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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 June 2017 (29.06.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/111962 A1

(51) International Patent Classification:
H04W 12/12 (2009.01) *G06F 21/88* (2013.01)
G06F 1/32 (2006.01) *H04M 1/73* (2006.01)

(21) International Application Number:
PCT/US2015/067500

(22) International Filing Date:
22 December 2015 (22.12.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **SONY MOBILE COMMUNICATIONS INC.** [JP/JP]; 1-8-15 Konan, Minato-Ku, Tokyo, Tokyo 108-0075 (JP).

(71) Applicant *(for LC only)*: **SONY MOBILE COMMUNICATIONS (USA) INC.** [US/US]; c/o Capitol Services Inc., 615 South DuPont Highway, Dover, Delaware 19901 (US).

(72) Inventor: **WÄSSINGBO, Tomas**; Hallstorpsvägen 17, 212 32 Malmö (SE).

(74) Agent: **GALIN, M. David**; Tucker Ellis LLP, 950 Main Avenue, Suite 1100, Cleveland, Ohio 44113 (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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURING ELECTRONIC DEVICE DURING LOW POWER AND FOLLOWING HARDWARE CHANGE

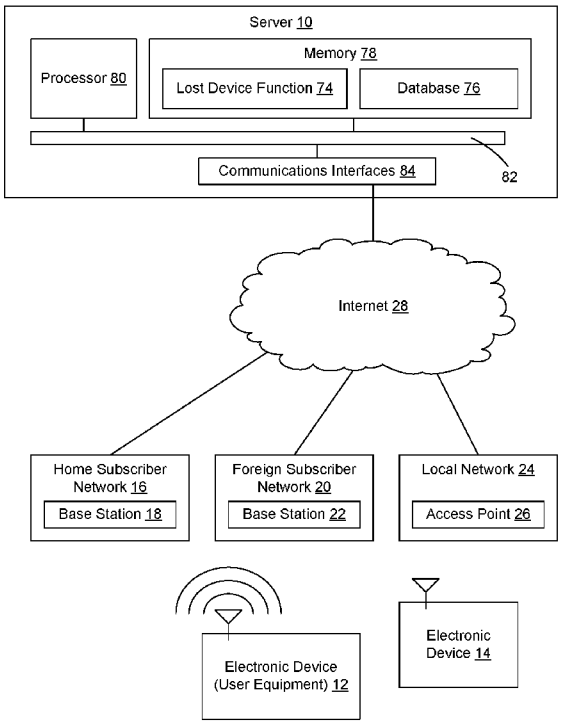

FIG. 1

(57) Abstract: Tracking of a location of an electronic device includes detecting a condition for which long term location tracking functions of the electronic device are preprogrammed in the electronic device; locking the electronic device, the locking of the electronic device restricting access to one or more user functions of the electronic device available to the user in an unlocked state; and transmitting a message by narrow band (NB) long term evolution (LTE), the message for relay by one or more receiving devices to a server that identifies the location of the electronic device and the message containing an identifier value for the electronic device.

WO 2017/111962 A1

DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

TITLE: SYSTEM AND METHOD FOR SECURING ELECTRONIC DEVICE DURING LOW POWER AND FOLLOWING HARDWARE CHANGE

TECHNICAL FIELD OF THE INVENTION

The technology of the present disclosure relates generally to electronic devices and, more particularly, to a system and method for improving the ability to find a lost electronic device as well as improving the security of the device in certain situations. The disclosed operations may make the electronic device less attractive to being stolen.

BACKGROUND

Some mobile electronic devices have location discovery tools to facilitate finding the device if lost or stolen. Exemplary tools of this nature are "Find my iPhone" by Apple and "Find my Xperia" by Sony. These types of tools can be very effective, but rely on relatively power intensive processes. Once the battery is drained, the location discovery tool and other operations of the device will no longer be available.

SUMMARY

According to one aspect of the disclosure, disclosed is a method of tracking location of an electronic device. The method includes detecting a condition for which long term location tracking functions of the electronic device are preprogrammed in the electronic device; locking the electronic device, the locking of the electronic device restricting access to one or more user functions of the electronic device available to the user in an unlocked state; and transmitting a message by narrow band (NB) long term evolution (LTE), the message for relay by one or more receiving devices to a server that identifies the location of the electronic device and the message containing an identifier value for the electronic device.

According to one embodiment of the method, the condition is remaining charge of a battery that powers the electronic device is below a predetermined amount of charge.

According to one embodiment of the method, the predetermined amount of charge is a charge amount that is less than five percent.

According to one embodiment of the method, the condition is removal or replacement of a subscriber identity module (SIM) card associated with the electronic device.

According to one embodiment of the method, the message includes a location value corresponding to a location of the electronic device determined by the electronic device.

According to one embodiment of the method, the location value is determined before the locking of the electronic device.

According to one embodiment of the method, the location value is updated upon determination of at least one of movement of the electronic device, receipt of a message from the server to update the location value, or upon a time trigger preprogrammed in the electronic device.

According to one embodiment, the method further includes unlocking the electronic device if a security challenge is met.

According to one embodiment of the method, the transmitting of the message is repeated on a periodic basis or according to a predetermined schedule.

According to one embodiment of the method, the identifier value is a value obtained from a SIM card associated with the electronic device.

According to another aspect of the disclosure, disclosed is an electronic device. The electronic device includes communication circuitry and control circuitry configured to execute long term location tracking functions embodied in executable logic, the executable logic includes logic to: detect a condition that triggers the long term location tracking functions; lock the electronic device to restrict access to one or more user functions of the

electronic device available to the user in an unlocked state; and transmit a message by narrow band (NB) long term evolution (LTE) via the communication circuitry, the message for relay by one or more receiving devices to a server that identifies the location of the electronic device and the message containing an identifier value for the electronic device.

According to one embodiment of the electronic device, the condition is remaining charge of a battery that powers the electronic device is below a predetermined amount of charge.

According to one embodiment of the electronic device, the predetermined amount of charge is a charge amount that is less than five percent.

According to one embodiment of the electronic device, the condition is removal or replacement of a subscriber identity module (SIM) card associated with the electronic device.

According to one embodiment of the electronic device, the message includes a location value corresponding to a location of the electronic device determined by the electronic device.

According to one embodiment of the electronic device, the location value is determined before the locking of the electronic device.

According to one embodiment of the electronic device, the location value is updated upon determination of at least one of movement of the electronic device, receipt of a message from the server to update the location value, or upon a time trigger preprogrammed in the electronic device.

According to one embodiment of the electronic device, the executable logic further includes logic to unlock the electronic device if a security challenge is met.

According to one embodiment of the electronic device, the transmitting of the message is repeated on a periodic basis or according to a predetermined schedule.

