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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 May 2002 (23.05.2002)

PCT

(10) International Publication Number
WO 02/41661 A2

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/US01/47160

(22) International Filing Date:
5 November 2001 (05.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/707,565 6 November 2000 (06.11.2000) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventors: **CHMAYTELLI, Mazen**; 1752 Linwood Street #G, San Diego, CA 92110 (US). **KHAZAKA, Samir, K.**; 1621 Hotel Circle South #E209, San Diego, CA 92108 (US).

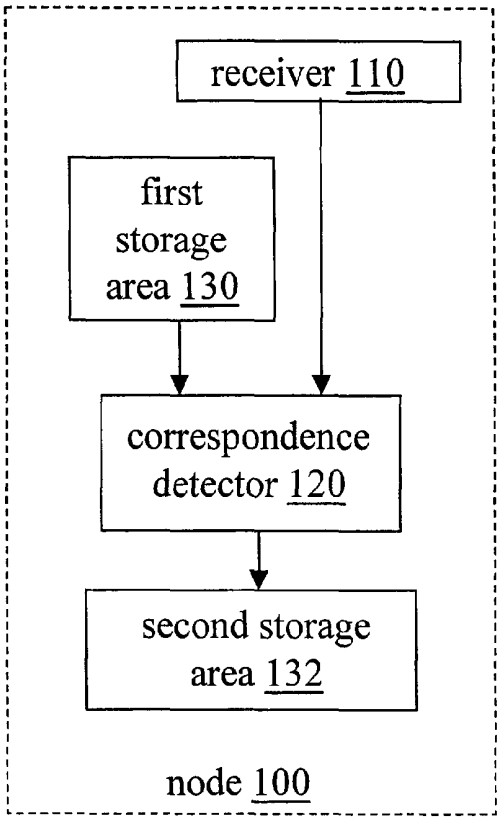
(74) Agents: **WADSWORTH, Philip, R.** et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, 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, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PREVENTING ACCESS TO INFORMATION STORED AT A NODE



(57) Abstract: In one implementation of the present invention, a cellular network for wireless communications (e.g. a cellular telephone network) receives a transmission including an identification token from a mobile unit (e.g. a telephone). Via a service provider, the network also receives a command to prevent access to information stored at the mobile unit. Upon detecting a correspondence between the identification token and the command to prevent access to information stored at the mobile unit, the network instructs the mobile unit to prevent access to local information, which information may include a directory of telephone numbers and other personal and/or confidential items.

WO 02/41661 A2

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.

METHOD AND APPARATUS FOR PREVENTING ACCESS TO INFORMATION STORED AT A NODE

BACKGROUND

Field of the Invention

The present invention relates to communications systems. More particularly, the present invention relates to control of information access.

Background Information

A communications system comprises a communications network and a set of nodes that communicate with the network. The communications links between the network and the nodes may be wired and/or wireless. The network may also communicate with other networks, such that a node may communicate with an entity within the network, with another node connected to the network, and/or with an entity and/or a node on another network.

One example of a communications network is a local-area network (LAN), where the entities within the network may include one or more servers and the individual nodes may include workstations, personal computers, and/or peripheral devices such as storage units and printers. Another example of a communications network is a cellular network for wireless communications, where the entities within the network may include one or more base stations (having base station transceivers or 'BTSs') and administrative units (such as base station controllers (BSCs), mobile services switching centers (MSCs), and home and visitor location registers (HLRs and VLRs, respectively)) and the individual nodes may be mobile units (also called 'mobile stations') that communicate with one or more base stations over a radiolink. A mobile unit may be a cellular telephone, a computer or other processing device connected to a

wireless modem, a wireless local loop (WLL) station, or a wireless personal digital assistant (PDA). Through the base stations, the mobile units may communicate with each other and/or with devices on other networks such as the Internet and/or the public switched telephone network (PSTN).

If a mobile unit such as a cellular telephone is lost or stolen, the owner or account holder may instruct the service provider to reject attempts by the mobile unit to access the network. This action helps to prevent an unauthorized user from incurring usage charges to a service account associated with the unit. However, the mobile unit may contain semiconductor flash random-access memory (or 'flash RAM') that holds confidential information such as telephone numbers. As a consequence of the trend toward combining cellular telephony capabilities with other capabilities (such as e-mail communications, personal organizing, and Web browsing) within the same portable device, the flash RAM may store additional confidential information such as e-mail addresses and messages, voicemail messages, schedules and personal contact information, passwords, and/or banking or credit account numbers. Even though the mobile unit may be refused access to the network if lost or stolen, confidential information stored on the mobile unit may remain accessible to an interloper and subject to abuse.

SUMMARY

In a method according to one embodiment of the invention, a node is instructed to prevent access to information stored at the node. This instructing occurs as a consequence of detecting a correspondence between a command to prevent access to information stored at the node (or at least a portion of such a command) on one hand, and an identifier associated with the node on the other hand.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings, like reference numerals represent similar parts of the present invention throughout the several views and wherein:

FIG. 1 is a block diagram of a communications system according to an embodiment of the invention;

FIG. 2 is an illustration of a command to prevent access to information stored at node 100;

FIG. 3 is a block diagram of a communications system according to an embodiment of the invention;

FIG. 4 illustrates a flowchart of a method according to an embodiment of the invention;

FIG. 5 is a block diagram of a network 150 according to an embodiment of the invention;

FIG. 6 is a block diagram of a cellular network for wireless communications 152 according to an embodiment of the invention;

FIG. 7 is a block diagram of a network 150a according to an embodiment of the invention;

FIG. 8 is a block diagram of a cellular network for wireless communications 152a according to an embodiment of the invention;

FIG. 9 illustrates a flowchart of a method according to an embodiment of the invention;

FIG. 10 is a block diagram of a node 100 according to an embodiment of the invention;

FIG. 11 is a block diagram of a node 102 according to an embodiment of the invention;

FIG. 12 is a block diagram of a node 100a according to an embodiment of the invention;

FIG. 13 illustrates a flowchart of a method according to an embodiment of the invention;

FIG. 14 illustrates a flowchart of a method according to an embodiment of the invention;

FIG. 15 illustrates a flowchart of a method according to an embodiment of the invention; and

FIG. 16 illustrates a flowchart of a method according to an embodiment of the invention.

DETAILED DESCRIPTION

In some systems, a link between a node and a network is transient. In a cellular telephone network or wireless LAN, for example, the link between a mobile unit and the network does not exist when the mobile unit is not powered on. Even after such a link is created, its location and nature with respect to the network may change as the mobile unit moves from within the range of one network terminal (e.g., a base station or a sector thereof) to within the range of another. Therefore, it may not be possible for the network to identify a node connected in this fashion by using only a static location or address.

In other systems, a link between a node and a network may be transient but static. Such a network may include one or more terminals to which nodes may connect on a transient basis. One example includes a personal computer (possibly connected to a LAN) that may communicate with one or more PDAs or similar devices through a serial or parallel port. Although a network terminal that communicates with a node in this manner may be fixed, more than one node may connect to the network through that

terminal (e.g. at different times) and/or a single node may connect to the network through different terminals (e.g. at different times), such that it may not be possible for the network to identify a node by using only a static location or address.

Several important network functions may depend upon an ability of the network to identify or locate a node. Examples of such functions include locating a particular node for paging purposes (e.g., to notify a cellular telephone of an incoming call) and associating an active node with a known identity or profile for purposes such as billing, message forwarding, service differentiation, data synchronization, etc.

An identification token is one mechanism that may be used to identify a node that connects to a network through a transient link. In an example of a system that uses this mechanism, the node stores at least one such token, while the network stores a correspondence between the token and a network identity (in some cases, the network may have assigned the token to the node). During an initial transmission, the node transmits the token to the network over a communications link. The network receives the token, recognizes it, and associates the corresponding network identity with the mobile unit. This association may continue even as the link changes character within the network (e.g. as in a cellular telephone handoff situation). The node–identity association may also undergo subsequent revalidation (e.g. periodically and/or upon specified events).

In a CDMA (code-division multiple access) system for cellular communications that complies with Interim Standard-95B (or 'IS-95B,' entitled "MOBILE STATION–BASE STATION COMPATIBILITY STANDARD FOR DUAL-MODE WIDEBAND SPREAD SPECTRUM CELLULAR SYSTEMS," published by the Telecommunications Industry Association/Electronics Industries Association (TIA/EIA) on February 3, 1999) or with Interim Standard-2000 (or 'IS-2000,' a six-part standard

published by TIA/EIA in July 1999), for example, a mobile unit is programmed to store identity information as a 10-digit mobile identification number (MIN). The MIN includes four digits from the mobile unit's unique electronic serial number (ESN) and six digits from an identification string that is known to the network. The MIN may be stored within the mobile unit in a nonvolatile memory, such as Read-Only Memory ("ROM"), Programmable ROM ("PROM"), Erasable PROM ("EPROM"), and/or Electrically EPROM ("EEPROM") (e.g., flash memory).

Presentation of the MIN (or a portion thereof) by the mobile unit upon communication with the network allows the network to associate the particular mobile unit with a known identity or profile that may contain information concerning service options, billing plan, home area, etc. In an IS-95B- or IS-2000-compliant system, this process is called 'registration.' This association also enables the network to properly route transmissions (such as incoming telephone calls) that are intended to terminate at the mobile unit. Once the node is associated with the known identity or profile, the association may continue even as the link between the node and the network moves from one terminal (e.g., a base station or a sector thereof) to another. At least a portion of the registration process, which may initially take place upon power-up of the mobile unit, may be repeated after the link is established (e.g., periodically and/or upon other events as specified in the TIA/EIA documents referenced above).

