(51) **International Patent Classification:** Not classified

(21) **International Application Number:**
PCT/US2005/006608

(22) **International Filing Date:** 28 February 2005 (28.02.2005)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
10/802,366   16 March 2004 (16.03.2004)   US

(71) **Applicant** *(for all designated States except US)*: AIRESPACE, INC. [US/US]; 110 Nortech Parkway, San Jose, CA 95134 (US).

(72) **Inventors: DIETRICH, Paul, F.**; 6258 Palatine Ave. North, Seattle, WA 98103 (US). **DAVI, Gregg, Scott**; 647 Martil Way, Milpitas, CA 95035 (US). **FRIDAY, Robert,**

J.; 16081 Redwood Lodge Road, Los Gatos, CA 95033 (US).

(74) **Agent: SPOLYAR, Mark, J.**; Law Office of Mark J. Spolyar, 38 Fountain Street, San Francisco, CA 94114 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

(54) **Title:** LOCATION OF WIRELESS NODES USING SIGNAL STRENGTH WEIGHTING METRIC
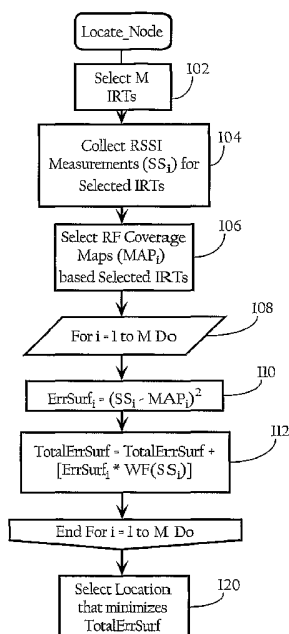
(57) **Abstract:** Methods, apparatuses, and systems directed to a wireless node location mechanism that uses a signal strength weighting metric to improve the accuracy of estimating the location of a wireless node based on signals detected among a plurality of radio transceivers. In certain implementations, the wireless node location mechanism further incorporates a differential signal strength metric to reduce the errors caused by variations in wireless node transmit power, errors in signal strength detection, and/or direction-dependent path loss. As opposed to using the absolute signal strength or power of an RF signal transmitted by a wireless node, implementations of the present invention compare the differences between signal strength values detected at various pairs of radio receivers to corresponding differences characterized in a model of the RF environment. One implementation of the invention searches for the locations in the model between each pair of radio receivers where their signal strength is different by an observed amount.

AA ... LOCALISATION DE NŒUD
BB ... FIN DE SÉLECTION DE RECEPTEUR/ÉMETTEURS D'INFRASTRUCTURE
102... SÉLECTION DE EMÉMETTEURS/RÉCEPTEURS RADIO
      D'INFRASTRUCTURE
104... COLLECTE DE MESURES DES INDICATEURS D'INTENSITÉ DE SIGNAL
      DE RÉCEPTION POUR LES ÉMETTEURS/RECEPTEURS RADIO
      D'INFRASTRUCTURE SELECTIONNES
106... SÉLECTION D CARTES DE COUVERTURES EN FONCTION DES
      ÉMETTEURS/RÉCEPTEURS RADIO D'INFRASTRUCTURE SÉLECTIONNÉS
108... RÉCEPTEURS/ÉMETTEURS D'INFRASTRUCTURE SÉLECTIONNÉS
110... CARTE DE COUVERTURE
112... CHEVAUCHEMENT DE SURFACE D'ERREURS
120... SÉLECTION DE LOCALISATION MINIMISANT SURFACE D'ERREURS
      TOTALE

FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID,*

IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CROSS-REFERENCE TO RELATED PATENT APPLICATIONS

[0001] This application makes reference to the following commonly owned U.S. patent applications and/or patents, which are incorporated herein by reference in their entirety for all purposes:

[0002] U.S. patent application Ser. No. 10/155,938 in the name of Patrice R. Calhoun, Robert B. O'Hara, Jr. and Robert J. Friday, entitled "Method and System for Hierarchical Processing of Protocol Information in a Wireless LAN;"

[0003] U.S. Application Ser. No. 10/183,704 in the name of Robert J. Friday, Patrice R. Calhoun, Robert B. O'Hara, Jr., Alexander H. Hills and Paul F. Dietrich, and entitled "Method and System for Dynamically Assigning Channels Across Multiple Radios in a Wireless LAN;"

[0004] U.S. patent application Ser. No. 10/407,357 in the name of Patrice R. Calhoun, Robert B. O'Hara, Jr. and Robert J. Friday, entitled "Method and System for Hierarchical Processing of Protocol Information in a Wireless LAN;"

[0005] U.S. patent application Ser. No. 10/407,370 in the name of Patrice R. Calhoun, Robert B. O'Hara, Jr. and David A. Frascone, entitled "Wireless Network System Including Integrated Rogue Access Point Detection;" and

[0006] U.S. Application Ser. No. 10/447,735 in the name of Robert B. O'Hara, Jr., Robert J. Friday, Patrice R. Calhoun, and Paul F. Dietrich and entitled "Wireless Network Infrastructure including Wireless Discovery and Communication Mechanism."

FIELD OF THE INVENTION

[0007] The present invention relates to estimating the location of wireless nodes in RF environments and, more particularly, to a signal strength weighting metric directed to improving the accuracy of wireless node location mechanisms.

6561/53799

[0008] Market adoption of wireless LAN (WLAN) technology has exploded, as users from a wide range of backgrounds and vertical industries have brought this technology into their homes, offices, and increasingly into the public air space. This inflection point has highlighted not only the limitations of earlier-generation systems, but the changing role WLAN technology now plays in people's work and lifestyles, across the globe. Indeed, WLANs are rapidly changing from convenience networks to business-critical networks. Increasingly users are depending on WLANs to improve the timeliness and productivity of their communications and applications, and in doing so, require greater visibility, security, management, and performance from their network.

[0009] The rapid proliferation of lightweight, portable computing devices and high-speed WLANs enables users to remain connected to various network resources, while roaming throughout a building or other physical location. The mobility afforded by WLANs has generated a lot of interest in applications and services that are a function of a mobile user's physical location. Examples of such applications include: printing a document on the nearest printer, locating a mobile user or rogue access point, displaying a map of the immediate surroundings, and guiding a user inside a building. The required or desired granularity of location information varies from one application to another. Indeed, the accuracy required by an application that selects the nearest network printer, or locates a rogue access point, often requires the ability to determine in what room a wireless node is located. Accordingly, much effort has been dedicated to improving the accuracy of wireless node location mechanisms.

[0010] The use of radio signals to estimate the location of a wireless device or node is known. For example, a Global Positioning System (GPS) receiver obtains location information by triangulating its position relative to four satellites that transmit radio signals. The GPS receiver estimates the distance between each satellite based on the time it takes for the radio signals to travel from the satellite to the receiver. Signal propagation time is assessed by determining the time shift required to synchronize the pseudo-random signal transmitted by the satellite and

2

distance measurements from three points, an additional distance measurement from a fourth satellite is used for error correction.

[0011] The distance between a wireless transmitter and a receiver can also be estimated based on the strength of the received signal, or more accurately the observed attenuation of the radio signal. Signal attenuation refers to the weakening of a signal over its path of travel due to various factors like terrain, obstructions and environmental conditions. Generally speaking, the magnitude or power of a radio signal weakens as it travels from its source. The attenuation undergone by an electromagnetic wave in transit between a transmitter and a receiver is referred to as path loss. Path loss may be due to many effects such as free-space loss, refraction, reflection, and absorption.

[0012] In business enterprise environments, most location-tracking systems are based on RF triangulation or RF fingerprinting techniques. RF triangulation calculates a mobile user's location based upon the detected signal strength of nearby access points (APs). It naturally assumes that signal strength is a factor of proximity, which is true a majority of the time. However, the multipath phenomenon encountered in indoor RF environments does present certain difficulties in locating wireless nodes, since reflection and absorption of RF signals affects the correlation between signal strength and proximity. RF fingerprinting compares a mobile station's view of the network infrastructure (i.e., the strength of signals transmitted by infrastructure access points) with a database that contains an RF physical model of the coverage area. This database is typically populated by either an extensive site survey or an RF prediction model of the coverage area. For example, Bahl et al., "A Software System for Locating Mobile Users: Design, Evaluation, and Lessons," http://research.microsoft.com/~bahl/Papers/Pdf/radar.pdf, describes an RF location system (the RADAR system) in a WLAN environment, that allows a mobile station to track its own location relative to access points in a WLAN environment.

[0013] The RADAR system relies on a so-called Radio Map, which is a database of locations in a building and the signal strength of the beacon packets emanating

3

6561/53799

an entry in the Radio Map may look like $(x, y, z, ss_i (i = 1..n))$, where (x, y, z) are the physical coordinates of the location where the signal is recorded, and ss_i is the signal strength of the beacon signal emanating from the ith access point. According to Bahl et al., Radio Maps may be empirically created based on heuristic evaluations of the signals transmitted by the infrastructure radios at various locations, or mathematically created using a mathematical model of indoor RF signal propagation. To locate the position of the mobile user in real-time, the mobile station measures the signal strength of each of access points within range. It then searches a Radio Map database against the detected signal strengths to find the location with the best match. Bahl et al. also describe averaging the detected signal strength samples, and using a tracking history-based algorithm, to improve the accuracy of the location estimate. Bahl et al. also address fluctuations in RF signal propagation by using multiple Radio Maps and choosing the Radio Map which best reflects the current RF environment. Specifically, one access point detects beacon packets from other access points and consults a radio map to estimate its location, and evaluates the estimated location with the known location. The RADAR system chooses the Radio Map which best characterizes the current RF environment, based on a sliding window average of received signal strengths.