According to one embodiment of the electronic device, the identifier value is a value obtained from a SIM card associated with the electronic device.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of an operational environment for an electronic device.

FIG. 2 is a schematic diagram of the electronic device.

FIG. 3 is a flow-diagram of a power management operation for the electronic device.

FIG. 4 is a flow-diagram of a security operation for hardware changes of the electronic device.

DETAILED DESCRIPTION OF EMBODIMENTS

Embodiments will now be described with reference to the drawings, wherein like reference numerals are used to refer to like elements throughout. It will be understood that the figures are not necessarily to scale. Features that are described and/or illustrated with respect to one embodiment may be used in the same way or in a similar way in one or more other embodiments and/or in combination with or instead of the features of the other embodiments.

Introduction

Described below in conjunction with the appended figures are various embodiments of systems and methods for improving the security of an electronic device and prolonging the time during which location of a lost electronic device may be identified. The disclosed techniques are primarily described in the context of a portable electronic device, such as smart phone or tablet computer. But the techniques may be applied in other contexts, such as other types of electronic devices, computers, gaming

consoles, vehicles, appliances, shipping containers, and other valuable or commonly stolen items.

The techniques involve entering a low power transmission mode to periodically transmit an identifier for the electronic device and, in some cases, a last known location value. The low power transmission mode may be a narrow-band (NB) long-term evolution (LTE) transmission technique sometimes employed for machine type communications and/or machine-to-machine (M2M) transmissions. These types of transmissions are sometimes referred to as Internet of Things (IoT) transmissions. In a typical implementation, the NB LTE transmission is made using unlicensed spectrum and base stations that receive the transmission will process the transmission (e.g., relay the transmission) even if the transmitting device does not have a service agreement with the subscriber network associated with the base station. Under these operations, the electronic device may remain visible for very long periods of time without recharging. As such, long-term location tracking of the electronic device by a server may be made, such as tracking for at least one day, at least one week, at least one month, or at least one year.

The electronic device may enter the low power transmission mode when the electronic device has remaining battery charge under a predetermined threshold, such as about three percent to about five percent, or when a hardware change is made, such as replacement of a subscriber identity module (SIM) card. To exit the low power transmission mode, a security operation may be need to be satisfied. Therefore, since the electronic device may remain visible for an extended time after one of these events until a security operation is satisfied, the electronic device may be less attractive to being stolen.

System Architecture

FIG. 1 is a schematic diagram of an exemplary system for implementing the disclosed techniques. It will be appreciated that the illustrated system is representative and other systems may be used to implement the disclosed techniques. Also, functions disclosed as being carried out by a single device, such as the disclosed server, may be carried out in a distributed manner across nodes of a computing environment.

The system includes a server 10 that, at times, may be in operative communication with an electronic device 12 (also referred to as a user equipment or UE). The server 10 also may be in operative communication with other electronic devices (e.g., electronic device 14), with one or more subscriber networks and/or with one or more local networks. In the illustrated embodiment, the subscriber networks are cellular networks operated by respective mobile telephone service providers. One of the illustrated subscriber networks is a home network 16 for the electronic device 12 that has at least one base station 18 (or other access point) in operative range from the electronic device 12. The other of the illustrated networks is a foreign network 20 relative to the electronic device 12 that has at least one base station 22 (or other access point) in operative range from the electronic device 12. In the illustrated embodiment, the local network, identified by reference numeral 24, is a wireless network such as a WiFi network that has at least one access point 26 (e.g., a router) in operative range from the electronic device 12. The subscriber networks 16, 20 and the local network 24 may communicate with the server 10 by way of a communications medium, such as the Internet 28 and/or one or more intermediate networks. In one embodiment, the server 10 may be part of one of the subscriber networks 16, 20 or may be separate from the subscriber networks 16, 20.

As will be described, the electronic device 14 may detect NB transmissions from the electronic device 12. The NB transmissions may be relayed from the electronic device 14 to the server 10 via one of the networks 16, 20, 24 or another network or communication medium. Other communication operations of the electronic device 14 are possible, but will not be described further. NB transmissions from the electronic device 14 that are detected by any of the base stations 18, 22 or the access point 26 may be relayed to the server 10 via the respective networks 16, 20, 24.

The electronic device 12 may be one of a variety of types of devices, such as a mobile phone, a tablet computer, a laptop computer, a desktop computer, a gaming device, etc. As will be described, the server 10 and the electronic device 12 are configured to carry out the respective logical functions that are described herein. In addition to carrying out the operations described herein, the server 10 may carry out other support and service operations for the electronic device 12.

With additional reference to FIG. 2, illustrated is a schematic block diagram of the electronic device 12 in its exemplary embodiment as a mobile telephone. The electronic device 12 includes a control circuit 30 that is responsible for overall operation of the electronic device 12, including controlling the electronic device 12 to carry out the operations described in greater detail below. The control circuit 30 includes a processor 32 that executes an operating system 34 and various applications 36. The functions described in this disclosure document may be embodied as part of the operating system 34. In other embodiments, these functions may be embodied as a dedicated application or part of an application used for other tasks.

The operating system 34, the applications 36, and stored data 38 (e.g., data associated with the operating system 34, the applications 36, and user files), are stored on a memory 40. The operating system 34 and applications 36 are embodied in the form of executable logic routines (e.g., lines of code, software programs, etc.) that are stored on a non-transitory computer readable medium (e.g., the memory 40) of the electronic device 12 and are executed by the control circuit 30. The functions described herein may be thought of as methods that are carried out by the electronic device 12.

The processor 32 of the control circuit 30 may be a central processing unit (CPU), microcontroller, or microprocessor. The processor 32 executes code stored in a memory (not shown) within the control circuit 30 and/or in a separate memory, such as the memory 40, in order to carry out operation of the electronic device 12. The memory 40 may be, for example, one or more of a buffer, a flash memory, a hard drive, a removable media, a volatile memory, a non-volatile memory, a random access memory (RAM), or other suitable device. In a typical arrangement, the memory 40 includes a non-volatile memory for long term data storage and a volatile memory that functions as system memory for the control circuit 30. The memory 40 may exchange data with the control circuit 30 over a data bus. Accompanying control lines and an address bus between the memory 40 and the control circuit 30 also may be present. The memory 40 is considered a non-transitory computer readable medium.