FIGURE 1 shows a block diagram of a system according to an embodiment of the invention. Node 100 passes an identification token to network 150 via communications link 140. Over control link 160, network 150 also receives a command to prevent access to information stored at the node. Communications link 140 and/or control link 160 may be conducted through intervening devices and may be wired and/or wireless (i.e. carried over one or more radio and/or optical frequencies). In an

example as shown in FIGURE 2, the command to prevent access to information stored at node 100 includes an operation code (or 'opcode') that corresponds to the command action and an identifier that corresponds to node 100. Upon detecting a correspondence between the identification token and at least a portion of the command (e.g. the identifier), network 150 transmits a command to node 100 to prevent access to local information.

In an exemplary implementation of such a system, as shown in FIGURE 3, network 150 receives the command to prevent access to information stored at node 100 via the public switched telephone network (PSTN). In a particular implementation, the command to prevent access is communicated to network 150 using a Signaling System 7 (SS7) protocol (e.g. as detailed in ITU-T Q.701–Q.741, International Telecommunications Union, Geneva, Switzerland). In one application, the command is communicated to network 150 by a service provider in response to a report from the user that the node has been lost or stolen.

FIGURE 4 illustrates a flowchart for a method according to an embodiment of the invention that may be performed within network 150. In one implementation, a method as shown in FIGURE 4 is performed upon the occurrence of an access request or a registration event as described, for example, in section 6.6.5 ("Registration") of one of the TIA/EIA CDMA standards documents referenced above (e.g., power-up of a mobile unit, timer expiration, or zone change of a mobile unit). In another instance, a method as shown in FIGURE 4 is performed when a node that is not registered attempts to use the network (e.g. to place a telephone call).

In command reception task P110, network 150 receives a command to prevent access to information stored at node 100. As described above, this command may include an operation code and an identifier that corresponds to node 100. In token

reception task P120, network 150 receives an identification token from a node via communications link 140. This token may be received as a part of a transmission such as an access request or a registration request. The identification token includes information from which network 150 may uniquely identify the node and is based on identity information that is stored at the node.

In correspondence detection task P130, network 150 determines a correspondence between the identification token received from node 100 and at least a portion of the command to prevent access to information stored at node 100 (e.g. the identifier). In one embodiment, the decision is based on a correspondence between at least a part of the identification token (e.g., the first six digits of a MIN) and the identifier. As more than one command to prevent access may be pending in network 150, it is possible that task P130 may be repeated to determine a correspondence between the identification token and a portion of another instance of a command to prevent access.

If the determination in task P130 succeeds (e.g., if the identification token and the identifier correspond), then in command transmission task P140 network 150 transmits a command to node 100 to prevent access to local information. If the determination in task P130 fails, then the method may terminate with respect to the token received in task P120, although tasks P120 and P130 may be repeated with respect to other identification tokens.

FIGURE 5 shows a block diagram for a network 150 according to an embodiment of the invention. In an exemplary application of such a network, terminal 210 receives an identification token from node 100 over communications link 140. Control unit 230 receives a command to prevent access to information stored at node 100 over control link 160. From terminal 210, control unit 230 receives the

identification token. Upon detecting a correspondence between the identification token and at least a portion of the command to prevent access, control unit forwards a command to prevent access to local information to terminal 210 for transmission to node 100.

FIGURE 6 shows a block diagram for a cellular network for wireless communications 152 according to an exemplary implementation of network 150. In this implementation, terminal 212 includes one or more base station transceivers (BTSs) 310 that communicate over radio links with mobile units. Control unit 232 includes a base station controller (BSC) 333, which may perform link management functions such as handoff control, and a mobile services switching center (MSC) 336, which communicates with one or more BSCs, administrative units, and/or other networks such as (and/or via) the PSTN to perform higher-level functions such as call setup and management and user authentication.

Although this feature is not explicitly shown in FIGURE 5 or 6, a network as described herein may also be coupled via a communications link to another network such as the Internet. This communications link may include one or more wired connections and/or wireless links such as microwave or satellite links, and information (e.g. a command to prevent access to information stored at node 100) may be transferred across this communications link as one or more analog and/or digital signals.

In a general implementation of an embodiment of the invention, the identification token may be any identifier suitable to identify node 100 to network 150. In one example, the identification token is self-contained, providing all of the information necessary to uniquely characterize node 100 (e.g. a mobile unit's unique ESN). In an alternative implementation, the identification token may provide part of the information necessary for network 150 to uniquely characterize node 100. For a node

that communicates with a CDMA network, for example, the identification token may include all or part of a MIN as described above. In one particular implementation, the identification token comprises the first six digits of the MIN. For a node that communicates with a network compliant with a GSM standard, the identification token may comprise all or part of an identifier such as the mobile unit's current IMSI or TMSI (International or Temporary Mobile Station Identification, respectively) or MSRN (Mobile Station Roaming Number). Other situations and corresponding suitable tokens that are similar to the examples described above are possible with respect to other networks and/or other embodiments or variations of node 100. Note that in certain situations it may be undesirable for a mobile unit such as a cellular telephone to transmit an identification token that includes portions of the ESN (to prevent interception of the ESN by an interloper, for example).

FIGURE 7 shows a block diagram for a network 150a according to an embodiment of the invention. In one implementation of such a network, database 240 receives the identification token from control unit 230 and returns an identifier suitable for comparison with at least a portion of the command to prevent access to information stored at node 100 (e.g. as received via control link 160). In an alternative implementation of such a network, database 240 receives at least a portion of the command to prevent access to information stored at node 100 (e.g. an identifier as illustrated in FIG. 2) and returns an identifier suitable for comparison with the identification token. A network configured in accordance with one of these implementations may have benefits with respect to support for user mobility and/or management of identity-related functions such as security, authentication, billing, etc.

FIGURE 8 shows a block diagram for a cellular network for wireless communications 152a according to a particular implementation of network 150a. In this

implementation, database 242 includes a home location register (HLR) 340 and/or a visitor location register (VLR) 350. HLR 340 stores primary copies of correspondences between identification tokens and identifiers (e.g. for mobile units whose users reside in the geographical vicinity), while VLR 350 stores temporary copies of such correspondences (e.g. for mobile units active in the geographical vicinity whose users may reside elsewhere). In conjunction with one or more of HLR 340 and VLR 350, MSC 336a receives the identification token and obtains a corresponding identifier that is suitable for comparison with an identifier from a command to prevent access (e.g. as received over control link 160). In an alternative implementation, one or both of HLR 340 and VLR 350 may be integrated into MSC 336a.

FIGURE 9 shows a flowchart for a method according to an implementation of a method as shown in FIGURE 3 that may be performed within an implementation of network 150a. In one implementation, a method as shown in FIGURE 9 is performed upon the occurrence of an access request or a registration event as described, for example, in section 6.6.5 ("Registration") of one of the TIA/EIA CDMA standards documents referenced above (e.g., power-up of a mobile unit, timer expiration, or zone change of a mobile unit). In another implementation, a method as shown in FIGURE 9 is performed when a node that is not registered attempts to use the network (e.g. to place a telephone call).

In such an implementation, correspondence detection task P130 includes two subtasks P150 and P160. In lookup subtask P150, a second identifier corresponding to the identification token received in task P120 is obtained (e.g. by referencing a database 240 as described above). In comparison subtask P160, the second identifier is compared with the identifier received in task P110 (as a part of a command to prevent access to information stored at node 100). If a match is detected, then in command

transmission task P140 a command to prevent access to local information is transmitted to node 100. If no match is detected, then the method may terminate with respect to the token received in task P120, although tasks P120 and P130 may be repeated with respect to other identification tokens.

As illustrated in FIGURE 10, a node 100 according to an embodiment of the invention contains a receiver 110 that is configured to receive information from a network 150 over a communications link 140 and is coupled to a correspondence detector 120. First storage area 130, which stores identity information (e.g., a MIN and/or an ESN), is also coupled to correspondence detector 120. Correspondence detector 120 detects a correspondence between a token based on identity information and a string based on information received from network 150. As shown in FIGURE 11, a comparator 122 may be used to implement correspondence detector 120 in an instance 102 of node 100. If a correspondence is detected, access to information in second storage area 132 is prevented. (Note that in an operation of other embodiments of node 100 (e.g. as shown in FIGURE 14), correspondence detector 120 may not be required, in that access to information in second storage area 132 may be prevented based on information received by receiver 110.)

Note that one or both of first storage area 130 and second storage area 132 may be found in a different physical location than another element of node 100. For example, one implementation of node 100 may include a laptop computer connected to a wireless modem. In this case, one or more elements of node 100 may be found within the wireless modem (e.g. receiver 110), while one or both of first storage area 130 and second storage area 132 may be found within the laptop computer (e.g. on the computer's hard disk drive).

FIGURE 12 illustrates an implementation 100a of a node 100 which contains a node transceiver 110a, a processor 120a, and memory 134. Node transceiver 110a includes a transmitter 112 that allows node 100a to transmit information to network 150 over communications link 140. Node transceiver 110a also includes a receiver 114 that allows node 100a to receive information from network 150 over communications link 140. Such transmission and reception operations over communications link 140 may be conducted using the same or different data rates, communications protocols, carrier frequencies, and/or modulation schemes. Likewise, the operations and/or circuit configurations of transmitter 112 and receiver 114, respectively, may be completely independent of one another or, alternatively, may be partially or fully integrated.

