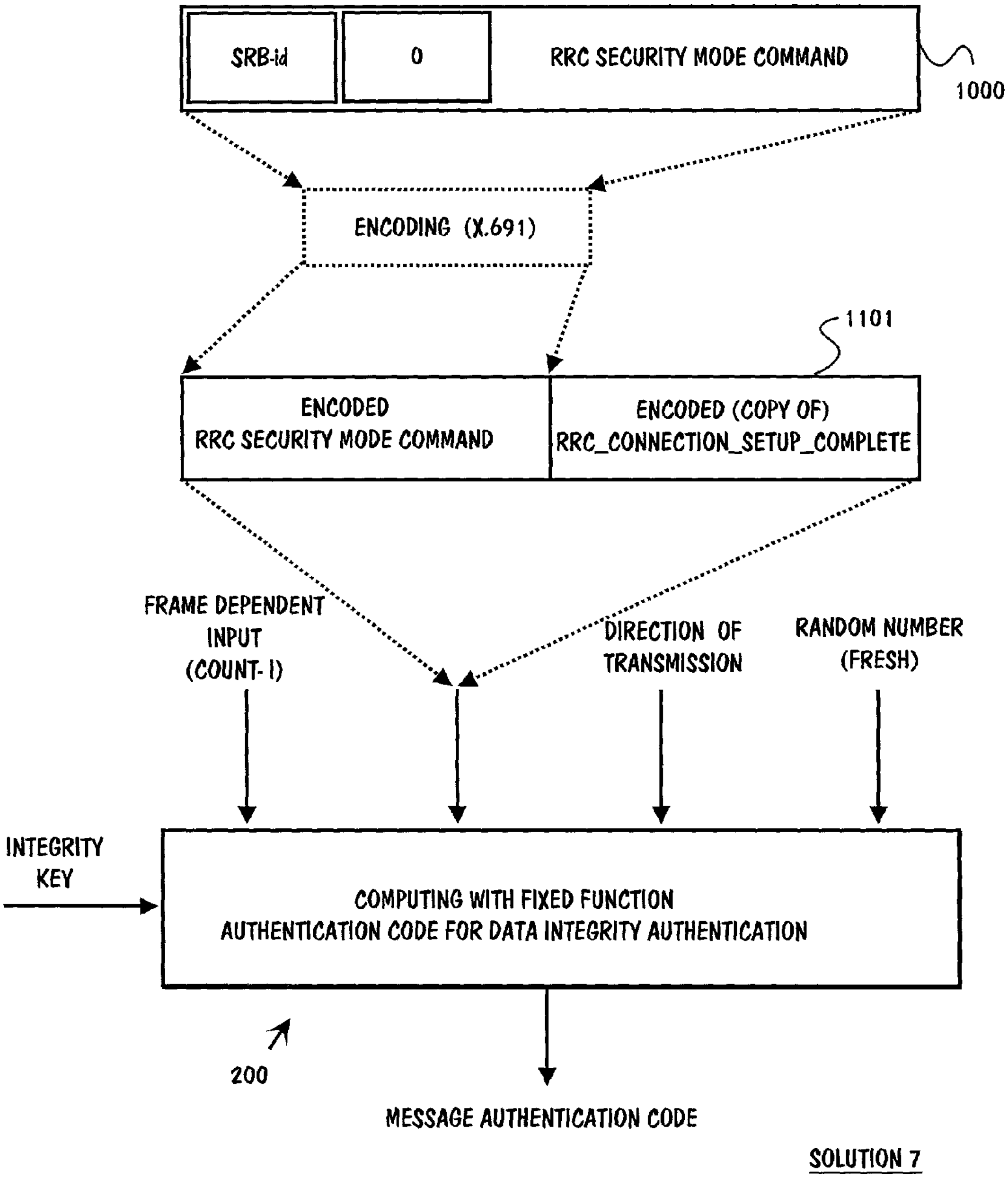

SRB-id
0
RRC SECURITY MODE COMMAND
1000
ENCODING (X.691)
1101
ENCODED
RRC SECURITY MODE COMMAND
ENCODED (COPY OF)
RRC_CONNECTION_SETUP_COMPLETE
FRAME DEPENDENT
INPUT
(COUNT- I)
DIRECTION OF
TRANSMISSION
RANDOM NUMBER
(FRESH)
INTEGRITY
KEY
COMPUTING WITH FIXED FUNCTION
AUTHENTICATION CODE FOR DATA INTEGRITY AUTHENTICATION
200
MESSAGE AUTHENTICATION CODE
SOLUTION 7

Fig. 11

SYSTEM FOR ENSURING ENCRYPTED COMMUNICATION AFTER HANDOVER

FIELD OF THE INVENTION

The present invention relates generally to an integrity protection in a telecommunications network.

BACKGROUND OF THE INVENTION

A third generation mobile communications system is in Europe named UMTS (Universal Mobile Telecommunications System). It is a part of the International Telecommunications Union's IMT-2000 system. UMTS/IMT-2000 is global wireless multimedia system which provides higher transmission speed (2 Mbit/s) than the existing mobile networks.

FIG. **1** shows with a simplified block diagram a GSM (Global System for Mobile communications) network and a UMTS network. The main parts of the network are user terminals **100** and a network part that comprises the GSM base station subsystem BSS **105** and the UMTS terrestrial radio access network UTRAN **101** (which is a wideband multiple access radio network currently being specified in the 3GPP (Third Generation Partnership Project)) and a core network CN **104**. The radio interface between a user terminal and the UTRAN is called Uu and the interface between the UTRAN and the 3G core network is called Iu. The interface between the GSM base station subsystem BSS and general packet radio service GPRS core network is called Gb and interface between the GSM base station subsystem BSS and GSM core networks is called A. The user terminals can be multi-mode terminals, which can operate using at least two radio access technologies, in this example UMTS and GSM. The UTRAN consists of a radio network subsystems RNS **102** that further consists of radio network controller RNC **103** and one or more nodes B (not shown in FIG. **1**). An interface between two RNS is called Iur. The interface between the user terminal and the GSM base station subsystem BSS is simply called "Radio Interface". The GSM base station subsystem BSS consists of the base station controllers BSC **106** and the base transceiver stations BTS **107**. The core network nodes, e.g. the (GSM) Mobile Switching Center MSC and the (GPRS) serving GPRS support node SGSN, can be capable of controlling both types of radio access networks—UTRAN and BSS. Another possible network configuration is such that each radio access network (UTRAN and BSS) has its own controlling core network node, MSC and SGSN, respectively—2G MSC, 2G SGSN and 3G MSC, 3G SGSN—but all these core network elements are connected to one and the same home location register HLR (not shown in FIG. **1**), which contains all static user information, e.g. the billing of users can be controlled from one location even when the user terminals are able to operate via several different radio access networks.