The electronic device 12 includes communications circuitry that enables the electronic device 12 to establish various wireless communication connections. In the exemplary embodiment, the communications circuitry includes a radio circuit 42. The

radio circuit 42 includes one or more radio frequency transceivers and an antenna assembly (or assemblies). In the case that the electronic device 12 is a multi-mode device capable of communicating using more than one standard and/or over more than one radio frequency band, the radio circuit 42 represents one or more than one radio transceiver, one or more than one antenna, tuners, impedance matching circuits, and any other components needed for the various supported frequency bands and radio access technologies. Exemplary network access technologies supported by the radio circuit 42 include cellular circuit-switched network technologies and packet-switched network technologies (e.g., WiFi). The radio circuit 42 further represents any radio transceivers and antennas used for local wireless communications directly with another electronic device, such as over a Bluetooth interface.

The electronic device 12 further includes the display 44 for displaying information to a user. The display 44 may be coupled to the control circuit 30 by a video circuit 46 that converts video data to a video signal used to drive the display 44. The video circuit 46 may include any appropriate buffers, decoders, video data processors and so forth.

The electronic device 12 may include one or more user inputs 48 for receiving user input for controlling operation of the electronic device 12. Exemplary user inputs 48 include, but are not limited to, a touch sensitive input 50 that overlays or is part of the display 44 for touch screen functionality, and one or more buttons 52. Other types of data inputs may be present, such as one or more motion sensors 54 (e.g., gyro sensor(s), accelerometer(s), etc.).

The electronic device 12 may further include a sound circuit 56 for processing audio signals. Coupled to the sound circuit 56 are a speaker 58 and a microphone 60 that enable audio operations that are carried out with the electronic device 12 (e.g., conduct telephone calls, output sound, capture audio, etc.). The sound circuit 56 may include any appropriate buffers, encoders, decoders, amplifiers and so forth.

The electronic device 12 may further include a power supply unit 62 that includes a rechargeable battery 64. The power supply unit 62 supplies operating power from the battery 64 to the various components of the electronic device 12 in the absence a connection from the electronic device 12 to an external power source. The power supply

unit 62 may monitor the amount of charge of the battery 64, which is typically expressed as a percentage of charge remaining.

The electronic device 12 also may include various other components. For instance, the electronic device 12 may includes one or more input/output (I/O) connectors (not shown) in the form electrical connectors for operatively connecting to another device (e.g., a computer) or an accessory (e.g., earphones) via a cable, or for receiving power from an external power supply.

Another exemplary component may be one or more cameras 66 for taking photographs or video, or for use in video telephony. As another example, a position data receiver 68, such as a global positioning system (GPS) receiver, may be present to assist in determining the location of the electronic device 12. The electronic device 12 also may include a subscriber identity module (SIM) card slot 70 in which a SIM card 72 is received. The slot 70 includes any appropriate connectors and interface hardware to establish an operative connection between the electronic device 12 and the SIM card 72.

The server 10 may be implemented as a computer-based system that is capable of executing computer applications (e.g., software programs), including a lost device function 74 that, when executed, carries out functions of the server 10 that are described herein. The lost device function 74 and a database 76 may be stored on a non-transitory computer readable medium, such as a memory 78. The database 76 may be used to store various information sets used to carry out the functions described in this disclosure. The memory 78 may be a magnetic, optical or electronic storage device (e.g., hard disk, optical disk, flash memory, etc.), and may comprise several devices, including volatile and non-volatile memory components. Accordingly, the memory 78 may include, for example, random access memory (RAM) for acting as system memory, read-only memory (ROM), solid-state drives, hard disks, optical disks (e.g., CDs and DVDs), flash devices and/or other memory components, plus associated drives, players and/or readers for the memory devices.

To execute logical operations, the server 10 may include one or more processors 80 used to execute instructions that carry out logic routines. The processor 80 and the

memory 78 may be coupled using a local interface 82. The local interface 82 may be, for example, a data bus with accompanying control bus, a network, or other subsystem.

The server 10 may have various input/output (I/O) interfaces for operatively connecting to various peripheral devices, as well as one or more communications interfaces 84. The communications interface 84 may include for example, a modem and/or a network interface card. The communications interface 84 may enable the server 10 to send and receive data signals to and from other computing devices via an external network. In particular, the communications interface 84 may operatively connect the server 10 to one or more external communications mediums, including establishing operative connection to the Internet 28.

Power Management for Lost Device Operation

With additional reference to FIG. 3, shown is an exemplary flow diagram representing steps that may be carried out by the electronic device 12 when executing logical instructions to carry out a power management for lost device operation. It will be understood that the power management for lost device operation may be carried out regardless of whether the electronic device 12 is actually lost (e.g., in a location unknown to the user of the device). More specifically, the electronic device 12 may carry out the power management for lost device operation when charge of the battery 64 falls below a predetermined threshold. Therefore, in one embodiment, a trigger for entering a "lost mode" is based on battery change and not on the user's knowledge of the location of the electronic device 12. Other triggering events may cause the electronic device 12 to enter the lost mode. For instance, the server 10 may send a command to the electronic device 12 to enter the lost mode. This may occur if the user discovers that he or she cannot find the electronic device 12 and, using another device, communicates this condition to the server 10 that, in turn, begins an operation to attempt to assist the user locate the electronic device 12.

FIG. 3 illustrates an exemplary process flow representing steps that may be carried out by the electronic device 12 when executing the logical instructions to implement the power management for lost device operation. Complimentary operations of the server 10 also will be understood from this disclosure. Although illustrated in a logical progression,

the illustrated blocks of FIG. 3 may be carried out in other orders and/or with concurrence between two or more blocks. Therefore, the illustrated flow diagram may be altered (including omitting steps) and/or may be implemented in an object-oriented manner or in a state-oriented manner.

In one embodiment, the power management for lost device operation may run in the background during normal device operation to check for a condition that triggers entry into a lost mode. For example, in block 86, the remaining battery charge may be compared to a predetermined threshold. The predetermined threshold may be, for example, three percent. Other predetermined battery charge thresholds are possible, such five percent or seven percent. If the charge of the battery is above the predetermined threshold, the electronic device 12 may carry out normal operations in block 88, such as engage in user controlled activities, enter a power save mode when not in use, enter a locked state when not in use, etc.

If the charge of the battery is below the predetermined threshold or another trigger for entering the lost mode occurs (e.g., the above-described receipt of a command from the server 10), then the logical flow may progress to block 90. In block 90, the electronic device 12 enters the lost mode. The lost mode includes locking the electronic device 12 to prevent use of certain operations without satisfying an unlock challenge. The lost mode also may include shutting down as many operations as possible to conserve power. Various components and functions may be activated at appropriate times to carry out the functions described below. In one embodiment, however, the lost mode may exit at anytime during the lost mode if the user satisfies the unlock challenge even if the charge of the battery is below the threshold. Also, in one embodiment, if the user is using the electronic device 12 when the condition of block 86 is satisfied, then entry into lost may be delayed until the electronic device 12 enters a power save or locked state by action of the user or inactivity of the electronic device 12.