[0014] While the RADAR system works for its intended objective, even in this system, location accuracy decreases with the error in detecting the strength of RF signals. For example, the accuracy of signal strength detection between a radio transmitter and a radio receiver whose signal strength measurements are used to estimate location, and thus, the accuracy of locating a wireless node, decreases as the detected signal strength decreases. As discussed above, the RADAR, and other RF fingerprinting, systems estimate the location of a wireless node by finding the best fit in the Radio Maps, treating the signal strength measurements associated with the different access points equally. As discussed below, however, the error injected by errors in signal strength detection can inject large amounts of error in computing the location of a wireless node, especially where the detected signal, at the radio receiver, is weak. Still further, while the RADAR system allows a mobile

6561/53799

WLAN infrastructure to track the location of wireless nodes, such as rogue access points. Such a system is desirable as it obviates the need for special client software to be installed on the mobile stations.

[0015] Moreover, individual differences as to how two different wireless nodes detect and report signal strength can cause errors in location, since the Radio Maps assume no error in such measurements. Accordingly, two wireless nodes in the same location that detect different signal strengths will compute different estimated locations. Still further, while the RADAR system allows a mobile station to track its own location, it does not disclose a system that allows the WLAN infrastructure to track the location of wireless nodes, such as rogue access points. Such a system is desirable as it obviates the need for special client software to be installed on the mobile stations.

[0016] This paradigm shift, however, presents certain problems. As discussed above, the Radio Maps in the RADAR system are constructed from the point of view of a wireless node in an RF environment that includes access points in known locations. In other words, the Radio Maps are constructed based on heuristic and/or mathematical evaluations of the propagation of signals from the access points to a wireless node at a given location. Accordingly, the RADAR system need not assume symmetry of path loss between a given location and the access points in the RADAR system, since the mobile station detects the signal strength of the access points and computes its own location. In addition, since the location of a wireless node is based on path loss, the transmit power of the radio transmitters used to determine location must also be known. In the RADAR system, this is not problematic, since the signals used to determine location are transmitted by access points, whose transmit power can be controlled or easily determined. Estimating location based on signals transmitted by a wireless node, however, can be problematic, since transmit power can vary among wireless device manufacturers, and/or may be individually configured by the mobile user.

[0017] One approach to this problem is to assume symmetry in path loss between a given location in an RF environment and the radio transceivers used to detect

5

6561/53799

assume a uniform transmit power for the wireless nodes in light of the fact that legal regulations, as well as current chip set technology, generally places an upper limit on transmit power. These two assumptions, however, can significantly impact the accuracy of locating a wireless node. As discussed above, the RADAR system, for example, finds the location coordinates in the Radio Map that are the best fit based on the detected signal strengths. That is, for each point in the Radio Map, the location metric computes the Euclidean distance between the detected signal strength values and the values in the Radio Map.

[0018] The following equation provides an illustrative example, assume for didactic purposes that a given wireless node is detected by three access points. The signal strength samples are RSSIap1 RSSIap2, and RSSIap3, while the RF coverage maps for each of the access points are denoted as MAPap1, MAPap2, MAPap3, where the coverage maps include access point signal strength values detected or computed for different locations in a defined region. Further assume that all coverage maps have values at all locations within the search region. Again, assuming path loss symmetry and a uniform transmit power, individual error surfaces for each access point can be created based on the signal strength detected at each access point, (RSSIap1, etc.) and the signal strength values in the individual coverage maps (e.g., MAPap1, etc.). That is, the error surface is the difference between the observed signal strength at a given access point less the signal strength values in the coverage map. The locations in this coverage map where the difference is zero are generally the likely or estimated locations relative to each radio receiver. In many situations, however, the measured signal strengths, RSSIap1 RSSIap2, and RSSIap3, do not match the signal strengths recorded in the coverage maps MAPap1, MAPap2, MAPap3 at any one location. In this case, it is desirable to find the location that is "closest" to matching RSSIap1 RSSIap2, and RSSIap3--in other words, the location that minimizes some function of MAPap1, MAPap2, MAPap3, RSSIap1 RSSIap2, and RSSIap3. Bahl et al., supra, describe several ways in which this function is created, including minimum mean squared error, minimum distance, and minimum Manhattan grid distance.

6561/53799

sum of the squares (to neutralize positive and negative differences) of the individual error surfaces (i.e., the difference between the detected signal strength values and the signal strength values in each coverage maps), as follows: ErrSurf = [(RSSIap1 - MAPap1)^2 + (RSSIap2 - MAPap2)^2 + (RSSIap3 - MAPap3)^2]/3. In one implementation, the estimated wireless node location is derived from the minimum or minimum of this total error surface.

[0020] However, a change in the wireless node's transmit power (or, in the RADAR system, inaccuracies in detecting signal strength by the wireless nodes) will adversely affect the accuracy of this metric. For example, a N dB difference between the actual and assumed transmit power of a wireless node would cause a N dB change in the detected signal strengths. Rather than merely shifting the individual signal strength differences for each point in the individual error surfaces up by some fixed amount, the individual differences between the detected signal strengths and the signal strength values in the error surface can change quite dramatically. Indeed, each point in the individual error surfaces are shifted an amount proportional to the dB error. This circumstance moves some areas of the total error surface up relative to others, and some areas of the total error surface down relative to others, significantly altering the shape of the error surface, as well as the location, shape, and size of its minima. It also creates unpredictable error with changes in transmit power. Similar problems will occur for a fixed error in the "link or path loss symmetry" where the path loss from access point to wireless node differs from the path loss from wireless node to access point by some fixed amount due to propagation characteristics, vantage point, and the like. In addition, sources of RF interference typically have unknown transmit powers, and may only partially overlap the frequency band in which wireless nodes operate. Estimating the location of these interference sources requires a method that does not depend entirely on the absolute detected signal strength value.

[0021] In light of the foregoing, a need in the art exists for a wireless node location mechanism that reduces the errors in computing the location of a wireless node due to errors in signal strength detection. A need in the art also exists for a wireless

6561/53799

wireless node due to commonly occurring circumstances, such as variations in wireless node transmit power, errors in signal strength detection, and/or direction-dependent path loss. Embodiments of the present invention substantially fulfill these needs.

SUMMARY OF THE INVENTION

[0022] The present invention provides methods, apparatuses, and systems directed to a wireless node location mechanism that uses a signal strength weighting metric to improve the accuracy of estimating the location of a wireless node based on signals detected among a plurality of radio transceivers. In certain implementations, the wireless node location mechanism further incorporates a differential signal strength metric to reduce the errors caused by variations in wireless node transmit power, errors in signal strength detection, and/or direction-dependent path loss. As opposed to using the absolute signal strength or power of an RF signal transmitted by a wireless node, implementations of the present invention compare the differences between signal strength values detected at various pairs of radio receivers to corresponding differences characterized in a model of the RF environment. One implementation of the invention searches for the locations in the model between each pair of radio receivers where their signal strength is different by an observed amount. As discussed in more detail below, the wireless node location mechanism can be incorporated into wireless network environments, such as 802.11 networks, to estimate the location of mobile stations, rogue access points and other wireless nodes.

DESCRIPTION OF THE DRAWINGS

[0023] Figure 1 is a schematic diagram including a wireless node location mechanism according to an implementation of the present invention.
[0024] Figure 2 is a flow chart diagram illustrating the overall process flow directed to the location of a wireless node according to an implementation of the present invention.

6561/53799

according to an implementation of the present invention.

[0026] Figure 4 is a functional block diagram showing the wireless node location functionality of a central control element in the wireless network system of Figure 3.

[0027] Figure 5 is a flow chart diagram illustrating the overall process flow directed to estimating the location of a wireless node that incorporates a weighted, differential signal strength metric.

DESCRIPTION OF PREFERRED EMBODIMENT(S)

A.   Wireless Node Location and Signal Strength Weighting Metric

[0028] Figure 1 illustrates the basic operating components of the wireless node location mechanism according to an implementation of the present invention. As Figure 1 shows, the wireless node location mechanism includes a wireless node location module 59 and a plurality of infrastructure radio transceivers 58 disposed throughout a physical space. One skilled in the art will recognize that the system depicted in Figure 1 represents an example of the basic components of the invention and is mostly for didactic purposes. As discussed more fully below, the functionality generally denoted by infrastructure radio transceivers 58 and wireless node location module 59 can be integrated into a variety of systems, such as wireless systems dedicated for location of wireless nodes, or WLAN or other wireless network systems.

[0029] Infrastructure radio transceivers 58 generally comprise at least one antenna, a radio transmit/receive unit, and control logic (e.g., a 802.11 control unit) to control the transmission and reception of radio signals according to a wireless communications protocol. Infrastructure radio transceivers 58, in one implementation, are disposed in known and/or fixed locations throughout a physical space, such as a room, a collection of rooms, a floor of a building, an entire building, or an arbitrarily-defined region, including outside environments, over which infrastructure radio transceivers 58 provide RF coverage.

