

EXHIBIT M

Skyhook Wireless, Inc. v. Google Inc.
Case No. 11-11571-RWZ

Redline showing changes in U.S. Patent No. 7,474,897 over U.S. Patent No. 7,414,988

Text present in both patents is black.

Text present in the '988 patent but not in the '897 patent is marked in **red**.

Text present in the '897 patent but not in the '988 patent is marked in **blue**.

US ~~7,414,988~~7,474,897

~~SERVER FOR UPDATING LOCATION BEACON DATABASE~~CONTINUOUS DATA OPTIMIZATION BY FILTERING AND POSITIONING SYSTEMS CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit under 35 U.S.C. §119 (e) ~~of U.S. Provisional Patent Application No. 60/623,108, filed on Oct. 29, 2004, entitled Wireless Data Scanning Network for Building Location Beacon Database, which is herein incorporated by reference in its entirety, to the following Provisional Patent Application the contents of which are incorporated herein in its entirety by reference:~~

U.S. Provisional Patent Application No. 60/654,811, filed on Feb. 22, 2005, entitled Continuous Data Optimization in Positioning System.

This application is a continuation-in-part of and claims the benefit under 35 U.S.C. §120 to the following application, the contents of which are incorporated herein in its entirety by reference:

U.S. patent application Ser. No. 11/261,988, filed on Oct. 28, 2005, entitled Location-Based Services that Choose Location Algorithms Based on Number of Detected Access Points Within Range of User Device.

This application is related to the following U.S. patent applications, filed on an even date herewith, entitled as follows:

U.S. patent application Ser. No. 11/359,154 Continuous Data Optimization of Moved Access Points In Positioning System; and

U.S. patent application Ser. No. 11/359,144 Continuous Data Optimization of New Access Points in Positioning Systems.

This application is related to the following U.S. Patent Applications, filed on **an even date herewith**Oct. 28, 2005, entitled as follows:

U.S. patent application Ser. No. ~~11/261,848~~, Filed on Oct. 28, 2005, entitled Location Beacon Database;

U.S. patent application Ser. No. 11/~~261,988, entitled Location Based Services that Choose Location Algorithms Based on Number of Detected Access Points Within Range of User Device~~261, 898, Filed on Oct. 28, 2005, entitled Server for Updating Location Beacon Database;
and

U.S. patent application Ser. No. 11/261,987, Filed on Oct. 28, 2005, entitled Method and System for Building a Location Beacon Database.

This application is related to U.S. Provisional Patent Application No. 60/658,481, filed on Mar. 4, 2005, entitled Encoding and Compressing the Access Point Database.

BACKGROUND

1. Field of the Invention

The invention is generally related to location-based services and, more specifically, to methods ~~and systems of determining locations of Wi-Fi access points and using such information to locate a Wi-Fi-enabled device~~of continuously optimizing or improving the quality of WiFi location data in such systems.

2. Discussion of Related Art

In recent years the number of mobile computing devices has increased dramatically creating the need for more advanced mobile and wireless services. Mobile email, walkie-talkie services, multiplayer gaming and call following are examples of how new applications are emerging on mobile devices. In addition, users are beginning to demand/ seek applications that not only utilize their current location but also share that location information with others. Parents wish to keep track of their children, supervisors need to track the location of the company's delivery vehicles, and a business traveler looks to find the nearest pharmacy to pick up a prescription. All of these examples require the individual to know their own current location or that of someone else. To date, we all rely on asking for directions, calling someone to ask their whereabouts or having workers check-in from time to time with their position.

Location-based services are an emerging area of mobile applications that leverages the ability of new devices to calculate their current geographic position and report that to a user or to a service. Some examples of these services include local weather, traffic updates, driving directions, child trackers, buddy finders and urban concierge services. These new location sensitive devices rely on a variety of technologies that all use the same general concept. Using radio signals coming from known reference points, these devices can mathematically calculate the user's position relative to these reference points. Each of these approaches has its strengths and weaknesses based on the radio technology and the positioning algorithms they employ.

The Global Positioning System (GPS) operated by the US Government leverages dozens of orbiting satellites as reference points. These satellites broadcast radio signals that are picked up by GPS receivers. The receivers measure the time it took for that signal to reach to the receiver. After receiving signals from three or more GPS satellites the receiver can triangulate its position on the globe. For the system to work effectively, the radio signals must reach the received with little or no interference. Weather, buildings or structures and foliage can cause interference

because the receivers require a clear line-of-sight to three or more satellites. Interference can also be caused by a phenomenon known as multipath. The radio signals from the satellites bounce off physical structures causing multiple signals from the same satellite to reach a receiver at different times. Since the receiver's calculation is based on the time the signal took to reach the receiver, multipath signals confuse the receiver and cause substantial errors.

Cell tower triangulation is another method used by wireless and cellular carriers to determine a user or device's location. The wireless network and the handheld device communicate with each other to share signal information that the network can use to calculate the location of the device. This approach was originally seen as a superior model to GPS since these signals do not require direct line of site and can penetrate buildings better. Unfortunately these approaches have proven to be suboptimal due to the heterogeneous nature of the cellular tower hardware along with the issues of multipath signals and the lack of uniformity in the positioning of cellular towers.

Assisted GPS is a newer model that combines both GPS and cellular tower techniques to produce a more accurate and reliable location calculation for mobile users. In this model, the wireless network attempts to help GPS improve its signal reception by transmitting information about the clock offsets of the GPS satellites and the general location of the user based on the location of the connected cell tower. These techniques can help GPS receivers deal with weaker signals that one experiences indoors and helps the receiver obtain a 'fix' on the closest satellites quicker providing a faster "first reading". These systems have been plagued by slow response times and poor accuracy greater than 100 meters in downtown areas.

There have been some more recent alternative models developed to try and address the known issues with GPS, A-GPS and cell tower positioning. One of them, known as TV-GPS, utilizes signals from television broadcast towers. (See, e.g., Muthukrishnan, Maria Lijding, Paul Havinga, Towards Smart Surroundings: Enabling Techniques and Technologies for Localization, Lecture Notes in Computer Science, Volume 3479, [January](#)[Jan](#) 2Hazas, M., Scott, J., Krumm, J.: Location-Aware Computing Comes of Age. IEEE Computer, 37(2):95-97, February 2004 005, Pa005, Pages 350-362.) The concept relies on the fact that most metropolitan areas have 3 or more TV broadcast towers. A proprietary hardware chip receives TV signals from these various towers and uses the known positions of these towers as reference points. The challenges facing this model are the cost of the new hardware receiver and the limitations of using such a small set of reference points. For example, if a user is outside the perimeter of towers, the system has a difficult time providing reasonable accuracy. The classic example is a user along the shoreline. Since there are no TV towers out in the ocean, there is no way to provide reference symmetry among the reference points resulting in a calculated positioning well inland of the user.

