(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2004 (05.02.2004)

PCT

(10) International Publication Number
WO 2004/012424 A2

(51) International Patent Classification[7]: H04M

(21) International Application Number:
PCT/US2003/023367

(22) International Filing Date: 28 July 2003 (28.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/398,834 29 July 2002 (29.07.2002) US
10/270,003 15 October 2002 (15.10.2002) US

(71) Applicant *(for all designated States except US)*: **MESH-NETWORKS, INC.** [US/US]; 485 North Keller Road, Maitland, FL 32751 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WHITEHILL, Eric, A.** [US/US]; 6021 Highgate Place, Fort Wayne, IN 46815 (US). **WHITE, Eric, D.** [US/US]; 564 Horns Corner Road, Cedarburg, WI 53012 (US).

(74) Agents: **BUCZYNSKI, Joseph** et al.; 1300 19th Street, N.W., Suite 600, Washington, DC 20036 (US).

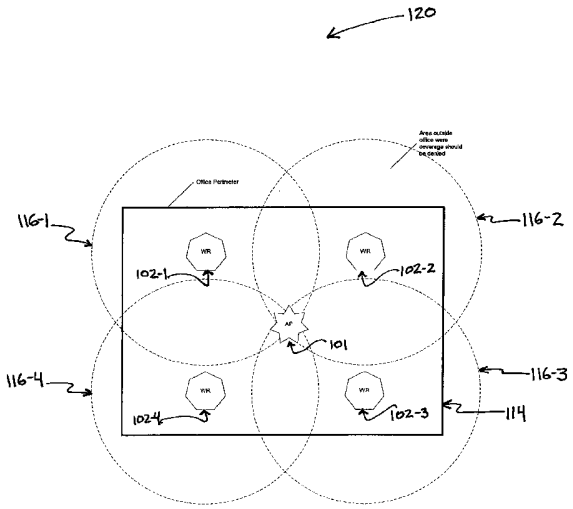
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID,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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, 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, IT, LU, MC, NL, 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.

(54) Title: A SYSTEM AND METHOD FOR DETERMINING PHYSICAL LOCATION OF A NODE IN A WIRELESS NETWORK DURING AN AUTHENTICATION CHECK OF THE NODE



(57) Abstract: A system and method for providing security to a wireless network by using a mobile node's location as a parameter for deciding if access is to be given to the node. The system and method employ access points, wireless routers and mobile nodes, each including at least one transceiver adapted to transmit and receive communication signals to and from other wireless routers, mobile nodes and other mobile access points. Each access point is connected to a network management system which allows enhanced network monitoring and control. Each network node includes technology which may determine an absolute node location containing latitude, longitude and altitude of a node, or a relative node location containing the distance and angle between nodes, or a combination of both absolute and relative location data.

WO 2004/012424 A2

A System And Method For Determining Physical Location Of A Node In A Wireless Network During An Authentication Check Of The Node

BACKGROUND OF THE INVENTION

Field of the Invention:

[0001] The present invention relates to a system and method for providing security for a wireless network, such as an ad-hoc wireless communications network, based on the position information relating to mobile nodes. More particularly, the present invention relates to a system and method for trusted infrastructure devices to compute the location of a mobile node in a wireless communications network, such as an ad-hoc terrestrial wireless communications network, during the authentication process. This application claims benefit under 35 U.S.C. §119(e) from U.S. provisional patent application serial no. 60/398,834 entitled "A System And Method For Determining Physical Location Of A Node In A Wireless Network During An Authentication Check Of The Node", filed July 29, 2002, the entire contents of which is incorporated herein by reference.

Description of the Related Art:

[0002] Wireless communications networks, such as mobile wireless telephone networks, have become increasingly prevalent over the past decade. These wireless communications networks are commonly referred to as "cellular networks" because the network infrastructure is arranged to divide the service area into a plurality of regions called "cells".

[0003] Specifically, a terrestrial cellular network includes a plurality of interconnected base stations that are distributed geographically at designated locations throughout the service area. Each base station includes one or more transceivers that are capable of transmitting and receiving electromagnetic signals, such as radio frequency (RF) communications signals, to

and from user nodes, such as wireless telephones, located within the base station coverage area. The communications signals include, for example, voice data that has been modulated according to a desired modulation technique and transmitted as data packets. As can be appreciated by one skilled in the art, the transceiver and user nodes transmit and receive such data packets in multiplexed format, such as time-division multiple access (TDMA) format, code-division multiple access (CDMA) format, or frequency-division multiple access (FDMA) format, which enables a single transceiver at the base station to communicate simultaneously with several user nodes in it's coverage area.

[0004] In recent years, a type of mobile communications network known as an "ad-hoc" network has been developed for use by the military. In this type of network, each user node is capable of operating as a base station or router for the other user nodes, thus eliminating the need for a fixed infrastructure of base stations. Details of an ad-hoc network are set forth in U.S. Patent No. 5,943,322 to Mayor, the entire content of which is incorporated herein by reference.

[0005] More sophisticated ad-hoc networks are also being developed which, in addition to enabling user nodes to communicate with each other as in a conventional ad-hoc network, further enable the user nodes to access a fixed network and thus communicate with other user nodes, such as those on the public switched telephone network (PSTN), and on other networks such as the Internet. Details of these types of ad-hoc networks are described in U.S. Patent Application Serial No. 09/897,790 entitled "Ad Hoc Peer-to-Peer Mobile Radio Access System Interfaced to the PSTN and Cellular Networks", filed on June 29, 2001, and in U.S. Patent Application Serial No. 09/815,157 entitled "Time Division Protocol for an Ad-Hoc, Peer-to-Peer Radio Network Having Coordinating Channel Access to Shared Parallel Data Channels with Separate Reservation Channel", filed on March 22, 2001, the entire content of each being incorporated herein by reference.

[0006] In either conventional wireless communications networks, or in ad-hoc wireless communications networks, it may be necessary or desirable to know or determine the geographic location of user nodes. Different types of location determining services and techniques for wireless communications networks are described in a publication by Nokia which can be found on the Nokia website at "www.nokia.com/press/background/pdf/mlbs.pdf", the entire content of which being incorporated herein by reference. In particular, the Nokia document states that location

identification services are currently provided in wireless communications networks based on three major technologies. One of these technologies uses cell identification combined with Round Trip Time (RTT), Timing Advance (TA) and Measured Signal level (RX level), Time Difference of Arrival (TDOA) and Angle Of Arrival (AOA) techniques, the details of which can be appreciated by one skilled in the art. A second technology uses cellular signal timing based methods for code division multiple access (CDMA) and wideband code division multiple access (WCDMA). The third technology described in the Nokia document employs Global Positioning System (GPS) techniques.

