

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
9 April 2009 (09.04.2009)

PCT

(10) International Publication Number
WO 2009/045834 A1

(51) International Patent Classification:
H04W 48/04 (2009.01)

(21) International Application Number:
PCT/US2008/077640

(22) International Filing Date:
25 September 2008 (25.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/864,543 28 September 2007 (28.09.2007) US

(71) Applicant (for all designated States except US): **SYMBOL TECHNOLOGIES, INC.** [US/US]; Symbol Technologies, Inc., ATT: Patent Administrator, 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SELLIN, John** [US/US]; 571 Parvin, Milpitas, California 95035 (US). **BAHEL, Alex** [US/US]; 1533 Goody Lane, San Jose, California 95131 (US). **MAAN, Tajinder** [IN/US]; 2816 Croft Drive, San Jose, California 95148 (US). **MALIK, Ajay** [IN/US]; 3480 Granada Avenue #283, Santa Clara, California 95051 (US).

(74) Agent: **GIANNETTA, Michael**; One Motorola Plaza, A-6, Holtsville, New York 11742 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, 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))

[Continued on next page]

(54) Title: **RFID BASED NETWORK ADMISSION CONTROL**

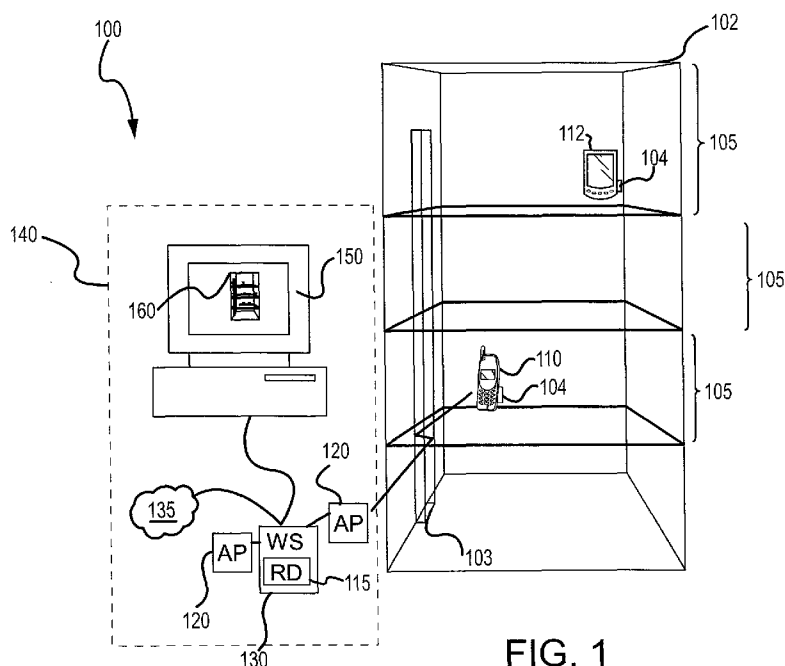


FIG. 1

(57) Abstract: A system for controlling access to a network (135) includes a wireless switch (130) configured for radio frequency communication with a mobile unit (110, 112) associated with a radio frequency identification tag (104). The wireless switch is adapted for determining if a radio frequency identification tag is located within a first area (105), and enabling the mobile unit to access the network according to a first scheme if the mobile unit is located within the first area.

WO 2009/045834 A1



-
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report*
- *with amended claims*

RFID BASED NETWORK ADMISSION CONTROL

FIELD OF THE INVENTION

[0001] The present invention relates generally to radio frequency identification (RFID) systems, wireless local area networks (WLANs), and other such networks incorporating RF tags, and, more particularly, to RFID based network admission control.

BACKGROUND OF THE INVENTION

[0002] In recent years, radio frequency identification (RFID) systems have achieved wide popularity in a number of applications, as they provide a cost-effective way to track the location of a large number of assets in real time. In large-scale applications (e.g., warehouses, retail spaces, and the like), many types of tags may exist in the environment (or "site"). Likewise, multiple types of readers, such as RFID readers, active tag readers, 802.11 tag readers, Zigbee tag readers, and the like are typically distributed throughout the space in the form of entryway readers, conveyer-belt readers, mobile readers, etc., and may be linked by network controller switches and the like.

[0003] In many instances it is desirable to know the location of a tag within a building or other such site. Furthermore, it is desirable to control access to one or more networks associated with the tags, particularly when the information accessed through the network is of a sensitive or proprietary nature.

[0004] Accordingly, it is desirable to provide systems and methods for controlling access to a network based on one or more RFID technologies. Furthermore, other desirable features and characteristics of the present invention will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings and the foregoing technical field and background.

BRIEF SUMMARY OF THE INVENTION

[0005] In one embodiment, by way of example only, a system for controlling access to a network is disclosed. The system includes a wireless switch configured for radio frequency communication with a mobile unit associated with a radio frequency identification tag. The

wireless switch is adapted for determining if a radio frequency identification tag is located within a first area, and enabling the mobile unit to access the network according to a first scheme if the mobile unit is located within the first area.

[0006] In another embodiment, again by way of example only, a method for controlling access to network services includes determining if a radio frequency identification tag is located within a first area, and enabling a mobile unit affiliated with the tag to access the network services according to a first scheme if the mobile unit is located within the first area.