9

[0030] Infrastructure radio transceivers 58 are operative to detect the strength of received radio-frequency signals, such as the signals 57 transmitted by wireless node 56 and by other radio transceivers, and provide the detected signal strength data for corresponding wireless nodes to wireless node location module 59. In one implementation, infrastructure radio transceivers 58 are also operative to transmit and receive wireless or radio-frequency signals according to a wireless communications protocol, such as the IEEE 802.11 WLAN protocol. Infrastructure radio transceivers 58, in one implementation, can operate on a selected channel from a plurality of channels in a given band. In another implementation, infrastructure radio transceivers 58 can also operate in more than one band. For example, infrastructure radio receivers 58 may be configured to operate in either the 802.11a-5 GHz band, and/or the 802.11b/g-2.4 GHz band. In one implementation, infrastructure radio transceivers 58 can be configured to collect the signal strength information associated with wireless nodes and transmit the collected data in response to SNMP or other requests by wireless node location module 59. In other implementations, the infrastructure radio transceivers 58 can transmit signal strength information on a regular or periodic basis. As discussed below, other methods for collecting signal strength data may also be employed.

[0031] Identification of wireless nodes depends on the wireless communications protocol in use. For 802.11 WLAN environments, for example, wireless nodes can be identified based on MAC address. Furthermore, wireless nodes can be authorized mobile stations, such as remote client elements 16, 18 (see Figure 3), rogue systems (e.g., rogue access points and/or rogue mobile stations), as well as authorized access points for which no location information is known. In other implementations, wireless nodes can be identified based on a unique property of the RF signal, such as a given frequency channel, or a unique signal pattern, and the like. For example, the wireless node location functionality may be employed to locate a detected source of interference, such as a non-802.11 compliant device.

[0032] In one implementation, infrastructure radio transceivers 58 are also operable to communicate with one or more mobile stations, such as wireless node 56,

10

6561/53799

in one implementation, is an access point or other WLAN component. In one implementation, radio transceiver 58 is operably connected to a Local Area Network (LAN), Wide Area Network (WAN) or other wireline network to bridge traffic between mobile stations and the wireline network. As discussed more fully below, radio transceiver 58 may also be an access element or light weight access point in a wireless network featuring hierarchical processing of protocol information. In one implementation, the radio transceiver 58 implements the 802.11 protocols (where 802.11, as used herein, generically refers to the IEEE 802.11 standard for wireless LANs and all its amendments). Of course, the present invention can be used in connection with any suitable radio-frequency-based wireless network or communications protocol.

[0033] In one implementation, infrastructure radio transceivers 58 make use of the signal strength detection functionality residing on a wireless network interface adapter to detect signal strength on a frame-by-frame basis. For example, the IEEE 802.11 standard defines a mechanism by which RF energy is measured by the circuitry (e.g., chip set) on a wireless network interface controller. The IEEE 802.11 protocol specifies an optional parameter, the receive signal strength indicator (RSSI). This parameter is a measure by the PHY layer of the energy observed at the antenna used to receive the current packet or frame. RSSI is measured between the beginning of the start frame delimiter (SFD) and the end of the PLCP header error check (HEC). This numeric value is an integer with an allowable range of 0-255 (a 1-byte value). Typically, 802.11 chip set vendors have chosen not to actually measure 256 different signal levels. Accordingly, each vendor's 802.11-compliant adapter has a specific maximum RSSI value ("RSSI_Max"). Therefore, the RF energy level reported by a particular vendor's wireless network adapter will range between 0 and RSSI_Max. Resolving a given RSSI value reported by a given vendor's chip set to an actual power value (dBm) can be accomplished by reference to a conversion table. In addition, some wireless networking chip sets actually report received signal strength in dBm units, rather than or in addition to RSSI. Other attributes of the signal can also be used in

6561/53799

detected Signal-to-Noise Ratio (SNR) during packet reception can be used in determining overlay signal transmit power. Again, many chip sets include functionality and corresponding APIs to allow for a determination of SNRs associated with packets received from other transceivers 58 and/or wireless node 56. The resulting signal strength information, in one implementation, can be associated with a time stamp corresponding to the receipt of the frame. As discussed herein, this signal strength information can be collected at each infrastructure radio transceiver 58 and/or the wireless node location module 59 in suitable data structures.

A.2. Wireless Node Location Module

[0034] Wireless node location module 59, in one implementation, collects signal strength data received from infrastructure radio transceivers 58 and maintains the signal strength data in association with a wireless node identifier, and an identifier for the infrastructure radio transceiver 58 which provided the signal strength data. Wireless node location module 59, in one implementation, is also configured to distinguish between signals received from infrastructure radio transceivers 58 and signals received from other wireless nodes based on the wireless node identifier. In one implementation, wireless node location module 59 maintains a variety of data structures for storing signal strength information. For example, one data structure is used to store the signal strength of signals transmitted between infrastructure radio transceivers 58. In one implementation, wireless node location module 59 stores this signal strength data in a N x N IRT matrix, where N is the number of infrastructure radio transceivers 58. The column entries can correspond to the transmitting transceiver, while the row entries correspond to the receiving transceiver, or vice versa. Various entries in this matrix may be null values as all infrastructure radio transceivers may not, and in most deployments probably will not, be able to detect one another. Wireless node location module 59, in one implementation, maintains signal strength data for all other wireless nodes in tables or other suitable data structures. In one implementation, wireless node

6561/53799

including at least two fields: 1) a wireless node identifier; and 2) the detected signal strength. Additional fields may also include a time stamp indicating the time the infrastructure radio transceiver 58 received the signal. In one implementation, when the memory space allocated to the wireless node tables is depleted, the least recently used/updated entry as indicated by the time stamps is overwritten. In one implementation, wireless node location module 59 filters the signal strength data received from the infrastructure radio transceivers 58 against a list of wireless node identifiers in order to identify the appropriate data structure to update. One skilled in the art will recognize that a variety of data structures beyond matrixes and tables can be used.

[0035] As discussed above, signal strengths are detected, in one implementation, on a frame-by-frame basis. Accordingly, in one embodiment, the signal strength data maintained by wireless node location module 59 can be up dated as the frames/packets are received. In one implementation, the latest signal strength value is used to essentially overwrite the old value. In other implementations, however, an average, moving average or weighted moving average can be used if successive wireless frames corresponding to a given wireless node are encountered within a threshold time interval (e.g., typically resulting from a data stream transmission). In such a situation, the time stamp can correspond to the time of the last packet or frame. In addition, while radio transceivers 58 when operating as access points typically operate on different channels, mobile stations at various times (e.g., transmitting probe requests to find access points) transmit wireless frames on all available operating channels. This helps to ensure that a plurality of infrastructure radio transceivers 58 detect the mobile station. In some implementations, one or more infrastructure radio transceivers 58 that are adjacent to a radio transceiver 58 that detected a given wireless node may be directed to switch to a given operating channel to listen for signals transmitted by the mobile station. Still further, as discussed below, the infrastructure radio transceivers 58 may be commanded to specifically transmit frames on a given

13

wireless node location module 59.

[0036] Wireless node location module 59 also maintains a RF physical model of the coverage area associated with the RF environment. As discussed in more detail below, the RF physical model returns an estimated physical location of a wireless node, given the strength of signals detected by the infrastructure radio transceivers 58, as well as an indication of the infrastructure radio transceivers reporting the signal strengths. In one implementation, the RF physical model characterizes for each infrastructure radio transceiver 58 the received signal strength associated with a wireless transmitter at a given location. For example, in one implementation, the RF physical model comprises, for each antenna, a radio coverage map or matrix that indicates the expected signal strength detected at an infrastructure radio transceiver received from a wireless node, assuming a uniform transmit power, at a given location defined in x-, and y- coordinates. This database can be populated in a variety of ways. For example, the radio coverage maps can be populated with the results of an extensive site survey, according to which a wireless transmitter is placed at different locations in the physical space. During the site survey, the infrastructure radio transceivers 58 operate in a listening mode that cycles between the antennas and report the resulting signal strength of the signal transmitted by the wireless node used to conduct the site survey. In one implementation, the infrastructure radio transceivers 58 can be configured to transmit the signal strength data back to the wireless transmitter, which may be a laptop computer or other wireless device. The coverage maps are constructed by associating the signal strength and location data in the coverage maps corresponding to each infrastructure radio transceiver. The coverage maps may also be constructed by having a WLAN tester (or other wireless node) simply measure the signal strength of frames transmitted by the infrastructure radio transceivers 58 (e.g., beacon packets) at desired locations within the deployment region. If path loss symmetry is assumed, these values can be used to construct the coverage maps for each of the infrastructure radio transceivers. To estimate the location of the wireless node, wireless node location module 59 determines the

14

maps associated with the infrastructure radio transceivers 58 selected to locate the wireless node based on the detected signal strength data, as discussed in more detail below.

[0037] In one implementation, a coverage map, for each infrastructure radio transceiver 58, is maintained that includes the signal strengths in an N x M matrix, where N is the number of x-coordinates in the coverage map, and M is the number of y-coordinates in the coverage map. In one implementation, the extent of the physical space model by the coverage maps for each infrastructure radio transceiver 58 are co-extensive. The coverage maps for all infrastructure radio transceivers 58 can be co-extensive with the physical space in which the location system is deployed, or with a boundary configured by a network administrator. In one implementation, however, knowledge of various antenna attributes associated with each infrastructure radio transceiver 58--such as antenna type (e.g., omni-directional, directional), peak gain orientation, beamwidth, front-to-back isolation--can be used to compress or reduce the size of the coverage maps. In one implementation, the coverage maps can be configured to be substantially coextensive with the antenna pattern of each antenna connected to the infrastructure radio transceivers 58 out to a threshold signal strength or gain level. For example, the coverage map for a given antenna can be compressed to the front or intended coverage area of the directional antenna. Of course, other data structures can be used such as a table including location coordinates stored in association with tuples of signal strengths and infrastructure radio transceiver antenna identifiers. In addition, if the coverage maps are compressed, the search for the best fit across selected coverage maps can be isolated to the overlap between coverage maps associated with the antennas selected to locate the wireless node.