[0007] Another list of methods and techniques currently used in the wireless communications industry for providing location services can be found at "www.911dispatch.com/911_file/location_tech.html", the entire content of which being incorporated herein by reference. Although the GPS technique is the last technique mentioned in this list, it is generally viewed as being more accurate than all of the other methods. Further details and descriptions of GPS based methods are set forth in a publication by J. J. Spilker Jr. entitled "Satellite Constellation and Geometric Dilution of Precision", in a publication by P. Axelrad et al. entitled "GPS Navigation Algorithms", in a publication by Bradford W. Parkinson entitled "GPS Error Analysis", and in a publication by N. Ashby et al. Entitled "Introduction to Relativistic Effects on the Global Positioning System", each found in "GPS - Theory and Applications", American Institute of Astronautics, 1996, the entire content of each being incorporated herein by reference.

[0008] Despite the fact that the GPS technique has been in use for a considerable period of time and most of the world's navigation relies on this technique, the GPS technique is very susceptible to errors in measurement. Therefore, the GPS technique is capable of providing location determination results with very high accuracy only after performing a relatively large number of measurements to remove such errors. A description of the shortcomings of GPS is set forth in a document by IMA entitled "Mathematical Challenges in Global Positioning Systems (GPS)" which can be found at "www.ima.umn.edu/gps", the entire content of this document being incorporated herein by reference. Certain other tests also demonstrate that the GPS technique is unsuitable for terrestrial-based networks.

[0009] In addition, other methods and techniques which do not use GPS satellites for determining mobile station locations in a wireless communications network typically require that the signal from the mobile station be received by at least two cell sites that can measure

and process the delay between signal arrivals, identify the direction of the signal based on "path signature", and determine the distance between mobile station and the cell towers. In all of these methods, information processing is executed in a designated central processing unit (CPU) which is typically located at a cell tower next to the base station (BTS). Also, most of these methods were designed to comply with E911 requirements without requiring that excessive modifications be made to existing wireless communications systems. Examples of other location determining techniques are set forth in a document by CERN - European Organization for Nuclear Research, which can be found at "rkb.home.cern.ch/rkb/ANI16pp/node98.html#SECTION00098000000000000000", in a document by Wendy J Woodbury Straight entitled "Exploring a New Reference System", which can be found at "menstorsoftwareince.com/profile/newref.html", and in a document entitled "An Introduction to SnapTrac Server-Aided GPS Technology", which can be found at "www.snaptrack.com/pdf/ion.pdf", the entire content of each being incorporated herein by reference. Additional details may also be found in U.S. Patent Application Serial No. 09/988,001 entitled "A System and Method for Computing the Location of a Mobile Terminal in a Wireless Communications Network", filed on November 16, 2001, which describes a system and method for determining location with the use of technologies such as GPS, the entire content being incorporated herein by reference.

[0010] Accordingly, a need exists for a system and method for determining the location of a mobile user node in a wireless communications network by trusted infrastructure devices to determine if the device is physically within a predetermined "safe zone", and provide access to the network based on this location determination.

SUMMARY OF THE INVENTION

[0011] An object of the present invention is to provide a system and method for determining if a mobile node is physically located within a predetermined area of coverage. This may be accomplished with either absolute latitude/longitude location, or by a relative location to a known piece of infrastructure.

[0012] Another object of the present invention is to provide a system and method for providing network access to a mobile node based on determined location.

[0013] These and other objects are substantially achieved by providing a system and method for obtaining the location of a node in a wireless communications network and using the location information when determining if the node should be allowed access to the network. The wireless communications network can be an ad-hoc wireless communications network with each node and reference node being adapted to operate in the ad-hoc wireless communications network. The system and method further performs the operation of estimating a respective distance from the node to each of the reference nodes based on the respective signals received at the node, calculating a respective simulated pattern, such as a sphere or circle about each of the respective reference nodes based on the respective distance from the node to each respective reference node and the respective locations of the respective reference nodes, estimating a location at which each of the simulated patterns intersect each other, and identifying the estimated location as representing the location of the node. When estimating the respective distances from the node to the reference nodes, the system and method can also perform error minimizing techniques.

[0014] The system and method of the present invention determines if a mobile node is physically located in a secure area by the authentication server or it's agent. The location determination agent, at the request of the authentication server, initiates multiple (optimally 4, but at least one) range measurements taken from trusted infrastructure devices (wireless routers or access points) whose physical location is known. These measurements along with the infrastructure device locations are fed into the position algorithm that calculates the mobile node's location. If the result of the algorithm (i.e mobile node's location) is within the physical perimeter defined by the network administrator, then the authentication server receives a confirmation that the mobile node is within the building or area and can proceed with the authentication confirmation.

[0015] This algorithm is essentially identical to the location calculation algorithm that a mobile node may perform in other applications. However, in an embodiment of the present invention, all measurements are under the physical control of assets owned by the network administrator. Also, the position algorithm used is under the control of the trusted authentication server, and avoids relying on the mobile node to provide a valid answer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] These and other objects, advantages and novel features of the invention will be more readily appreciated from the following detailed description when read in conjunction with the accompanying drawings, in which:

[0017] Fig. 1 is a block diagram of an example of an ad-hoc packet switched wireless communications network including a plurality of nodes employing an embodiment of the present invention;

[0018] Fig. 2 is a block diagram illustrating an example of a node employed in the network shown in Fig. 1;

[0019] Fig. 3 is a diagram illustrating an example of the maximum and secure ranges of an infrastructure device in accordance with an embodiment of the present invention;

[0020] Fig. 4 is a diagram illustrating an example of a network layout with multiple infrastructure devices which have a radio ranges which extend beyond the desired secure area in accordance with an embodiment of the present invention;

[0021] Fig. 5 is a diagram illustrating an example of the secure ranges for each wireless router in Fig. 4 in accordance with an embodiment of the present invention;

[0022] Fig. 6 is a diagram illustrating an example location of several mobile nodes which are within radio range of the wireless network in Fig. 4 in accordance with an embodiment of the present invention; and

[0023] Fig. 7 is a ladder diagram illustrating an example of the flow of messages between devices during the authorization process in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0024] Wireless nodes wishing to obtain access to an enterprise LAN are typically required to authenticate themselves via the IP standard. Although this verifies that the user has the required challenge information, it does not prevent a computer that has been compromised from accessing the network. Due to the wireless interface, a user doesn't have to be inside the building in order to obtain access. Thus, a compromised computer with a wireless interface could be outside a business' secured environment, such as sitting in a

parking lot, and obtain full access to the network services within a business building. Unlike a wired network, the wireless user doesn't need to pass the physical security checks such as a guard desk to obtain building access prior to plugging into the LAN.