[0007] In still another embodiment, again by way of example only, a system for controlling access to a network includes means for associating a radio frequency identification tag with a mobile unit, means for determining if the radio frequency identification tag is located within a first area, and means for enabling access to the network according to a first scheme if the radio frequency identification tag is within the first area.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The present invention will hereinafter be described in conjunction with the following drawing figures, wherein like numerals denote like elements, and

[0009] FIG. 1 illustrates an exemplary system for controlling access to a network;

[0010] FIG. 2 is an exemplary table of RFID and network related information that may be maintained by a wireless switch; and

[0011] FIG. 3 is a flow chart diagram of an exemplary method for RFID based network admission control.

DETAILED DESCRIPTION OF THE INVENTION

[0012] The following detailed description of the invention is merely exemplary in nature and is not intended to limit the invention or the application and uses of the invention. Furthermore, there is no intention to be bound by any theory presented in the preceding background of the invention or the following detailed description of the invention.

[0013] For simplicity and clarity of illustration, the drawing figures depict the general structure and/or manner of construction of the various embodiments. Descriptions and details of well-known features and techniques may be omitted to avoid unnecessarily obscuring other features. Elements in the drawings figures are not necessarily drawn to

scale: the dimensions of some features may be exaggerated relative to other elements to assist improve understanding of the example embodiments.

[0014] Terms of enumeration such as “first,” “second,” “third,” and the like may be used for distinguishing between similar elements and not necessarily for describing a particular spatial or chronological order. These terms, so used, are interchangeable under appropriate circumstances. The embodiments of the invention described herein are, for example, capable of use in sequences other than those illustrated or otherwise described herein. Unless expressly stated otherwise, “connected” means that one element/node/feature is directly joined to (or directly communicates with) another element/node/feature, and not necessarily mechanically. Likewise, unless expressly stated otherwise, “coupled” means that one element/node/feature is directly or indirectly joined to (or directly or indirectly communicates with) another element/node/feature, and not necessarily mechanically.

[0015] The terms “comprise,” “include,” “have” and any variations thereof are used synonymously to denote non-exclusive inclusion. The terms “left,” “right,” “in,” “out,” “front,” “back,” “up,” “down,” and other such directional terms are used to describe relative positions, not necessarily absolute positions in space. The term “exemplary” is used in the sense of “example,” rather than “ideal.”

[0016] For the sake of brevity, conventional techniques related to signal processing, data transmission, signaling, network control, the 802.11 family of specifications, wireless networks, RFID systems and specifications, and other functional aspects of the system (and the individual operating components of the system) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent example functional relationships and/or physical couplings between the various elements. Many alternative or additional functional relationships or physical connections may be present in a practical embodiment.

[0017] The following description and claimed subject matter generally relate to systems and methods for RFID based network admission control. Specifically, the systems and methods determine if an RFID tag, associated with a mobile unit, is located within an area. In one embodiment, a wireless switch is configured to determine if the RFID tag is located within a specific area. If the RFID tag is determined by the RFID switch to be within the area, the switch may apply a script setting to enable a network admission scheme dedicated to the area for the mobile unit.

[0018] If the mobile unit (and thereby, the RFID tag associated with the mobile unit) is determined to have left the area, the switch may terminate the network admission scheme.

Accordingly, the mobile unit then is denied access to the network. Alternatively, if the mobile unit is determined to have moved to second area having a second dedicated network access scheme, the wireless switch may then enable the second scheme for the mobile unit.

[0019] Referring now to FIG. 1, an example environment 102 useful in describing the present invention generally includes a building or other site (alternatively referred to as an “environment”). Note that while a three-dimensional, multi-floored building is illustrated in FIG. 1, the invention is not so limited. That is, environment 102 may be any two-dimensional or three-dimensional space within or without a building and other structure. Example environments include, for example, single-story buildings, multi-story buildings, school campuses, commercial buildings, warehouses, and like structures.

[0020] A number of RF tags (“RFID tags,” or simply “tags”) 104 are associated with mobile units which are distributed throughout environment 102. In general, these tags 104 may be associated with a variety of mobile units (MUs), such as cellular phones 110, or personal desktop assistants (PDAs) 112 as shown. As one skilled in the art will appreciate, the tags 104 may be associated with the mobile units in a variety of ways. For example, the tags 104 may be physically attached to, or integrated within the mobile units 110 and 112. Tags 104 may be provided within mobile units 110 and 112 at the time of their manufacture.

[0021] In the depicted embodiment, and as described in further detail below, a system 100 includes a wireless switch 130 incorporating or otherwise associated with such devices as a RFID reader 115 (RD) that suitably activates any nearby tags 104 and receives the relevant tag data. The system 100 has access to network services 135, such as the internet, voice over internet protocol (VOIP) services to make phone calls, email, instant messaging, and like services. Additionally, the configuration of system 100 with wireless access points 120 (which may be integrated within or otherwise associated with the wireless switch 130) may establish a wireless local area network (WLAN). The mobile units 110 and 112 may access the WLAN to access the network 135 and thereby, access network 135 services. Various software and hardware (e.g., computer 150, etc.) may also produce a display 160 indicative of the position of a mobile unit 110 or 112 within environment 102 or elsewhere.