Processor 120a, which may comprise one or more microprocessors, microcontrollers, or other arrays of logic elements, controls the operation of node 100a according to a sequence of commands that may be (A) stored in memory 134 or in another storage device within or coupled to node 100a, (B) entered by a user through an interface such as a data entry device (i.e., a keypad) (not shown), and/or (C) received from network 150 over communications link 140.

Memory 134, which may comprise read-only memory (ROM), random-access memory (RAM), and/or nonvolatile memory, stores programmable parameters and may also store information including executable instructions, non-programmable parameters, and/or other data such as telephone numbers, passwords, account numbers, personal contact information, etc. (For example, executable instructions defining a method as illustrated in one or more of FIGURES 13–16 may be stored in memory 134 for execution by processor 120.) Identity information may also be stored in memory 134 and/or may be stored elsewhere within node 100a. In one instance of an operation of an implementation of node 100a, receipt of a command to prevent access to local

information (and determination that the command is directed to node 100a) causes node 100a to prevent access to information stored at area 135 of memory 134.

In an exemplary implementation, node 100 is a mobile unit such as a cellular telephone that communicates with a network 150 over a communications link 140 that complies with one of the CDMA standards referenced above. In another implementation, the communications link 140 complies with a TDMA (time-division multiple access) standard such as GSM (Global System for Mobile Communications, as issued by European Telecommunications Standards Institute (ETSI), Sophie Antipolis, France) or a FDMA (frequency-division multiple access) standard such as the Advanced Mobile Phone System (AMPS). In an alternative implementation, node 100 may receive and transmit information according to the wireless Bluetooth™ protocol (as defined in the Bluetooth Specification, ver 1.0B, published by the Bluetooth Special Interest Group, New York, NY). Note, however, that it is not necessary for communications link 140 to be wireless. In a further implementation, for example, node 100 may comprise a portable device (e.g., a laptop computer or PDA) that establishes a wired but temporary communications link 140 to network 150 by connecting to a terminal (e.g., a data communications port conforming to a standard such as Universal Serial Bus (USB) version 1.1 or 2.0, FireWire (IEEE 1394), or RS-232) of network 150.

FIGURE 13 shows a flowchart for a method according to another embodiment of the invention. Such a method may be performed within a node 100 as described herein. In task P310, a command to prevent access to local information is received (e.g. from a network 150 via a communications link 140). This command may be sent in response to an access request or a registration event as described, for example, in section 6.6.5 ("Registration") of one of the TIA/EIA CDMA standards documents referenced above (e.g., power-up of a mobile unit, timer expiration, or zone change of a

mobile unit). Alternatively, the command to prevent access to local information may be received during a normal use of node 100 (for example, over a dedicated control channel associated with an ongoing cellular telephone call). In various other implementations relating to a cellular telephone or similar network, the command to prevent access to local information may be received over a non-dedicated channel such as a paging channel or broadcast channel.

The command to prevent access to local information includes an identifier that identifies a node (or a specified group of nodes) and may have a form as illustrated in FIGURE 2. As described above, this command may relate to information residing in second storage area 132 of node 100, which may be implemented as a predetermined area 135 of memory 134 on node 100a. In an exemplary implementation, second storage area 132 is nonvolatile (e.g., information is retained in area 132 even after a supply of power is removed).

In task P320, an identification token is retrieved from first storage area 130, which may be implemented in a node 100a as a part of memory 134 or as a separate storage element. In one example, the identification token includes the first six digits of the MIN. In task P330, a correspondence between the identifier and the identification token is determined (e.g. by correspondence detector 120, which may be implemented in a node 100a as processor 120).

If a correspondence is detected in task P330, then in task P340 access to local information (e.g. information stored in second storage area 132, or in area 135 of memory 134) is prevented. Such prevention may be accomplished by one or more of several techniques. For example, the information may be erased (e.g. deleted) or otherwise altered. Such an operation may include overwriting the information.

Alternatively, the area where the information is stored may be altered such that it becomes incapable of storing information.

In another example, access to information may be prevented by altering a mechanism for locating the information. In a storage system that includes an operating system, for example, access to information may be prevented by erasing or otherwise altering directory entries associated with the information. Access to information may also be prevented by altering a stored reference password in a password-protected storage system.

In a further example, access to information may be prevented by erasing or otherwise altering a decoding or decryption mechanism by which the information is transformed into an intelligible or otherwise useful form. For example, a key necessary to decode the stored information (e.g. a string of symbols that is associated with a correspondence between the stored information and an unencrypted form of the stored information) may be erased or otherwise altered.

In one implementation, processor 120 prevents access to the information stored on area 135 of memory 134 by overwriting the information with default data (e.g. zero values). If the determination in task P330 fails, then the method terminates.

FIGURE 14 shows a flowchart for a method according to another embodiment of the invention that may be performed within a node 100 as described herein. In task P315, a command to prevent access to local information is received (e.g. from a network 150 via a communications link 140) over a dedicated channel (for example, a dedicated control channel associated with an ongoing cellular telephone call). This command may be sent subsequently to an access request (e.g. by node 100) or in response to a registration event as described, for example, in section 6.6.5 ("Registration") of one of the TIA/EIA CDMA standards documents referenced above (e.g., power-up of a mobile

unit, timer expiration, or zone change of a mobile unit). In a CDMA system, for example, the dedicated channel may be defined in part by one or more spreading and/or covering codes known to both the transmitter of the command (e.g. network 150) and the receiver of the command (e.g. node 100). By virtue of the establishment of the dedicated channel, a correspondence between the command and a receiving node may already exist, thereby avoiding a need to reestablish such a correspondence and/or to include information identifying the node in the command. In task P340, access to local information (e.g. information stored at node 100 in second storage area 132, or in area 135 of memory 134) is prevented in accordance with the command.

FIGURE 15 illustrates a flowchart for a method 400 according to another embodiment of the invention. In task P340 of this method, access to local information is prevented as described above. In task P332, receipt of a command (as in task P315 described above) or detection of a correspondence (as described in task P330 above) occurs to cause execution of task P340 via logical OR task P480. However, this method also includes an alternate mechanism by which execution of task P340 may be caused (via logical OR task P480).

In the example of FIGURE 15, execution of task P340 may be caused upon the expiration of a timer. According to one example, a timer may be implemented as a location in a memory that is updated (e.g. decremented) periodically until a contents of the memory location reaches a predetermined value (e.g. zero). In task P470, an amount of time remaining is tested to determine whether the predetermined period has expired. In task P450, the amount of time remaining is reset to a start or default value. In another implementation of the method of FIGURE 15, a timer tracks the occurrence of some other event or events (e.g. a number of times that a device is powered up) rather than a passage of time.

A method as shown in FIGURE 15 may be used to provide a limited period of accessibility to local information. Before leaving for a business trip, for example, a user may store information at a node 100 such as a PDA or cellular telephone via synchronization to a fixed computer (e.g. an office desktop or laptop computer). While the information is now portable, it may also become subject to abuse if the node on which it resides is lost or stolen. A method as shown in FIGURE 15 may be used to prevent access to the information after a specified period even if the loss or theft of the node is not discovered.

FIGURE 16 illustrates a flowchart for a method according to another embodiment of the invention. In this method, resetting of the amount of time remaining is performed only after an authentication procedure. A string of symbols is entered (e.g. from a keypad or keyboard of node 100) in task P410. In task P420, a correspondence between the input string and a stored authentication string is tested (e.g. by a comparator). If a correspondence is detected, the amount of time remaining is reset to a start or default value in task P450. Otherwise, the authentication failure is logged in task P430 (e.g. by updating a fail count value). In task P440, the number of failures is compared to a predetermined threshold T. If the threshold is exceeded, execution of task P340 is caused (via logical OR task P480). Otherwise, a further authentication attempt is permitted in task P410. In an alternative implementation, authentication test P420 may include comparing parameters characterizing a user's voice, iris pattern, fingerprint, or one or more other identifying features to stored parameter values. Timing and authentication operations as described herein (e.g. tasks P420, P430, P440, P450, and P470) may be performed by one or more arrays of logic elements such as processor 120a, possibly in combination with other tasks.

The foregoing presentation of the described embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments are possible, and the generic principles presented herein may be applied to other embodiments as well. For example, the invention may be implemented in part or in whole as a hard-wired circuit, as a circuit configuration fabricated into an application-specific integrated circuit, or as a firmware program loaded into non-volatile memory or a software program loaded from or into a data storage medium as machine-readable code, such code being instructions executable by an array of logic elements such as a microprocessor or other digital signal processing unit. Thus, the present invention is not intended to be limited to the embodiments shown above, any particular sequence of instructions, and/or any particular configuration of hardware but rather is to be accorded the widest scope consistent with the principles and novel features disclosed in any fashion herein.

What is Claimed is:

CLAIMS

1. A method of instructing a node to prevent access to information stored at the node, said method comprising:

detecting a correspondence between (1) a first identifier associated with the node and (2) at least a portion of a command to prevent access to information stored at the node; and

consequent to said detecting, instructing the node to prevent access to the information.

2. The method according to claim 1, wherein instructing the node occurs at least in part over a wireless communications link.

3. The method according to claim 1, wherein instructing the node occurs at least in part over a wireless communications link associated with a cellular network for wireless communications.