[0025] In an embodiment of the present invention, or any other wireless technology which could be extended to add a location measurement (e.g. 802.11), the authentication server can request the wireless routers or access points to take time of flight measurements and report either the time of flight or the calculated distance. The authentication server can then determine if the location of the wireless user is within a defined space, such as a building outline, and the authentication server may reject users that are outside the perimeter.

[0026] Fig. 1 is a block diagram illustrating an example of a wireless communications network 100 employing mobile access nodes, or terminals, according to an embodiment of the present invention. As shown in Fig. 1, network 100 includes a plurality of devices, including access points (101-1 to 101-2), wireless routers (102-1 to 102-n) and mobile nodes (103-1 to 103-n) on the wireless side of the network, and a Network Operations Center 104 on the wired part of the network. Further details of the network 100 and its operation will now be described. For purposes of this discussion, the terms "user terminal" and "mobile node" will be used interchangeably.

[0027] As shown in Fig. 2, each access point 101, wireless routers 102 and mobile node 103 includes at least one transceiver 106 and at least one controller 107. Each transceiver 106 is coupled to an antenna 109 and can transmit and receive data packets over any frequency band, for example, over the 2nd Institutional Scientific Medical (ISM) band.

[0028] The frequency and modulation scheme used by the transceiver 106 however, does not impact the implementation of the mobile access points 101, wireless routers 102, or nodes 103. Each node 101, 102 and 103 further includes a memory 108, such as a random access memory (RAM), that is capable of storing, among other things, routing information pertaining to itself and other nodes in the network 100. Certain nodes, in particular, mobile nodes 103-1 through 103-n, can be coupled to a host device 110, such as a personal computer (PC), personal data assistant (PDA), or any other suitable device for use by a user.

[0029] Each access point 101 and wireless router 102 maintains knowledge of their geographic location. This information may be manually entered, or the devices may include positioning functionality, such as global positioning system (GPS) functionality, differential

navigation functionality, or other positioning functionality such as various triangulation techniques as can be appreciated by one skilled in the art, or as described in U.S. Patent Application Serial No. 09/988,001 referenced above, and in a U.S. Patent Application of Eric A. Whitehill, Serial No. 09/973,799, for "A System And Method For Efficiently Performing Two-Way Ranging To Determine The Location Of A Wireless Node In A Communications Network", filed on October 11, 2001, the entire contents of which being incorporated herein by reference.

[0030] Referring to Fig. 1, each node 101, 102 and 103 can be in communication with the Network Operations Center 104, either directly or via other nodes. The Network Communication Center typically consists of equipment used to configure and manage the wireless network, however, for the purposes of this description, only the Authentication, Authorization and Accounting (AAA) server 105 is shown.

[0031] Coverage graph 112 of Fig. 3 shows an example of a network 100 deployment where a single access point 101 is used to provide wireless coverage to an area, such as an office, bounded by an office perimeter 114. In this example, the range of the transceiver 106 of the access point 101, shown bounded by 116, is greater than the perimeter 114 of the office. This could potentially allow an unauthorized user, located beyond the perimeter 114 but within the bounded area 116, to access the network 100. As part of the configuration of the network 100, however, the maximum radius of the transceiver range of access point 101 which guarantees that the user is physically in the secure space is determined. This range, shown bounded by 118, is subsequently used during the authorization process to determine if a node requesting access is within a network access restrict boundary.

[0032] Coverage graph 120 of Fig. 4 shows an example of a larger network 100 configuration consisting of a single access point 101 and four wireless routers 102-1, 102-2, 102-3 and 102-4. In this example, the range of the transceiver 106 of each wireless router, shown bounded by 116-1, 116-2, 116-3 and 116-4 respectively, is greater than the perimeter 114 of the office, which could potentially allow an unauthorized user to access the network as described in Fig. 3. Therefore, as in Fig. 3, a maximum radius of each transceiver range which guarantees that the user is physically in the secure space is determined and subsequently used during the authorization process as shown in Fig. 5. As described in greater detail below, in each of Figs. 3, 4 and 5, nodes requesting access to the network are first located by the fixed devices 101 and 102 within the network. Location of the requesting

node is determined by measuring a distance at which the requesting node is located from a fixed device, including both wireless routers 102 and access point 101. If the requesting node is located within the secure space 118, access for the node is allowable on the basis of position.

[0033] Due to the placement of the devices in Fig. 4 and 5 however, simply utilizing the distance of a mobile node to a wireless router may be insufficient for determining if the node is in the secure zone of any one wireless router, shown bounded by 118-1, 118-2, 118-3 and 118-4 respectively. As shown in coverage graph 124 of Fig. 6, mobile nodes 103-2 and 103-3 are both beyond the secure space of each fixed device, however, node 103-2 is located within the perimeter 114 and should be allowed access to the network on the basis of position. As described in greater detail below, the distance between each mobile node 103-1, 103-2 and 103-3 and multiple infrastructure devices must be determined to decide if the "absolute location" of a mobile node is within the perimeter 114, as shown in the coverage graph 124 of Fig. 6.

[0034] The ladder diagram 126 of Fig. 7 shows an example of the process flow that occurs for one embodiment of the present invention. Using the coverage graph 124 of Fig. 6 as an example, the process flow of Fig. 7 may be used to accurately locate mobile nodes requesting access and restrict network access based upon improper node location. Referring to Figs. 6 and 7, the restricted access process of the embodiment of the present invention begins when a mobile node, such as node 103-2, powers up and the transceiver 106 of the node chooses a path to an access point 101, such as via the wireless router 102-1. The mobile node 103-2 sends a request to join the wireless network 100 and the wireless router 102-1 passes the message to the access point 101, which in turn passes the message to the Authentication, Authorization and Accounting (AAA) server 105.

[0035] As part of the authentication process, the AAA server 105 sends a message to the access point 101 requesting the range information of the mobile node 103-2, such as the location of the wireless router 102-1, and the distance between wireless router and the mobile device 103-2. The access point 101 receives the message from the AAA server and sends a request to the wireless router 102-1 to determine the distance between the mobile device 103-2 and the wireless router 102-1. The wireless router 102-1 executes a series of measurements, such as time of flight measurements, and determines the requested distance information, which is then sent to the AAA server 105 via the access point 101. The AAA

server then calculates a position for the mobile node 103-2 and determines if the mobile node is within a secure zone 118-1, that is, within a zone in which network access by mobile nodes is allowed.