[0038] In another implementation, the coverage maps of the RF physical model may be constructed using RF prediction to model the coverage area, employing   ' mathematical techniques like ray-tracing, and the like. In one implementation, the RF prediction model can be computed for each coordinate location in a desired physical space, assuming a uniform wireless node transmit power. The estimated

6561/53799

to populate the coverage maps discussed above. In an alternative embodiment, RF prediction models can be computed relative to each infrastructure radio transceiver antenna. If path loss symmetry and transmit power symmetry between the wireless nodes and the infrastructure radio transceivers 58 are assumed, the coverage maps for each infrastructure radio transceiver antenna can be populated by using the computed values at each of the coordinate locations in the coverage map. Of course, site survey data can also be used to adjust one or more parameters associated with the RF prediction model used to estimate expected signal strength at the various locations. As above, the boundaries of the coverage maps can be contoured based on the properties of the antennas connected to the infrastructure radio transceivers 58. In addition, the location coordinates in the coverage maps can be two-dimensional, x- and y-coordinates, defining location in a horizontal plane. The location coordinates can also be three-dimensional, x-, y- and z-coordinates. Other coordinate systems can be used, such as spherical coordinates or cylindrical coordinates. In addition, the values of the coordinates can be either global (i.e., longitude and latitude) or expressed relative to an arbitrarily-defined origin. In addition, the granularity of the coordinates in the coverage maps depends on the desired granularity of the wireless node location estimates. In addition, in dual-band configurations, separate coverage maps may be maintained for each infrastructure radio transceiver 58 for the different frequency bands (e.g., 2.4 GHz and 5 GHz).

[0039] In one implementation, the wireless node location module 59 includes more than one RF physical model of the environment (in one implementation, each RF physical model is a set of coverage maps corresponding to the antennas of the infrastructure radio transceivers 58), and uses signals transmitted between the infrastructure radio transceivers 58 to dynamically select one of the RF physical models (such as a set of coverage maps) that best characterizes the current RF environment. As discussed above, the propagation of RF signals is effected by a variety of objects, including people, that move within an RF environment. In one implementation, the wireless node location functionality can compare the signal

6561/53799

the infrastructure radio transceivers against the RF physical models to find the best fit. In one implementation, infrastructure radio transceivers 58 can be configured to transmit wireless frames at regular intervals on one to a plurality of operating channels within a given frequency band to allow for the other infrastructure radio transceivers 58 to detect the signals. U.S. Application Ser. No. 10/447,735 discloses the transmission of frames for detection by neighboring WLAN transceivers. In another implementation, infrastructure radio transceivers 58 transmit frames, on demand, in response to a command issued by wireless node location module 59.

[0040] Figure 2 illustrates a method, according to one implementation of the present invention, directed to estimating the location of a wireless node. The wireless node location functionality can be triggered on demand, for example, in response to a command issued by a network administrator using a control interface to locate a mobile station identified by a MAC address or other suitable identifier, such as an arbitrary name associated with a MAC address in a table or other data structure. Wireless node location module 59 may also be triggered automatically in response to the detection of a rogue access point. U.S. Application Serial No. 10/407,370, incorporated by reference above, discloses detection of rogue access points in a wireless network system. Wireless node location module 59 can also be configured to periodically determine the location of a given mobile station in order to track its movement over a period of time.

A.3.   Signal Strength Weighting Metric

[0041] As Figure 2 illustrates, wireless node location module 59, in one implementation, begins by selecting the infrastructure radio transceivers (IRTs) 58 whose signal measurements will be used in locating the desired wireless node (102). In one implementation, wireless node location module 59 scans the data structures discussed above to identify the infrastructure radio transceivers 58 that see or detect wireless frames transmitted by the desired wireless node. In implementations where signal strength data is regularly collected (as opposed to on

17

infrastructure radio transceivers 58 that have not detected the desired wireless node within a threshold period of time. Additional or alternative filter criteria can include a threshold signal strength level (such as -80 dBm). In the implementation shown, wireless node location module 59 selects the M infrastructure radio transceivers 58 that report the strongest signal strengths (where M is a configurable parameter). In one implementation, if an insufficient number of infrastructure radio transceivers 58 are identified, wireless node location module 59 can command the infrastructure radio transceivers 58 to actively scan for the desired wireless node and return signal strength information. Wireless node location module 59 collects the signal strength (e.g., RSSI) measurements corresponding to the selected infrastructure radio transceivers 58 (104), and identifies the RF coverage maps to be used in estimating the location of the wireless node based on selected infrastructure radio transceivers 58 (106).

[0042] As Figure 2 shows, wireless node location module 59, for all selected infrastructure radio transceivers (108), computes, for each point in the coverage map, MAP_i, an error surface, $ErrSurf_i$, characterizing the difference between the signal strength, SS_i, detected by the infrastructure radio transceiver and the value in the corresponding coverage map (110). To neutralize positive and negative errors, wireless node location module 59, in one implementation, uses the square of the error for each point in the error surface. As Figure 2 illustrates, wireless node location module 59 sums the individual error surfaces, $ErrSurf_i$, to create a total error surface, TotalErrSurf, for all points for which the error surfaces overlap (112). However, as Figure 2 shows, the contribution of each error surface, $ErrSurf_i$, is weighted by a weighing function, WF, whose value depends on the detected signal strength, SS_i, reported by the infrastructure radio transceiver 58. To estimate the location of the desired wireless node, wireless node location module 59, in one implementation, selects the location that minimizes the total error surface, TotalErrSurf (120). In one implementation, wireless node location module 59 computes the estimated location by finding the location that minimizes the Euclidian distance in signal space of the Total Err Surf, which essentially

6561/53799

strength values and the signal strength values in the corresponding coverage maps.

[0043] The weighting function, WF, in one implementation, expresses the confidence in the individual error surface (ErrSurf$_i$) location relative to error in distance caused by potential errors in signal strength detection. In the implementation shown, confidence in the error surface (ErrSurf$_i$) is defined by how much distance error would be caused by a 1 dB change in the signal strength measurement, SS$_i$, from the infrastructure radio transceiver 58. This confidence weighting function could vary depending on topology (e.g., the presence and location of interior walls, dividers, doors, etc.) and path loss exponent. However, in one implementation, it is assumed that this error in unit distance per dB error is a function of only detected signal strength and the path loss exponent. According to this implementation, the error in unit distance per dB is a geometric or exponential function. The weights for each error surface, therefore, are exponential with higher detected signal strengths resulting in higher weighting values. For a single DB change the error, er, in unit distance (e.g., feet, meters, etc.) changes by:

[0044] $$er = 10^{1/10 * PL}$$

[0045] So, for example, if the path loss exponent, PL, is 2.4, the error, er, is 1.1007. Accordingly, for a 1 dB error at 100 feet, for example, would cause 10.07 feet of error in the estimated location. in estimated distance, while a 1dB error at 1000 feet would cause 100.7 feet of error.

[0046] Given the error values discussed above, the weighting function, WF, in one implementation, is as follows:

[0047]   WF(SS$_i$) equals   1,   if SS$_i$ > Th; else, equals $er^{(SS_i - Th)}$.

[0048] As the weighting function equation set forth above, demonstrates, WF equals one for signal strength measurements above a threshold, Th (such as -50 dBm). Furthermore, as the weighting function above demonstrates, the weighting function decreases with decreasing signal strength measurements as lower measurements indicate increased distance between the transmitting radio and receiving radio. Moreover, as one skilled in the art will recognize the weights will change with respect to path loss exponent, frequency (2.4 v 5.1 GHz), and threshold (Th). Still

19

is collected in more than one frequency band, the signal strength weighting metric may weight samples from one band (e.g., 2.4 GHz) higher than samples obtained in another band (e.g., 5 GHz). The difference in weighting between bands can be based on an empirical study of the location error employing each separate band.

A.4. Signal Strength Weighting Metric and Differential Metric

[0049] Figure 5 illustrates an alternative implementation of the present invention in which the signal strength weighting metric is incorporated into an algorithm that estimates the location of wireless nodes based on the differences in reported signal strength across selected infrastructure radio transceivers 58. As Figure 5 illustrates, wireless node location module 59, in one implementation, begins by selecting the infrastructure radio transceivers (IRTs) 58 whose signal measurements will be used in locating the desired wireless node (102). In addition, wireless node location module 59 collects signal strength measurements (104) and selects RF coverage maps (106) in a manner similar to that described in connection with Figure 2.

[0050] As Figure 5 illustrates, wireless node location module 59, computes the difference, ΔSS_{ij}, for each pair of signal strength measurements (SS_i and SS_j) among the selected infrastructure radio transceivers 58 (212), as well as the difference, ΔMAP_{ij}, at each point between the coverage maps (MAP_i and MAP_j) corresponding to the selected infrastructure radio transceivers 58 (214). In the case of M selected infrastructure radio transceivers 58, there are N choose 2 or N!/((N-2)! 2!) pairs of differences. Wireless node location module 59 constructs a total difference error surface, ErrSurfDiff, by computing, for each unique pair of infrastructure radio transceivers 58 (see 208, 210), the square of the difference between ΔSS_{ij} and ΔMAP_{ij}, and adding the contribution from each unique pair to ErrSurfDiff (216a, 216b). Wireless node location module 59, however, weights each contribution by the weighting function, WF. As Figure 5 shows, each contribution is weighted using the lesser value of the signal strength measurements, SS_i and SS_j, for each unique pair of infrastructure radio transceivers 58 (215), since the potential error

20

6561/53799

attributable to the higher of the signal strength values in the pair. Lastly, to estimate the location of the desired wireless node, wireless node location module 59 selects the location that minimizes the total difference error surface, ErrSurfDiff (220).