After entry of the lost mode, the electronic device 12 may periodically transmit data in block 92. As will be described, the transmission of block 92 may be made on a predetermined schedule and/or the time between transmissions may change based on certain events or the length of time that the electronic device 12 remains in the lost mode.

The data transmitted in block 92 may include a device identifier. One exemplary identifier is an international mobile subscriber identity (IMSI) value retrieved from the SIM card 72. Other device identifier values are possible, such a serial number of the device, subscriber information, telephone number, or a unique identification code that was previously associated with the SIM card 72. Other data that is transmitted may include a last known location of the electronic device 12, such a location determined using the position data receiver 68 or a position determined by the home subscriber network 16. This location determination may be made before the electronic device 12 enters the lost mode 90. If a confidence level in the last known location is relatively low, then the last known location may not be transmitted. Alternatively, the last known location may be transmitted if a message is received from the server 10 that prompts determination and transmission of the location of the electronic device 12.

Other data that may be transmitted includes an identification of the server 10. The identification of the server 10 may be used by devices that receive the transmission to relay the data from the transmission to the server 10.

The transmission may be made using a NB LTE protocol (also referred to as IoT communication or NB IoT). The use of NB LTE consumes a relatively low amount of power, which will allow the electronic device 12 to periodically make the transmission over a long period of time before the charge of the battery 64 is depleted to the point where there is insufficient power from the battery 64 to make the transmission. Depending on the frequency of transmission and other operations that the electronic device 12 may make while in the lost mode, it is possible that the electronic device 12 may remain visible to the server 10 for one or more years.

Also, the transmission may be made as a machine type communication. Machine type communications under NB LTE, and similar radio access technologies, follow a protocol under which a wide variety of devices that detect the transmission will process the transmission, such as by serving as a relay device that forwards the transmission or its content to another device. In this manner, the other devices serve as multiple possible pathways for communications from the electronic device 12 to reach the server 10. Thus, using the illustrated example, one or more of the base station 18 of the home network 16, the base station 22 of the foreign subscriber network 20, the access point 36 or the

electronic device 14 may detect the transmission and relay the transmission or its content to the server 10. As other devices move within range of the electronic device 12 and/or as the electronic device 12 moves within range of other devices, the number and identity of the devices that detect the transmission from the electronic device 12 and relay the transmission to the server 10 will change.

When the transmission from the electronic device 12 is received by a compatible device, the device may relay the transmission to the server 10. The relayed transmission may be in the transmission's original form or as a message containing data from the transmission. The relayed transmission may include a way for the server 10 to determine the location of the relaying device. For fixed location devices, such as the base stations 18 and 22, the location of the device may be known in advance by the server 10 or may be ascertainable from a database by the server 10. For other relaying devices, the relaying device may provide its location as part of the relayed transmission or the device may be polled by the server 10 to supply the device's location. The server 10 may analyze each relayed transmission and the locations of the devices that detected and relayed the transmission to estimate a location of the electronic device 12. If possible from the information collected by the server 10, the estimate may be derived by triangulation. In one embodiment, the relayed transmission may include signal strength of the transmission from the electronic device 12, which may be used by the server 10 to improve the triangulation results. In other embodiments, or when only one or two devices relay the transmission, the estimated location of the electronic device 12 may be an area surrounding the relaying device(s). The area may be based on the effective transmission range of the transmitted signal. Effective transmission range of the transmitted signal may be dependent on the transmission characters of the electronic device 12 and the receive characteristics of the receiving/relaying device.

The server 10 may share the estimated location with an authorized user of the electronic device 12. Since, during the lost mode, the electronic device 12 is locked and its location may not be known to the authorized user, the location may be shared via another device that accesses the server 10 or receives communications from the server 10. In other situations, the estimated location may be shared with other parties, such as law enforcement, rescue personnel, or other authorized person or entity. The server 10 may

require authentication of the user or other party prior to sharing the estimated location information. In one embodiment, the estimated location information may be displayed on a map. When the user is close to the estimated location and if the electronic device 12 still cannot be found, the user may interface with server 10 to have the server 10 send a wake signal to the electronic device 12 to which the electronic device 12 reacts by playing a sound and/or emitting light.

The transmission of block 92 may take any appropriate form, such as a data message or signal. The message or signal may be addressed to the server 10.

The transmission of block 92 may be sent on a periodic basis, such as every five minutes, every ten minutes or every fifteen minutes. In one embodiment, the transmission may be sent relatively frequently after entering the lost mode and then transmission frequency may decrease the longer the electronic device 12 stays in the lost mode. For instance, in the first day of lost mode the transmission may be sent every five minutes. Then in the second through seventh day of the lost mode, the transmission may be sent every fifteen minutes. Then, for the next month, the transmission may be sent once an hour and, thereafter, the transmission may be sent once or twice a day. Of course, other transmission schedules may be followed. Also, certain events may trigger the transmission and/or cause an increase in the transmission frequency. For instance, if the electronic device 12 detects movement as indicated by the motion sensor 54, then a transmission may be made and additional transmissions may be made at a relatively frequent rate (e.g., every minute or every five minutes) for a period of time or until the motion stops.

The electronic device 12 may check for one or more events during the lost mode. For instance, in block 94, the electronic device 12 may determine if an event occurs that triggers the electronic deice 12 to attempt to determine its location. An exemplary event of this nature includes receipt of a message from the server 10 that commands the electronic device 12 to attempt to determine the location of the electronic device 12. For this purpose, the electronic device 12 may periodically wake up radio operations to attempt to detect inbound messages for the electronic device 12. Turning on of the receiving functionality may be carried out at predetermined times that are scheduled to coincide with the transmission of messages from the server 10. The messages may be

received over any suitable radio access technology, such as a control message transmitted over cellular protocols (e.g., 3G or 4G signaling protocols) or over NB LTE signaling protocols. Another event that may trigger a positive determination in block 94 is the elapsing of a predetermined amount of time since entering the lost mode or the elapsing of a predetermined amount of time since the last attempt to determine location of the electronic device 12. Another event that may trigger a positive determination in block 94 is detection of movement of the electronic device 12 by the motion sensor 54.

If a positive determination is made in block 94, the electronic device 12 may attempt to determine its location in block 96. Location may be determined by signaling with the home subscriber network 16, by using GPS, etc. If location can be ascertained in block 96, the determined location may be used in future transmissions at block 92.