[0036] If the mobile node 103-2 is not found within the secure zone 118-1 by measurements provided by the wireless router 102-1, the AAA server 105 sends a request for an "absolute position" determination to the access point 101. The access point then requests neighboring wireless routers, such as 102-2, 102-3 and 102-4, to determine the distance between mobile node 103-2 and each wireless router 102-2, 102-3 and/or 102-4 respectively. In addition, the access point 101 may also determine the distance between the mobile node 103-2 and the access point 101. Each wireless router executes a series of measurements, such as time of flight measurements, and determines the requested distance information, which is then sent to the access point 101.

[0037] Upon receiving the additional distance information, the access point 101 calculates the absolute position of the mobile node 103-2 and sends the result to the AAA server 105. The AAA server 105 evaluates the absolute position of the mobile node 103-2 and determines if the mobile node is within the perimeter 114, and if so, sends a response to the original request for access from the wireless router 102-1 to allow the mobile node 103-2 to join the network on the basis of location.

[0038] There can be variations to the process flow in Fig. 7. For example, in another embodiment of the present invention, the AAA server 105 may request an absolute location without previously requesting the range information. The AAA server 105 may perform the calculations to determine if the mobile node 103 is in the secure zone, or it may send the information to an agent and subsequently use the agent's response. In each embodiment, the AAA server requests and receives location information and uses the location information received as part of the decision to provide service to the node.

[0039] In embodiments of the invention described above, security is maintained as the mobile nodes 103 cannot "spoof" the time of flight measurement used, since any attempt at processing the message would only delay the signal's return and effectively cause a greater distance to be calculated. Likewise, the mobile nodes 103 cannot provide an erroneous location since it they never queried for a self-determined location. All location determinations are done by infrastructure devices under control of the network.

[0040] Although only a few exemplary embodiments of the present invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the exemplary embodiments without materially departing from the novel teachings and advantages of this invention. Accordingly, all such modifications are intended to be included within the scope of this invention as defined.

What is claimed is:

1. A method for restricting network access between nodes in an ad-hoc communications network, said nodes being adapted to transmit and receive signals to and from other nodes in said ad-hoc network, the method comprising:

controlling a first node in an ad-hoc communications network to receive a request for network access from a second node and in response, controlling at least one node in said network to calculate a location of said second node; and

controlling said first node to allow said second node to have access to said network if said location of said second node is within a network access restriction boundary.

2. A method as claimed in claim 1, further comprising:

calculating said location of said second node based on at least one of a time of flight calculation, a known location of said first node and a known location of said at least one node.

3. A method as claimed in claim 2, further comprising:

calculating said known location of said first node and said at least one node based on at least one of manual position entry, global positioning, differential navigation and triangulation.

4. A method as claimed in claim 1, wherein said at least one node includes said first node.

5. A method as claimed in claim 1, further comprising:

controlling said first node to communicate said request for network access to a third node.

6. A method as claimed in claim 5, wherein said third node is coupled to a network operations center.

7. A method as claimed in claim 5, wherein said third node includes an authentication, authorization and accounting server.

8. A method as claimed in claim 5, further comprising:

controlling said third node to communicate to said first node a request for said location calculation of said second node and in response, controlling said first node to calculate said location of said second node and communicate said location to said third node

9. A method as claimed in claim 5, further comprising:

controlling said third node to control said first node to allow said second node to have access to said network if said location of said second node is within said network access restriction boundary.

10. A method as claimed in claim 5, further comprising:

controlling said third node to communicate a request for an absolute location of said second node to said first node of said ad-hoc communications network and in response, controlling said first node to calculate said absolute location and communicate said absolute location to said third node; and

controlling said third node to control said first node to allow said second node to have access to said network if said absolute location of said second node is within said network access restriction boundary.

11. A method as claimed in claim 10, further comprising:

controlling said first node to calculate said absolute location of said second node based on said known location of at least one node of said network and a calculated location of said second node relative to said at least one node.

12. A system, adapted to restrict network access between nodes in an ad-hoc communications network, said nodes being adapted to transmit and receive signals to and from other nodes in said ad-hoc network, the system comprising:

a first node in said ad-hoc communications network, adapted to receive a request for network access from a second node and in response, to calculate a location of said second node; and

said first node being further adapted to allow said second node to have access to said network if said location of said second node is within a network access restriction boundary.

13. A system as claimed in claim 12, wherein:

said first node is further adapted to calculate said location of said second node based on at least one of a time of flight calculation, a known location of said first node and a known location of at least one node.

14. A system as claimed in claim 13, wherein:

said first node is further adapted to calculate said known location of said first node and said at least one node based on at least one of manual position entry, global positioning, differential navigation and triangulation.

15. A system as claimed in claim 12, wherein said at least one node includes said first node.

16. A system as claimed in claim 12, wherein:

said first node is further adapted to communicate said request for network access to a third node.

17. A system as claimed in claim 16, wherein said third node is coupled to a network operations center.

18. A system as claimed in claim 16, wherein said third node includes an authentication, authorization and accounting server.

19. A system as claimed in claim 16, wherein:

said third node is adapted to communicate to said first node a request for said location calculation and in response, said first node is further adapted to calculate said location of said second node and communicate said location to said third node

20. A method as claimed in claim 16, wherein:

said third node is further adapted to control said first node to allow said second node to have access to said network if said location of said second node is within said network access restriction boundary.

21. A method as claimed in claim 16, wherein:

said third node is further adapted to communicate a request for an absolute location of said second node to said first node of said ad-hoc communications network and in response, said first node is further adapted to calculate said absolute location and communicate said absolute location to said third node; and

said third node is further adapted to control said first node to allow said second node to have access to said network if said absolute location of said second node is within said network access restriction boundary.

22. A method as claimed in claim 21, wherein:

said first node is further adapted to calculate said absolute location of said second node based on said known location of at least one node of said network and a calculated location of said second node relative to said at least one node.

23. A computer-readable medium of instructions, adapted to restrict network access between nodes in an ad-hoc communications network, said nodes being adapted to transmit and receive signals to and from other nodes in said ad-hoc network, comprising:

a first set of instructions, adapted to control a first node in said ad-hoc communications network to receive a request for network access from a second node and in response, to calculate a location of said second node; and

a second set of instructions, adapted to control said first node to allow said second node to have access to said network if said location of said second node is within a network access restriction boundary.