The radio interface protocols which are needed to set up, reconfigure and release the radio bearer services are discussed shortly in the following. The radio interface protocol architecture in the access stratum consists of three different protocol layers which are from top to bottom: the radio network layer (L3), the data link layer (L2), and the physical layer (L1). The protocol entities in these layers are the following. The radio network layer consists of only one protocol, which in the UMTS radio interface is called RRC (Radio Recourse Control) and in the 2G GSM radio interface is called RR (Radio Resource protocol). The data link layer consists of several protocols in the UMTS radio interface called PDCP (Packet Data Convergence Protocol), BMC (Broadcast Multicast Control protocol), RLC (Radio Link Control protocol), and MAC (Medium Access Control protocol). In the GSM/GPRS radio interface, the layer 2 protocols are LLC (Logical Link Control), LAPDm (Link Access Protocol on the Dm channel), RLC (Radio Link Control), and MAC (Medium Access Control protocol). The physical layer is only one 'protocol', which has no specific name. All the mentioned radio interface protocols are specific for each radio access technique, which means that they are different for the GSM radio interface and the UMTS Uu interface, for example.

In the UMTS, the RRC layer offers services to higher layers i.e. to a non access stratum NAS via service access points which are used by the higher protocols in the user terminal side and by the Iu RANAP (Radio Access Network Application Part) protocol in the UTRAN side. All higher layer signaling (mobility management, call control, session management, etc.) is encapsulated into RRC messages for transmission over the radio interface.

All telecommunication is subject to the problem of how to make sure that the information received has been sent by an authorized sender and not by somebody who is trying to masquerade as the sender. The problem is particularly evident in cellular telecommunication systems, where the air interface presents an excellent platform for eavesdropping and replacing the contents of a transmission by using higher transmission levels, even from a distance. A basic solution to this problem is the authentication of the communicating parties. An authentication process aims to discover and check the identity of both the communicating parties, so that each party receives information about the identity of the other party and can rely on the identification to a sufficient degree. Authentication is typically performed in a specific procedure at the beginning of the connection. However, this does not adequately protect subsequent messages from unauthorized manipulation, insertion, and deletion. Thus, there is a need for the separate authentication of each transmitted message. The latter task can be carried out by appending a message authentication code (MAC-I) to the message at the transmitting end and checking the MAC-I value at the receiving end.

A MAC-I is typically a relatively short string of bits based in some specified way on the message it protects and on a secret key known both by the sender and by the recipient of the message. The secret key is generated and agreed on typically in connection with the authentication procedure at the beginning of the connection. In some cases the algorithm that is used to calculate the MAC-I based on the secret key and on the message is also secret, but this is not usually the case.

The process of authentication of single messages is often called integrity protection. To protect the integrity of signaling, the transmitting party computes a MAC-I value based on the message to be sent and the secret key using the specified algorithm, and sends the message with the MAC-I value. The receiving party recomputes a MAC-I value based on the message and the secret key according to the specified algorithm, and compares the received MAC-I and the calculated MAC-I. If the two MAC-I values match, the recipient can trust that the message is intact and has been sent by the authorized party.

FIG. **2** illustrates the computation of a message authentication code in the UTRAN. The length of the MAC-I used in UTRAN is 32 bits.

The UMTS integrity algorithm used in block **200** is a one-way cryptographic function for calculating the Message Authentication Code (MAC-I) based on the input parameters shown in FIG. **2**. The one-way function means that it is impossible to derive the unknown input parameters from a MAC-I, even if all but one input parameter are known.

The input parameters for calculating the MAC-I are the actual signaling message (after encoding) to be sent, a secret integrity key, a sequence number COUNT-I for the message to be integrity protected, a value indicating the direction of transmission, i.e. whether the message is sent in uplink (from the user terminal to the network) or downlink (from the network to the user terminal) direction, and a random number (FRESH) generated by the network. COUNT-I is composed of a short sequence number SN and a long sequence number called hyper frame number HFN. Only the short sequence number is normally sent with the message; the HFN is updated locally at each communicating party.

The computing block **200** calculates the message authentication code by applying the afore-mentioned parameters to the integrity algorithm, which is called f9 algorithm in 3GPP Release'99 specifications. It is possible that more algorithms will be available in future releases of new specifications. Before integrity protection is started, the user terminal informs the network, which integrity algorithms it supports, and the network then selects one of these algorithms to be used for the connection. A similar mechanism regarding the supported algorithms is also used for the ciphering.

FIG. **3** illustrates a message to be sent over e.g. a radio interface. The message is a layer N protocol data unit (PDU) **300**, which is transferred as a payload in layer N−1 PDU **301**. In the present example, layer N represents the Radio Resource Control (RRC) protocol in the radio interface and layer N−1 represents the Radio Link Control (RLC) layer. The layer N−1 PDU normally has a fixed size, which depends on the physical layer (the lowest layer, not visible in FIG. **2**) channel type used and on the parameters, e.g. modulation, channel coding, interleaving. If layer N PDUs are not exactly the size of the payload offered by layer N−1 as is normally the case, layer N-1 can utilize functions like segmentation, concatenation, and padding to make layer N−1 PDUs always a fixed size. In the present application we are concentrating on a layer N PDU consisting of the actual signaling data and the Integrity Check Info. The Integrity Check Info consists of the MAC-I and the message sequence number SN needed at the peer end for the recalculation of MAC-I. The total length of the message is then a combination of the signaling data bits and the Integrity Check Info bits.

FIG. **4** illustrates intersystem handover from a radio access network to a GSM base station subsystem. For simplicity only one mobile switching center is shown in the FIG. **4**. Actually it consists of a GSM (2G or second generation) mobile switching center MSC and a UMTS (3G or third generation) mobile switching center, which may be physically either one or two separate MSC's. Interaction between these two mobile switching centers (if they would be two separate entities) is not essential in view of the actual invention and therefore it is not described in the following.