[0022] Wireless switch(es) 130 and access point(s) 120 may be positioned throughout environment 102 with a density and number that is appropriate given the power of the WLAN as well as structural details (e.g., internal architecture) of environment 102. That is, WS(s) 130 and/or AP(s) 120 may be distributed evenly throughout the site, or may be associated with predefined “zones.” In the illustrated embodiment, for example, zones 105 are defined for each floor 105, as well as for an elevator bank 103. The mobile units 110

and 112 (and thereby, tags 104) may be located on a particular zone 105. As a user of the mobile units 110 and 112 moves from one zone to another zone, WS 130 and/or RD 115 may monitor the location of an associated tag 104 and apply various script settings to enable a particular network access scheme dedicated to a particular zone 105. If a user leaves a zone 105, the WS 130 and/or RD 115 may determine that the associated tag 104 is not within a particular zone allowing network access, and discontinue access of the associated mobile unit to the network 135 services.

[0023] Tags 104 may be one or more of various types of tags. Examples of tags 104 include, but are not limited to, active tags, passive tags, semi-active tags, WiFi tags, 801.11 tags, and the like RFID tags. Note that the term “RFID” is not meant to limit the invention to any particular type of tag. That is, the term “tag” refers, in general, to any RF element that can be communicated with and has an ID (or “ID signal”) that can be read by another component. In general, RFID tags (sometimes referred to as “transponders”) may be classified as either an active tag, a passive tag, or a semi-active tag. Active tags are devices that incorporate some form of power source (e.g., batteries, capacitors, or the like) and are typically always “on,” while passive tags are tags that are exclusively energized via an RF energy source received from a nearby antenna. Semi-active tags are tags with their own power source, but which are in a standby or inactive mode until they receive a signal from an external RFID reader, whereupon they “wake up” and operate for a time just as though they were active tags. While active tags are more powerful, and exhibit a greater range than passive tags, they also have a shorter lifetime and are significantly more expensive. Such tags are well known in the art, and need not be described in detail herein.

[0024] During operation, each tag 104 may be read by RD 115 when the RD 115 is within a range of the particular tag, as is known in the art. In one embodiment, the data transmitted from each tag 104 is read by RD 115 and provided to WS 130. The data transmitted from tag 104, via RD 115, can then be used to determine the approximate location of the tag 104 and thereby, an associated mobile device 110 or 112.

[0025] RD 115 and/or WS 130 may have multiple associated antennas (not shown), and may incorporate additional functionality, such as filtering, cyclic-redundancy checks (CRC), and tag writing, as is known in the art. Each antenna within RD 115 or WS 130 has an associated RF range (or “read point”), which depends upon, among other things, the strength of the respective antenna. The read point corresponds to the area around the antenna in which a tag 104 may be read by that antenna, and may be defined by a variety of shapes,

depending upon the nature of the antenna. It is not uncommon for RF ranges or read points to overlap in real-world applications (e.g., doorways, small rooms, etc.).

[0026] Switching device 130 (alternatively referred to as an “RF switch,” “WS,” or simply “switch”) may be coupled to a network 135 (e.g., a WiFi network coupled to one or more other networks or devices) and communicate with one or more software applications (not shown). Wireless access ports 120 (alternatively referred to as “access ports” or “APs”) may be configured to wirelessly communicate with RD 115. Access ports 120 suitably communicate with WS 130 via appropriate communication lines (e.g., conventional Ethernet lines, or the like). Any number of additional and/or intervening switches, routers, servers and other network components may also be present in system 100. Additionally, as previously described, an AP 120 may be integrated into WS 130.

[0027] In general, WS 130 determines the destination of the packets it receives and routes those packets to the appropriate AP 120. Thus, each AP 120 acts primarily as a conduit, sending/receiving RF transmissions via RF switches 130, and sending/receiving packets via a network protocol with WS 130.

[0028] WS 130 may support any number of tags that use wireless data communication protocols, techniques, or methodologies, including, without limitation: RF; IrDA (infrared); Bluetooth; ZigBee (and other variants of the IEEE 802.15 protocol); IEEE 802.11 (any variation); IEEE 802.16 (WiMAX or any other variation); Direct Sequence Spread Spectrum; Frequency Hopping Spread Spectrum; cellular/wireless/cordless telecommunication protocols; wireless home network communication protocols; paging network protocols; magnetic induction; satellite data communication protocols; wireless hospital or health care facility network protocols such as those operating in the WMTS bands; GPRS; and proprietary wireless data communication protocols such as variants of Wireless USB. As described in further detail below, WS 130 includes hardware, software, and/or firmware capable of carrying out the functions described herein. Thus, WS 130 may comprise one or more processors accompanied by storage units, displays, input/output devices, an operating system, database management software, networking software, and the like. Such systems are well known in the art, and need not be described in detail. WS 130 may be configured as a general purpose computer, a network switch, or any other such network host. In a preferred embodiment, WS 130 is modeled on a network switch architecture but includes RF network controller software (or “module”) whose capabilities include, among other things, the ability to allow it to configure and monitor RD 115 and its antenna(s).