24. A computer-readable medium of instructions as claimed in claim 23, wherein:

said first set of instructions is further adapted to control said first node to calculate said location of said second node based on at least one of a time of flight calculation, a known location of said first node and a known location of at least one node.

25. A computer-readable medium of instructions as claimed in claim 24, wherein:

said first set of instructions is further adapted to control said first node to calculate said known location of said first node and said at least one node based on at least one of manual position entry, global positioning, differential navigation and triangulation.

26. A computer-readable medium of instructions as claimed in claim 23, wherein:

said first set of instructions is further adapted to control said first node to communicate said request for network access to a third node.

27. A computer-readable medium of instructions as claimed in claim 26, further comprising:

a third set of instructions, adapted to control said third node to communicate to said first node a request for said location calculation and in response, said first set of instructions is further adapted to control said first node to calculate said location of said second node and communicate said location to said third node

28. A computer-readable medium of instructions as claimed in claim 27, wherein:

said second set of instructions is further adapted to control first node to allow said second node to have access to said network if said location of said second node is within said network access restriction boundary.

29. A computer-readable medium of instructions as claimed in claim 27, wherein:

said third set of instructions is further adapted to control said third node to communicate a request for an absolute location of said second node to said first node of said ad-hoc communications network and in response, said first set of instructions is further adapted to

control said first node to calculate said absolute location and communicate said absolute location to said third node; and

said second set of instructions is further adapted to control first node to allow said second node to have access to said network if said absolute location of said second node is within said network access restriction boundary.

30. A computer-readable medium of instructions as claimed in claim 29, wherein:

said first set of instructions is further adapted to control said first node to calculate said absolute location of said second node based on said known location of at least one node of said network and a calculated location of said second node relative to said at least one node.

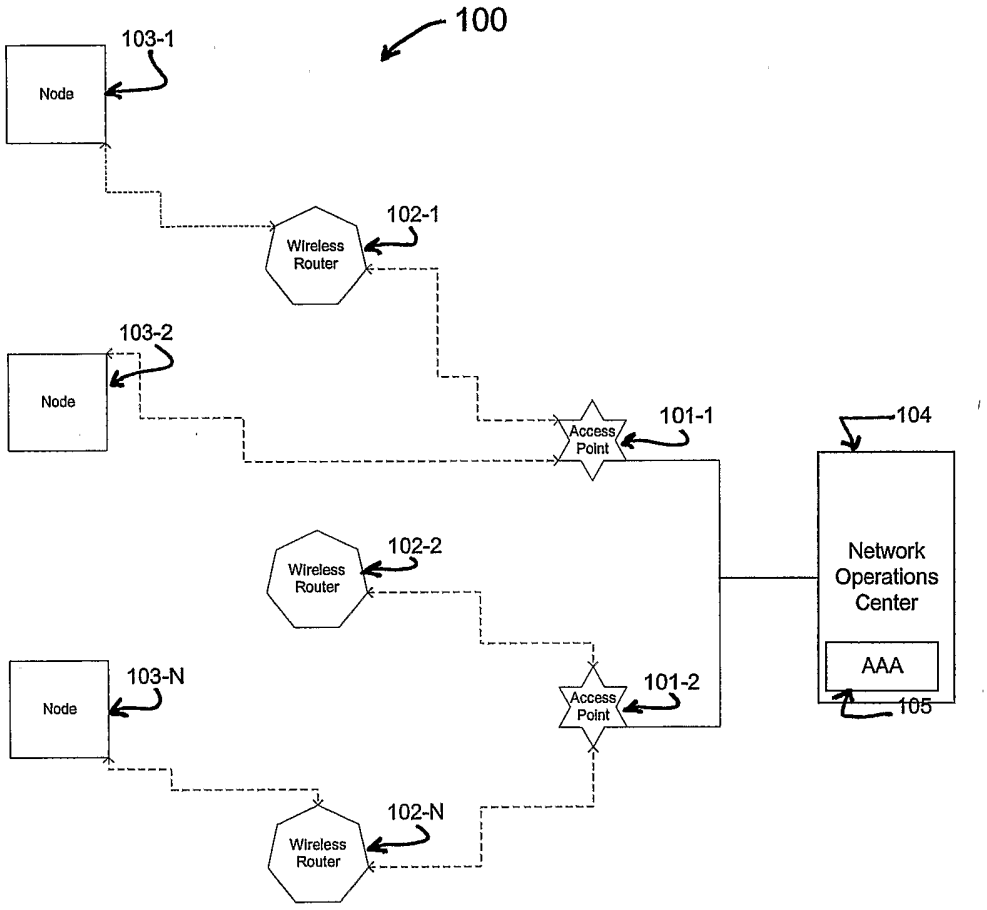

100
103-1
Node
102-1
Wireless Router
103-2
Node
101-1
Access Point
104
Network Operations Center
AAA
105
102-2
Wireless Router
103-N
Node
101-2
Access Point
102-N
Wireless Router