At the beginning, a connection exists between the user terminal and the radio access network, which in this particular example is a UTRAN. Based on various parameters, e.g. the neighboring cell load information, measurements from the user terminal, and the existence of GSM cells in the nearby geographical area as well as existence of the user terminal capabilities (to support also GSM mode), the radio access network may initiate an intersystem handover to base station subsystem BSS. First, the UTRAN requests the user terminal to start intersystem measurements on GSM carriers by sending a MEASUREMENT CONTROL message **400** containing intersystem specific parameters. When the criteria (as described in the MEASUREMENT CONTROL message) to send a measurement report is fulfilled, the user terminal sends a MEASUREMENT REPORT(s) **401**. Intersystem handover decision is then made at the UTRAN. After the decision a serving radio network controller SRNC, which is located in the UTRAN, sends a RELOCATION REQUIRED **402** message through Iu interface to the mobile switching center (3G MSC). Once after receiving, the message the mobile switching center (2G MSC) sends a HANDOVER REQUEST message **403** to a target base station subsystem, containing information, such as the ciphering algorithm and ciphering key to be used for the connection, and the MS classmark information, indicating, for example, which ciphering algorithms are supported by the user terminal. Thus, it is possible that either the mobile switching center MSC selects the ciphering algorithm and indicates only the selected algorithm to the base station subsystem BSS, or that the mobile switching center MSC sends a list of possible ciphering algorithms to the base station subsystem BSS, which then makes the final selection. The MS classmark information was sent by the user terminal to the mobile switching center MSC at the beginning of the (UMTS) connection. It is also possible that the MS classmark information is sent from the user terminal to the UMTS radio access network (UTRAN) at the beginning of the (UMTS) connection. When an inter-system handover from UMTS to GSM is triggered, the MS classmark information is forwarded from UTRAN to MSC. When a GSM base station controller receives the message it makes reservation from the indicated GSM cell and responds by sending back a HANDOVER REQUEST ACK message **404** indicating that the requested handover at the base station subsystem BSS can be supported and also to which radio channel(s) the user terminal should be directed. The HANDOVER REQUEST ACK **404** also indicates that the requested handover algorithm has been accepted, or, if the HANDOVER REQUEST **403** contained several algorithms, which handover algorithm has been selected. If the base station subsystem BSS is not able to support any of the indicated ciphering algorithms, it returns a HANDOVER FAILURE message (instead of **404**) and the mobile switching center MSC indicates failure of the handover to the UTRAN. At stage **405**, the mobile switching center (3G MSC) responds with a RELOCATION COMMAND message over the Iu interface to the message sent at stage **402** from the serving radio network controller located in the UTRAN. The RELOCATION COMMAND carries in a payload e.g. the information about the target GSM channels together with the cipher mode information. The UTRAN commands the user terminal to execute the handover by sending an INTERSYSTEM HANDOVER COMMAND **406** message including channel information for the target GSM. In addition, other information may be included, such as the GSM cipher mode setting information, which indicates at least the ciphering algorithm to be used in the GSM connection. After having switched to the assigned GSM channels, the mobile station normally sends four times the HANDOVER ACCESS message **407** in four successive layer **1** frames on the main DCCH. These messages are sent in GSM access bursts, which are not ciphered. In some situations it may not be necessary to send these HANDOVER ACCESS messages, if so indicated in the INTERSYSTEM HANDOVER COMMAND **406**. The terminal may receive a PHYSICAL INFORMATION **408** message as a response to the HANDOVER ACCESS messages. The PHYSICAL INFORMATION message contains only the GSM Timing Advance information. Reception of a PHYSICAL INFORMATION message causes the terminal to stop sending access bursts. The HANDOVER ACCESS messages, if used, trigger the GSM base station controller in the base station system to inform about the situation to the mobile switching center (2G) with a HANDOVER DETECT message **409**.

After lower layer connections are successfully established, the mobile station returns a HANDOVER COMPLETE **410** message to the GSM base station subsystem on the main DCCH. When receiving the HANDOVER COMPLETE message **410**, the network releases the old channels, in this example the UTRAN channels. In FIG. **4**, three messages from this release procedure are shown, although in reality many other messages between network elements, which are not shown in FIG. **4**, would be needed. These three messages are first the HANDOVER COMPLETE message **411** from GSM base station subsystem to the mobile switching center, then a IU RELEASE COMMAND **412** through Iu interface to the UTRAN or more accurately to the serving radio network controller. The third message is the IU RELEASE COMPLETE message **413**.

The ciphering key to be used after the intersystem handover is derived with a conversion function from the ciphering key used in UTRAN before the handover. This conversion function exists both in the mobile station and in the mobile switching center, thus no extra procedures over the radio interface are needed. As described above, the GSM ciphering algorithm to be used after the intersystem handover is selected either by the MSC or by the BSS and informed to the mobile station (in messages **405** and **406**). The GSM Ciphering algorithm capability (included in the GSM MS classmark information elements) is in current specifications transparent to the UTRAN. However, the GSM MS classmark information elements are sent from the mobile station to UTRAN during the RRC Connection Establishment procedure, to be later forwarded to the core network during the inter-system handover to GSM.

FIG. **5** is a signaling diagram showing the basic connection setup and security mode setup procedure used in the 3GPP UTRAN. FIG. **5** shows only the most important signaling between a mobile station and a serving radio network controller residing in the radio access network on the one hand and the serving radio network controller and a mobile switching center or a serving GPRS support node on the other.

Establishment of a radio resource control (RRC) connection between the mobile station and the serving radio network controller is performed through Uu interface **500**. During RRC connection establishment, the mobile station may transfer information such as the user equipment security capability and the START values, which are required for the ciphering and integrity protection algorithms. The user equipment security capability includes information about the supported (UMTS) ciphering algorithms and (UMTS) integrity algorithms. All the values mentioned above are stored for later use in the serving radio network controller at stage **501**. Also the GSM Classmark information (MS Classmark 2 and MS Classmark 3) is transmitted from the mobile station to UTRAN during RRC connection establishment, and it can be stored for later use in the serving radio network controller.