[0029] Locationing of a tag 104 (and thereby, a mobile device 110 and 112) generally involves examining all of the data from one or more RFID tags 104 at a particular time, and then using rules and a locationing algorithm to determine the most likely location of the RFID tag(s) 104 associated with the tag data. In accordance with one embodiment, system 100 is configured to reconcile the location an associated mobile device 110 or 112 based on a pre-defined floor map (i.e., a map of the location of RFID tags 104) and/or a zone map, and produce a graphical representation indicating the position of the mobile devices 110 and 112 within environment 102. This information may be transmitted to a base station 140 (e.g., control center, etc.) through network 135. Any such map and zone information may be preloaded, downloaded over network 135, or received from environment 102. Stated another way, the IDs for each tag 104, and their respective locations, are preferably known prior to beginning the locationing process; however, this knowledge may be distributed over a number of systems and networks. In a particular embodiment, the placement of each RFID tag 104 is predefined, and nomenclature related to that placement is embedded within each RFID tag 104 so that a quick understanding of the floor and/or zone can be determined without the use of drawings.

[0030] The following example may be useful in understanding the operation of system 100, wherein a mobile device 110 or 112 is a WiFi-enabled laptop computer, a cellular telephone, a PDA, a Palm' Handheld, or other similar device. Here, as mobile device 110 is transported (e.g., by a conveyor belt, a person, a motor vehicle, etc.) through environment 102, RD 115 reads data from each RFID tag 104 that RD 115 comes within range of. RD 115 then transmits the tag data (via WS 130) to computer 150 and is represented on display 160. That is, the location a mobile device 110 may be known in real-time as RFID reader 110 is transported through environment 102.

[0031] In one embodiment, a media access control (MAC) address of the mobile unit 110 or 112 may be associated with a particular tag 104. If the RD 115 and WS 130 determine that the particular tag 104 is located within a predefined zone, then the WS 130 may apply a settings script to implement a particular network access scheme dedicated to the particular zone.

[0032] Turning to FIG. 2, an exemplary table 200 of RFID and network related information is depicted. This information may be maintained and stored by WS 130 on system 100 or elsewhere. Table 200 affiliates such information as a MAC address of a particular mobile unit with a particular tag associated with the mobile unit. As one skilled in the art will appreciate, each mobile unit with the capability to access a WLAN or other

network resources has certain characteristics associated with it that may be stored and maintained. These characteristics may then be then associated with a particular tag which is integrated into or otherwise associated with the mobile device. Table 200 includes an internet protocol address (IP) 210 of a particular mobile unit, a domain name server (DNS) address 220 of the mobile unit, a MAC address 230 of the mobile unit, a network interface card (NIC) type 240 affiliated with the mobile unit, and the respective operating system 250 of the mobile unit.

[0033] Table 200 then shows the respective RFID tag 260 associated with the mobile unit, the source 270 of the tag information, a unique tag identification number (TIN) 280, and the tag time and date 290. Each of these characteristics may be monitored, stored and updated by such devices as a WS. By linking a characteristic of a mobile unit such as a MAC address with a tag associated with the mobile unit, a degree of security may be maintained such that access to network resources (by the mobile unit accessing resources over the WLAN, for example) is limited by virtue of where the mobile unit is in an environment. For example, an employee may be allowed access to the network to access email messages or make international phone calls over the company's voice over internet protocol (VOIP) system as long as the employee (the mobile device) is located within the building. The employee may be granted additional access to network resources if the employee is located in the building's data center and the employee (mobile unit) has further authenticated itself to the network.

[0034] FIG. 3 illustrates a flow chart of an exemplary method 300 of RFID based network admission control. The method 300 begins (step 302) with the affiliation of various locations (or zones, areas, etc.) with a predetermined level of access. This predetermined level of access may be referred to as a "scheme." A particular scheme may allow certain kinds of access to network resources. For example, a first scheme may grant access to the network for email applications and international phone calls as previously described. Another scheme may grant access to a database located on a datacenter mainframe. Each of these schemes may be dedicated to a certain location, zone or area within the environment.

[0035] A MAC address of a mobile unit is then associated with a particular tag (step 306). The association of MAC address with mobile unit may be stored and/or maintained in the WS or elsewhere. The WS may later refer to the table of associated MAC addresses with tags to identify which mobile unit to provide a particular scheme.

[0036] Once the MAC address is associated, the mobile unit monitored throughout the environment. Using the methods described previously, the location of a tag (and thereby, a

mobile unit) is determined (step 308). Again the location may be determined by use of a RD associated with a WS. If it is determined that the tag is in a first location (step 310) such as a cubicle in the office environment, the WS may then allow access to email pursuant to a first scheme (step 312). If the tag is determined to be in a second location, such as a particular floor within the environment, the WS then allows access to the network resources for international calls and email pursuant to a second scheme (step 316). If either the result of queries 310 or 314 are affirmative, once the scheme is implemented, the method returns to the query 310 as the mobile device is continuously monitored in the environment.

[0037] If the tag is determined to not be in a first or second location, but in a third location, such as in the company's datacenter room (step 318), then the method may allow a limited amount of access to the network for a user on the mobile unit to authenticate the device further to the WS or other network resource (step 320). The limited amount of access may be pursuant to a graduated, third scheme. The user may use a biometric authentication, such as a fingerprint scan on the mobile device, which is sent over the WLAN to the WS (or other component in the system) and analyzed for authenticity. In another embodiment, the authentication may be a password.