4. The method according to claim 1, wherein instructing the node is performed by at least a portion of a cellular network for wireless communications.

5. The method according to claim 1, wherein said information includes a list of telephone numbers stored on a device configured and arranged to communicate with a cellular network for wireless communications over a wireless communications link.

6. The method according to claim 1, said method further comprising:

prior to said detecting, receiving a transmission from the node,

wherein the transmission includes an identification token, and

wherein the identification token is associated with the first identifier.

7. The method according to claim 6, wherein receiving a transmission from the node includes receiving a request for access to a cellular network for wireless communications.

8. The method according to claim 6, wherein receiving a transmission from the node includes receiving a registration request directed to a cellular network for wireless communications.

9. The method according to claim 6, wherein said identification token is based at least in part on an identification number assigned to a mobile unit and associated with a cellular network for wireless communications.

10. The method according to claim 6, wherein said identification token is based at least in part on a serial number of the node.

11. The method of claim 1, wherein the command to prevent access to information stored at the node includes a second identifier, and

wherein said detecting a correspondence comprises comparing said first identifier and said second identifier.

12. A method of preventing access to information stored at a node, said method comprising:

transmitting a request from the node to a network;

receiving a response to the request, the response including a command to prevent access to information stored at the node; and

consequently to said receiving a response, preventing access to the information, wherein the request includes an identification token.

13. The method according to claim 12, wherein the network includes a cellular network for wireless communications.

14. The method according to claim 12, wherein the request includes at least one among a request for access to the network and a registration request.

15. The method according to claim 12, wherein the command to prevent access to information stored at the node includes information corresponding to the node.

16. The method according to claim 12, wherein the command to prevent access to information stored at the node includes information corresponding to identity information stored at the node.

17. The method according to claim 12, wherein the command to prevent access to information stored at the node is received at least in part over a wireless communications link.

18. The method according to claim 12, wherein preventing access to the information includes altering the information.

19. The method according to claim 18, wherein said altering the information includes overwriting at least a portion of the information.

20. The method according to claim 12, wherein preventing access to the information includes altering at least one directory entry associated with the information.

21. The method according to claim 12, wherein preventing access to the information includes altering a key, wherein the key is associated with a correspondence between stored and nonencrypted forms of the information.

22. A method of preventing access to information stored at a node, said method comprising:

receiving a command to prevent access to information stored at the node; and

consequent to said receiving, preventing access to the information,

wherein the command to prevent access to information is received at least in part over a wireless communications link to a cellular network for wireless communications.

23. The method according to claim 22, wherein the command includes a first identifier, said method further comprising detecting a correspondence between said first identifier and an identification token stored at the node.

24. The method according to claim 23, wherein said preventing access to the information occurs consequent to said detecting.

25. The method according to claim 22, wherein said preventing access to the information includes altering the information.

26. An apparatus comprising:

a receiver configured and arranged to receive command information over a communications link;

a first storage area configured and arranged to store identity information;

a correspondence detector coupled to said receiver and said first storage area; and

a second storage area,

wherein said correspondence detector is configured and arranged to detect a correspondence between (A) a token based at least in part on the identity information and (B) a string based at least in part on the information received over the communications link, and

wherein access to information in said second storage area is prevented subsequent to a detection by said correspondence detector.

27. The method according to claim 26, wherein said correspondence detector comprises a first comparator.

28. The method according to claim 27, said apparatus further comprising a second comparator configured and arranged to detect a correspondence between an

input string and a stored string, wherein access to information in said second storage area is prevented subsequent to at least one among a detection by said correspondence detector and a detection by said second comparator.

29. The method according to claim 27, said apparatus further comprising a timer, wherein access to information in said second storage area is prevented subsequent to at least one among a detection by a correspondence detector, a detection by said second comparator, and an expiration of said timer.

30. The method according to claim 26, said apparatus further comprising a timer, wherein access to information in said second storage area is prevented subsequent to at least one among a detection by said correspondence detector and an expiration of said timer.

31. An apparatus comprising:

a receiver configured and arranged to receive a command from a cellular network for wireless communications;

a memory, at least a portion of said memory having information; and

a processor configured and arranged to prevent a user from accessing said information in response to said command.

32. The apparatus according to claim 31, said apparatus further comprising a transmitter configured and arranged to transmit a request to the cellular network for wireless communications,

wherein the command is received in response to the request.

33. The method according to claim 32, wherein the request includes at least one among a request for access to the cellular network for wireless communications and a registration request.

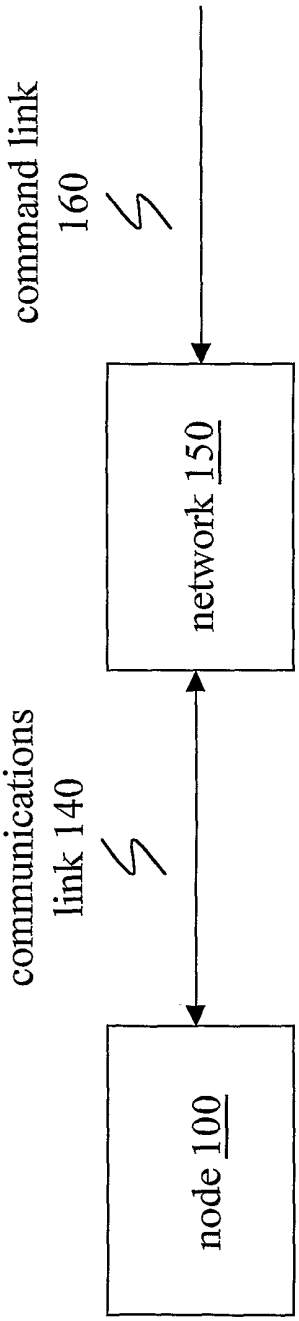

command link
160
network 150
communications
link 140
node 100

FIG. 1

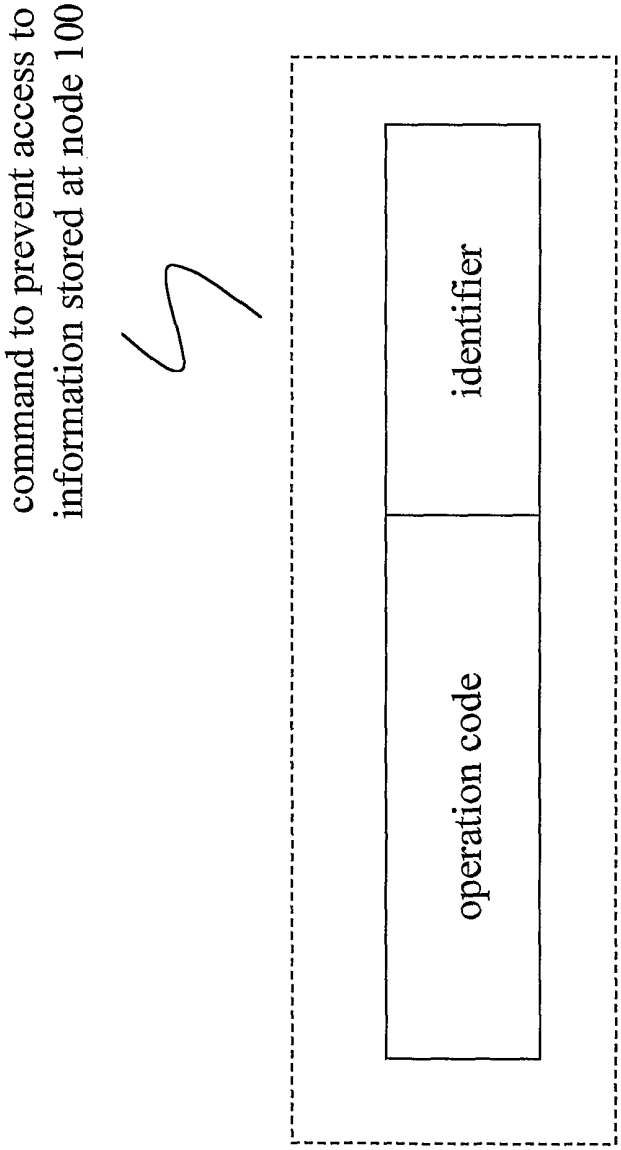

command to prevent access to
information stored at node 100
identifier
operation code