Next the mobile station sends an initial higher layer message **502** (which can be e.g. CM SERVICE REQUEST, LOCATION UPDATING REQUEST or CM RE-ESTABLISHMENT REQUEST) via the serving radio network controller through a Iu interface to the mobile switching center, including e.g. the user identity, a key set identifier KSI and the MS classmark indicating, for example, the supported GSM ciphering algorithms when intersystem handover to the GSM is initialized. The network initiates authentication procedure which also leads to generation of new security keys **503**. Next, the network decides the set of UMTS Integrity Algorithms UIAs and UMTS Encryption Algorithms UEAs from which the UIA and UEA for this connection has to be selected **504**. Then, at stage **505**, the mobile switching center sends a SECURITY MODE COMMAND message to the serving radio network controller, in which it informs the used ciphering key CK, integrity key IK, and the set of permissible UIAs and UEAs.

On the basis of the user equipment security capabilities stored at stage **501** and the list of possible UIAs and UEAs received from the mobile switching center at stage **505**, the serving radio network controller selects the algorithms to be used during the connection. It also generates a random value FRESH to be used as input parameter for the integrity algorithm (FIG. **2**) and for the ciphering algorithm. It also starts deciphering and the integrity protection **506**.

A first integrity protected message SECURITY MODE COMMAND **507** is sent through the radio interface from the serving radio network controller to the mobile station. The message includes the selected UIA and UEA together with the UE FRESH parameter to be used. In addition, the SECURITY MODE COMMAND contains the same UE security capability which was received from the user equipment during the RRC connection establishment **500**. The reason for replaying this information back to UE is to give the user equipment a possibility to check that the network has received this information correctly. This mechanism is necessary, since the messages sent during RRC connection establishment **500** are not ciphered nor integrity protected. A message authentication code MAC-I, used for the integrity protection, is attached to the SECURITY MODE COMMAND message **507**.

At stage **508** the mobile station compares whether the received UE security capability is same as that which has been sent during the RRC connection establishment procedure **500**. If the two UE security capabilities match, the mobile station can trust that the network has received the security capability correctly. Otherwise, the UE releases the RRC connection and enters idle mode.

If comparison is successful the mobile station responds with a SECURITY MODE COMPLETE message **509**. This is also an integrity protected message; thus before sending this message the mobile station generates the MAC-I for the message.

When the serving radio network controller receives the message it verifies it, at stage **510**, first by calculating the expected message authentication code XMAC-I and then comparing the calculated XMAC-I with the received MAC-I. If the values match, the serving radio network controller sends a SECURITY MODE COMPLETE message **511** to the mobile switching center including e.g. information of the selected UIA and UEA.

In the UTRAN radio interface integrity protection is a function of the radio recourse control protocol between the user terminal and the radio network controller. All higher layer signaling is integrity protected by the radio resource control protocol layer because all higher layer signaling is carried as a payload in specific radio recourse control messages (e.g. INITIAL DIRECT TRANSFER, UPLINK DIRECT TRANSFER, DOWNLINK DIRECT TRANSFER). The problem is that no authentication can be performed before the first higher layer message is sent, which is carried in the INITIAL DIRECT TRANSFER. This leads to a situation where the very first higher layer i.e. the non-access stratum message **502** cannot be integrity protected.

A major problem arises from the fact that integrity protection is not yet in effect when the first messages are sent during RRC Connection Establishment (step **500** in the FIG. **5**). Without integrity protection there is always a risk that an intruder changes the encryption algorithm information included in the messages at step **500** into the value "GSM encryption algorithms not available". In the case of GSM, the core network receives this information with the mobile station classmark CM information elements (CM2 and CM3) that are included in the RELOCATION REQUIRED message (message **402** in FIG. **4**). When the user equipment carries out an intersystem handover, e.g. from the UTRAN to the GSM base station subsystem BSS (FIG. **4**) the mobile switching center recognizes that the UE does not support any GSM ciphering algorithms and must set up the connection in the GSM BSS with no ciphering. Now it is easy to the intruder to start eavesdropping of the call.

SUMMARY OF THE INVENTION

An objective of the present invention is to devise a mobile telecommunications system that reveals an attempt of a fraudulent intruder to remove information about an encryption algorithm when a multimode mobile station sends an unprotected signaling message containing this information over radio interface to the mobile telecommunications system. According to existing specifications, this signaling message is RRC CONNECTION SETUP COMPLETE.

The system comprises at least two radio access networks providing mobile stations with access to at least one core network, a multimode mobile station, and at least one core network. The multimode mobile station sends, during connection setup with a first radio access network, at least one unprotected signaling message, including information about encryption algorithms supported by the multimode mobile station in a second radio access network. The core network receives information about the encryption algorithms via the first radio access network when a handover to the second radio access network is triggered (message **402** in FIG. **4**). The first radio access network has inventive features. Namely, in receipt of a command message from the core network instructing the multimode mobile station to cipher further communication in the first radio access network, the first radio access network composes an integrity protected command message that includes information about the encryption algorithms supported by the multimode mobile station in the second radio access network.

The protected command message comprises a payload and a message authentication code. The information about the supported algorithms in the second radio access network is located either in the payload or the information is used as a parameter when computing the message authentication code.

In both cases the multimode mobile station is able to conclude from the protected message received whether the information embedded in the message corresponds to the information sent by the multimode mobile station in the previous signaling message. If the information sent and the information received by the multimode mobile station differ from each other, it is likely that a fraudulent intruder has changed the encryption information. Then the multimode mobile station initiates release of the connection.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described more closely with reference to the accompanying drawings, in which

FIG. **1** illustrates with a simplified block diagram a GSM and a UMTS radio access networks, connected to the same core network;

FIG. **2** depicts the computation of a message authentication code;

FIG. **3** shows the contents of a message;

FIG. **4** is a signaling chart illustrating intersystem handover from the UMTS network to the GSM network;

FIG. **5** is a signaling chart showing the basic connection setup and security mode setup procedure used in the 3GPP UTRAN;

FIG. **6** shows as a flowchart of the first example of the implementation of the method according to the invention;

FIG. **7** shows as a flowchart of a second example of the implementation of the method according to the invention;

FIG. **8** shows as a flowchart of a third example of the implementation of the method according to the invention;

FIG. **9** shows as a flowchart of a fourth example of the implementation of the method according to the invention;

FIG. **10** shows a fifth example of the implementation of the method according to the invention;

FIG. **11** shows a sixth example of the implementation of the method according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The idea of the method described in the following is to increase security in telecommunications network, especially security pertaining to signaling through the radio interface.