[0038] If the mobile unit successfully authenticates (step 328), then the WS allows the mobile unit access to a greater degree of network services, such as access to the database previously described. Again, once the larger degree of access is authorized, the method returns to step 310 to continue to monitor the location of the mobile unit. If the mobile unit is unable to authenticate itself (step 330), then the WS refuses or terminates access to the network services (step 330) and generates a notification to an administrator, such as an alarm (step 332). The system may prevent the boot of the mobile device, or the boot of a related device in the third location, for example. The system may disable the mobile device so that the mobile device is no longer operational. In one embodiment, while method 300 is operational, a display of the location of the mobile unit may be rendered on a remote computer (e.g., display 160, FIG. 2) so as to continually monitor the location of approved mobile units within the environment. The method 300 then ends (step 324).

[0039] The systems and methods described provide an efficient and effective way to leverage RFID technology to regulate network access. While at least one exemplary embodiment has been presented in the foregoing detailed description of the invention, it should be appreciated that a vast number of variations exist. It should also be appreciated that the exemplary embodiment or exemplary embodiments are only examples, and are not intended to limit the scope, applicability, or configuration of the invention in any way.

Rather, the foregoing detailed description will provide those skilled in the art with a convenient road map for implementing an exemplary embodiment of the invention, it being understood that various changes may be made in the function and arrangement of elements described in an exemplary embodiment without departing from the scope of the invention as set forth in the appended claims and their legal equivalents.

CLAIMS

We claim:

1. A system for controlling access to a network, comprising:
a wireless switch configured for radio frequency communication with a mobile unit associated with a radio frequency identification tag, the wireless switch adapted for:
determining if a radio frequency identification tag is located within a first area, and
enabling the mobile unit to access the network according to a first scheme if the mobile unit is located within the first area.
2. The system of claim 1, wherein the wireless switch is further adapted for monitoring the radio frequency identification tag to determine if the mobile unit remains located within the first area, and continuing to enable the mobile unit to access the network according to the first scheme while the mobile unit is located within the first area.
3. The system of claim 2, wherein the wireless switch is further adapted for terminating access to the network if the mobile unit is not located within the first area.
4. The system of claim 2, wherein the wireless switch is further adapted for determining if the radio frequency identification tag is located within a second area, and enabling the mobile unit to access the network according to a second scheme if the mobile unit is located within the second area.
5. The system of claim 4, wherein the wireless switch applies a settings script to change the first scheme to the second scheme as the radio frequency identification tag moves from the first area to the second area.
6. The system of claim 1, wherein the wireless switch associates a media access control address of the mobile unit with the radio frequency identification tag.
7. The system of claim 1, wherein the wireless switch is compliant with an 802.11 or WiMAX wide local area network specification.

8. A method for controlling access to network services, the method comprising the steps of:
- determining if a radio frequency identification tag is located within a first area; and
 - enabling a mobile unit affiliated with the tag to access the network services according to a first scheme if the mobile unit is located within the area.
9. The method of claim 8, further comprising the step of monitoring the radio frequency identification tag to determine if the mobile unit remains located within the area, and continuing to enable the mobile unit to access the network services according to the first scheme while the mobile unit is located within the area.
10. The method of claim 8, wherein the first scheme is a graduated access scheme that provides limited access to the network services for the mobile unit to perform an authentication step.
11. The method of claim 10, further including, if the authentication step is validated by the network services, enabling the mobile unit to access the network services according to a second scheme.
12. A system for controlling access to a network, comprising:
- means for associating a radio frequency identification tag with a mobile unit;
 - means for determining if the radio frequency identification tag is located within a first area; and
 - means for enabling access to the network according to a first scheme if the radio frequency identification tag is within the first area.
13. The system of claim 12, further including means for monitoring a location of the mobile unit based on a location of the radio frequency identification tag.
14. The system of claim 13, further including means for continuing to enable access to the network according to the first scheme so long as the location of the mobile unit remains within the first area.

15. The system of claim 12, wherein the first scheme is a graduated access scheme that provides limited access of the network to the mobile unit in order for the mobile unit to perform an authentication step.
16. The system of claim 15, further including, if the mobile unit satisfactorily performs the authentication step, means enabling access to the network according to a second scheme allowing an access level to the network greater than the limited access.
17. The system of claim 12, wherein the means for associating a radio frequency identification tag with a mobile unit is performed using a wireless switch operational on the network.
18. The system of claim 12, wherein the means for associating the radio frequency identification tag with the mobile unit further includes means for associating a media access control address of the mobile unit with the radio frequency identification tag.
19. The system of claim 12, wherein the first scheme further includes means for enabling access to the internet, email, instant messaging, or a wireless local area network.
20. The system of claim 16, further including, if the mobile unit does not satisfactorily perform the authentication step, means for terminating access to the network and enabling an alarm.

**AMENDED CLAIMS received by the International Bureau on 18
February 2009 (18.02.09)**

WHAT IS CLAIMED IS:

1. A system for controlling access to a network, comprising:
a wireless switch configured for radio frequency communication with a mobile unit associated with a radio frequency identification tag, the wireless switch adapted for:
determining if a radio frequency identification tag is located within a first area of the network;
enabling the mobile unit to access network resources of the network according to a first scheme if the mobile unit is located within the first area, the first scheme providing a predetermined level of access to the network resources of the first area;
monitoring the radio frequency identification tag to determine if the mobile unit remains located within the first area; and
continuing to enable the mobile unit to access the network according to the first scheme while the mobile unit is located within the first area.
3. The system of claim 1, wherein the wireless switch is further adapted for terminating access to the network if the mobile unit is not located within the first area.
4. The system of claim 1, wherein the wireless switch is further adapted for determining if the radio frequency identification tag is located within a second area, and enabling the mobile unit to access the network according to a second scheme if the mobile unit is located within the second area.
5. The system of claim 4, wherein the wireless switch applies a settings script to change the first scheme to the second scheme as the radio frequency identification tag moves from the first area to the second area.
6. The system of claim 1, wherein the wireless switch associates a media access control address of the mobile unit with the radio frequency identification tag.