Figure 1

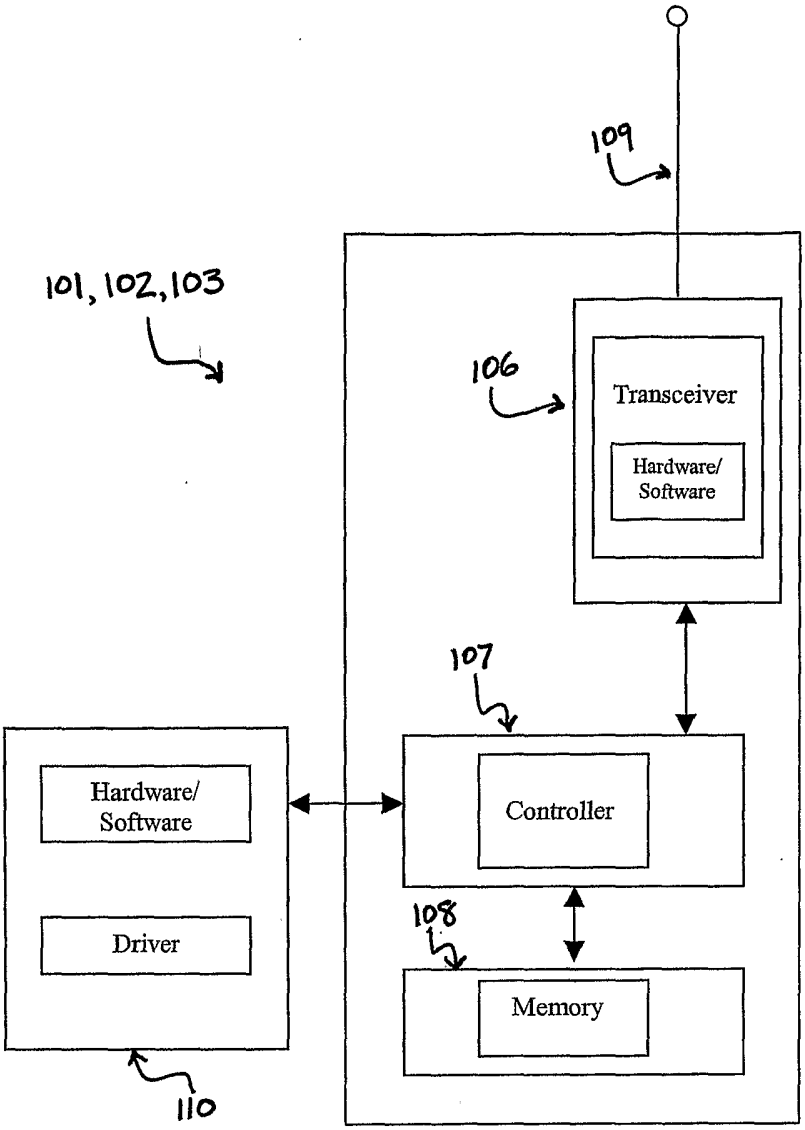

109
101, 102, 103
106
Transceiver
Hardware/
Software
107
Hardware/
Software
Controller
Driver
108
Memory
110

Figure 2

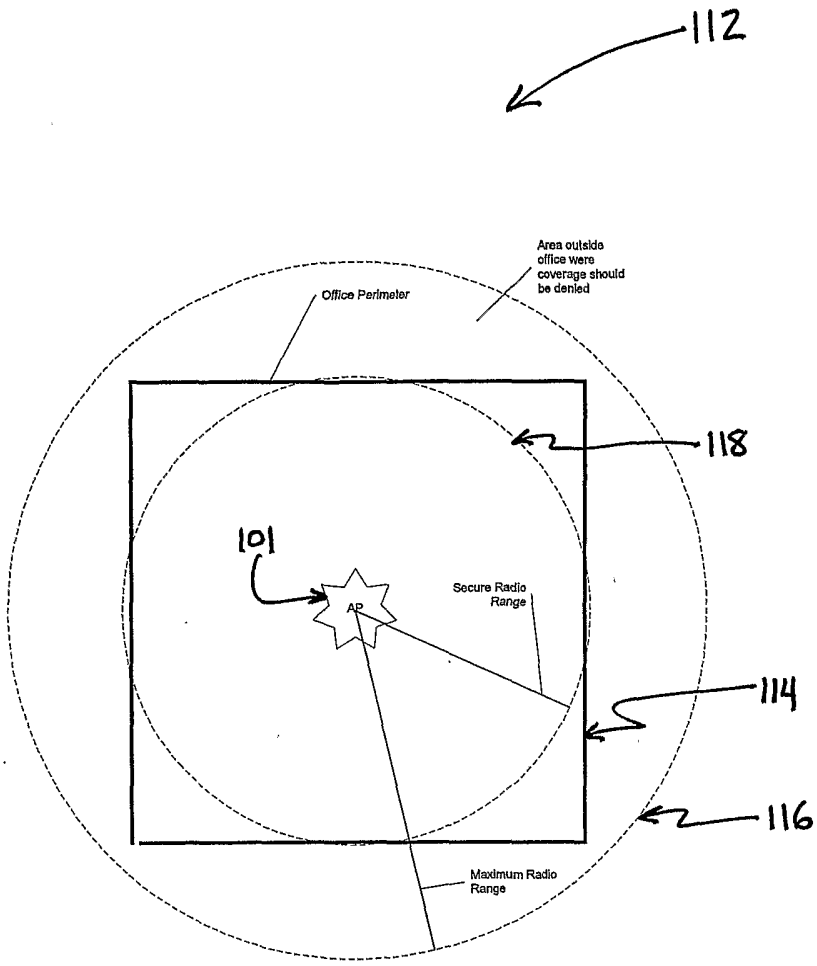

112
Area outside office were coverage should be denied
Office Perimeter
118
101
AP
Secure Radio Range
114
116
Maximum Radio Range