Another event that the electronic device 12 may monitor for is whether the electronic device 12 is connected to external power to charge the battery 64. For example, in block 98, if a determination is made that the charge of the battery exceeds the predetermined threshold of block 86, then the logical flow may proceed to block 100. In block 100, the user is prompted to complete a security challenge. The challenge may be based on entering biometric information (e.g., a fingerprint), entering a password or PIN, entering a dynamic key value, entering a predetermined sequence of gestures, etc. In one embodiment, the challenge is the same challenge used to unlock the electronic device 12 after the electronic device 12 goes into a locked state following a period of inactivity or by user action to lock the device. In other embodiment, the challenge may be an advanced challenge requiring additional or different actions than the challenge used to unlock the electronic device 12 after the electronic device 12 goes into a locked state following a period of inactivity or by user action to lock the device. If the challenge is met, the electronic device 12 may be unlocked and enter normal operation at block 88. If the challenge is not met, the electronic device may remain in the lost mode. As indicated, in the lost mode, the electronic device 12 may remain locked and periodically transmit data in block 92.

SIM Security Operation

With additional reference to FIG. 4, shown is an exemplary flow diagram representing steps that may be carried out by the electronic device 12 when executing logical instructions to carry out a hardware security operation. In the illustrated and described embodiment, the hardware security operation is carried out if the SIM card 72 is removed or is replaced with a different SIM card. Other hardware changes to the electronic device 12 may result in execution of the security operation, such as removal of a case, housing component, replacement of the battery 64, removal from a cradle, disconnection from an external power source, etc.

FIG. 4 illustrates an exemplary process flow representing steps that may be carried out by the electronic device 12 when executing the logical instructions to implement the hardware security operation. Complimentary operations of server 10 also will be understood from this disclosure. Although illustrated in a logical progression, the illustrated blocks of FIG. 4 may be carried out in other orders and/or with concurrence between two or more blocks. Therefore, the illustrated flow diagram may be altered (including omitting steps) and/or may be implemented in an object-oriented manner or in a state-oriented manner.

In one embodiment, the hardware security operation may run in the background during normal device operation to check for a condition that triggers entry into a security mode. For example, in block 102, the electronic device 12 may monitor for removal or replacement of the SIM card 72. If the SIM card 72 is not removed or replaced, the electronic device 12 may carry out normal operations in block 104, such as engage in user controlled activities, enter a power save mode when not in use, enter a locked state when not in use, etc.

If the electronic device 12 detects that the SIM card 104 is removed, then the logical flow may progress to block 106. In block 106, the electronic device 12 enters a security mode. The security mode includes locking the electronic device 12 to prevent use of certain operations without satisfying an unlock challenge.

In the locked state, the electronic device 12 may prompt the user for an input to complete a security challenge to unlock the electronic device 12 in block 108. The challenge may be based on entering biometric information (e.g., a fingerprint), entering a password or PIN, entering a dynamic key value, entering a predetermined sequence of gestures, etc. In one embodiment, the challenge is the same challenge used to unlock the electronic device 12 after the electronic device 12 goes into a locked state following a period of inactivity or by user action to lock the device. In other embodiment, the challenge may be an advanced challenge requiring additional or different actions than the challenge used to unlock the electronic device 12 after the electronic device 12 goes into a locked state following a period of inactivity or by user action to lock the device. If the challenge is met in block 110, the electronic device 12 may be unlocked and enter normal operation at block 104.

If the challenge is not met, the electronic device may remain in the security mode. As indicated, in the security mode, the electronic device 12 may remain locked. Additionally, in block 112, the electronic device may periodically transmit data in block 112. Similar to the transmission of block 92, the transmission of block 112 may be made on a predetermined schedule and/or the time between transmissions may change based on certain events or the length of time that the electronic device 12 remains in the security mode.

Also similar to block 92, the data transmitted in block 112 may include a device identifier, such as an IMSI value. The IMSI value may have been retrieved from the SIM card 72 at a prior time and securely stored in memory 40. Other device identifier values are possible, such as serial number of the device, subscriber information, telephone number, or a unique identification code that was previously associated with the SIM card 72 prior to its removal or replacement. The IMSI value, other data retrieved from the SIM card 72 or other device identifier used for the data transmission may be stored in a secure, possibly hidden, location of the memory 40. Additional data that is transmitted may include a last known location of the electronic device 12, such a location determined using the position data receiver 68 or a position determined by the home subscriber network 16. This location determination may be made before the electronic device 12 enters the security mode 112 or during the security mode. Other data that may be transmitted

includes an identification of the server 10 for use by devices that receive the transmission to relay the data from the transmission to the server 10. Also, the IMSI value of other data retrieved from the new SIM card may be included in the data transmission of block 112.

In one embodiment, the transmission of block 112 may be made using full power operations over normal cellular and/or pack-switch transmission protocols (e.g., 3G, 4G, LTE, WiFi, etc.). In an alternative embodiment or in addition to the full power transmission, the transmission of block 112 may be made using a NB LTE protocol (also referred to as IoT communication or NB IoT) and/or made as a machine type communication. In this manner, the advantages of low power consumption and/or potentially more transmission delivery pathways to the server 10 may be realized. The transmission of block 112 may be communicated to the server 10 by devices that receive the transmission and are configured to process the transmission type.

The server 10 may then track location of the electronic device 12, such as by using the techniques described herein. Since replacement of the SIM card is an activity that thieves of mobile devices typically perform, there will be less incentive for thieves to steal mobile devices. This is because the mobile device will be subject to the security mode in which the device will remain locked and is traceable as soon as the SIM card is removed or replaced.

It is noted that the check of block 102 may be carried out at start up of the electronic device 12. In this manner, even if the electronic device 12 is powered off for replacement of the SIM card and reactivated, the replacement of the SIM card will cause the electronic device 12 to enter the security mode. For this purpose, the electronic device 12 may store the IMSI value of an approved SIM card in long term memory for comparison against an IMSI read at start up.

Other Applications

The security operation may be used in other contexts. For instance, an item (e.g., an appliance, electronic device, machine, shipping container, vehicle, etc.) may be configured to monitor for a condition that, if changed, would indicate possible unauthorized movement of the item. Exemplary monitored conditions include, but are not

limited to, the application of external power, an operative communication connection with another device (e.g., over a cable such as USB or over a wireless link such as Bluetooth), and the presence of another item (e.g., a coordinating cradle or stand on which the item is placed). If the condition changes (e.g., removal of the external power source, disruption of the communication connection, or separation from the coordinating item), the item may be further configured to emit the transmission of block 112 unless a security challenge is met. The item may include a battery to power electronics in the item that carry out these functions.

Conclusion

Although certain embodiments have been shown and described, it is understood that equivalents and modifications falling within the scope of the appended claims will occur to others who are skilled in the art upon the reading and understanding of this specification.