[0051] As the foregoing illustrates, wireless node location module 59, in this implementation, essentially searches for the area between each pair of infrastructure radio transceivers 58 where the detected signal strength is different by X dB, where X dB is the observed difference in the RSSI or other signal strength measurements of the desired wireless node as detected by the two infrastructure radio transceivers. In the ideal case involving no physical barriers are located in the RF environment (and assuming the use of omni-directional antennas or antenna patterns approximating omni-directional antenna patterns), the contour where the difference between the two infrastructure radio transceivers 58 predicted signals is a constant X dB can be described by a Cartesian oval. In the practical world, this shape is arbitrary. In the ideal world, summing up several of these create a region of zero error where the Cartesian ovals overlap and non-zero error terms elsewhere. In the real world, the summing up of several of these surfaces create a total error surface, whose minimums represent the estimated location of the wireless node.

[0052] To illustrate the benefits of this differential signal strength metric, assume a N dB difference in the transmit power of the wireless node from an assumed or default transmit power. In the case of three selected infrastructure radio transceivers, this N dB difference factors into the total difference error surface as:

[0053] $ErrSurfDiffTxErr = (((RSSIap1 + N) - (RSSIap2+N)) - (MAPap1 - MAPap2))^2$

$$+ (((RSSIap1+N) - (RSSIap3+N)) - (MAPap1 - MAPap3))^2$$

$$+ (((RSSIap2+N) - (RSSIap3+N)) - (MAPap2 - MAPap3))^2,$$

[0054] which reduces to the original ErrSurfDiff with no additional errors added. In addition, the differential signal strength metric also addresses the errors in detecting the strength of wireless signals and errors resulting from assuming path

21

(e.g., MAPap1, MAPap2) may be incorrect by K dB for each client independently. In this metric, those errors are also removed, as shown in the following:

[0055] ErrSurfDiffAPErr = ((RSSIap1 - RSSIap2) - ((MAPap1+K) - (MAPap2+K)))^2

$$+ ((RSSIap1 - RSSIap3) - ((MAPap1+K) - (MAPap3+K)))^2$$
$$+ ((RSSIap2 - RSSIap3) - ((MAPap2+K) - (MAPap3+K)))^2,$$

[0056] which also reduces to ErrSurfDiff. Accordingly, the differential signal strength metric described herein minimizes the effects of absolute error caused by variations in transmit power, or signal strength detection, as well as lack of symmetry in path loss between a detecting node and a transmitting node.

B.   Integration into Wireless Network Systems

[0057] In one implementation, the wireless node location functionality discussed above can be integrated into a wireless network infrastructure, such as the hierarchical WLAN system illustrated in Figure 3. For example, the wireless node location functionality described herein may be integrated into a WLAN environment as disclosed in U.S. application Ser. Nos. 10/155,938 and 10/407,357 incorporated by reference herein. The wireless node location functionality according to the present invention, however, may be applied to other wireless network architectures. For example, the wireless node location functionality may be integrated into a wireless network infrastructure including a plurality of substantially autonomous access points that operate in connection with a central network management system.

[0058] Referring to Figure 3, there is shown a block diagram of a wireless Local Area Network system according to an embodiment of the invention. A specific embodiment of the invention includes the following elements: access elements 11-15 for wireless communication with selected client remote elements 16, 18, 20, 22, central control elements 24, 25, 26, and means for communication between the access elements and the central control elements, such as direct line access, an Ethernet network, such as LAN segment 10. As disclosed in U.S. patent

22

6561/53799

are directly connected to LAN segment 10 or a virtual local area network (VLAN) for communication with a corresponding central control element 24, 26. See Figure 3. As disclosed in U.S. patent application Ser. No. 10/155,938, however, access elements 11-15 may also be directly connected to respective central control elements 24, 26 via direct access lines.

[0059] The access elements 11-15 are coupled via communication means using a wireless local area network (WLAN) protocol (e.g., IEEE 802.11a or 802.11b, etc.) to the client remote elements 16, 18, 20, 22. As described in U.S. Application Ser. Nos. 10/155,938 and 10/407,357, the access elements 12, 14 and the central control element 24 tunnel network traffic associated with corresponding remote client elements 16, 18; 20, 22 via direct access lines or a LAN segment 10. Central control elements 24, 26 are also operative to bridge the network traffic between the remote client elements 16, 18; 20, 22 transmitted through the tunnel with corresponding access elements 11-15. In another implementation, access elements 11-15 may be configured to bridge the network traffic on LAN segments 10, while sending copies of the bridged frames to the access elements for data gathering and network management purposes.

[0060] As described in the above-identified patent applications, central control elements 24, 26 operate to perform data link layer management functions, such as authentication and association on behalf of access elements 11-15. For example, the central control elements 24, 26 provide processing to dynamically configure a wireless Local Area Network of a system according to the invention while the access elements 11-15 provide the acknowledgment of communications with the client remote elements 16, 18, 20, 22. The central control elements 24, 26 may for example process the wireless LAN management messages passed on from the client remote elements 16, 18; 20, 22 via the access elements 11-15, such as authentication requests and authorization requests, whereas the access elements 11-15 provide immediate acknowledgment of the communication of those messages without conventional processing thereof. Similarly, the central control elements 24, 26 may for example process physical layer information. Still further, the central

6561/53799

information collected at the access elements 11-15 on channel characteristics, signal strength, propagation, and interference or noise.

[0061] Central control elements 24, 26, as shown in Figure 4, may be configured to gather the signal strength data discussed above to support the wireless node location functionality according to the present invention. The signal strength data gathering functionality described herein is quite similar to the data gathering disclosed in U.S. Application Ser. No. 10/183,704, incorporated by reference above. In that application, access elements 11-15 append signal strength data to packets received from wireless nodes, typically, in encapsulating headers. The central control elements 24, 26 process the encapsulating packet headers to update various data structures, such as the N x N AP signal strength matrix and wireless node tables discussed above in Section A. U.S. Application Ser. No. 10/183,704 discloses the internal operating components and general configuration of access elements 11-15 that can be used in connection with the integrated wireless node location functionality described herein.

[0062] Figure 4 illustrates the logical configuration of central control elements 24, 26, according to an implementation of the present invention. As discussed in U.S. Application Ser. No. 10/183,704, in one implementation, there is both a logical data path 66 and a control path 68 between a central control element 24 or 26 and an access element (e.g., access element 11). The control path 68 allows the central control element 24 or 26 to communicate with the radio access elements 11-15 and acquire the signal strength between the radio access elements. By monitoring the data path 66, the central control element 24, 26 can obtain the signal strength of the signals transmitted by other wireless nodes.

[0063] More specifically, the wireless node locator 90 in the central control element 24 or 26 collects information from a plurality of access elements via a control channel 68 and a data channel 66. The central control element 24 or 26 receives and transmits data packets and control packets from/to a plurality of access elements 11-15 as described above. A flag detector 62 distinguishes between data packets and control packets, routing them through a logical switch 64 to a high-

68 within the central control element 24 or 26. The data path 66 is monitored by a wireless node data collector 70. Associated with each data packet is a resource management header which contains RF physical layer information, such as the power in the channel before each received packet, an identifier for the access element receiving the signal, as well as an identifier for the antenna selected to receive the signal. This information, together with the 802.11 protocol information in the native frames, can be used to maintain one or more data structures that maintain signal strength data for the wireless nodes detected by the access elements 11-15, as discussed in section A, above. The control path 68 is coupled to a processor element 76 in which an AP signal strength matrix 78 is maintained. The AP signal strength matrix 78 collects information quantifying the signal strength between access elements 11-15. All of the signal strength data are collected at the access elements 11-15 and communicated over the data path and control path to the central control element 24 or 26, in one implementation, as packetized information in the resource management header in the data path and resource management control packets in the control path, respectively.

[0064] As discussed above, in one implementation, the wireless node location function uses signal strength data between access elements to select a RF physical model that best characterizes the current RF environment. To support such an implementation, one task is to create and maintain an AP signal strength matrix for all the remote access elements in the various wireless networks which detect each other's signals. This is accomplished, in one implementation, by having the wireless node locator 90 in the central control element 24 or 26 and a Resource Manager in the access elements 11-15 both passively listen to surrounding access elements and actively probe for surrounding access elements. The wireless node locator in the central control element 24 or 26 can schedule an access element 11-15 in the wireless network to transmit a data measurement request on a specified channel and then record responses from surrounding access elements. The data measurement probe request and the receiver information bandwidth can have a narrower information bandwidth than the normal information bandwidth in order

25

operational range. This allows a radio element to "see" access elements beyond its
normal operating range. Scheduling these measurements allows multiple
measurements to be made with a single transmission and allows the detection of
the transmitting signal to be recognized as a change in amplitude relative to the
background noise at the scheduled time, allowing for easier detection of the
measurement signal and greater dynamic range. The resulting data can be
transmitted in control packets collected by AP signal strength matrix 78 on the
control path 68. Passively, for each packet received on the data channel at the
access element a measurement of the power in the RF channel is made immediately
before the received packet. This interference measurement is sent to the central
control element via the data channel by appending a Radio Resource Manager
header to the data packet. Alternatively, the access elements may be configured to
flag packets received from other access elements such that they are transmitted on
the control path 68. The AP signal strength data can be used to select from
different coverage maps that best characterize the current RF environment, as
discussed above. The AP signal strength data can also be used to dynamically
compute or adjust the path loss exponent(s) used in the weighting function
described above. For example, since the distance between two or more access
elements are known, path loss exponent(s) may be computed based on the observed
signal attenuation between pairs of access elements.