7. The system of claim 1, wherein the wireless switch is compliant with an 802.11 or WiMAX wide local area network specification.

8. A method for controlling access to network services, the method comprising the steps of:

determining if a radio frequency identification tag is located within a first area;
and

enabling a mobile unit affiliated with the tag to access network services of the network according to a first scheme if the mobile unit is located within the area, the first scheme providing a pre-determined level of access to network resources of the first area;

monitoring the radio frequency identification tag to determine if the mobile unit remains located within the area; and

continuing to enable the mobile unit to access the network services according to the first scheme while the mobile unit is located within the area.

10. The method of claim 8, wherein the first scheme is a graduated access scheme that provides limited access to the network services for the mobile unit to perform an authentication step.

11. The method of claim 10, further including, if the authentication step is validated by the network services, enabling the mobile unit to access the network services according to a second scheme.

12. A system for controlling access to a network, comprising:

means for associating a radio frequency identification tag with a mobile unit;

means for determining if the radio frequency identification tag is located within a first area;

means for enabling access to the network according to a first scheme if the radio frequency identification tag is within the first area;

means for monitoring a location of the mobile unit based on a location of the radio frequency identification tag; and

continuing to enable access to the network according to the first scheme so long as the location of the mobile unit remains within the first area.

15. The system of claim 12, wherein the first scheme is a graduated access scheme that provides limited access of the network to the mobile unit in order for the mobile unit to perform an authentication step.

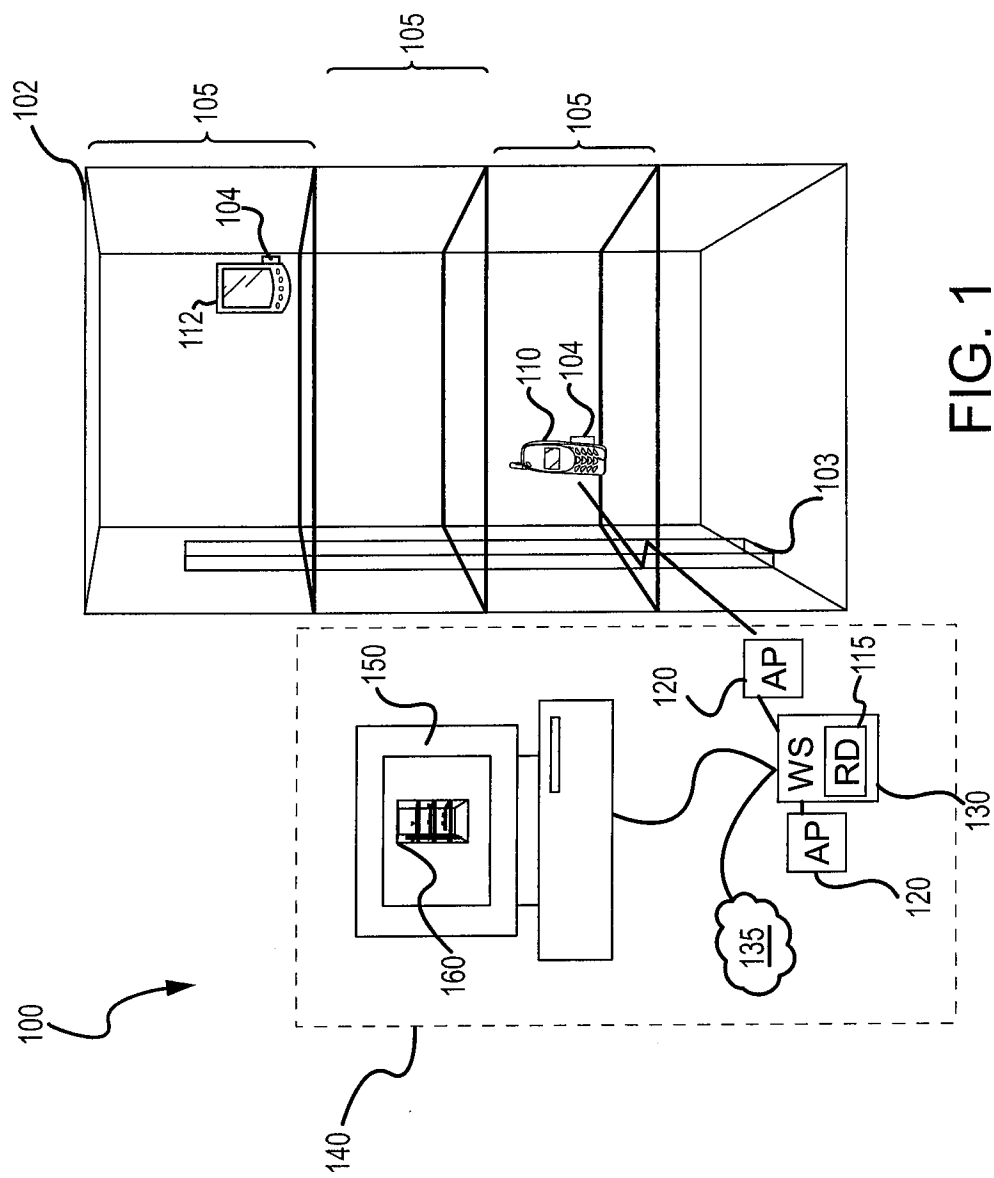
16. The system of claim 15, further including, if the mobile unit satisfactorily performs the authentication step, means enabling access to the network according to a second scheme allowing an access level to the network greater than the limited access.