CLAIMS

What is claimed is:

1. A method of tracking location of an electronic device, comprising:

detecting a condition for which long term location tracking functions of the electronic device are preprogrammed in the electronic device;

locking the electronic device, the locking of the electronic device restricting access to one or more user functions of the electronic device available to the user in an unlocked state; and

transmitting a message by narrow band (NB) long term evolution (LTE), the message for relay by one or more receiving devices to a server that identifies the location of the electronic device and the message containing an identifier value for the electronic device.

2. The method of claim 1, wherein the condition is remaining charge of a battery that powers the electronic device is below a predetermined amount of charge.

3. The method of claim 2, wherein the predetermined amount of charge is a charge amount that is less than five percent.

4. The method of claim 1, wherein the condition is removal or replacement of a subscriber identity module (SIM) card associated with the electronic device.

5. The method of any of claims 1-4, wherein the message includes a location value corresponding to a location of the electronic device determined by the electronic device.

6. The method of claim 5, wherein the location value is determined before the locking of the electronic device.

7. The method of claim 5, wherein the location value is updated upon determination of at least one of movement of the electronic device, receipt of a message from the server to update the location value, or upon a time trigger preprogrammed in the electronic device.

8. The method of any of claims 1-7, further comprising unlocking the electronic device if a security challenge is met.

9. The method of any of claims 1-8, wherein the transmitting of the message is repeated on a periodic basis or according to a predetermined schedule.

10. The method of any of claims 1-9, wherein the identifier value is a value obtained from a SIM card associated with the electronic device.

11. An electronic device, comprising:

communication circuitry; and

control circuitry configured to execute long term location tracking functions embodied in executable logic, the executable logic comprising logic to:

detect a condition that triggers the long term location tracking functions;

lock the electronic device to restrict access to one or more user functions of the electronic device available to the user in an unlocked state; and

transmit a message by narrow band (NB) long term evolution (LTE) via the communication circuitry, the message for relay by one or more receiving devices to a server that identifies the location of the electronic device and the message containing an identifier value for the electronic device.

12. The electronic device of claim 11, wherein the condition is remaining charge of a battery that powers the electronic device is below a predetermined amount of charge.

13. The electronic device of claim 12, wherein the predetermined amount of charge is a charge amount that is less than five percent.

14. The electronic device of claim 11, wherein the condition is removal or replacement of a subscriber identity module (SIM) card associated with the electronic device.

15. The electronic device of any of claims 11-14, wherein the message includes a location value corresponding to a location of the electronic device determined by the electronic device.

16. The electronic device of claim 15, wherein the location value is determined before the locking of the electronic device.

17. The electronic device of claim 15, wherein the location value is updated upon determination of at least one of movement of the electronic device, receipt of a message from the server to update the location value, or upon a time trigger preprogrammed in the electronic device.

18. The electronic device of any of claims 11-17, wherein the executable logic further includes logic to unlock the electronic device if a security challenge is met.

19. The electronic device of any of claims 11-18, wherein the transmitting of the message is repeated on a periodic basis or according to a predetermined schedule.

20. The electronic device of any of claims 11-19, wherein the identifier value is a value obtained from a SIM card associated with the electronic device.

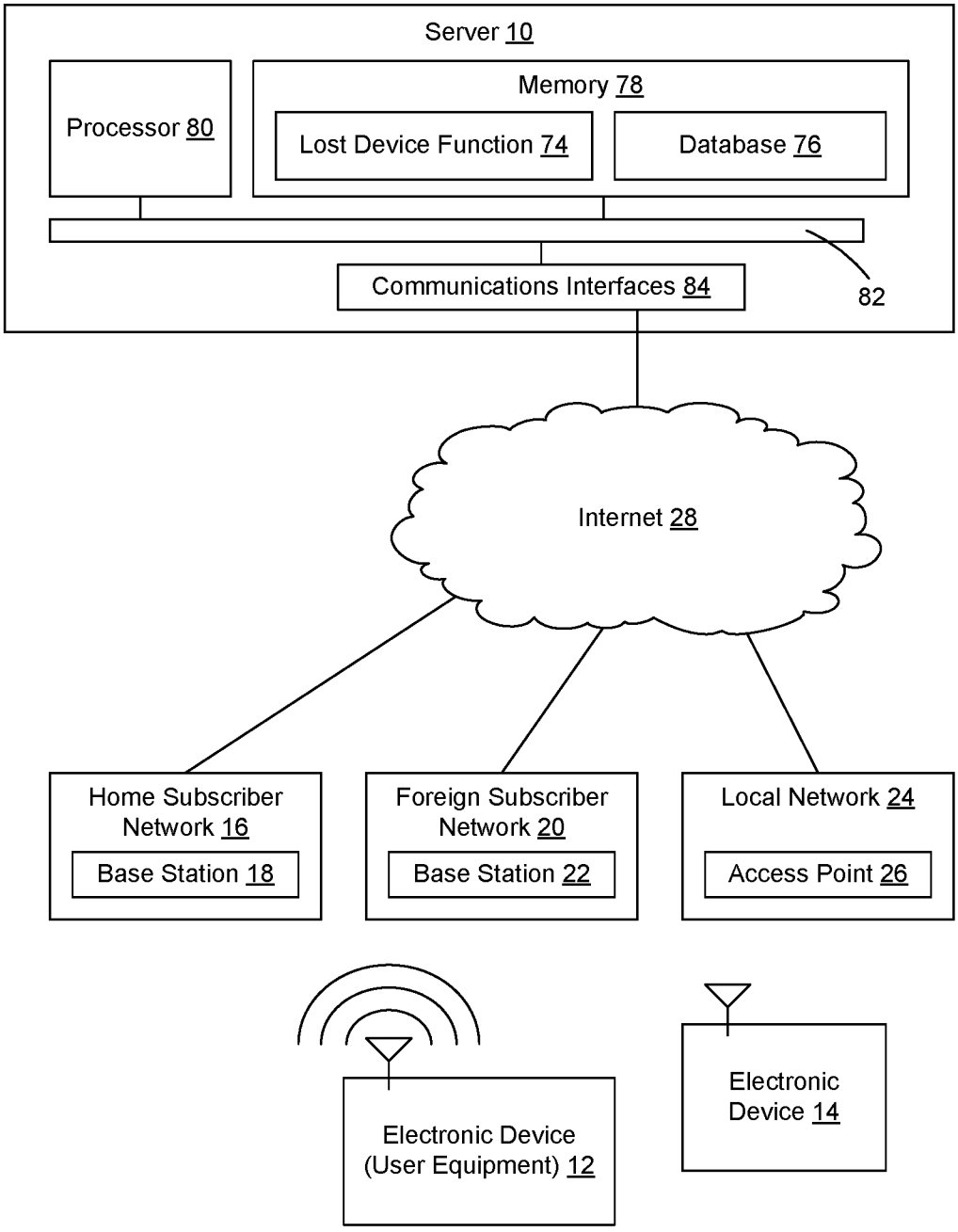
Server 10
Processor 80
Memory 78
Lost Device Function 74
Database 76
Communications Interfaces 84
82
Internet 28
Home Subscriber Network 16
Base Station 18
Foreign Subscriber Network 20
Base Station 22
Local Network 24
Access Point 26
Electronic Device (User Equipment) 12
Electronic Device 14