[0065] Figure 4 also illustrates an RF physical model database 80 containing the
one or more coverage maps associated with the access elements 11-15. When
activated, the wireless node locator 90 can operate as discussed above to compute
the estimated location of a desired wireless node, and return the estimated location
to the requesting system, such as a network management system or a control
interface. In the WLAN system depicted in Figure 3, several implementations are
possible. For example, central control element 24 may be configured as a "master"
central control element for purposes of wireless node location. That is, data
collected at all central control elements is ultimately transmitted (either regularly
or on demand) from other central control elements (e.g., central control element 26)

Alternatively, the collected data can be transmitted to a network management
system that performs the location computations discussed above. Alternatively,
central control elements 24, 26 (when deployed in separate physical spaces, such as
separate floors or buildings) may operate substantially autonomously.

[0066]

[0067] The invention has been explained with reference to specific embodiments.
For example, although the embodiments described above operate in connection with
802.11 networks, the present invention can be used in connection with any wireless
network environment. In addition, although the embodiments described above
operate in connection with a RF physical model including a plurality of coverage
maps or matrixes, other data structures can be used to store the RF physical model
data. Still further, although the embodiments described above compute estimated
location based on signal strengths detected by infrastructure access points or
elements, the signal strength weighting metric can be used by client wireless nodes,
such as mobile stations in the RADAR system. In addition, while the location
algorithms discussed above consider the square of the Euclidean distance between
the RSSI vector and the MAP vector at a particular location, other minimization
functions can be considered, including minimum mean squared error, minimum
distance, and minimum Manhattan grid distance. Other embodiments will be
evident to those of ordinary skill in the art. It is therefore not intended that the
invention be limited except as indicated by the appended claims.

6561/53799

What is claimed is:

1. A method for estimating the location of a wireless node relative to a plurality of radio receivers operative to detect the strength of RF signals, wherein a RF coverage map, corresponding to each of the radio receivers, characterizes the signal strength values for locations in a physical region, comprising

collecting signal strength values, detected at a plurality of radio receivers, corresponding to signals transmitted by a wireless node;

computing the estimated location of the wireless node based on the collected signal strength values and the RF coverage maps corresponding to the plurality of radio receivers, wherein the contribution of each detected signal strength value to the estimated location is weighted according to a weighting function that varies with the signal strength values detected by the radio receivers.

2. The method of claim 1 wherein the computing step comprises

computing, for each radio receiver, an individual error surface based on the RR coverage map associated with the radio receiver and the signal strength detected by the radio receiver;

weighting each of the individual error surfaces according to a weighting function that varies with the signal strength detected by corresponding radio receivers;

aggregating the individual error surfaces to create a total error surface;

finding the location of the minimum of the total error surface.

3. The method of claim 2 wherein each individual error surface comprises the sum of the squares of the difference between the signal strength values detected by a radio receiver and the signal strength values in a corresponding RF coverage map.

28

in the individual error surface location relative to the distance error caused by potential errors associated with the signal strength detected by a radio receiver.

5. The method of claim 1 wherein the weighting function is configured such that contributions associated with detected signal strengths above a predetermined threshold value are equally weighted.

6. The method of claim 1 wherein the weighting function is based in part on the distance error caused by a 1 dB change in the signal strength detected by a radio receiver.

7. The method of claim 1 further comprising

    detecting, at a plurality of radio transceivers, the strength of signals transmitted by a wireless node.

8. The method of claim 1 wherein the RF coverage maps each comprise a plurality of location coordinates associated with corresponding signal strength values.

9. The method of claim 8 wherein the RF coverage maps are heuristically constructed.

10. The method of claim 8 wherein the RF coverage maps are based on a mathematical model.

11. The method of claim 1 wherein the signals transmitted by the wireless nodes are formatted according to a wireless communications protocol.

12. The method of claim 11 wherein the wireless communications protocol is the IEEE 802.11 protocol.

6561/53799

transmitted by the wireless node in a first frequency band, and wherein at least one other of the collected signals is transmitted by the wireless node in a second frequency band.

14. The method of claim 13 wherein the weighing function weights the signal strength values associated with the first frequency band higher than the signal strength values associated with the second frequency band.

15. The method of claim 1 wherein only signal strength values above a threshold signal strength value are used to compute the estimated location of the wireless node.

16. An apparatus facilitating the location of a wireless node in a RF environment, comprising

a plurality of radio receivers comprising at least one antenna, the plurality of radio receivers operative to detect the strength of signals transmitted by wireless nodes and provide the detected signal strengths to a wireless node location model; wherein a RF coverage map, corresponding to each of the radio receivers, characterizes the signal strength values for locations in a physical region, and

a wireless node location module operative to compute the estimated location of the wireless node based on the collected signal strength values and the RF coverage maps corresponding to the plurality of radio receivers, wherein the contribution of each detected signal strength value to the estimated location is weighted according to a weighting function that varies with the signal strength values detected by the radio receivers.

17. The apparatus of claim 16 wherein the wireless node location module, in computing the estimated location of the wireless node, is operative to

6561/53799

coverage map associated with the radio receiver and the signal strength detected by the radio receiver;

weight each of the individual error surfaces according to a weighting function that varies with the signal strength detected by corresponding radio receivers;

aggregate the individual error surfaces to create a total error surface; and

find the location of the minimum of the total error surface.

18. The apparatus of claim 17 wherein each individual error surface comprises the sum of the squares of the difference between the signal strength values detected by a radio receiver and the signal strength values in a corresponding RF coverage map.

19. The apparatus of claim 16 wherein the weighting function expresses the confidence in the individual error surface location relative to the distance error caused by potential errors associated with the signal strength detected by a radio receiver.

20. The apparatus of claim 16 wherein the weighting function is configured such that contributions associated with detected signal strengths above a predetermined threshold value are equally weighted.

21. The apparatus of claim 16 wherein the weighting function is based in part on the distance error caused by a 1 dB change in the signal strength detected by a radio receiver.

22. The apparatus of claim 16 wherein the RF coverage maps each comprise a plurality of location coordinates associated with corresponding signal strength values.

6561/53799

constructed.

24. The apparatus of claim 22 wherein the RF coverage maps are based on a mathematical model.

25. The apparatus of claim 16 wherein the signals transmitted by the wireless nodes are formatted according to a wireless communications protocol.

26. The apparatus of claim 25 wherein the wireless communications protocol is the IEEE 802.11 protocol.

27. A method for estimating the location of a wireless node relative to a plurality of radio receivers operative to detect the strength of RF signals, wherein a RF coverage map, corresponding to each of the radio receivers, characterizes the signal strength values for locations in a physical region, comprising

collecting signal strength values, detected at a plurality of radio receivers, corresponding to signals transmitted by a wireless node; and

computing the estimated location of the wireless node by comparing, for all unique pairs of radio receivers, the differences in the signal strength values detected by the plurality of radio receivers to corresponding differences in the signal strength values in the RF coverage maps associated with the plurality of radio receivers, wherein the comparison is weighted as a function of at least one of the signal strength values detected by each unique pair of radio receivers.

28. The method of claim 27 wherein the computing step comprises

computing, for all unique pairs of radio receivers, the sum of the squares of the difference between the signal strength values detected by a pair of radio receivers less the difference between the signal strength values in the RF coverage maps associated with the pair of radio receivers;

32

strength values detected by the corresponding pair of radio receivers;

combining the weighted sums to create a differential error surface; and

finding the minimum of the differential error surface.

29. The method of claim 27 further comprising

detecting, at a plurality of radio transceivers, the strength of signals transmitted by a wireless node.

30. The method of claim 27 wherein the RF coverage maps each comprise a plurality of location coordinates associated with corresponding signal strength values.

31. The method of claim 30 wherein the RF coverage maps are heuristically constructed.

32. The method of claim 30 wherein the RF coverage maps are based on a mathematical model.

33. The method of claim 27 wherein the signals transmitted by the wireless nodes are formatted according to a wireless communications protocol.

34. The method of claim 33 wherein the wireless communications protocol is the IEEE 802.11 protocol.

35. A wireless node location mechanism operating in association with a wireless network environment comprising a plurality of radio receivers operative to detect the signal strength of signals transmitted by wireless nodes, wherein a RF coverage map, corresponding to each of the radio receivers, includes signal strength values for locations in a physical region, comprising:

a wireless node location module operative to

6561/53799

detected signal strength of RF signals transmitted by a wireless node; and

compute the estimated location of the wireless node based on the received signal strength values and the RF coverage maps corresponding to the plurality of radio receivers, wherein the contribution of each detected signal strength value to the estimated location is weighted according to a weighting function that varies with the signal strength values detected by the radio receivers.

36. The wireless node location mechanism of claim 35 wherein the wireless node location module, in computing the estimated location of the wireless node, is operative to

compute, for each radio receiver, an individual error surface based on the RF coverage map associated with the radio receiver and the signal strength detected by the radio receiver;

weight each of the individual error surfaces according to a weighting function that varies with the signal strength detected by corresponding radio receivers;

aggregate the individual error surfaces to create a total error surface; and

find the location of the minimum of the total error surface.

37. The wireless node location mechanism of claim 36 wherein each individual error surface comprises the sum of the squares of the difference between the signal strength values detected by a radio receiver and the signal strength values in a corresponding RF coverage map.