Microsoft Corporation and Intel Corporation (via a research group known as PlaceLab) have deployed a Wi-Fi Location system using the access point locations acquired from amateur scanners (known as "wardrivers") who submit their Wi-Fi scan data to public community web sites. (See, e.g., LaMarca, A., et. al., Place Lab: Device Positioning Using Radio Beacons in the Wild.) Examples include WiGLE, Wi-FiMaps.com, Netstumbler.com and NodeDB. Both Microsoft and Intel have developed their own client software that utilizes this public wardriving data as reference locations. Because individuals voluntarily supply the data the systems suffer a number of performance and reliability problems. First, the data across the databases are not contemporaneous; some of the data is new while other portions are 3-4 years old. The age of the

access point location is important since over time access points can be moved or taken offline. Second, the data is acquired using a variety of hardware and software configurations. Every 802.11 radio and antenna has different signal reception characteristics affecting the representation of the strength of the signal. Each scanning software implementation scans for Wi-Fi signals in different ways during different time intervals. Third, the user-supplied data suffers from arterial bias. Because the data is self-reported by individuals who are not following designed scanning routes, the data tends to aggregate around heavily traffic areas. Arterial bias causes a resulting location pull towards main arteries regardless of where the user is currently located causing substantial accuracy errors. Fourth, these databases include the calculated position of scanned access points rather than the raw scanning data obtained by the 802.11 hardware. Each of these databases calculates the access point location differently and each with a rudimentary weighted average formula. The result is that many access points are indicated as being located far from their actual locations including some access points being incorrectly indicated as if they were located in bodies of water.

There have been a number of commercial offerings of Wi-Fi location systems targeted at indoor positioning. (See, e.g., Kavitha Muthukrishnan, Maria Lijding, Paul Havinga, Towards Smart Surroundings: Enabling Techniques and Technologies for Localization, Lecture Notes in Computer Science, Volume 3479, Jan 2 Hazas, M., Scott, J., Krumm, J.: Location-Aware Computing Comes of Age. IEEE Computer, 37(2):95-97, February 2004 005, Pa005, Pages 350-362.) These systems are designed to address asset and people tracking within a controlled environment like a corporate campus, a hospital facility or a shipping yard. The classic example is having a system that can monitor the exact location of the crash cart within the hospital so that when there is a cardiac arrest the hospital staff doesn't waste time locating the device. The accuracy requirements for these use cases are very demanding typically calling for 1-3 meter accuracy. These systems use a variety of techniques to fine tune their accuracy including conducting detailed site surveys of every square foot of the campus to measure radio signal propagation. They also require a constant network connection so that the access point and the client radio can exchange synchronization information similar to how A-GPS works. While these systems are becoming more reliable for these indoor use cases, they are ineffective in any wide-area deployment. It is impossible to conduct the kind of detailed site survey required across an entire city and there is no way to rely on a constant communication channel with 802.11 access points across an entire metropolitan area to the extent required by these systems. Most importantly outdoor radio propagation is fundamentally different than indoor radio propagation rendering these indoor positioning algorithms almost useless in a wide-area scenario.

There are numerous 802.11 location scanning clients available that record the presence of 802.11 signals along with a GPS location reading. These software applications are operated manually and produce a log file of the readings. Examples of these applications are Netstumber, Kismet and Wi-FiFoFum. Some hobbyists use these applications to mark the locations of 802.11 access point signals they detect and share them with each other. The management of this data and the sharing of the information is all done manually. These application do not perform any calculation as to the physical location of the access point, they merely mark the location from which the access point was detected.

Performance and reliability of the underlying positioning system are the key drivers to the successful deployment of any location based service. Performance refers to the accuracy levels

that the system achieves for that given use case. Reliability refers to the percentage of time that the desired performance levels are achieved.

Performance Reliability

Local Search/Advertising <100 meters 85% of the time

E911 <150 meters 95% of the time

Turn-by-turn driving directions 10-20 meters 95% of the time

Gaming <50 meters 90% of the time

Friend finders <500 meters 80% of the time

Fleet management <10 meters 95% of the time

Indoor asset tracking <3 meters 95% of the time

SUMMARY

The invention provides ~~a location beacon database and server, method of building location beacon database, and location based service using same.~~ methods and systems of continuously optimizing data in WiFi positioning systems. For example, data is monitored to infer whether a WiFi access point has moved or is new. In this fashion, data is continuously optimized. Likewise, suspect data may be avoided when determining the position of the WiFi-enabled device using such a system.

~~Under another aspect of the invention, a Wi-Fi location server includes a database of Wi-Fi access points for at least one target area having a radius on the order of tens of miles, said database being recorded in a computer-readable medium and including database records for substantially all Wi-Fi access points in the target area, each record including identification information for a corresponding Wi-Fi access point and calculated position information for the corresponding Wi-Fi access point, wherein said calculated position information is obtained from recording multiple readings of the Wi-Fi access point to provide reference symmetry when calculating the position of the Wi-Fi access point and to avoid arterial bias in the calculated position information. The server also includes computer implemented logic to add records to the database for newly discovered Wi-Fi access points said computer logic including logic to recalculate position information for Wi-Fi access points previously stored in the database to utilize the position information for the newly discovered Wi-Fi access points.~~ one aspect of the invention, a location-based services system for WiFi-enabled devices calculates the position of WiFi-enabled devices. A WiFi-enabled device communicates with WiFi access points within range of the WiFi-enabled device so that observed WiFi access points identify themselves. A reference database is accessed to obtain information specifying a recorded location for each observed WiFi access point. The recorded location information for each of the observed WiFi access points is used in conjunction with predefined rules to determine whether an observed WiFi access point should be included or excluded from a set of WiFi access points. The recorded location information of only the WiFi access points included in the set are used and the recorded

location information of the excluded WiFi access points are excluded when calculating the geographical position of the WiFi-enabled device.

Under another aspect of the invention, ~~the server includes computer implemented clustering logic to identify position information based on error prone GPS information.~~ signal strength information for WiFi access points included in the set is recorded and the signal strength information is used when calculating the geographical position of the WiFi-enabled device.

Under another aspect of the invention, the predefined rules include rules to determine a reference point and to compare the recorded location information for each of the observed WiFi access points to the reference point, and wherein WiFi access points having a recorded location within a predefined threshold distance of the reference point are included in the set and wherein WiFi access points having a recorded location in excess of the predefined threshold distance of the reference point are excluded from the set.