17. The system of claim 12, wherein the means for associating a radio frequency identification tag with a mobile unit is performed using a wireless switch operational on the network.

18. The system of claim 12, wherein the means for associating the radio frequency identification tag with the mobile unit further includes means for associating a media access control address of the mobile unit with the radio frequency identification tag.

19. The system of claim 12, wherein the first scheme further includes means for enabling access to the internet, email, instant messaging, or a wireless local area network.

20. The system of claim 16, further including, if the mobile unit does not satisfactorily perform the authentication step, means for terminating access to the network and enabling an alarm.



2/3

IP ADDRESS	DNS NAME	MAC ADDRESS	NIC TYPE	SYSTEM	ASSOCIATED RFID TAG	SOURCE	TAG ID	TAG TIME
192.168.1.4	SERVER.SALES.COM	00:50:8D:AF:19:D5	COMP CORP.	LINUX	WIDGET RFID_8633...	BUILT-IN ANT..	0000000F0000005050309	6/9/2007 11:31:14AM
192.168.1.7	EMP1.SALES.COM	00:48:54:13:66:9B	BIT TECH, LTD.	WINDOWS	WIDGET RFID_8633...	BUILT-IN ANT..	0000000D000000334008	6/9/2007 11:31:06AM
192.168.1.33	EMP2.SALES.COM	00:50:83:36:2E:3E	ABC CORP	WINDOWS	WIDGET RFID_8633...	BUILT-IN ANT..	0000000F0000000034223	6/9/2007 11:30:51AM
192.168.1.34	EMP3.SALES.COM	00:90:27:28:84:AC	ABC CORP	WINDOWS	WIDGET RFID_8633...	BUILT-IN ANT..	0000000A00000000B0323	6/9/2007 11:30:44AM
192.168.1.45	EMP4.SALES.COM	00:03:47:22:BF:7C	ABC CORP	WINDOWS	WIDGET RFID_8633...	BUILT-IN ANT..	0000000D000000423323	6/9/2007 11:32:11AM
192.168.1.56	EXEC1.SALES.COM	00:90:27:52:33:24	ABC CORP	WINDOWS	WIDGET RFID_8633...	BUILT-IN ANT..	000000000B32442233	6/9/2007 11:31:14AM
192.168.1.67	EXEC2.SALES.COM	00:CO:B3:9F:AF:56	COMP CORP.	WINDOWS	WIDGET RFID_8633...	BUILT-IN ANT..	0000000A00000000B0324	6/9/2007 11:31:16AM
192.168.1.68	EXEC1.SALES.COM	00:DO:A5:99:33:44	COMP CORP.	LINUX	WIDGET RFID_8633...	BUILT-IN ANT..	0000000A00000000B0325	6/9/2007 11:31:21AM
192.168.1.78	ADMIN.SALES.COM	00:90:27:A8:33:D4	BIT TECH, LTD.	LINUX	WIDGET RFID_8633...	BUILT-IN ANT..	0000000A00000000B0326	6/9/2007 11:31:13AM
192.168.1.79	IT.SALES.COM	00:06:29:77:40:76	BIT TECH, LTD.	LINUX	WIDGET RFID_8633...	BUILT-IN ANT..	0000000A00000000B0327	6/9/2007 11:31:34AM
192.168.1.100	EMP33.SALES.COM	00:33:44:55:66:77	ABC CORP	LINUX	WIDGET RFID_8633...	BUILT-IN ANT..	0000000A00000000B0238	6/9/2007 11:31:33AM
192.168.1.133	EMP10.SALES.COM	00:11:22:33:44:55	BIT TECH, LTD.	LINUX	WIDGET RFID_8633...	BUILT-IN ANT..	0000000A00000000B0329	6/9/2007 11:31:10AM
192.168.1.144	EMP20.SALES.COM	00:33:44:23:A7:A9	ABC CORP	LINUX	WIDGET RFID_8633...	BUILT-IN ANT..	0000000A00000000B0330	6/9/2007 11:31:19AM