38. The wireless node location mechanism of claim 35 wherein the weighting function expresses the confidence in the individual error surface location relative to the distance error caused by potential errors associated with the signal strength detected by a radio receiver.

6561/53799

function is configured such that contributions associated with detected signal strengths above a predetermined threshold value are equally weighted.

40. The wireless node location mechanism of claim 35 wherein the weighting function is based in part on the distance error caused by a 1 dB change in the signal strength detected by a radio receiver.

41. The wireless node location mechanism of claim 35 wherein the RF coverage maps each comprise a plurality of location coordinates associated with corresponding signal strength values.
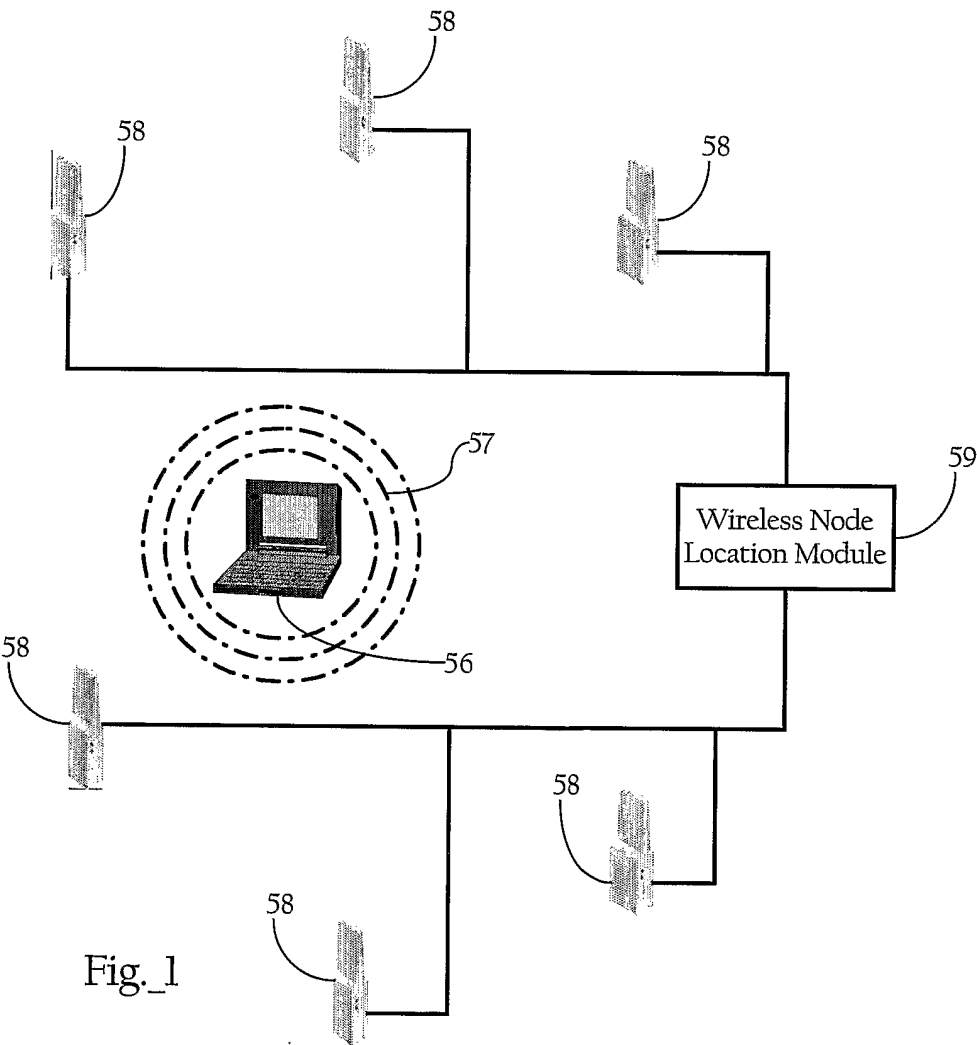
42. The wireless node location mechanism of claim 41 wherein the RF coverage maps are heuristically constructed.

43. The wireless node location mechanism of claim 41 wherein the RF coverage maps are based on a mathematical model.

44. The wireless node location mechanism of claim 35 wherein the signals transmitted by the wireless nodes are formatted according to a wireless communications protocol.

45. The wireless node location mechanism of claim 44 wherein the wireless communications protocol is the IEEE 802.11 protocol.

46. The wireless node location mechanism of claim 35 further comprising a plurality of radio receivers operative to detect the signal strength of signals transmitted by wireless nodes.
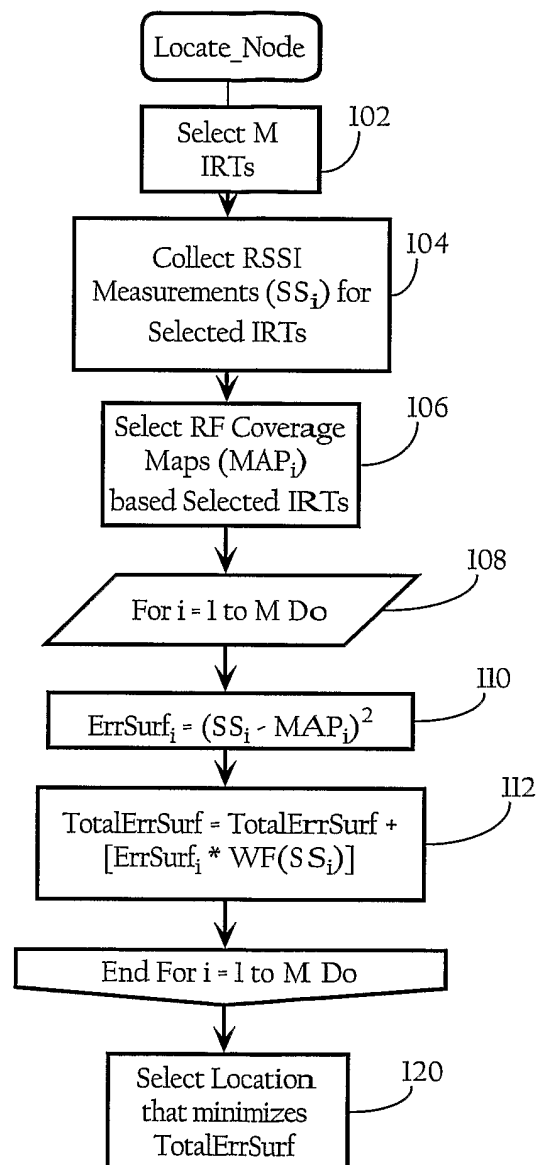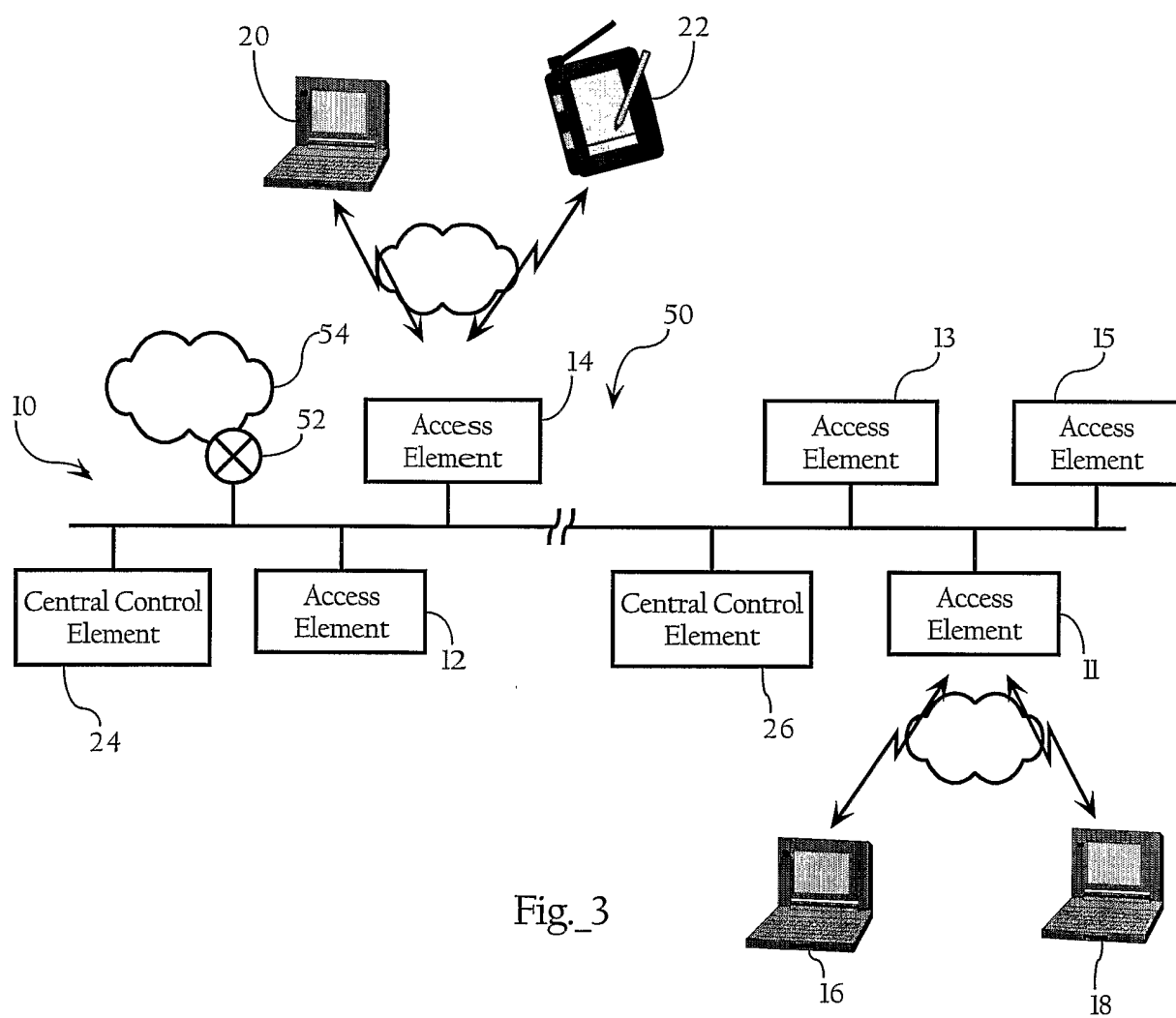
Fig._1