Under another aspect of the invention, the ~~clustering logic includes logic to determine a weighted centroid position for all position information reported for an access point and logic to identify position information that exceeds a statistically based deviation threshold amount away from the centroid position and excludes such deviating position information from the database and from influencing the calculated positions of the Wi-Fi~~ reference point is determined by identifying a cluster of WiFi access points and determining an average position of the WiFi access points in the cluster.

BRIEF DESCRIPTION OF DRAWINGS

In the drawing,

FIG. 1 depicts certain embodiments of a Wi-Fi positioning system;

~~FIG. 2 depicts scanning vehicles including scanning devices according to certain embodiments of the invention;~~

~~FIG. 3 depicts an example of a scanning scenario to illustrate the problem of arterial bias in data collection;~~

~~FIG. 4 depicts an example using a programmatic route for a scanning vehicle according to certain embodiments of the invention;~~

~~FIG. 5 depicts an example scenario to illustrate the problem of lack of reference symmetry of Wi-Fi access points in locating a user device;~~

~~FIG. 6 depicts an example scenario to illustrate reference symmetry of Wi-Fi access points in locating a user device;~~

~~FIG. 7 depicts scanning vehicles including scanning devices according to certain embodiments of the invention;~~

~~FIG. 8 depicts a central network server including a central database of Wi-Fi access points according to certain embodiments of the invention;~~ FIG. 9 depicts an exemplary architecture of positioning software according to certain embodiments of the invention;

~~FIG. 10 depicts an exemplary architecture of a scanning client according to certain embodiments of the invention; and~~ 3 depicts the data transfer process in certain client device centric embodiments;

FIG. 4 depicts the data transfer process in certain network centric embodiments;

FIG. 5 depicts the data flows for the quality filtering and feedback process; and

~~FIG. 11 compares and contrasts the effects of a random scanning model with one using a model from the Chinese postman routing algorithm.~~ 6 depicts the operation of the Adaptive Filter in certain embodiments.

DETAILED DESCRIPTION

Preferred embodiments of the present invention provide a system and a methodology for ~~gathering reference~~ continuously maintaining and updating location data ~~to enable~~ in a ~~commercial~~ WiFi positioning system (WPS) using public and private 802.11 access points. Preferably, ~~the clients using location data is gathered in a programmatic way to fully explore and cover the streets of a target region. The programmatic approach identifies as many Wi-Fi access points as possible. By gathering location information about more access points, preferred embodiments not only provide a larger collection of location information about access points, but the location information for each access point may be calculated with more precision. Subsequently this larger set of more precise data may be used by location services to more precisely locate a user device utilizing preferred embodiments of the invention. Certain~~ embodiments gathered by the system use techniques to avoid erroneous data in determining the Wi-Fi positions and use newly-discovered position information to improve the quality of previously gathered and determined position information. Certain embodiments ~~use location-determination algorithms based on the context of the user device at the time the user requests a location. For example, the location-determination algorithm will be based on the number of Wi-Fi access points identified or detected when a location request is made, or based on the application making the request~~ communicate with the central location Access Point Reference Database to provide the location of newly discovered access points. Other embodiments notify the central location Access Point Reference Database of access points whose readings fall outside the bounds of what should be expected, based on previous readings of their location. Access points whose readings fall outside of what should be expected can be marked as suspect and filtered out of the triangulation formula so as not to introduce bad data into the location calculation.

Preferred embodiments of the invention build on techniques, systems and methods disclosed in earlier filed applications, including but not limited to U.S. patent application Ser. No. 11/261,988, filed on Oct. 28, 2005, entitled Location-Based Services that Choose Location Algorithms Based on Number of Detected Access Points Within Range of User Device, the contents of which are hereby incorporated by reference in its entirety. Those applications taught

specific ways to gather high quality location data for WiFi access points so that such data may be used in location based services to determine the geographic position of a WiFi-enabled device utilizing such services. In the present case, new techniques are disclosed for continuously monitoring and improving such data, for example by users detecting new access points in a target area or inferring that access points have moved. The present techniques, however, are not limited to systems and methods disclosed in the incorporated patent applications. Instead those applications disclose but one framework or context in which the present techniques may be implemented. Thus, while reference to such systems and applications may be helpful, it is not believed necessary to understand the present embodiments or inventions.

Under one embodiment of the invention, a WPS client device scans for access points to determine the physical location of the WPS client device, then it calculates the quality of the current access point locations in the Access Point Reference Database by comparing the observed readings against the recorded readings in the database. If the client determines that the observed readings fall outside the bounds of what should be expected based on the recorded readings, then the access point is marked as suspect. That suspect reading is logged into a feedback system for reporting back to the central location Access Point Reference Database.

Under another embodiment of the invention, a WPS client device filters identified suspect access points out of the triangulation calculation of the WPS client device in real time so as not to introduce bad data into the location calculation.

Under another embodiment of the invention, a WPS client device scans for access points to determine the physical location of the device and identifies access points that do not exist in the current Access Point Reference Database. After the known access points are used to calculate the device's current location, those newly found access points are recorded back to the central location Access Point Reference Database using the calculated location of the known access points to help determine their position, along with the observed power reading.

Under another embodiment of the invention, a device centric WPS client device periodically connects to the central location Access Point Reference Database to download the latest access point data. The WPS client device also uploads all feedback data about newly observed access points and suspect access points. This data is then fed into the central location Access Point Reference Database processing to recalibrate the overall system.

Under another embodiment of the invention, a network centric WPS client device directly records feedback data about newly observed access points and suspect access points into the central location Access Point Reference Database in real time.

By enlisting the WPS client device to continuously update the Access Point Reference Database with information on new and suspect access points, the WiFi positioning system provides higher quality data than a system scanned solely by the provider. Over time, WiFi access points are continually added and moved. Embodiments of the described invention provide systems and methods to ensure that the Access Point Reference Database is self-healing and self-expanding, providing optimal positioning data that continually reflects additions and changes to available access points. As more user client devices are deployed, the quality of the Access Point Reference Database improves because information in the database is updated more frequently.