FIG. 2

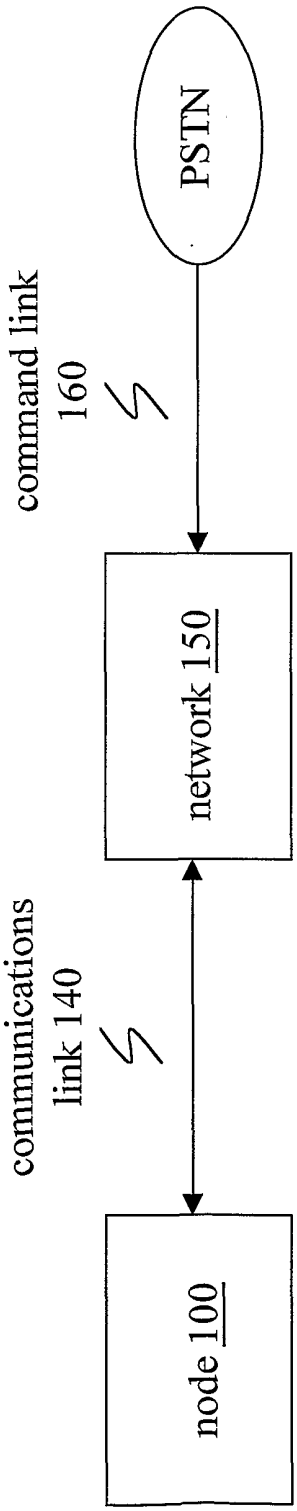

PSTN
command link
160
network 150
communications
link 140
node 100

FIG. 3

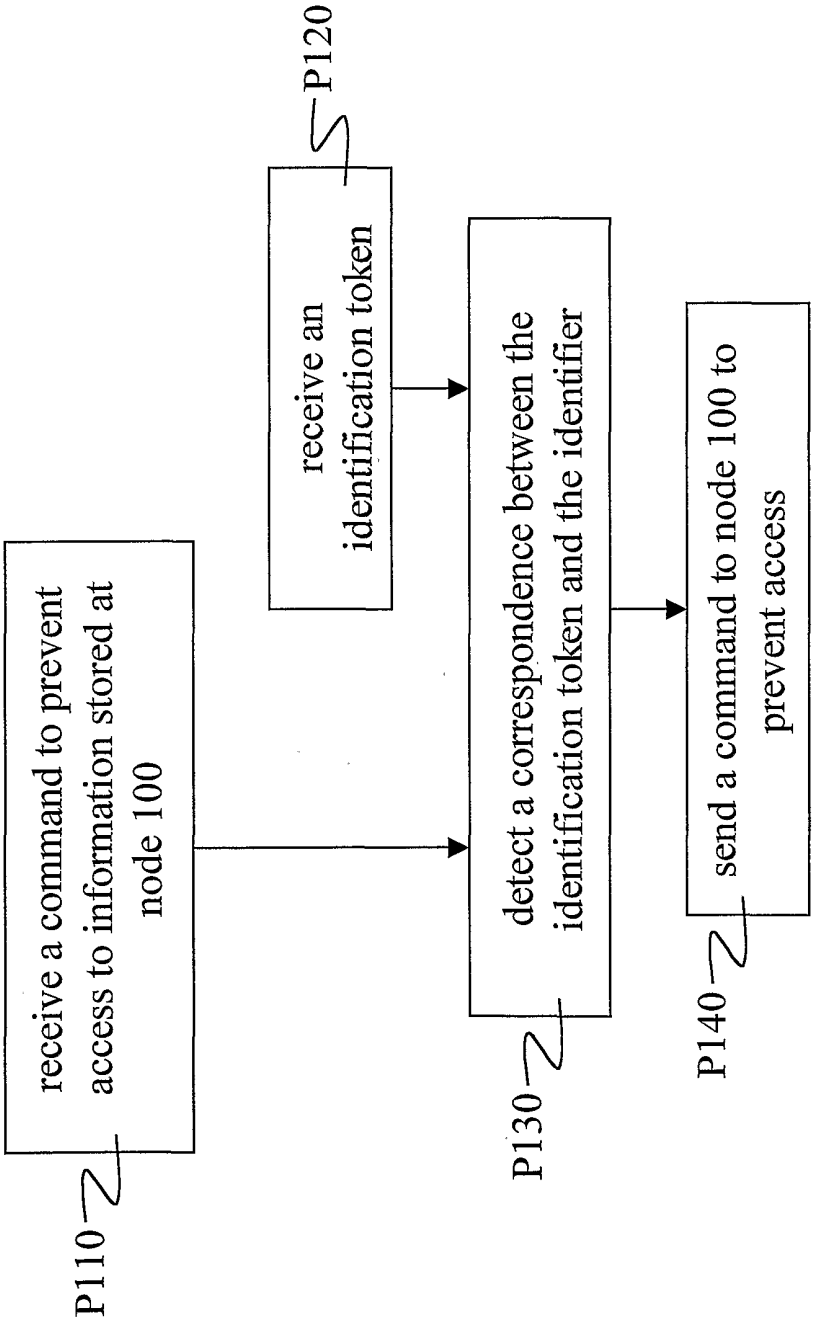

receive a command to prevent access to information stored at node 100
P110
receive an identification token
P120
detect a correspondence between the identification token and the identifier
P130
send a command to node 100 to prevent access
P140

FIG. 4

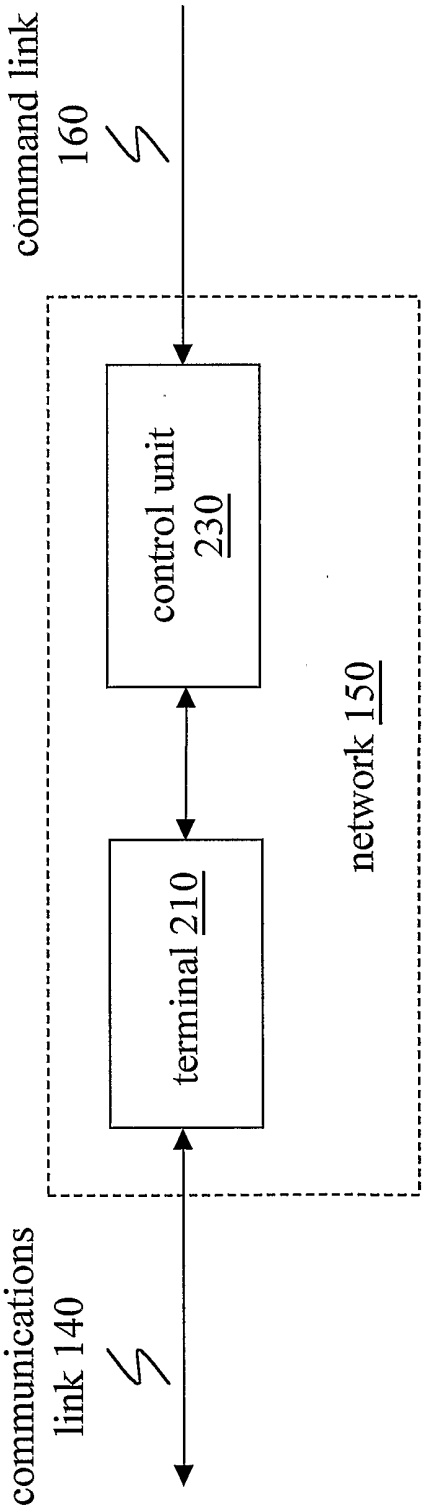

command link
160
control unit
230
network 150
terminal 210
communications
link 140

FIG. 5

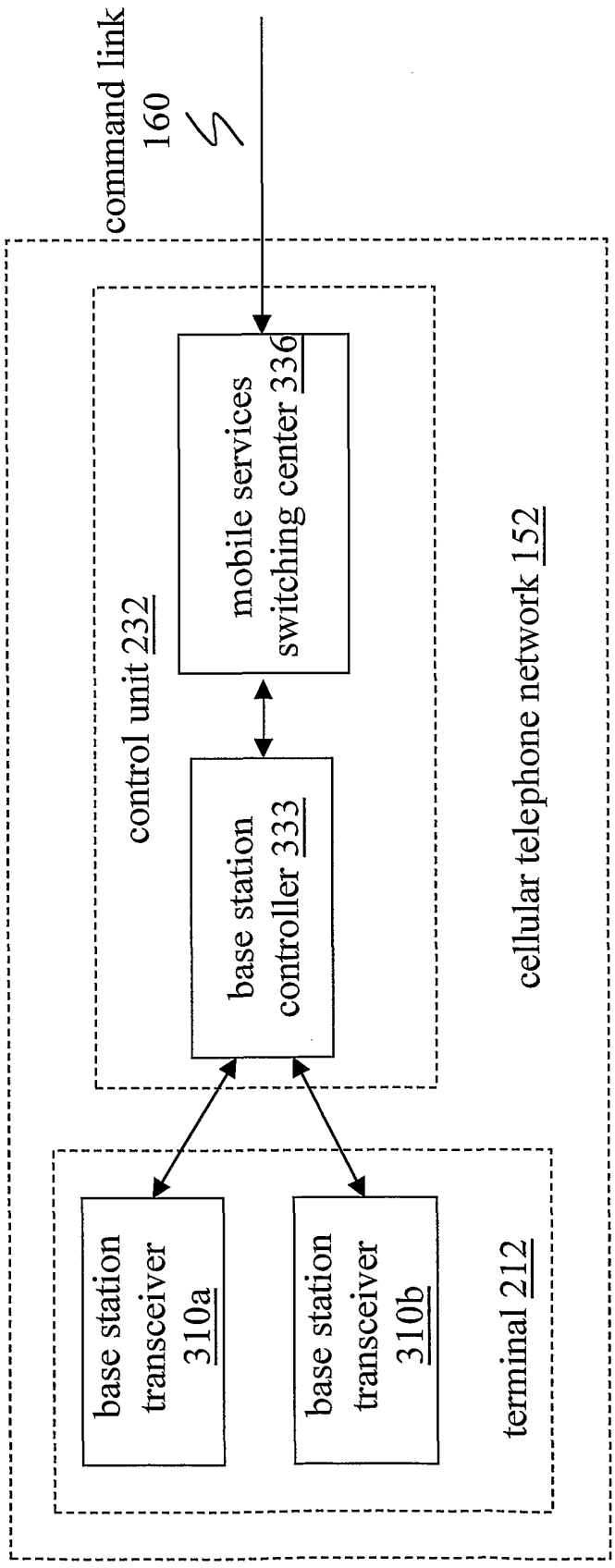

command link
160
mobile services
switching center 336
control unit 232
base station
controller 333
cellular telephone network 152
base station
transceiver
310a
base station
transceiver
310b
terminal 212