Figure 3

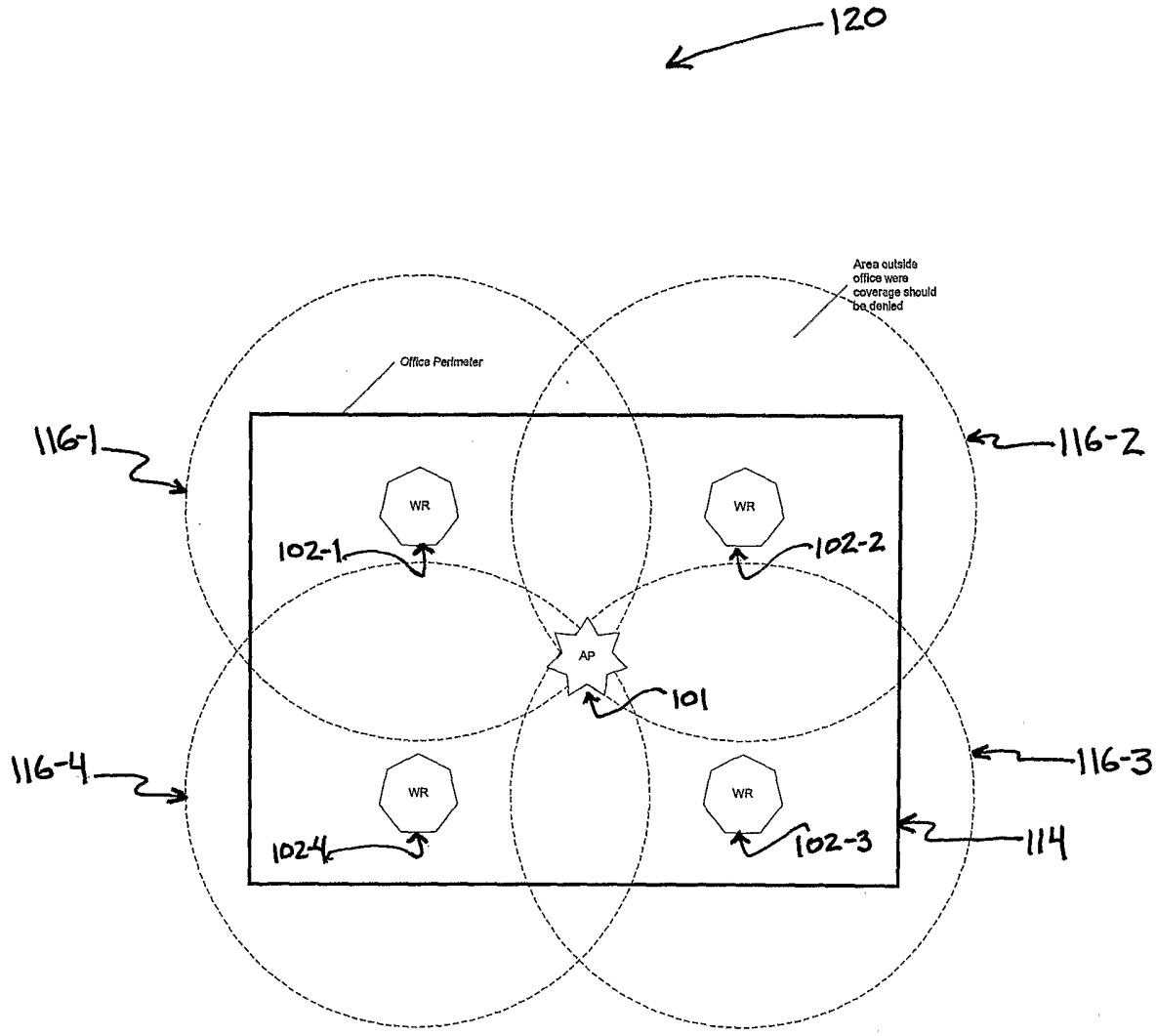

120
Area outside office were coverage should be denied
Office Perimeter
116-1
116-2
WR
WR
102-1
102-2
AP
101
116-4
116-3
WR
WR
102-4
102-3
114

Figure 4

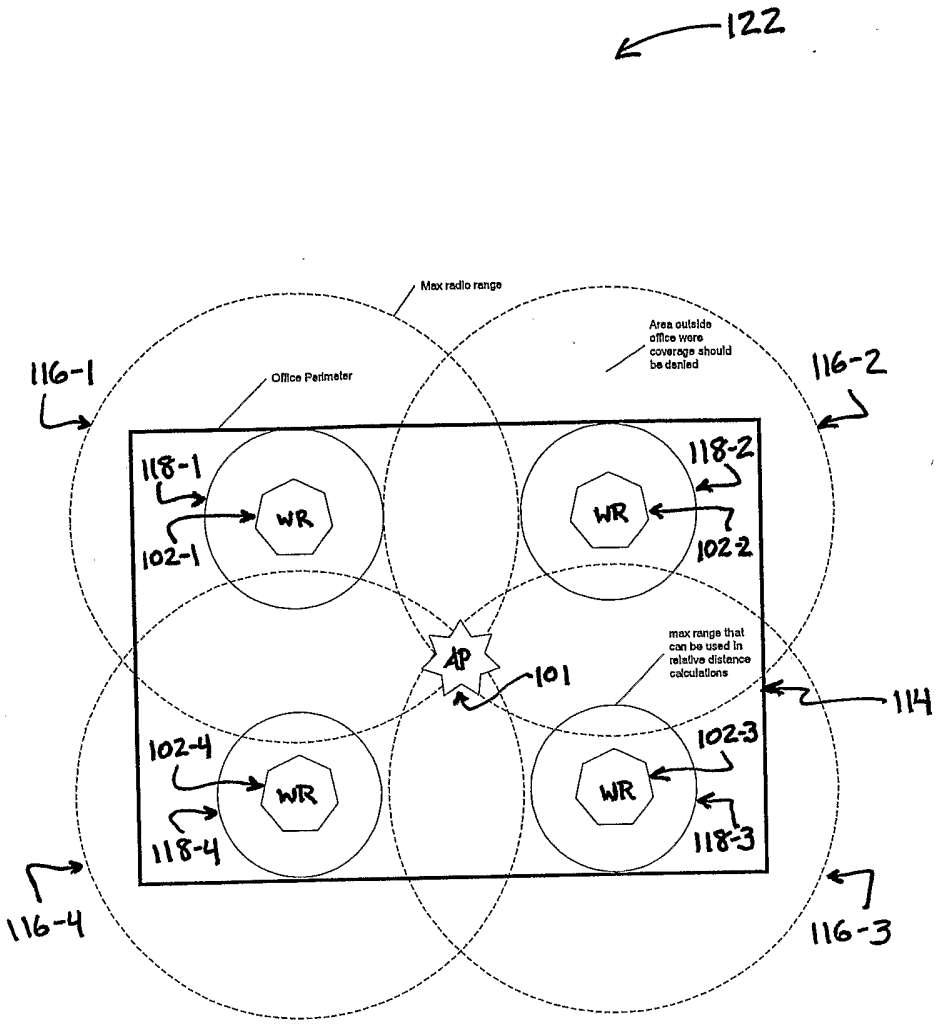

122
Max radio range
Area outside office were coverage should be denied
Office Perimeter
116-1
116-2
118-1
102-1
WR
118-2
102-2
AP
101
max range that can be used in relative distance calculations
114
102-4
118-4
102-3
118-3
116-4
116-3