FIG. 1 depicts a portion of a preferred embodiment of a Wi-Fi positioning system (WPS). The positioning system includes positioning software [103] that resides on a user-computing device [101]. Throughout a particular coverage area there are fixed wireless access points [102] that broadcast information using control/common channel broadcast signals. The client device monitors the broadcast signal or requests its transmission via a probe request. Each access point contains a unique hardware identifier known as a MAC address. The client positioning software receives signal beacons or probe responses from the 802.11 access points in range and calculates the geographic location of the computing device using characteristics from the signal beacons. ~~Those characteristics include the unique identifier of the 802.11 access point, known as the MAC address, and the strengths of the signal reaching the client device. The client software compares the observed 802.11 access points with those in its reference database [104] of access points, which may or may not reside on the device as well. The reference database contains the calculated geographic locations or power profile of all the access points the gathering system has collected. The power profile is a collection of readings that represent the power of the signal from various locations. Using these known locations, the client software calculates the relative position of the user device [101] and determines its geographic coordinates in the form of latitude and longitude readings. Those readings are then fed to location based applications such as friend finders, local search web sites, fleet management systems and E911 services~~received signal beacons or probe responses.

The positioning software is described in greater detail with reference to FIG. ~~9,2~~, which ~~depict~~depicts exemplary components of positioning software 103. Typically, in the user device embodiment of FIG. 1 there is an application or service [~~901~~201] that utilizes location readings to provide some value to an end user (for example, driving directions). This location application makes a request of the positioning software for the location of the device at that particular moment. ~~That~~The location application can be initiated continuously every elapsed period of time (every 1 second for example) or one time on demand by another application or user.

In FIG. 2, the location application makes a request of the positioning software to interrogate all access points within range at a particular moment and to determine which access points are suspect because the observed data does not correspond to the calculated location in the Reference Database. The information on suspect access points collected by the location application is used to optimize the position information in the Access Point Reference Database either in real time or at some later time.

In the embodiment depicted in FIG. 2, the location application or service request initiates the scanner [~~902~~202], which makes a “scan request” to the 802.11 radio [~~903~~203] on the device. The 802.11 radio sends out a probe request to all 802.11 access points [~~904~~204] within range. According to the 802.11 protocol, those access points in receipt of a probe request will transmit a broadcast beacon containing information about the access point. That beacon includes the MAC address of the device, the network name, the precise version of the protocol that it supports and its security configuration along with information about how to connect to the device. The 802.11 radio collects this information from each access point that responds, calculates the received signal strength (“RSS”) of each access point observed, and sends ~~that~~the identification and RSS information back to the scanner.

The scanner passes this array of access points to the Locator [906206] which checks the MAC addresses of each observed access point against the Access Point Reference Database [905205]. This database can either be located on the device or remotely over a network connection. The Access Point Reference Database ~~returns the location data for each of the observed access points that are known to the system~~ contains the raw 802.11 scanning data plus the calculated location for each access point that is known to the system. FIG. 5 describes the access point evaluation process in more detail. The list of observed access points [501] is obtained from the Scanner and the Locator [206] searches for each access point in the Access Point Reference Database. For each access point found in the Access Point Reference Database the recorded location is retrieved [502]. The Locator passes this collection of location information for known access points [502] along with the signal characteristics returned from each access point to the Bad DataQuality Filter [907207]. This filter applies a number of comparison tests against each access point to determine ~~determines~~ if any of the access points have moved since they were added to the access point database Access Point Reference Database and works continually to improve the overall system. The Quality Filter marks access points that fail the quality algorithm as “suspect” [504]. After removing bad data records, the Filter sends the remaining access points to the Location Calculation component [908208]. Using the set of validated reference data from the access point database Access Point Reference Database and the signal strength readings from the Scanner, the Location Calculation component computes the location of the device at that moment. The Location Calculation component also calculates the position of any newly observed access points [503] not found in the Access Point Reference Database. The raw scanning data and the location of new access points are stored in the Feedback File [212] as can be seen in FIG. 2. This feedback is either saved locally on the device for later transmission to the server or sent to the server in real time. ~~Before that~~ location data for known access points is sent back to the Locator, it is processed by the Smoothing engine [909209] which averages a past series of location readings to remove any erratic readings from the previous calculation. The adjusted location data is then sent back to the Locator.

The calculated location readings produced by the Locator are communicated to these location-based applications [904201] through the Application Interface [910210] which includes an application programming interface (API) or via a virtual GPS capability [911211]. GPS receivers communicate their location readings using proprietary messages or using the location standard like the one developed by the National Marine Electronics Association (NMEA). Connecting into the device using a standard interface such as a COM port on the machine retrieves the messages. Certain embodiments of the invention include a virtual GPS capability that allows any GPS compatible application to communicate with this new positioning system without have to alter the communication model or messages.

The location calculations are produced using a series of positioning algorithms intended to turn noisy data flows into reliable and steady location readings. The client software compares the list of observed access points along with their calculated signal strengths to weight the location of user to determine precise location of the device user. A variety of techniques are employed including simple signal strength weighted average models, nearest neighbor models combined with triangulation techniques and adaptive smoothing based on device velocity. Different algorithms perform better under different scenarios and tend to be used together in hybrid deployments to product the most accurate final readings. Preferred embodiments of the invention can use a number of positioning algorithms. The decision of which algorithm to use is driven by

the number of access points observed and the user case application using it. The filtering models differ from traditional positioning systems since traditional systems rely on known reference points that never move. In the model of preferred embodiments, this assumption of fixed locations of access points is not made; the access points are not owned by the positioning system so they may move or be taken offline. The filtering techniques assume that some access points may no longer be located in the same place and could cause a bad location calculation. So the filtering algorithms attempt to isolate the access points that have moved since their position was recorded. The filters are dynamic and change based on the number of access points observed at that moment. The smoothing algorithms include simple position averaging as well as advanced ~~bayesian~~[Bayesian](#) logic including ~~Kalman~~[particle](#) filters. The velocity algorithms calculate device speed by estimating the Doppler effect from the signal strength observations of each access point.