FIG.2

200

3/3

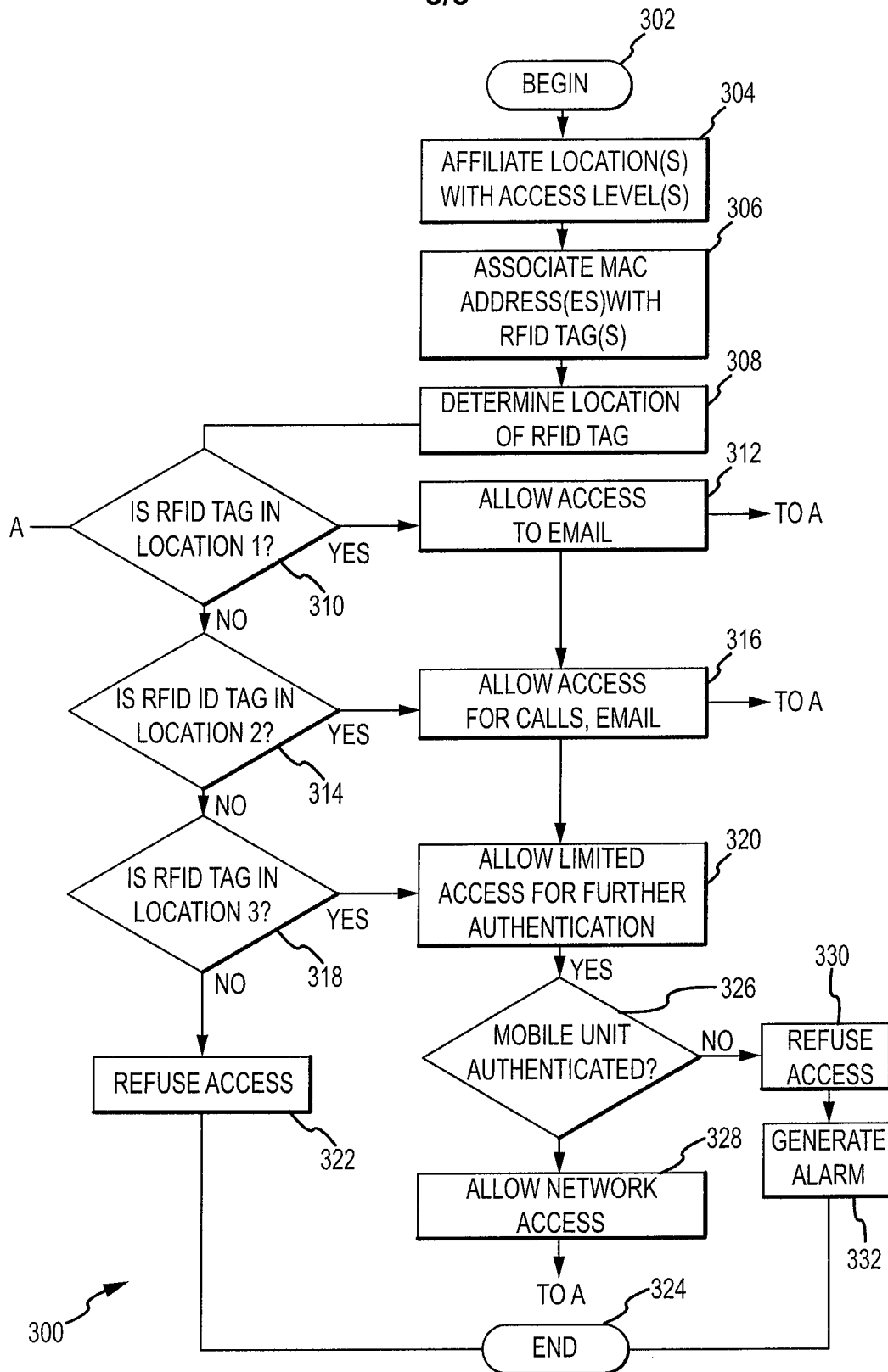


FIG.3

International application No
PCT/US2008/077640

According to International Patent Classification (IPC) or to both national classification and IPC

Minimum documentation searched (classification system followed by classification symbols)
H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/039119 A (SYMBOL TECHNOLOGIES INC [US]; KNOX MICHAEL [US]; BRIDGELALL RAJ [US]) 13 April 2006 (2006-04-13)	1, 8, 12
Y	paragraph [0006] - paragraph [0008] paragraph [0021] paragraph [0037] - paragraph [0045] paragraph [0056] - paragraph [0057] paragraph [0062] - paragraph [0063] paragraph [0067] figures 1, 3-5 ----- -/--	2-7, 9-11, 13-20

☒ See patent family annex.

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of mailing of the international search report

20/01/2009

Authorized officer

Rabe, Marcus

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2008/077640

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/129083 A1 (CREAMER THOMAS E [US] ET AL) 7 June 2007 (2007-06-07). paragraph [0006] - paragraph [0009] paragraph [0016] - paragraph [0024] figure 1 -----	2-7, 9-11, 13-20
A	GB 2 355 889 A (ENDEAVOUR CONSULTING LTD [GB]) 2 May 2001 (2001-05-02) page 4, line 19 - page 8, line 2 figures 1-3 -----	1-20
A	JIN SONG DONG ET AL: "Context Awareness Systems Design and Reasoning" LEVERAGING APPLICATIONS OF FORMAL METHODS, VERIFICATION AND VALIDATION, 2006. ISOLA 2006. SECOND INTERNATIONAL SYMPOSIUM ON, IEEE, PISCATAWAY, NJ, USA, 15 November 2006 (2006-11-15), pages 335-340, XP031237359 ISBN: 978-0-7695-3071-0 paragraph III -----	1,8,12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2008/077640

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006039119 A	13-04-2006	AU 2005292439 A1 CA 2581567 A1 EP 1794951 A1 JP 2008514920 T US 2006107307 A1	13-04-2006 13-04-2006 13-06-2007 08-05-2008 18-05-2006
US 2007129083 A1	07-06-2007	CN 1976532 A KR 20070058313 A	06-06-2007 08-06-2007
GB 2355889 A	02-05-2001	EP 1226732 A1 WO 0131960 A1	31-07-2002 03-05-2001