It is to be noted that all the terms "terminal", "user terminal", "mobile station" and "user equipment" refer to the same equipment.

Most signaling messages sent between a user terminal and the network, for example, must be integrity protected. Examples of such messages are RRC, MM, CC, GMM and SM messages. Integrity protection is applied at the RRC layer, both in the user terminal and in the network.

Integrity protection is usually performed for all RRC (Radio Recourse Control) messages, with some exceptions. These exceptions can be:

1. messages assigned to more than one recipient,
2. messages sent before the integrity keys were created for the connection, and
3. frequently repeated messages, including information not needing integrity protection.

Due to security, it is especially important to integrity protect the initial messages mentioned in alternative 2, or at least critical information elements in them. As already mentioned, without integrity protection there is always a risk that an intruder changes the encryption algorithm information included into message **500** to the value "encryption algorithm is not available".

There are several different ways of implementing the functionality required to increase security but only some of solutions are shown.

The invention is now described in detail with four examples by referring to FIG. **6-9**.

In the beginning a connection is established between a user terminal and a UMTS network. Afterwards a handover is carried out from the UMTS network to a GSM network.

FIG. **6** shows as a flowchart of one implementation of the method according to the invention. It is assumed that signaling corresponds to the situation shown in FIG. **5** until the core network receives message **503**.

In addition it is assumed that the user terminal is a dual mode (UMTS/GSM) terminal, which on the UMTS mode sends the first non-access-stratum message over the radio interface in a radio resource control INITIAL DIRECT TRANSFER message (corresponding message **502** in FIG. **5**). It is further assumed that the RRC Connection Establishment (**500**) has been performed, thus the user terminal was in an idle state and had no existing RRC Connection when a request arrived to set up a connection with the core network.

The core network receives GSM classmark information in the initial message **502** from the user terminal, here the mobile station. This information indicates general mobile station characteristics in the GSM mode including information about which GSM ciphering algorithms are supported at the terminal when it is in GSM mode. The term "classmark" has to be understood as GSM specific; another term may be used in other systems. The mobile switching center in the core network adds information about encryption algorithms supported by the mobile station into the SECURITY MODE COMMAND message **600**. The message is sent to the serving radio network controller through the Iu interface. The serving radio network controller adds this information about encryption algorithms supported by the mobile station, including information about supported encryption algorithms, to a SECURITY COMMAND message before encoding **601**. A 32-bit message authentication code MAC-I is computed and added to the encoded message.

Besides the encoded message the MAC-I code is also based on several other parameters. The following input parameters are needed for computation of the integrity algorithm: the encoded message, the 4-bit sequence number SN, the 28-bit hyper-frame number HFN, the 32-bit random number FRESH, the 1-bit direction identifier DIR, and the most important parameter—the 128-bit integrity key IK. The short sequence number SN and the long sequence number HFN together compose the serial integrity sequence number COUNT-I.

When the message authentication code is computed using the integrity algorithm and the above parameters, it is guaranteed that no one other than the actual sender can add the correct MAC-I code to the signaling message. COUNT-I, for example, prevents the same message from being sent repeatedly. However, if the same signaling message for some reason or other is to be sent repeatedly, the MAC-I code differs from the MAC-I code that was in the previously sent signaling message. The aim of this is to protect the message as strongly as possible against eavesdroppers and other fraudulent users. Thus, for this particular invention, it is important to note that also the GSM information about encryption algorithms supported by the mobile station is added to the SECURITY MODE COMMAND message **507**, is integrity protected, so that the mobile station can be sure that this information has not been changed by an intruder.

Next, at stage **602**, when the mobile station receives the SECURITY MODE COMMAND message, the information about encryption algorithms supported by the mobile station received with this message is compared with the information about encryption algorithms supported by the mobile station sent earlier from the mobile station to the network in the initial message **502**. Correspondingly, according to prior art, the received UE (UMTS) security capability parameter is compared with the sent UE security capability parameter. If both comparisons are successful the mobile station accepts the connection **604**, otherwise the connection is released **603**.

FIG. **7** shows as a flowchart of the second implementation of the method.

At stage **700** the mobile station sends an INITIAL DIRECT TRANSFER message (corresponding to message **502** in FIG. **5**) to the core network via the serving radio network controller in the radio access network. The message consists of two main parts: a RRC part and a non-access stratum part, which is seen by the RRC as a transparent payload. Moreover, the payload part includes one of the following messages: CM SERVICE REQUEST, LOCATION UPDATING REQUEST, CM RE-ESTABLISHMENT REQUEST or PAGING RESPONSE.

When the serving radio network controller receives the message it stores the message **701** and forwards the payload part or the NAS part through the Iu interface to the core network **702**. The core network responds with the normal SECURITY MODE COMMAND message **703**. As in the previous example, the message authentication code MAC-I is computed to protect the message to be transmitted to the mobile station. The code is then added to the message. The message authentication code depends in a specified way on the message that it is protecting. Here computation is carried out using the following concatenated bit string as a MESSAGE parameter:

MESSAGE=SECURITY MODE COMMAND+RRC CONNECTION REQUEST+RRC INITIAL DIRECT TRANSFER.

Thereafter, the integrity protected SECURITY MODE COMMAND message is sent to the mobile station **704**.

It should be noted that in this solution it is unnecessary to include the UE (UMTS) security capability parameter into the above message. However, both security related parameters, i.e. the UE security capability parameter and the GSM classmark parameter were input parameters when the MAC-I code was computed.

The receiving end, i.e. the mobile station, has the identical algorithm for computing the message authentication code in order to verify that the message authentication code received is the same as the computed code **705**. Thus, the mobile station has saved the messages earlier sent, the RRC CONNECTION REQUEST message (**500**) and the RRC INITIAL DIRECT TRANSFER message (**502**) in order to calculate XMAC-I for the received SECURITY MODE COMMAND message. When the MAC-I value received and the computed XMAC-I value match, the mobile station assumes that the network has received correct information as to the security capability and the GSM classmarks, and the connection is accepted **707**. Otherwise the connection is released **706**.