~~Gathering of Scan Data to Build Reference Database~~

~~FIG. 2 depicts the components used to gather location information for the various access points. A large fleet of vehicles [201] is deployed to build the reference database (104 of FIG. 1) for the positioning system. These vehicles 201 follow a programmatic route through target scan areas to gather data in the most optimal fashion producing the highest quality data. The target scan areas typically represent a large metropolitan area including every single drivable street in 15-20 mile radius. These vehicles are equipped with scanning devices [202] designed to record the locations and characteristics of 802.11 signals while traversing the coverage area. The scanning devices track the location of the scanning vehicle every second using signal from GPS satellites [204]. The scanning device also tracks the presence of any 802.11 access point within range and records the radio characteristics of that access point signal along with the GPS location of the scanning vehicle. The quality of the data collected is greatly affected by the scanning methodology employed by the scanning vehicles. Each model has its own benefits and limitations. One approach, known as the Random Model, places scanning devices in vehicles as they are conducting daily activities for business or personal use. These vehicles could be delivery trucks, taxi cabs, traveling salesman or just hobbyists. The concept is that over time these vehicles will cover enough streets in their own random fashion in order to build a reliable reference database. The model does in fact provide a simple means to collect data but the quality of the resulting data is negatively affected due to issues of "arterial bias". FIG. 3 describes the challenge of the random model. When scanning vehicles traverse routes designed to solve other problems than gathering data (e.g. delivering packages, people commuting to and from work) they tend to follow destination routes. A destination route is when a driver needs to get from A to B and seeks the fastest route to get there. So the driver looks for the shortest route to the nearest main artery whether it be a highway or a main thoroughfare. As a result, over time the random driving covers more and more ground by the cumulative coverage shows a bias to the main roads, or arteries at the expense of the smaller and surrounding roads. In FIG. 3, arteries [304] and [305] are heavily traversed by the scanning vehicles resulting in a healthy amount of scanning data for those streets. But streets [306] and [307] are rarely, if ever, covered because there is no frequent destination on those streets and the arteries are more optimal travel roads. The result is that access points [308] and [309] are not scanned at all by the scanning vehicles so the positioning system will struggle to identify a user who is traveling on streets [306] and [307]. The result is that when the system attempts to calculate the location of the access point from the scan data it is limited to a biased collection of input data. FIG. 11 shows the difference in resulting data quality.~~

~~As the scanning vehicle drives near the Access Point [1101], it records a reading and its location continuously. The positioning system must then calculate the location of the Access Point [1102] using the entire set of observed data [1103]. In the Random Scanning model the set of data is limited to one main road passing by the access point. That forces the system to calculate the access point's location near that road rather than close to the access point itself.~~

~~Another approach is develop routing algorithms that include every single street in the target area so as to avoid arterial bias in the resulting collection of data thus producing a more reliable positioning system for the end users. FIG. 4 describes an optimized routing algorithm known as the Chinese Postman to calculate the most efficient driving route for covering every single street in a target area. The Chinese Postman routing algorithm is a known technique used by postal agencies, utilities and census agencies and is a variant of the Eulerian cycle problem. The Eulerian cycle is a problem asking for the shortest tour of a graph which visits each edge at least once. (See, e.g., Kwan, M. K. "Graphic Programming Using Odd or Even Points." Chinese Math. 1, 273-277, 1962.) Preferred embodiments of the invention include a methodology for identifying a target region for coverage and then using the Chinese Postman routing algorithm for planning the vehicle route. The scanning vehicle [401] follows the optimal route according to the algorithm showing no bias to any street ensuring that all observable access points are detected and mapped by the system. So, by way of example, access points [408] and [409] are added to the access point database using the Chinese Postman model but would have been missed using the Random model. Referring back to FIG. 11, with the Chinese Postman Scanning model, the vehicle travels every single road getting as complete a set of scanning records [1106] for the Access Point [1104]. The system can then calculate the location [1105] of the access point with less error since it has a more uniform distribution of scan data for access point 1104 than for access 1102. So the Chinese Postman Scanning model not only gathers more access points uniformly across a target area but the resulting data produces more accurate calculations of access point locations.~~

~~Higher Quality AP Locations~~

~~Once collected (or partially collected), the scanning data is uploaded back to a central access point database (described later in this application) where it is processed. The raw observation points for each access point are used to reverse triangulate the actual physical location of the access points or create a power profile representing the radio propagation of that access point. In order to produce the most accurate calculated location for a particular access points or to create the most accurate power profile, the scanning vehicle must observe the access point from as many different angles as possible. In the random model [FIG. 3], many access points are observed from only one street forcing the system to calculate their location directly on the street [303]. These locations exhibit a directional bias and are significantly different than the actual locations of these access points [302]. Errors are introduced into a positioning system when its reference point locations are inaccurate. So in this positioning system, the accuracy of the access point locations play a large role in the accuracy of the end user positioning accuracy. Using the Chinese Postman model [FIG. 4] the scanning vehicles detect a particular access point from as many sides as possible of the building housing the access point. This additional data greatly improves the results of the reverse triangulation formula used to calculate the location of the access points [403]. More details on the access point location quality is described in connection with FIG. 11.~~

The scanning data collected from this system represents a reliable proxy for the signal propagation pattern for each access point in its specific environment. Every radio device and associated surrounding environment produces a unique signal fingerprint showing how far the signal reaches and how strong the signal is in various locations within the signal fingerprint. This fingerprint data is used in conjunction with the calculated access point location to drive high accuracy for the positioning system. This fingerprint is also known as a “power profile” since the signal strengths at each position is measured as signal power in watts. The positioning system can interpret the fingerprint data to indicate that a particular signal strength of an 802.11 access point radio is associated with a particular distance from that access point. Signal fingerprinting techniques are used in indoor Wi-Fi positioning but have proved difficult to replicate in the wider area outdoor environments because the difficulty associated with collecting the fingerprint data. When the fingerprints or power profiles of multiple access points are overlaid, the positioning system can determine a device location merely by finding the one position where the observed signal strengths match the combined fingerprints. Preferred embodiments of this invention provide a reliable system for obtaining this fingerprint data across a massive coverage area with millions of access points in order to utilize fingerprint based positioning algorithms.

Reference Symmetry

Positioning systems typically work by having three or more reference points around the device being tracked. These positioning systems use the radio signals from these reference points in various ways to calculate the device’s current location. Significant errors occur when there are an insufficient number of reference points or when the reference points lack balance or symmetry around the user. As illustrated in FIG. 5, the arterial bias that emerges from the random model introduces many scenarios where the end user [501] moves into physical areas in which there are only recorded access point locations [502] on one side of them. This lack of symmetry in the distribution of reference points around the end user causes the positioning algorithms to calculate the device location [503] with a great deal of error. With Chinese Postman model of scanning for access points, the user typically encounters a physical location [FIG. 6] in which there are numerous access point locations [602] on all sides of the user [601] within the range [604] of the device’s 802.11 radio. The resulting position calculation [603] has reduced location bias and is more accurate as a result. FIG. 11 is another example showing the impact of quality location calculations.