Figure 5

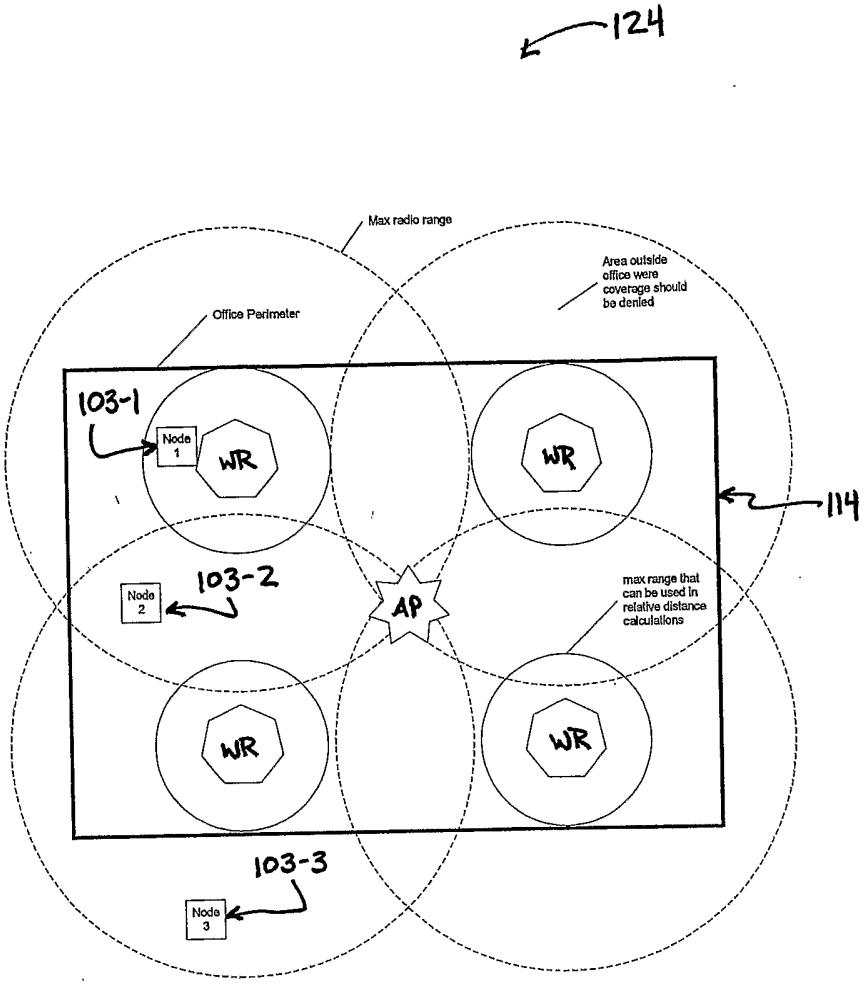

124
Max radio range
Area outside office were coverage should be denied
Office Perimeter
103-1
Node 1
WR
WR
114
Node 2
103-2
AP
max range that can be used in relative distance calculations
WR
WR
103-3
Node 3

Figure 6

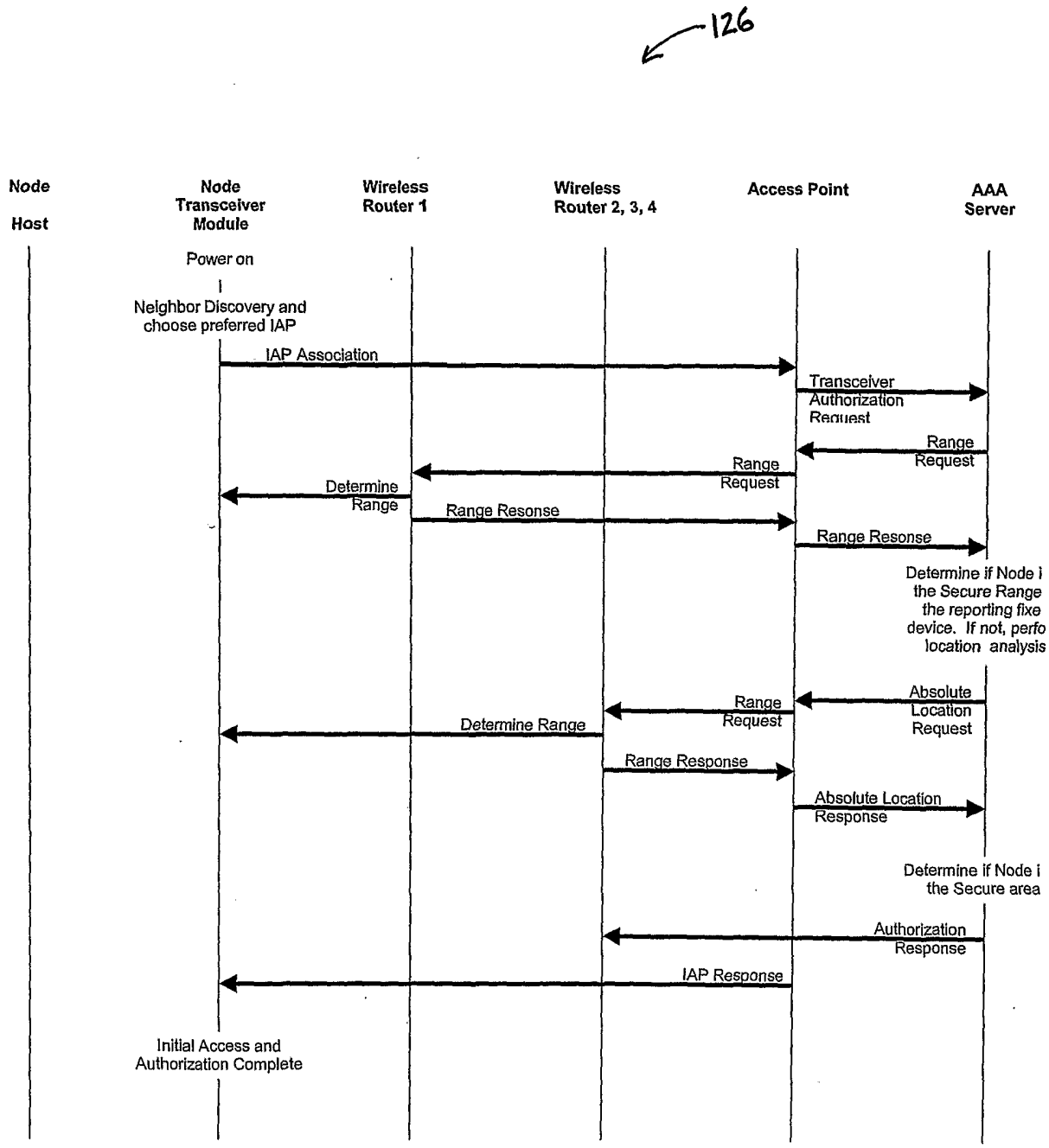

126
Node Host
Node Transceiver Module
Wireless Router 1
Wireless Router 2, 3, 4
Access Point
AAA Server
Power on
Neighbor Discovery and choose preferred IAP
IAP Association
Transceiver Authorization Request
Range Request
Range Request
Determine Range
Range Resonse
Range Resonse
Determine if Node i the Secure Range the reporting fixe device. If not, perfo location analysis
Absolute Location Request
Range Request
Determine Range
Range Response
Absolute Location Response
Determine if Node i the Secure area
Authorization Response
IAP Response
Initial Access and Authorization Complete

Figure 7