FIG. 1

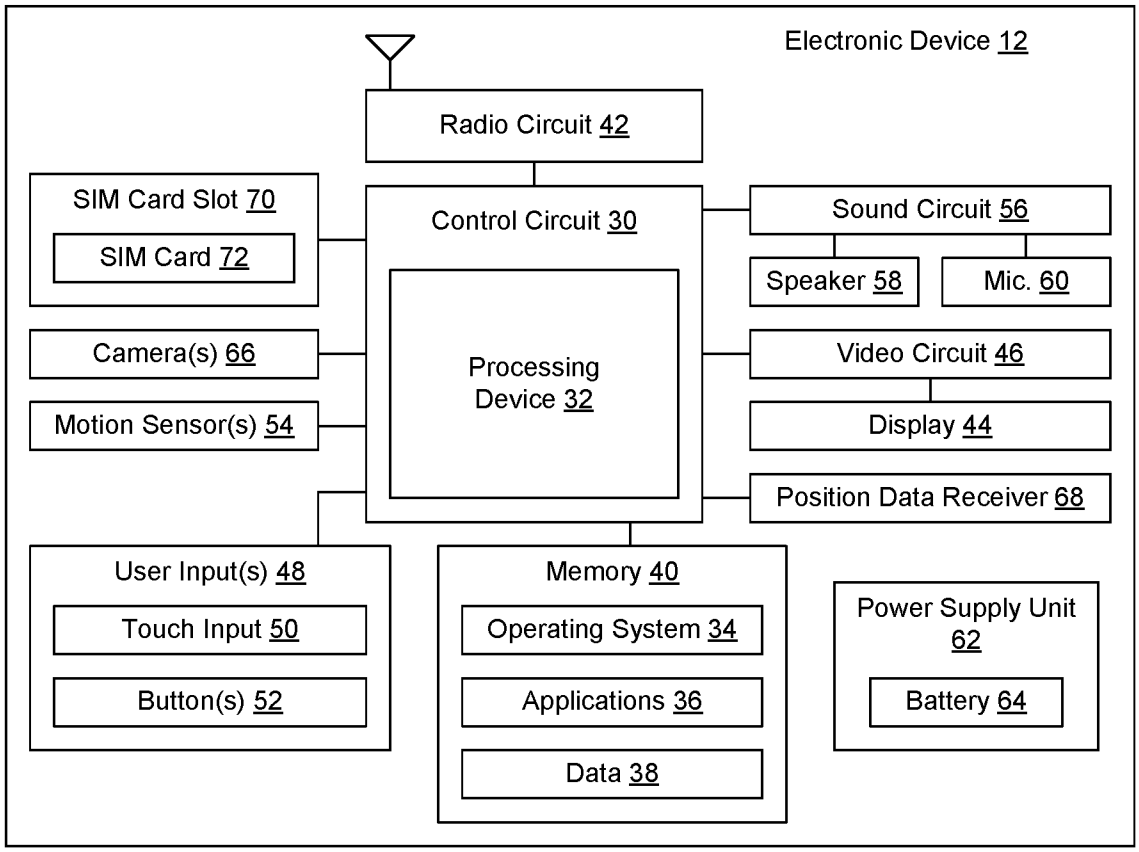
Electronic Device 12
Radio Circuit 42
SIM Card Slot 70
SIM Card 72
Control Circuit 30
Sound Circuit 56
Speaker 58
Mic. 60
Camera(s) 66
Processing Device 32
Video Circuit 46
Motion Sensor(s) 54
Display 44
Position Data Receiver 68
User Input(s) 48
Touch Input 50
Button(s) 52
Memory 40
Operating System 34
Applications 36
Data 38
Power Supply Unit 62
Battery 64

FIG. 2

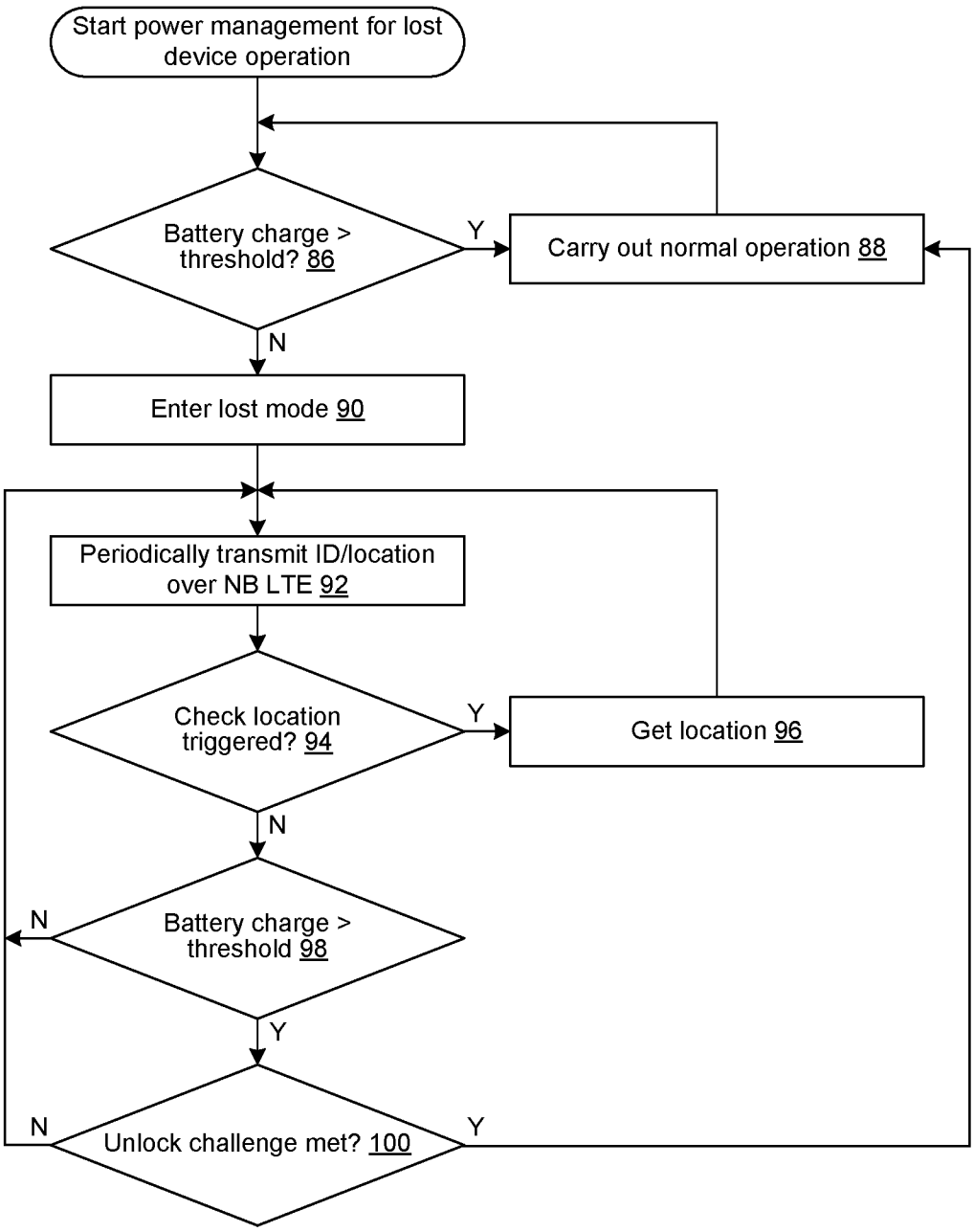
Start power management for lost device operation
Battery charge > threshold? 86
Y
Carry out normal operation 88
N
Enter lost mode 90
Periodically transmit ID/location over NB LTE 92
Check location triggered? 94
Y
Get location 96
N
N
Battery charge > threshold 98
Y
N
Unlock challenge met? 100
Y