Scanning Device

FIG. 7 depicts the details of a preferred embodiment of a scanning device 702 used to detect and identify the various Wi-Fi access points. A scanning vehicle [701] contains a scanning device [702] that continuously scans the airways for radio signals from GPS satellites [708] and 802.11 access points [707]. The scanning device runs the scanning client software [704] that controls the entire process. The scanning client activates both the GPS receiver [705] and the 802.11 radio [706]. The GPS receiver is set into a continuous reception mode calculating the geographic location of the device every second. That calculation is read by the scanning client and stored in the local data storage [703]. The scanning client initiates the 802.11 radio and begins sending out 802.11 probe requests using directional antennas [709]. Any 802.11 access point [707] within range of that probe request responds with a signal beacon as per the 802.11 protocol. The responding signal beacons contains the network name of the access point (known as an SSID);

~~the MAC address of the access point device as well as other meta information about the access point. The responding signals reach each of the directional antennas with a different strength of signal based on the vector of origin and the proximity of the access point. That vector is recorded along with the identifier of that particular antenna and the meta information about the access point. This probe receive record process occurs continuously every tenth of a second. The scanning device deployed is a combination of the iPAQ 4155 Pocket PC and Powered GPS PDA Mount Cradle with integrated SiRF II type GPS receiver with XTrac v. 2.0 firmware.~~

~~The Scanning Client 704 of certain embodiments is described in connection with FIG. 10. The client consist of three main components, the Data Manager [1001], the System Manager [1002] and the Upload Manager [1003]. The Data Manager [1001] controls the operations of both the GPS radio [1006] and the 802.11 radio [1007]. The Data Manager controls when and how often these radios scan for signals and process those signals. The GPS radio once activated receives signals from GPS satellites [1004] and calculates its geographic location. The GPS recorder [1008] logs all of those readings every second and sends them to the File Manager [1010]. The Wi-Fi Recorder [1009] activates the 802.11 Radio to scan every tenth of a second, and associates those 802.11 readings with the GPS readings coming from the GPS radio and sends the resulting data to the File Manager. The File Manager receives scan data from both the GPS Recorder and Wi-Fi Recorder and creates storage files on the device. This process continues the entire time the device is operational and both radios are functioning.~~

~~In the Upload Manager [1003] there is a Hotspot Detector [1017] that monitors the 802.11 scanning results to look for the configured network of public hotspots [1024] (e.g. T mobile) that the device is authorized to access. Once it detects a valid Hotspot it notifies the user of its presence. The user can select to connect to the hotspot by activating the Create Connection component [1018]. This component associates with the hotspot's access point and creates an 802.11 connection. Then the Hotspot Authentication module [1019] supplies valid authentication information for the device. The hotspot validates the account and then provides network access to the device. The Upload Manager then initiates the Upload Server Authentication process [1020] to connect to the Central Network Server [1025] and provides valid authentication information. Once authenticated, the Upload & Data Verification module [1021] is initiated. This module retrieves the scan data from the Scanning Data store [1011] and uploads the data to the Central Network Server using FTP. The Central Network Server initiates a process to store all the data in the Central Access Point Database. After the upload is complete the upload process moves the scan data from the Scanning Data store [1011] to the Backup Data store [1012] on the device. Once the upload is completed and verified, the New Version module [1022] checks the Central Network Server to determine if there is a new version of the client software available for the device. If there is a new version, the software is downloaded and the New Version Installation [1023] process begins to upgrade the client software. Once the installation process is completed the connection with the Central Network Server is terminated, the connection with the hotspot is terminated and the device returns to normal scanning operation.~~

~~Included in the Scanning Client 704 are a set of utilities that help to manage the device and reduce system errors. The Radio Manager [1013] monitors the operation of the GPS Radio and the Wi-Fi Radio to make sure they are functioning properly. If the Radio Manager encounters a problem with one of the radios, it will restart the radio. The User Interface Controller [1014] presents the tools and updates to the user so they can operate the device effectively. The Error~~

~~Handling and Logging [1015] records all system issues to the device and alerts the user so they can address. The System Restart module [1016] is called when issues cannot be resolved. This module shuts down the device and restarts the hardware, operating system and scanning client to ensure proper operation.~~

~~The 1/10 of a second 802.11 scanning interval was chosen since it provides the optimal scanning period for 802.11 under these conditions using off the shelf hardware. 802.11b/g/n operates using 14 channels of the unlicensed spectrum. An individual access point broadcasts its signal beacon over one of those channels at any given time. The scanning device needs to survey each channel in order to observe as many access points as possible. The scanning interval is correlated with the average speed of the scanning vehicle to optimize how the scanning client covers the frequency real estate of a particular region.~~

Optimizing the Quality of Current Access Point Data

The Quality Filter [207] component compares the data from the observed access points against the known access points in a local or remote Access Point Reference Database. For those observed access points whose MAC address is located in the Access Point Reference Database, the Quality Filter component then compares the information observed with the location of the access points stored in the database.

The Quality Filter's [207] high level functionality is to remove suspect access points from location calculation and as the result, increase the accuracy of location estimation. The Quality Filter uses only access points that are located in the Access Point Reference Database. In some cases the Quality Filter will have no current client device location history to utilize for quality determination. The process for identifying suspect access points for a no-history location estimation is based on the location of the biggest cluster of the access points stored in the database. The location of all the observed access points that are recorded in the Access Point Reference Database is considered and the average location of the biggest cluster of access points is used as the reference point. A cluster refers to distance-based clustering, which is a group of access points with the distance of each access point from at least one more access point in the cluster less than a threshold. The clustering algorithm is shown as follows and it is read as "Node n belongs to cluster K , if there is at least one element in cluster K like n_i , which its distance from n is less than the threshold":

[FORMULA OMITTED]

If no cluster can be found then the mathematical median of the access points serves as the best estimate of the distance average of a majority of the access points.

If the distance of any individual access point to the reference point is calculated to be more than a given distance, it is ruled as a suspect access point and recorded in the Feedback File to be sent back to the Access Point Reference Database. Those suspect access points are then removed from the list of access points used to calculate the location of the user device.

Identifying suspect access points for a client device when there is a history of user movement is based on the previous location of the client device. An exemplary implementation of this determination is shown in FIG. 6. In an embodiment where there is location history, the client

device location calculation is calculated continuously every period of time, usually once every second. If the distance of any individual observed access point [602] to that historical reference point (the prior location calculation) is more than a given distance [603], then it is ruled as a suspect access point, added to the Feedback File and removed from calculation. The intent of this filter is to try and use the access points that are nearest to the user/device [601] to provide the highest potential accuracy. This filter is called an adaptive filter since the threshold distance to filter suspect access points is changed dynamically. The threshold distance, which is used to identify suspect access points, is changed dynamically based on the number of access points that are considered of good quality to calculate location of the client device. Therefore, the adaptive filter contains two factors, 1) the minimum number of required access points to locate a user device and 2) the minimum threshold of distance to identify suspect access points. The adaptive filter starts with the minimum threshold of distance. If number of access points within that distance is above the minimum number of access points necessary to calculate the client location, then location of the device is calculated. For example, if we find five access points which are within 20 meters of the prior reading, then we filter out all observed access points greater than 20 meters. If the filter criteria is not met then the adaptive filter threshold [603] of the distance is increased until the minimum number of access points is considered or the maximum acceptable distance is reached, and then the access points within the threshold distance are used to locate the user device. If no access point can be located within the maximum threshold of distance [604] from the previous location, then no location is calculated.