FIG. 6

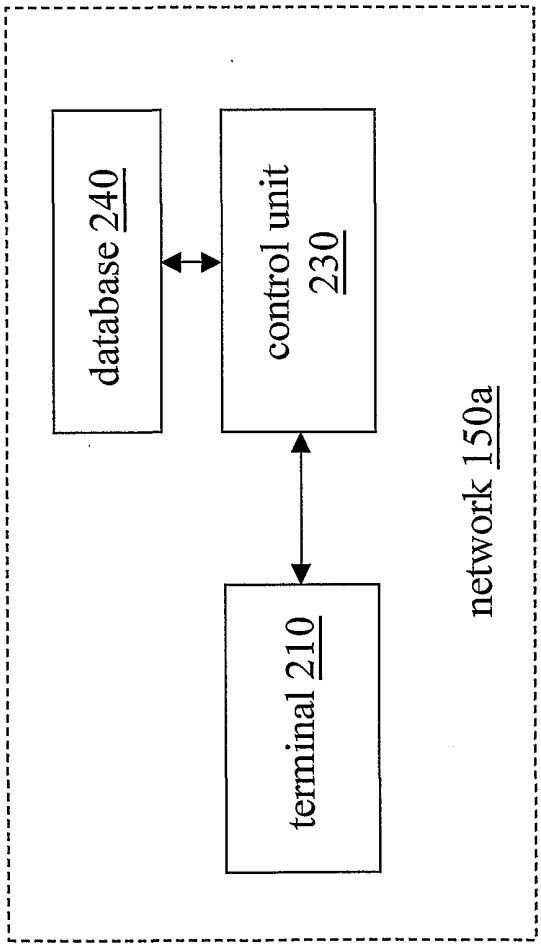


FIG. 7

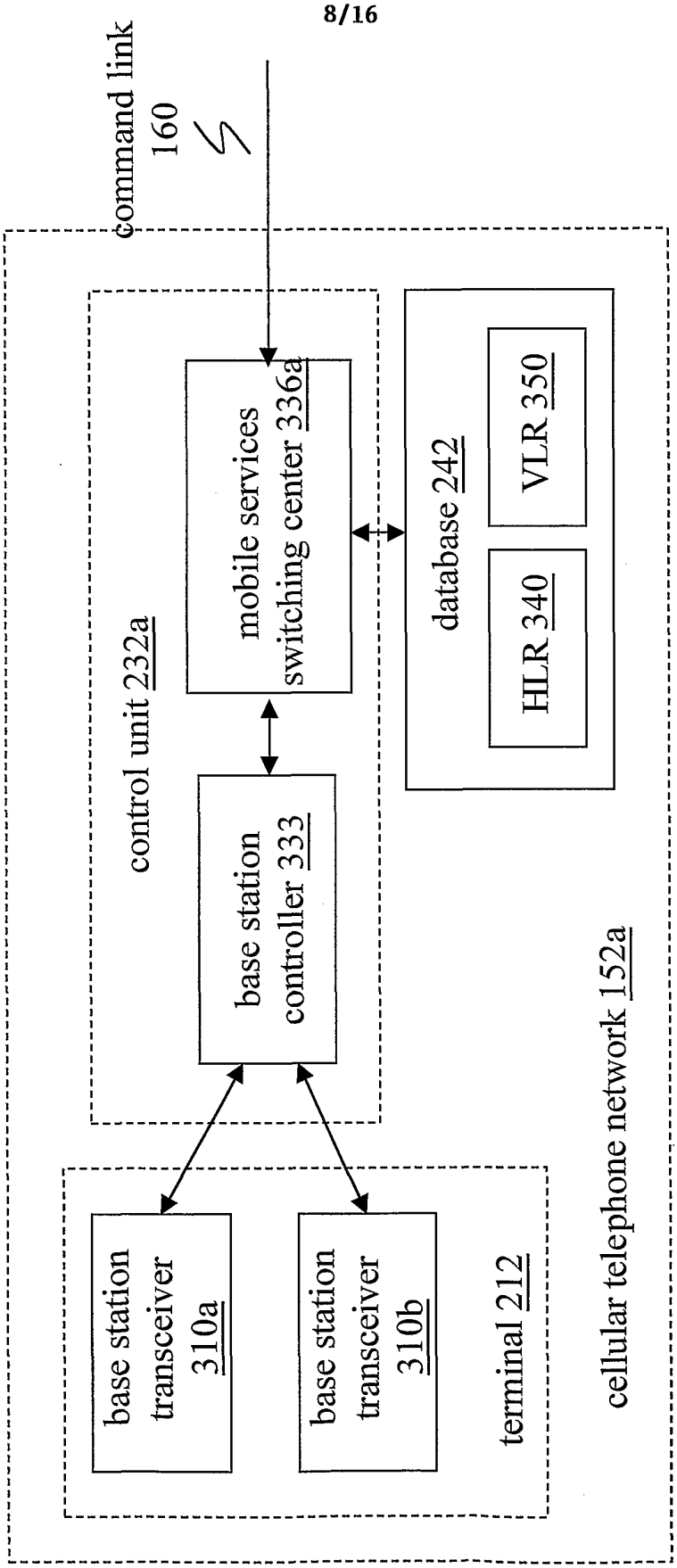

command link 160
cellular telephone network 152a
control unit 232a
mobile services switching center 336a
base station controller 333
database 242
HLR 340
VLR 350
terminal 212
base station transceiver 310a
base station transceiver 310b

FIG. 8

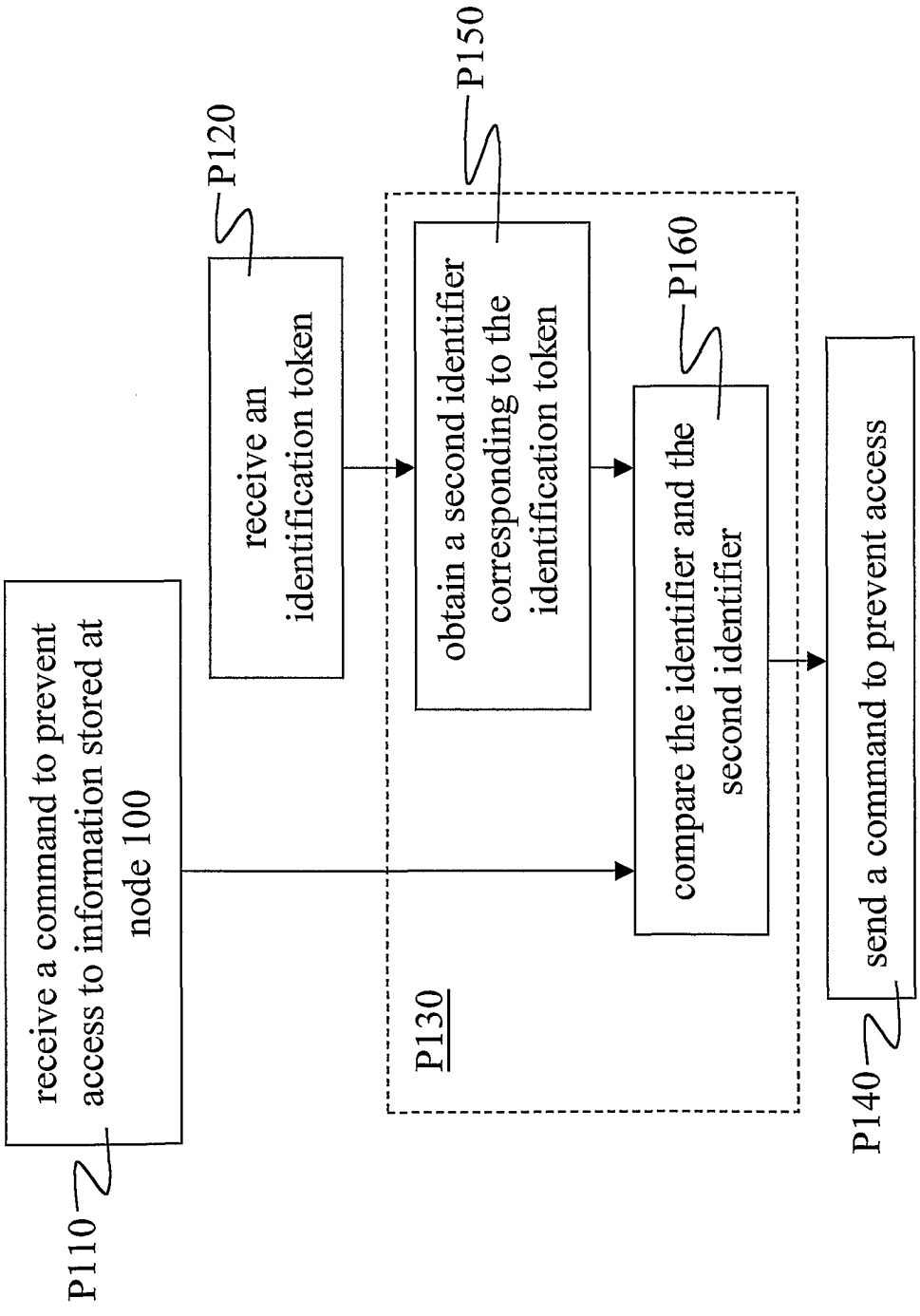

receive a command to prevent access to information stored at node 100
P110
receive an identification token
P120
P130
obtain a second identifier corresponding to the identification token
P150
compare the identifier and the second identifier
P160
send a command to prevent access
P140