Fig._2

Fig._3
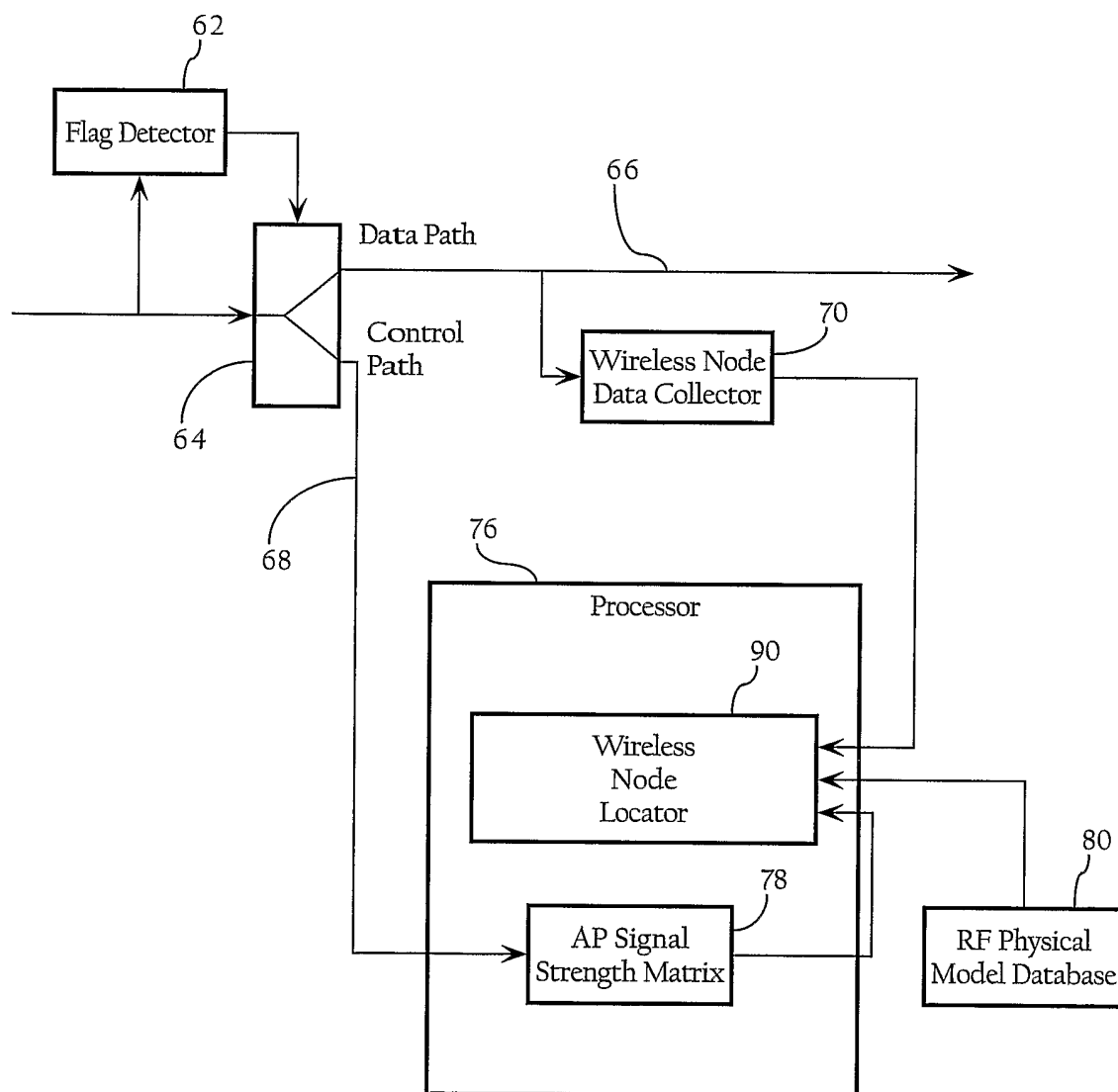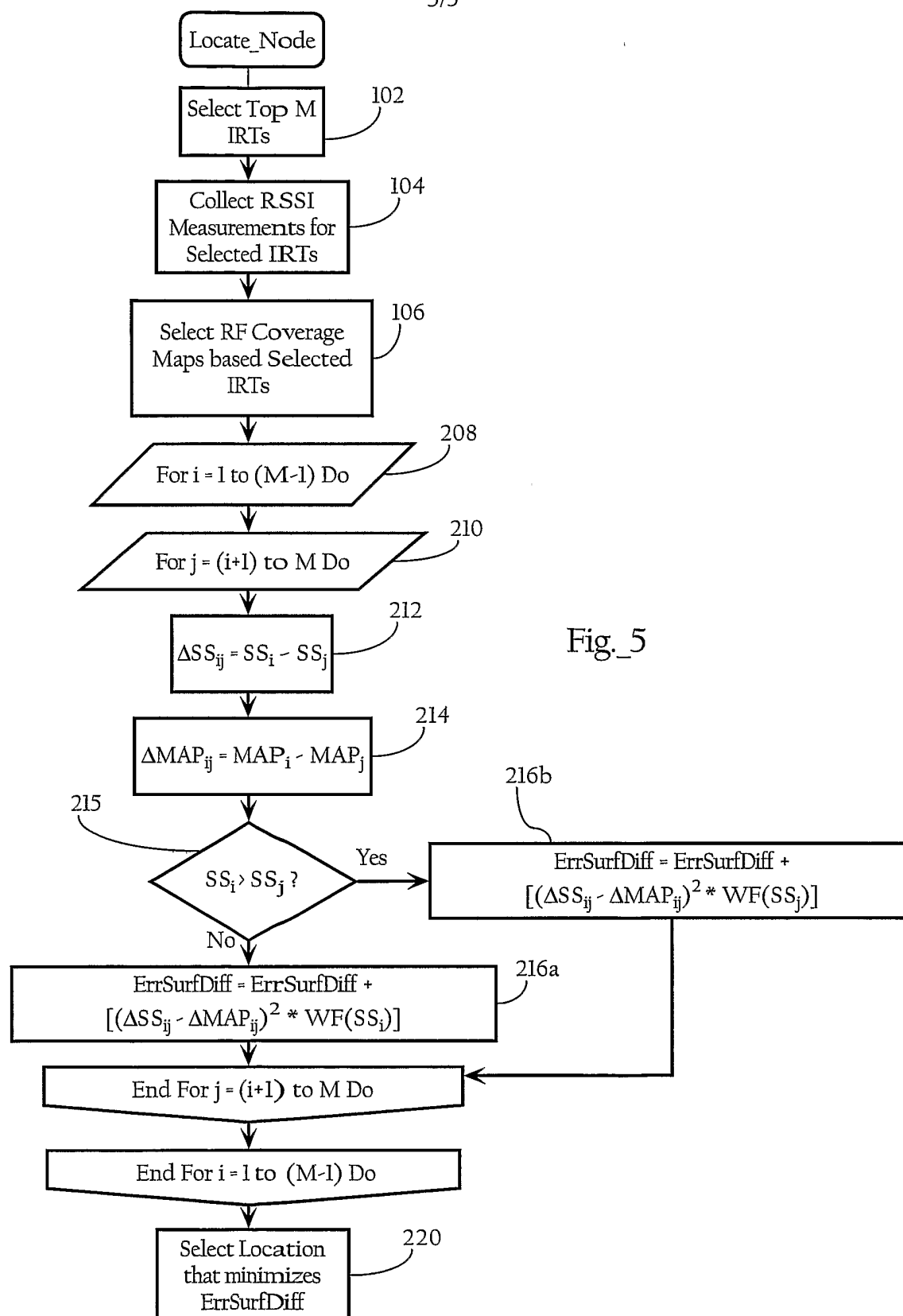
Fig._4

5/5

Locate_Node

Select Top M IRTs — 102

Collect RSSI Measurements for Selected IRTs — 104

Select RF Coverage Maps based Selected IRTs — 106

For i = 1 to (M-1) Do — 208

For j = (i+1) to M Do — 210

$\Delta SS_{ij} = SS_i - SS_j$ — 212

Fig._5

$\Delta MAP_{ij} = MAP_i - MAP_j$ — 214

215 — $SS_i > SS_j$?

Yes

216b — ErrSurfDiff = ErrSurfDiff + $[(\Delta SS_{ij} - \Delta MAP_{ij})^2 * WF(SS_j)]$

No

ErrSurfDiff = ErrSurfDiff + $[(\Delta SS_{ij} - \Delta MAP_{ij})^2 * WF(SS_i)]$ — 216a

End For j = (i+1) to M Do

End For i = 1 to (M-1) Do

Select Location that minimizes ErrSurfDiff — 220