The positioning software continues to attempt to locate the device based on its previous location up to a maximum given duration of time. During this timeout period, if no location can be determined, the maximum threshold of distance is adjusted using the calculated velocity of the device. If the vehicle is known to accelerate at a maximum of 6 m/s/s and it was previously calculated as traveling at 20 mph, then it would not possible be more than 42 meters away from the last location two seconds later. This 42 meter distance limit is used to adjust the outer boundary of the distance threshold if the earlier time period adapter filters did not work. If it is too difficult to calculate the actual velocity of client device, then a maximum velocity threshold is used. If any access point is calculated to be more than the maximum threshold of distance away from the reference point, it is marked as “suspect” and logged to the Feedback File. If no access point can be located within the maximum threshold of the distance during the timeout period, then the adaptive filter ignores the history and treats the next instance of location determination as a no-history case and returns back to the clustering filter described previously.

Real-Time Filtering of Suspect Access Points

Suspect access points are removed from the inputs into the triangulation calculation and only valid access point locations are used to triangulate the device position [502]. The inputs to the triangulation algorithm are the set of valid access points returned from the Quality Filter [207]. The triangulation component reads in the list of valid observed access point locations along with their respective signal strengths and calculates a latitude and longitude along with a Horizontal Position Error (an estimate of the accuracy error at that moment). The triangulation process also takes into consideration prior positions to add additional filters to the scanning in order to apply a smoothing process. By filtering out suspect access points we provide the triangulation algorithm a more reliable set of reference points to calculate against. Since access points can move at any time, Positioning Software must account for the dynamic nature of the reference points. Without

conducting filtering, the calculated location could result in a position hundreds or thousands of miles away.

Suspect access points are not discarded completely. Rather their newly observed locations are added back to the database via the Feedback File [212] with different attributes indicating it as suspect, allowing the server to determine whether to move the official location of that access point or just keep it on hold until its new location can be verified. By keeping it on hold, this access point will not corrupt any other user's location calculation.

Adding New Access Point Data

Observed access points found in the Access Point Reference Database of known access points are used to calculate the location of the client device after the elimination of suspect access points. Observed access points whose MAC address are not found in the Access Point Reference Database represent new access points [302][503] added since the database was created or updated. Those observed access points not found in the known Access Point Reference Database are added to the Feedback File as new access points. Those newly found access points are marked with the location of the client device calculated by the positioning system itself along with the observed signal strengths. This situation can occur in a number of scenarios. In many cases a new access point is purchased and deployed in the vicinity since the last physical scanning by the scanning fleet. This is most often the case due to the rapid expansion of Wi-Fi. In other cases, an access point may be situated deep in the center of a building and the scanning fleet was unable to detect that access point from the street. Another example is that an access point may be located up on a high floor of a tall building. These access points may be difficult to detect from down on the street where the scanning fleet operates, but may be received by client devices that pass closer to the building by users on foot or that enter the building itself

By having the system "self-expand" in this manner, the coverage area of the system slowly expands deep into buildings and upwards in tall buildings. It also leverages the large number of new access points that are deployed every day across the world.

Updating the Central Network Database Server

~~With reference to FIG. 8, the fleet of vehicles perform their scanning routines while driving their pre-designed routes. Periodically each vehicle [801] will connect to an available 802.11 access point and authenticate with the Data Communications Module [807] of the Central Network Server. Typically the access points used for communicating with the Central Network Server are public hotspots like those operated by T-Mobile ensuring reliable and metered access. The provisioning of this connection could be done via any available public access point. The scanning vehicle stops at a nearby hotspot location and begins the process of connecting to the access point. Once authenticated, the scanning client [704] identifies all the recently collected scan data from the local storage [703] and uploads that data to the Central Network Database [802]-3, in some embodiments the Access Point Reference Database of known access points will be located on a central network server remote from the client device. The provisioning of this connection could be done via any available network connection and is managed by the Data Exchange Component [303]. Once authenticated, the client device [103] identifies all the suspect~~

and new access point data from the local storage Feedback Files [212] and uploads that data to the Access Point Reference Database [205].

~~Once the data has been uploaded to the database, the Parser and Filter process [803] begins. The Parser and Filter process reads all of the upload scanning data and loads it up into the appropriate tables of the database. During this exercise the data is evaluated for quality issues. In some cases the GPS receiver may record erroneous or error records for some period of time, which could negatively affect the final access point location calculation. The parser and filter process identifies these bad records and either corrects them or removes them from the system. The filtering process uses clustering techniques to weed out error prone GPS readings. For example, if 90% of the readings are within 200 meters of each other but the remaining 10% of the readings are 5 kilometers away then those outliers are removed by the filter and stored in a corrupted table of the database for further analysis. In particular, the system first calculates the weighted centroid for the access point using all reported data. It then determines the standard deviation based on the distribution of the reported locations. The system uses a definable threshold based on the sigma of this distribution to filter out access points that are in error. Once these error records are marked, the centroid is recalculated with the remaining location records to determine the final centroid using the Reverse Triangulation method described below.~~

~~Note that the error records may be the result of an access point that has moved. In this instance, the centroid for the access points will quickly “snap” to the new location based on the preponderance of records. An additional enhancement to the algorithm would include a weighting value based on the age of the records such that new records represent a more significant indication of the present location for a given access point.~~

~~Once the parsing process has been completed the central network system initiates the Reverse Triangulation model [804] begins processing the new data. During this process 1) new access points are added to the database and their physical location is calculated and 2) existing access points are repositioned based on any new data recorded by the scanners. The reverse triangulation algorithm factors in the number of records and their associated signal strengths to weight stronger signal readings more than weaker signals with a quasi-weighted average model.~~

~~During data gathering, a WPS user is equipped with a Wi-Fi receiver device which measures Received Signal Strength (RSS) from all the available Wi-Fi access points, and then extracts location information of corresponding access points. RSS value of access points are shown as follows:~~