FIG. 3

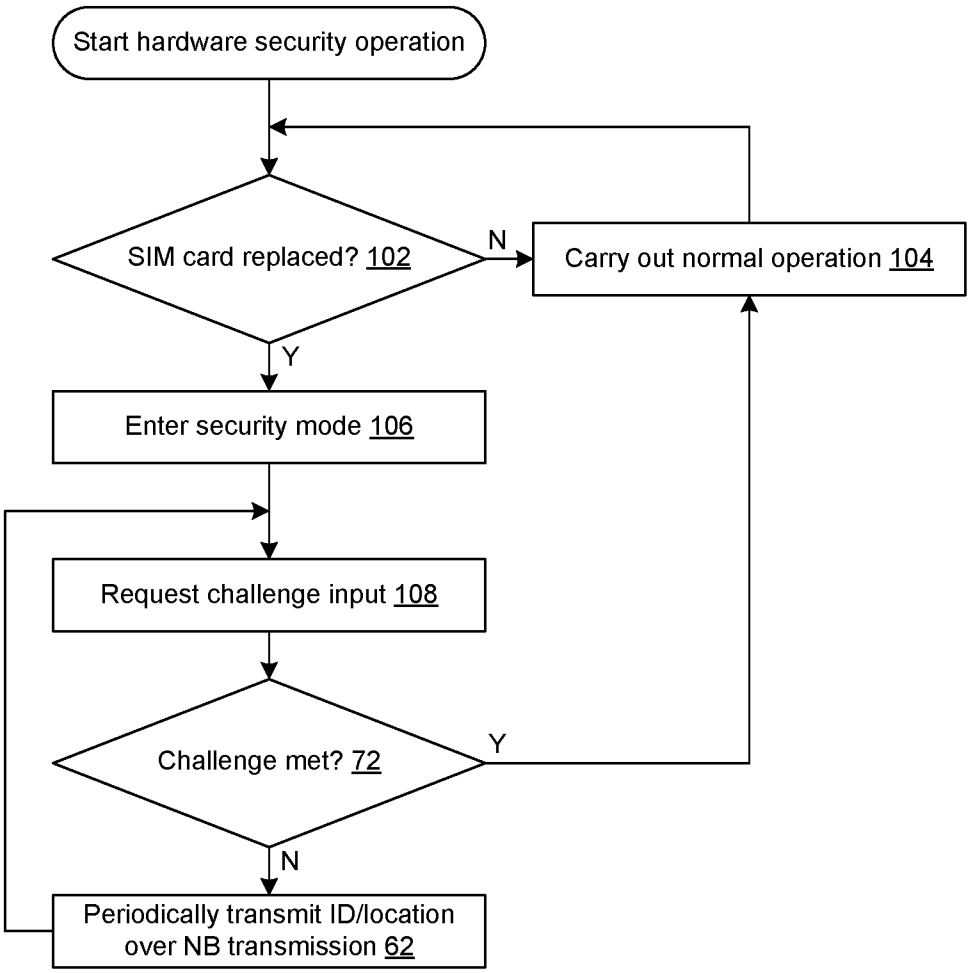
Start hardware security operation
SIM card replaced? 102
N
Carry out normal operation 104
Y
Enter security mode 106
Request challenge input 108
Challenge met? 72
Y
N
Periodically transmit ID/location over NB transmission 62

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/067500

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/12 G06F1/32 G06F21/88 H04M1/73
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04W H04L H04M

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 practicable, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Page: "LTE-M - Optimizing LTE for the Internet of Things White Paper Nokia Networks Nokia Networks white paper LTE-M - Optimizing LTE for the Internet of Things FutureWorks Contents", , 1 May 2015 (2015-05-01), XP055258450, Retrieved from the Internet: URL:http://networks.nokia.com/sites/default/files/document/nokia_lte-m_-_optimizing_lte_for_the_internet_of_things_white_paper.pdf [retrieved on 2016-03-15] page 5; figure 2 page 8 - page 9 ----- -/--	1,5,7, 9-11,15, 17,19,20

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent 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 the actual completion of the international search	Date of mailing of the international search report
18 August 2016	24/08/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Figiel, Barbara

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/067500

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 621 202 A1 (ALCATEL LUCENT [FR]) 31 July 2013 (2013-07-31) abstract paragraph [0006] - paragraph [0021] paragraph [0050] - paragraph [0065] -----	1-20
X	US 2009/280826 A1 (MALIK AJAY [US] ET AL) 12 November 2009 (2009-11-12) abstract paragraph [0003] - paragraph [0024] -----	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/067500

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2621202 A1	31-07-2013	CN 104081803 A	01-10-2014
		EP 2621202 A1	31-07-2013
		JP 2015515156 A	21-05-2015
		KR 20140107600 A	04-09-2014
		US 2015050945 A1	19-02-2015
		WO 2013110436 A1	01-08-2013
US 2009280826 A1	12-11-2009	NONE	