There is one drawback of this solution, which is that the encoded messages RRC CONNECTION REQUEST and RRC INITIAL DIRECT TRANSFER must be stored in the memory of both the serving radio network controller and the mobile station until the SECURITY MODE COMMAND message has been sent/received. But on the other hand, this solution makes it possible to omit the UE security capability from the prior art SECURITY MODE COMMAND message and in this way to save 32 bits space in the message.

FIG. **8** shows as a flowchart of the third implementation of the method.

This solution differs slightly from the second solution, i.e. only blocks **801**, **804** and **805** differ from the blocks in FIG. **7**. Therefore, these two blocks are now described in detail.

At stage **801**, instead of storing the whole message the serving radio network controller stores only the payload part of the message for later use. In other words, it stores one of the following messages: CM SERVICE REQUEST, LOCATION UPDATING REQUEST, CM RE-ESTABLISHMENT REQUEST or PAGING REQUEST. Thus, this solution saves memory space as compared to the second solution.

At stage **804**, to protect the message the message authentication code MAC-I is computed by using the previously stored payload. The MESSAGE is formed in this case as follows:

MESSAGE=SECURITY MODE COMMAND+UE SECURITY CAPABILITY+NAS message part of the INITIAL DIRECT TRANSFER message.

Only the SECURITY MODE COMMAND message is sent over the Uu interface to the mobile station. This means that both the security parameters for the UE security capability and the GSM MS classmarks are used in computing the message authentication code MAC-I, but there is no need to include them in the message. However, this does not in any way decrease the security.

At stage **805** the mobile station computes the XMAC-I by using the same MESSAGE parameter as the network used at stage **804**, i.e. the parameters, which were saved earlier of the UE Security Capability and the NAS message part of the INITIAL DIRECT TRANSFER message.

FIG. **9** shows as a flowchart the fourth implementation of the method. This solution is a combination of the first and the third solutions.

During connection establishment between the mobile station and the serving radio network controller in the radio access network, the latter receives and stores the user equipment capability information UEC in its memory for later use **900**. After that the mobile station sends the first nonaccess stratum message containing e.g. information about encryption algorithms supported by the mobile station, as a payload in a RRC INITIAL DIRECT TRANSFER message to the radio access network, which forwards the NAS message to the core network **901**. The mobile switching center in the core network adds the information about encryption algorithms supported by the mobile station parameter to the SECURITY MODE COMMAND message and sends the message through the Iu interface to the serving radio network controller in the radio access network, at stage **902** and **903**.

At stage **904** the serving radio network controller computes the MAC-I code in the previously described way, adding to the earlier described parameters the MESSAGE parameter, which is formed as follows:

MESSAGE=SECURITY MODE COMMAND+UE SECURITY CAPABILITY+GSM CLASSMARKS.

In the same way as in the previous example, both the security parameters UE security capability and the GSM classmark are used for computing the message authentication code MAC-I, but there is no need to include them in the message. The advantage of this solution is that no additional memory is needed in the mobile station or in the radio network controller.

It is essential that in the solutions described above the core network is a 3G network element, thus controlling at least UMTS Radio Access Network and optionally also the GSM Base Station Subsystem.

Implementation and embodiment of the present invention has been explained above with some examples. However, it is to be understood that the invention is not restricted to the details of the above embodiment and that numerous changes and modifications can be made by those skilled in the art without departing from the characteristic features of the invention. The embodiment described is to be considered illustrative but not restrictive. Therefore, the invention should be limited only by the attached claims. Thus, alternative implementations defined by the claims, as well as equivalent implementations, are included in the scope of the invention.

For example, the source radio access network can be, for example, the UTRAN, the GSM base station subsystem, the GPRS system (General Packet Radio Service), the GSM Edge, the GSM 1800, or some other system. Correspondingly, the target radio access network can be, for example, the

UTRAN, the GSM base station subsystem, the GPRS (General Packet Radio Service), the GSM Edge, the GSM 1800, or some other system.

Furthermore, information about GSM security algorithms (A5/1, A5/2, A5/3, etc.) that are supported by the multi-mode mobile terminal can be added as a part of the UMTS “UE Radio Access Capability”. Alternatively, the information can be a separate information element or even a part of the UE security capability parameter. In practice this information must be added to the RRC connection establishment procedure (see stage **500** in FIG. **5**), as well as to the SECURITY MODE COMMAND message (see stage **507** in FIG. **5**). Like in the other possible implementations described earlier, also in this case adding the actual “Inter-RAT Radio Access Capability” (including information about supported GSM security algorithms) information element to the RRC SECURITY MODE COMMAND message is just one alternative and introduces some overhead to the signaling, since the mobile does not necessarily need this information element, but only a confirmation that the network has received it correctly. Three alternative solutions, i.e. the fifth, sixth, and seventh example implementations of the method are described in the following.

In the fifth example of the implementation of the method, a new RRC information element, including only the GSM ciphering algorithm capability, is defined. This requires 7 bits. This information element is then added to the RRC SECURITY MODE COMMAND message. The drawback of this solution is that to encode this new information element into the said message, UTRAN RRC protocol first has to decode the GSM classmark 2 and classmark 3 information elements, whose encoding/decoding rules are not part of the UTRAN RRC protocol.

FIG. **10** illustrates the sixth example of the implementation of the method. On the UTRAN side, the GSM Classmark 2 and Classmark 3 information received (RRC information element “Inter-RAT UE radio access capability” **1001**), together with the “UE Security Capability” **1002** (containing information about supported UTRAN security algorithms), are used for calculating MAC-I (and XMAC-I) for the RRC SECURITY MODE COMMAND message **1000**. This is essentially the same solution as in FIG. **9** with the exception that the GSM Classmark information (from the mobile station and not from the core network (**902**)) has already been received and stored in the serving radio network controller during the RRC Connection Establishment phase (**900**). The SECURITY MODE COMMAND to be sent to the mobile station does not contain “UE security capability” nor “Inter-RAT UE radio access capability”; these information elements are only used when calculating the MAC-I for this message.