~~[FORMULA OMITTED]~~

~~If the corresponding recorded GPS location of access point i is denoted by $[Lat, Long]$, and the calculated access point location is denoted by $[Lat, Long]$, the triangulated position is found by applying the algorithm as follows:~~

~~[FORMULA OMITTED]~~

~~The quad root of power is selected to ease the implementation of the algorithm, since quad root is synonymous to taking two square roots.~~

~~The second point is referring to adjusting the dynamic range of coefficients. If the dynamic range of coefficients is a concern, the coefficient of the algorithm can be divided by a constant number, e.g.~~

~~[FORMULA OMITTED]~~

~~The Parameter C can be any number and it does not impact the results, theoretically. Since, the weighted average is based on the ratio of the coefficients and not the absolute value, theoretically, dividing all the coefficients by a constant value, C, does not impact the results, but it changes the dynamic range of the coefficient values.~~

~~This final [Lat, Long], is then used as the final centroid value for the location of that access point. The latitude and longitude will then be stored in the database including a timestamp to indicate the freshness of the triangulation calculation.~~

~~After the Central Network Database has been updated and each access point has been repositioned, the Data Pack Builder [805] creates subsets of the database based on regions of the country or world. The pack builder facilitates distribution of the database for a variety of use cases in which only region certain geographies are of interest. The pack builder is configured with region coordinates representing countries, time zones and metropolitan areas. Utilizing this technique a user can download just the location data for the west coast of the United States. The pack builder segments the data records and then compresses them.~~

In other embodiments the client device is connected to the Access Point Reference Database all the time using a network connection. FIG. 4 describes how the Network Centric embodiment works. Rather than store the reference data locally, the Locator [201] uses a set of Real-Time Network interfaces [401] to communicate with the Access Point Reference Database. The Locator sends the list of observed access points to the network interface which returns the list of observed access points and whether the database has recorded locations or whether the access points are newly found. The process continues as before with the Quality Filter marking suspect access points but the list of suspect access points is sent to the Access Point Reference Database in real-time. After the Calculation module determines the user device's location, the list of newly found access points is marked with the current location and sent back to the database in real-time. This allows the database to be up to date at all times and to remove the need for a Data Exchange Component.

After receiving feedback data, in either the device centric or the network centric model, the Access Point Reference Database determines whether to place suspect access points 'on hold' so as to prevent them from corrupting another user device's location request. There are a number of techniques being explored to optimize how this feedback data of suspect access points will be used to improve the overall quality of the database. There may be a voting scheme by which access points are moved to new positions if more than one user locates the access point in its new location. If only one user has marked the access point as suspect then the access point is marked as a low quality reading in its new position. Once its new position is validated by another user then the quality attribute of the access point is increased to reflect the higher level of confidence the system has in the new position. The more people who corroborate the access point's new

position the higher the quality level. The system's client software then favors access points with high quality ratings over those that have lower quality ratings.

~~The Fleet Management Module [806] helps operations personnel manage the scanning vehicles and ensure they are adhering the routing procedures. This module processes all the scan data and builds the location track for each vehicle in the system. The operations manager can create maps of the vehicle track using the Map Builder [808] to visually inspect the coverage for a particular region. The GPS tracking data from each device is reviewed with route mapping software to verify completion of coverage and to identify missed areas. This ability to audit and verify uniform coverage ensures that the system is getting the best data possible. The module also calculates the driving time of the vehicle to determine average speed and to subtract any idle time. These outputs are used to monitor efficiency of the overall system and in planning of future coverage.~~
In either the device centric or the network centric model, the Access Point Reference Database collects the access point identifying information, client device location and access point signal strength information of newly discovered access points from client devices. Once an acceptable number of readings of newly discovered access points is collected by the Access Point Reference Database, it can calculate a location for the new access points based on the systems and methods described in the related applications. The newly discovered access points can then be supplied to client devices for use in their location calculation.

It will be appreciated that the scope of the present invention is not limited to the above described embodiments, but rather is defined by the appended claims; and that these claims will encompass modifications of and improvements to what has been described.

What is claimed is:

1. ~~A Wi-Fi location server.~~In a location-based services system for WiFi-enabled devices, a method of calculating the position of WiFi-enabled devices comprising the acts of:

~~a database of Wi-Fi access points for at least one target area having a radius on the order of tens of miles, said database being recorded in a computer-readable medium and including database records for substantially all Wi-Fi access points in the target area, each record including identification information for a corresponding Wi-Fi access point and calculated position information for the corresponding Wi-Fi access point, wherein said calculated position information is obtained from recording multiple readings of the Wi-Fi access point at different locations around the Wi-Fi access point so that the multiple readings have reference symmetry relative to other Wi-Fi access points in the target area and so that the calculation of the position of the Wi-Fi access point avoids arterial bias in the calculated position information; and computer-implemented logic to add records to the database for newly discovered Wi-Fi access points said computer logic including logic to recalculate position information for Wi-Fi access points previously stored in the database to utilize position information for the newly discovered readings of previously stored Wi-Fi access points.)~~
a WiFi-enabled device communicating with WiFi access points within range of the WiFi-enabled device so that observed WiFi access points identify themselves;

b) accessing a reference database to obtain information specifying a recorded location for each observed WiFi access point;

c) using the recorded location information for each of the observed WiFi access points in conjunction with pre-defined rules to determine whether an observed WiFi access point should be included or excluded from a set of WiFi access points;

d) using the recorded location information of only the WiFi access points included in the set and omitting the recorded location information of the excluded WiFi access points to calculate the geographical position of the WiFi-enabled device.

2. The ~~server~~method of claim 1 further including ~~computer implemented clustering logic to identify position information based on error-prone GPS information~~recording signal strength information for WiFi access points included in the set and using the signal strength information when calculating the geographical position of the WiFi-enabled device.

3. The ~~server of claim 2 wherein the clustering logic includes logic to determine a weighted centroid position for all position information reported for an access point and logic to identify position information that exceeds a statistically based deviation threshold amount away from the centroid position and excludes such deviating position information from the database and from influencing the calculated positions of the Wi-Fi access points.~~method of claim 1 wherein the predefined rules include rules to determine a reference point and to compare the recorded location information for each of the observed WiFi access points to the reference point, and wherein WiFi access points having a recorded location within a predefined threshold distance of the reference point are included in these and wherein WiFi access points having a recorded location in excess of the predefined threshold distance of the reference point are excluded from the set.

4. The method of claim 3 wherein the reference point is determined by identifying a cluster of WiFi access points and determining an average position of the WiFi access points in the cluster.

* * * * *