FIG. 9

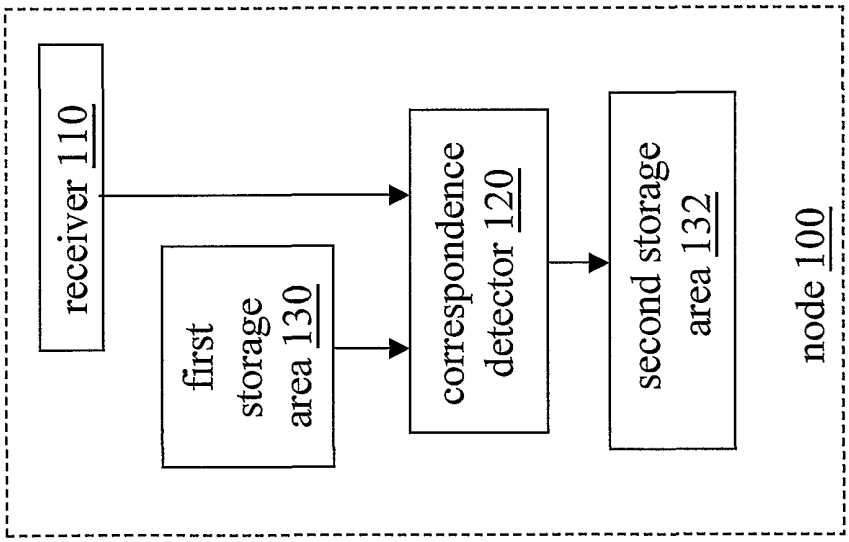

receiver 110
first storage area 130
correspondence detector 120
second storage area 132
node 100

FIG. 10

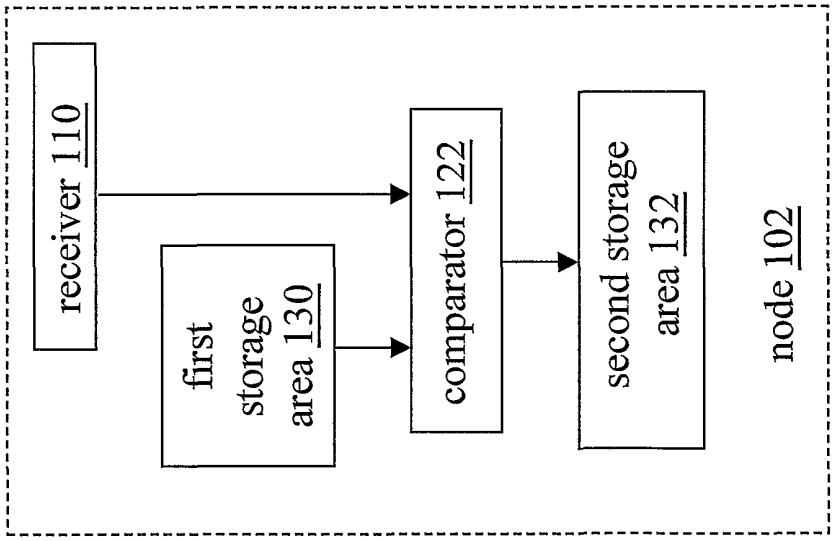

receiver 110
first storage area 130
comparator 122
second storage area 132
node 102

FIG. 11

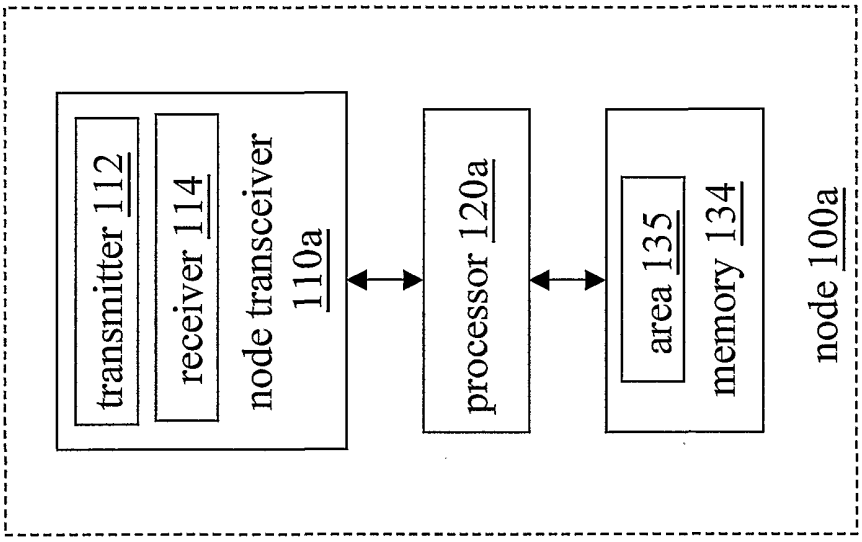

transmitter 112
receiver 114
node transceiver 110a
processor 120a
area 135
memory 134
node 100a

FIG. 12

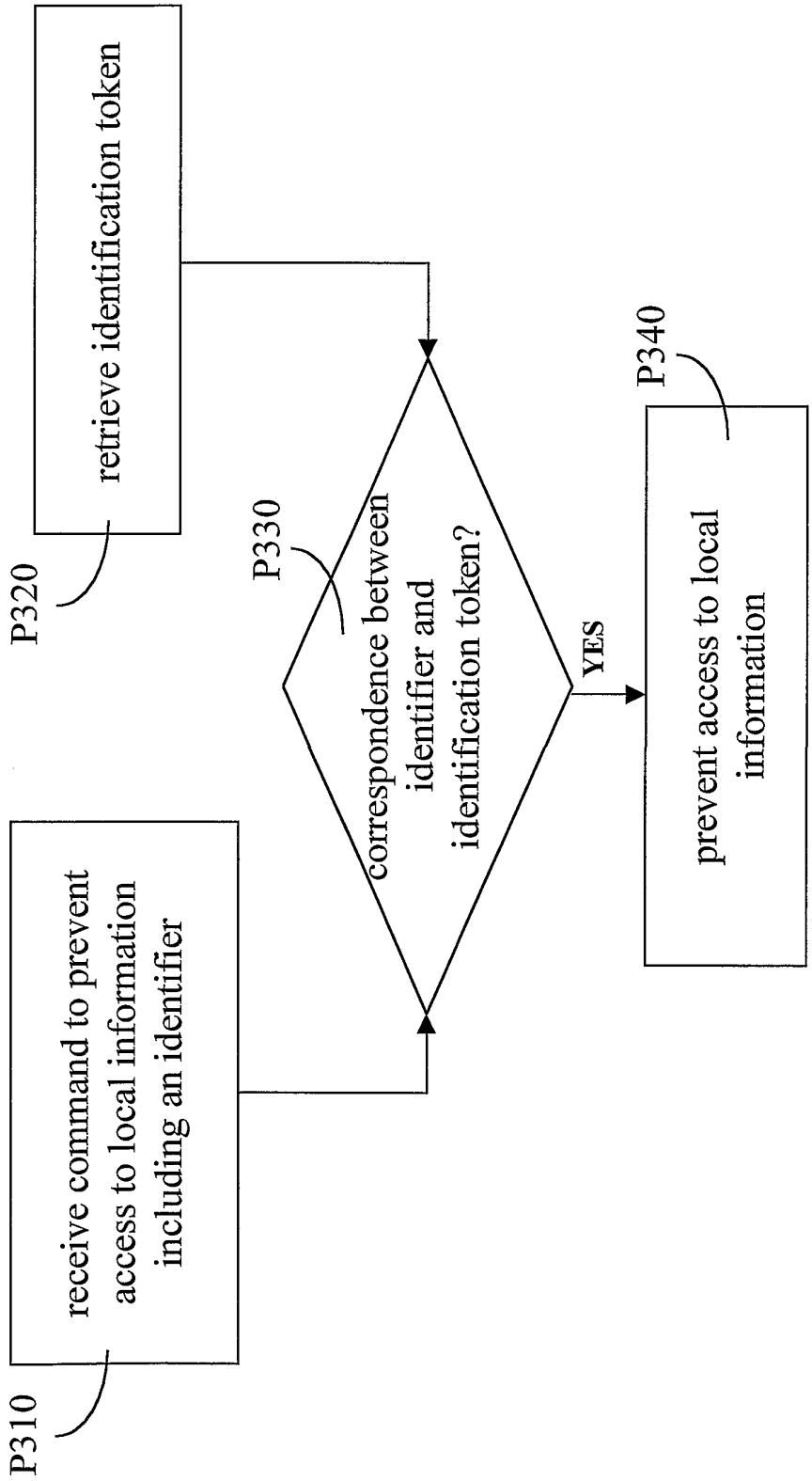

receive command to prevent access to local information including an identifier
P310
retrieve identification token
P320
correspondence between identifier and identification token?
P330
YES
prevent access to local information
P340