The drawback of the sixth implementation is that the coding of the extra information elements (“UE security capability” and “Inter-RAT UE radio access capability”) used for the MAC-I calculation has to be explicitly defined. If this is not acceptable, a more straightforward implementation is shown in FIG. **11** (a seventh implementation of the method). Here the entire encoded RRC_CONNECTION_SETUP_COMPLETE message is used when calculating MAC-I (and XMAC-I) for the RRC_SECURITY_MODE_COMMAND message **1000** (instead of the two information elements only as in the sixth implementation). In practice this means that during the RRC connection establishment procedure (see stage **500** in FIG. **5**), when sending the RRC_CONNECTION_SETUP_COMPLETE message the mobile station must save a copy of the encoded message in its memory until it receives the SECURITY_MODE_COMMAND message and has checked its integrity checksum. On the network side (in the case of UTRAN in the serving radio network controller) a copy of the (non-decoded) RRC_CONNECTION_SETUP_COMPLETE message received must be kept in the memory until the MAC-I code for the SECURITY_MODE_COMMAND message has been calculated. From the standpoint of implementation, it is probably quite easy to save the entire encoded message in the memory before it is sent (UE side) or just after receiving it and before it is passed to the decoder (UTRAN side). Thus, MAC-I for SECURITY_MODE_COMMAND would be calculated by setting the MESSAGE-input parameter for the integrity algorithm as:

MESSAGE=SECURITY_MODE_COMMAND+
RRC_CONNECTION_SETUP_COMPLETE

The drawback here, as compared to the sixth example of the implementation of the method, is that this solution requires a bit more memory, both in the mobile station and on the network side. The GSM classmark information includes the encryption algorithms supported by the mobile station.

The invention claimed is:

1. An apparatus, comprising:

a receiver, of a radio access network, configured to receive via a radio interface an unprotected signaling message including information about encryption algorithms supported by a multimode mobile station in a further radio access network, the further radio access network being different from the radio access network;

wherein said radio access network is configured to compose an integrity protected command message including information relating to the encrypting algorithms supported by the multimode mobile station in said further radio access network, said integrity protected command message comprising a payload and a message authentication code; and

a sender configured to send said integrity protected command message to said multimode mobile station.

2. The apparatus as defined in claim **1**, wherein the radio access network is configured to attach information about the encryption algorithms supported by the multimode mobile station in said further radio access network received in said unprotected signaling message to said payload and to apply said payload in an algorithm computing said message authentication code.

3. The apparatus as defined in claim **1**, wherein the radio access network is configured to save the unprotected signaling message and to use the unprotected signaling message in an algorithm computing said message authentication code.

4. The apparatus as defined in claim **1**, wherein the radio access network is configured to save a payload of the unprotected signaling message and to use the payload of the unprotected signaling message in an algorithm computing said message authentication code.

5. The apparatus as defined in claim **1**, wherein the radio access network is configured to save information about the encryption algorithms supported by the multimode mobile station in said farther radio access network and to use information about the encryption algorithms supported by the multimode mobile station in said farther radio access network together with information about encryption algorithm embedded in a command message received from a core network in computing said message authentication code.

6. The apparatus as defined in claim **1**, wherein the radio access network is configured to omit information about the encryption algorithms supported by the multimode mobile station in said farther radio access network and information about the security capability of said multimode mobile station in said radio access network in the integrity protected command message.

7. The apparatus as defined in claim **1**, wherein the radio access network is configured to include information about the encryption algorithms supported by the multimode mobile station in said further radio access network in the integrity protected command message.

8. The apparatus as defined in claim **1**, wherein the multimode mobile station sends said information about file encryption algorithms supported by the multimode mobile station in said further radio access network during connection setup, said radio access network configured to save said information about the encryption algorithms and to use said information about encryption algorithms in composing the integrity protected command message.

9. The apparatus as defined in claim **1**, wherein the radio access network is configured to send information about the encryption algorithms supported by the multimode mobile station in said further radio access network to a core network.

10. The apparatus as defined in claim **1**, wherein the radio access network is configured to receive a command message from a core network instructing the mobile station to cipher farther communications.

11. The apparatus as defined in claim **10**, wherein the radio access network is configured to send to said multimode mobile station said protected command message after receiving said command message from the core network.

12. The apparatus as defined in claim **1**, wherein said integrity protected command message instructs the multimode mobile station to cipher further communications.

13. An apparatus comprising:

a sender, of a multimode mobile station, configured to send to a first radio access network an unprotected signaling message including information about encryption algorithms supported by the multimode mobile station in a second radio access network,

a receiver configured to receive from the first radio access network an integrity protected command message including information relating to said encryption algorithms supported by the multimode mobile station in the second radio access network, said integrity protected command message comprising a payload and a message authentication code, and

wherein said mobile station is configured to conclude whether said information relating to said encryption algorithms in said integrity protected command message corresponds to said information about said encryption algorithms in said unprotected signaling message.

14. The apparatus as defined in claim **13**, wherein said payload comprises information about encryption algorithms, said multimode mobile station configured to compare information about the encryption algorithms received in said payload with stored information about said encryption algorithms supported by the multimode mobile station.

15. The apparatus as defined in claim **13**, wherein the multimode mobile station is configured to save the unprotected signaling message and to use the unprotected signaling message in an algorithm computing an expected message authentication code for the integrity protected command message.

16. The apparatus as defined in claim **13**, wherein the multimode mobile station is configured to save a payload of the unprotected signaling message and to use the payload of the unprotected signaling message in an algorithm computing an expected message authentication code for the integrity protected command message.

17. The apparatus as defined in claim **13**, wherein the multimode mobile station is configured to use information about the encryption algorithms supported by the multimode mobile station in said second radio access network together with information about an encryption algorithm for use with said first radio access network in computing an expected message authentication code for the integrity protected command message.

18. The apparatus as defined in claim **13**, wherein said integrity protected command message omits information about the encryption algorithms supported by the multimode mobile station in said second radio access network and information about the security capability of said multimode mobile station in said first radio access network.

19. The apparatus as defined in claim **13**, wherein said integrity protected command message comprises information about the encryption algorithms supported by the multimode mobile station in said second radio access network.

20. The apparatus as defined in claim **13**, wherein the multimode mobile station is configured to send said information about the encryption algorithms supported by the multimode mobile station in said second radio access network during connection setup.

21. The apparatus as defined in claim **13**, wherein said integrity protected command message instructs the multimode mobile station to cipher further communications.