FIG. 13

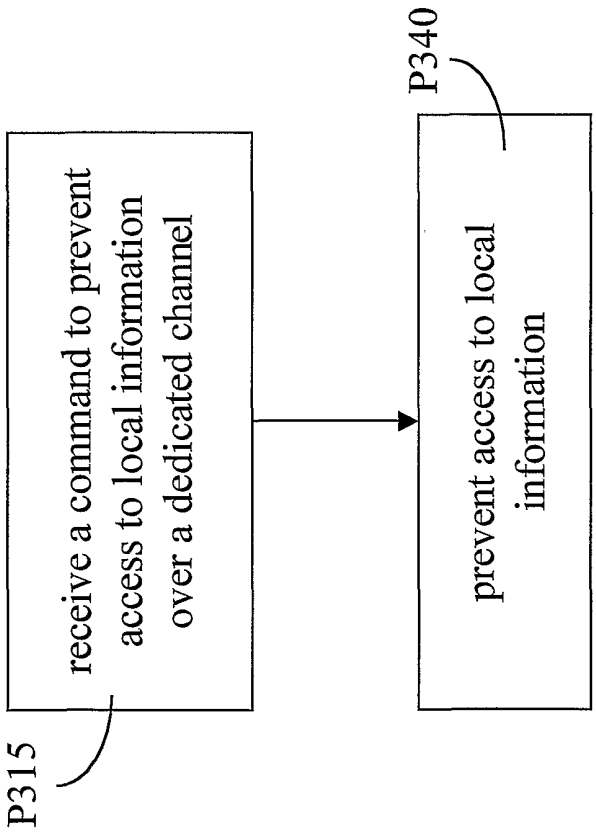

P315
receive a command to prevent access to local information over a dedicated channel
P340
prevent access to local information

FIG. 14

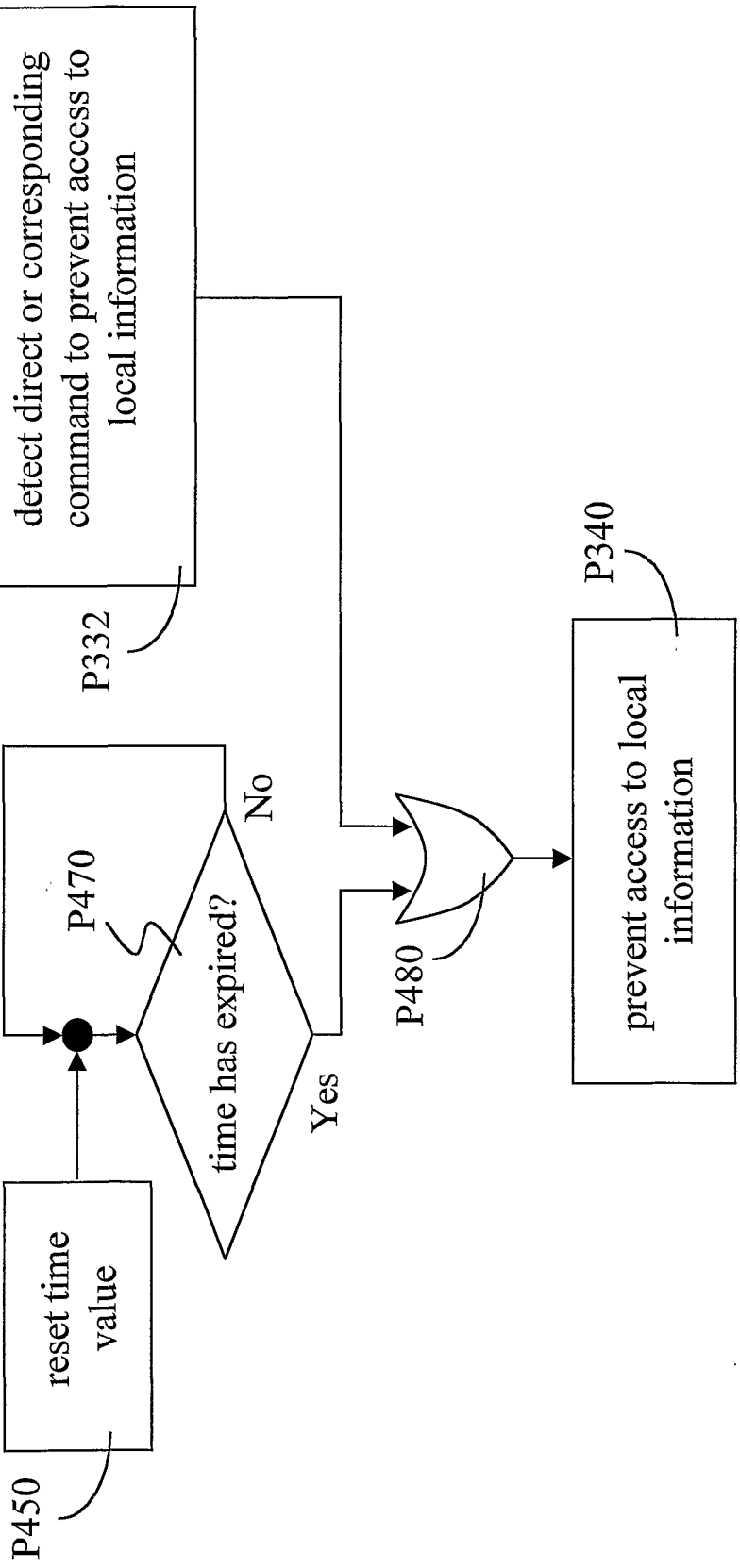

detect direct or corresponding command to prevent access to local information
P332
P340
prevent access to local information
P480
P470
time has expired?
No
Yes
reset time value
P450

FIG. 15

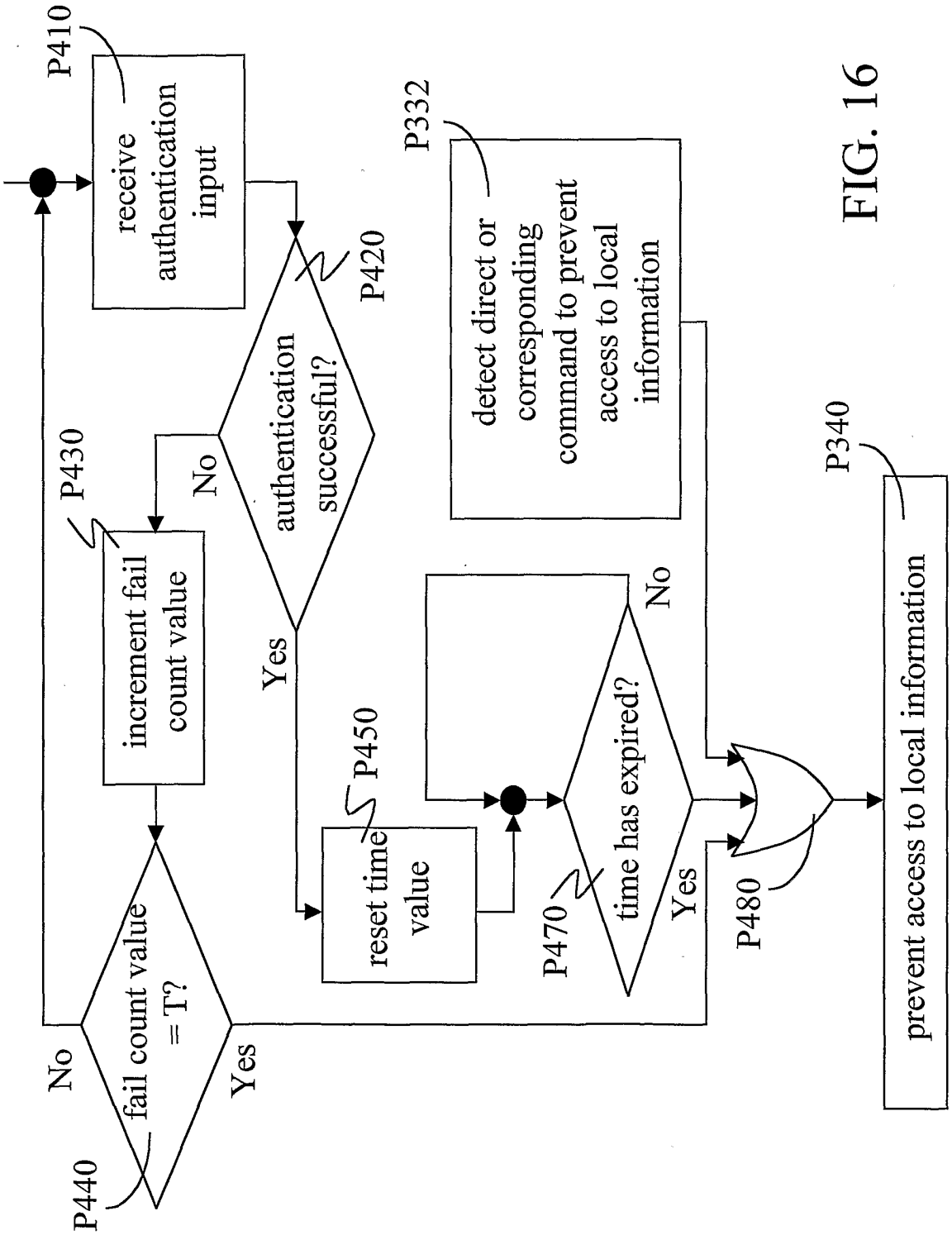

P410
receive authentication input
P420
authentication successful?
No
Yes
P430
increment fail count value
fail count value = T?
No
Yes
P440
P450
reset time value
P470
time has expired?
No
Yes
P480
P332
detect direct or corresponding command to prevent access to local information
P340
prevent access to local information

FIG. 16