22. A system, comprising:

a radio access network comprising a receiver configured to receive via a radio interface an unprotected signaling message including information about encryption algorithms supported by a multimode mobile station in a further radio access network, the further radio access network being different from the radio access network,

the radio access network being configured to compose an integrity protected command message including information relating to the encrypting algorithms supported by the multimode mobile station in said further radio access network, said integrity protected command message comprising a payload and a message authentication code, and

the radio access network also comprises a sender configured to send said integrity protected command message to said multimode mobile station; and a core network for receiving information about file encryption algorithms supported by the multimode mobile station in said further radio access network.

23. The system as defined claim **22**, comprising a further radio access network.

24. The system as defined claim **22**, comprising at least one multimode mobile station, configured to:

send to said radio access network an unprotected signaling message including information about encryption algorithms supported by the multimode mobile station in said further radio access network;

receive from the radio access network an integrity protected command message including information relating to said encryption algorithms supported by the multimode mobile station in the further radio access network, said integrity protected command message comprising a payload and a message authentication code; and

conclude whether said information relating to said encryption algorithms in said integrity protected command message corresponds to said information about said encryption algorithms in said unprotected signaling message.

25. A method comprising:

receiving from a multimode mobile station via a radio interface of a first radio access network an unprotected signaling message including information about encryption algorithms supported by the multimode mobile station in a second radio access network;

composing an integrity protected command message including information relating to the encrypting algorithms supported by the multimode mobile station in said second radio access network, said integrity protected command message including a payload and a message authentication code; and

sending said integrity protected command message to said multimode mobile station.

26. A method as defined in claim **25**, comprising sending information about the encryption algorithms supported by the multimode mobile station in said second radio access network to a core network.

27. A method as defined in claim **25**, comprising receiving a command message from the core network, said command message instructing the multimode mobile station to cipher further communication.

28. The method as defined in claim **27**, further comprising sending to said multimode mobile station said protected command message after receiving said command message from the core network.

29. A method as defined in claim **25**, comprising instructing the multimode mobile station to cipher further communications with said integrity protected command message.

30. The method in claim **25**, further comprising attaching information about the encryption algorithms supported by the multimode mobile station in said second radio access network received in said unprotected signaling message to said payload, and applying said payload in an algorithm computing said message authentication code.

31. The method as defined in claim **25**, further comprising saving the unprotected signaling message, and using the unprotected signaling message in an algorithm computing said message authentication code.

32. The method as defined in claim **25**, further comprising saving a payload of the unprotected signaling message, and using the payload of the unprotected signaling message in an algorithm computing said message authentication code.

33. The method as defined in claim **25**, further comprising saving information about the encryption algorithms supported by the multimode mobile station in said second radio access network, and using information about the encryption algorithms supported by the multimode mobile station in said second radio access network together with information about encryption algorithm embedded in a command message received from a core network in computing said message authentication code.

34. The method as defined in claim **25**, further comprising omitting information about the encryption algorithms supported by the multimode mobile station in said second radio access network and information about the security capability of said multimode mobile station in said first radio access network in the integrity protected command message.

35. The method as defined in claim **25**, further comprising including information about the encryption algorithms supported by the multimode mobile station in said second radio access network in the integrity protected command message.

36. The method as defined in claim **25**, further comprising receiving said information about the encryption algorithms supported by the multimode mobile station in said second radio access network during connection setup, saving said information about the encryption algorithms at said first radio access network, and using said information about encryption algorithms in composing the integrity protected command message.

37. An apparatus comprising:

receiving means for receiving via a radio interface an unprotected signaling message including information about encryption algorithms supported by a multimode mobile station in a further radio access network;

wherein a first radio access network is configured for composing an integrity protected command message including information relating to the encrypting algorithms supported by the multimode mobile station in said farther radio access network, said integrity protected command message comprising a payload and a message authentication code;

sending means for sending said integrity protected command message to said multimode mobile station; and

providing means for providing multimode mobile stations with access to at least one core network.

38. A method, comprising:

sending from a multimode mobile station to a first radio access network an unprotected signaling message including information about encryption algorithms supported by the multimode mobile station in a second radio access network;

receiving at the multimode mobile station from the first radio access network an integrity protected command message including information relating to the encrypting algorithms supported by the multimode mobile station in said second radio access network, said integrity protected command message comprising a payload and a message authentication code; and

concluding whether the information relating to the encryption algorithms in the integrity protected command message corresponds to the information about the encryption algorithms in the unprotected signaling message.

39. The method as defined in claim **38**, wherein said payload comprises information about encryption algorithms, and further comprising comparing at said multimode mobile station information about the encryption algorithms received in said payload with stored information about said encryption algorithms supported by file multimode mobile station.

40. The method as defined in claim **38**, further comprising saving the unprotected signaling message at said multimode mobile station, and using the unprotected signaling message in an algorithm computing an expected message authentication code for the integrity protected command message.

41. The method as defined in claim **38**, further comprising saving at the multimode mobile station a payload of the unprotected signaling message, and using the payload of the unprotected signaling message in an algorithm computing an expected message authentication code for the integrity protected command message.

42. The method as defined in claim **38**, farther comprising using information about the encryption algorithms supported by the multimode mobile station in said second radio access network together with information about an encryption algorithm for use with said first radio access network in computing an expected message authentication code for the integrity protected command message.

43. The method as defined in claim **38**, wherein said integrity protected command message omits information about the encryption algorithms supported by the multimode mobile station in said second radio access network and information about the security capability of said multimode mobile station in said first radio access network.

44. The method as defined in claim **38**, wherein said integrity protected command message comprises information about the encryption algorithms supported by the multimode mobile station in said second radio access network.

45. The method as defined in claim **38**, further comprising sending from the multimode mobile station said information about the encryption algorithms supported by the multimode mobile station in said second radio access network during connection setup.

46. The method as defined in claim **38**, wherein said integrity protected command message instructs the multimode mobile station to cipher further communications.

47. An apparatus, comprising:

sending means for sending from a multimode mobile station to a first radio access network an unprotected signaling message including information about encryption algorithms supported by the multimode mobile station in a second radio access network;

receiving means for receiving at the multimode mobile station from the first radio access network an integrity protected command message including information relating to the encrypting algorithms supported by the multimode mobile station in said second radio access network, said integrity protected command message comprising a payload and a message authentication code; and

wherein said mobile station is configured to conclude whether the information relating to the encryption algorithms in the integrity protected command message corresponds to the information about the encryption algorithms in the unprotected signaling message.

* * * * *