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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2015 (05.02.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/014075 A1

(51) International Patent Classification:
*H04M 1/725* (2006.01) *G08B 19/00* (2006.01)

(21) International Application Number:
PCT/CN2013/089511

(22) International Filing Date:
16 December 2013 (16.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201310333027.8 1 August 2013 (01.08.2013) CN

(71) Applicant: **SPREADTRUM COMMUNICATIONS (SHANGHAI) CO., LTD.** [CN/CN]; Building No.1, Spreadtrum Center, Lane 2288, Zuchongzhi Road, Zhangjiang High-tech Park, Pudong New Area, Shanghai, 201203 (CN).

(72) Inventor: **SHI, Yanshan**; Building No.1, Spreadtrum Center, Lane 2288, Zuchongzhi Road, Zhangjiang High-tech Park, Pudong New Area, Shanghai 201203 (CN).

(74) Agent: **SHANGHAI SAVVY INTELLECTUAL PROPERTY AGENCY**; Room 341, Building 1, 789 West Tianshan Road, Changning District, Shanghai 200335 (CN).

(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, LT, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, 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).

**Declarations under Rule 4.17**:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

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

**Published**:

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

(54) Title: A METHOD AND APPARATUS FOR AN ALARM FOR A MOBILE DEVICE

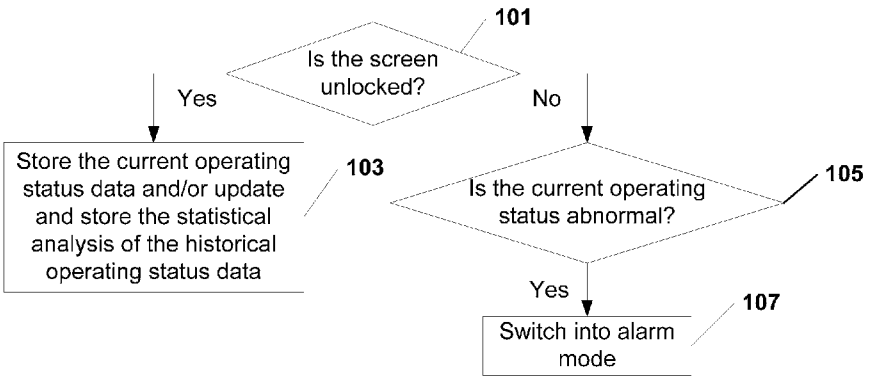


*Figure 1*

(57) Abstract: The present invention discloses a method and apparatus for an alarm for a mobile device. Said method includes storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data, and comparing the current operating status data of the mobile device with the stored historical operating status data and/or the statistical analysis of the historical operating status data to determine whether an abnormal event has occurred. The device will be switched into alarm mode if an abnormal event has occurred. Said method determines whether an abnormal event has occurred to the current status of the mobile device based on a user's daily habits, and the mobile device is switched into alarm mode if any abnormal event has occurred. Conditions for triggering an alarm are kept secret, which is particularly advantageous for alarms required in certain environments.

WO 2015/014075 A1

# A METHOD AND APPARATUS FOR AN ALARM FOR A MOBILE DEVICE

## FIELD OF THE INVENTION

The present invention relates to the field of mobile communication devices, particularly a method and apparatus for an alarm for a mobile device.

## BACKGROUND

The appeal of smart mobile device continues to increase with the advances in communication technology. They come in an ever-increasing array of forms, including smart phones, tablet computers with communication capabilities and watches with communication, navigation and medical testing functions. The major operating systems for smart devices include Apple's iOS, Google-backed Android and Microsoft's Windows Phone. Smart devices are typically characterized by having a substantial number of peripheral devices and a broad range of applications. They are often equipped with GPS systems, blue tooth, WiFi, FM radio, high resolution cameras and large touchscreens, and support one or more of the various communication modes such as 2G systems including GSM, GPRS and EDGE, and 3G systems including WCDMA, CDMA2000 and TD-SCDMA. Some also support the LTE system. There are thousands of applications that can be downloaded from the web and installed on cell phones, including map navigation, cell phone banking and games.

Various types of sensors can be put into smart devices, including gravity sensors, acceleration sensors, directional sensors, triaxial gyroscopes, distance sensors, light sensors and electronic compasses. A gravity sensor works using piezoelectricity. With the standard application for a gravity sensor, the screen display rotates in sync with the device itself when the smart device rotates by about 90 degrees, so that the information shown on the screen, such as text, is maintained in a state that is parallel to gravity, i.e. from top to bottom. An acceleration sensor is an electronic instrument measuring acceleration. A directional sensor detects what direction the device is positioned in, which is not the commonly understood function of a compass. Rather, it can detect whether the device is vertically upright, vertically upside down, horizontally to the left, horizontally to the right, lying face up or lying face down. A

directional sensor is more properly called an angular velocity sensor. A triaxial gyroscope detects positions in six different directions, along with mobile tracks and acceleration. A distance sensor uses the principle of time measurement to find distance as a means of detecting the distance of an object. When making a call the screen on the cell phone will automatically turn off, but when the face of the caller moves away from the phone the screen will automatically come back on again and unlock. A light sensor adjusts the brightness of the screen based on the degree of brightness of the light around it. An electronic compass, also known as an azimuth sensor or a digital compass, utilizes the geomagnetic field to establish the North Pole. Smart devices can be equipped with all or a portion of the aforementioned sensors.

Smart devices usually come with a large capacity battery and a large capacity storage unit such as a 4 GB to 32 GB SD card. Large capacity storage units can be internal or external. Internal storage units are installed internally in smart devices as part of their hardware, while external storage devices can be independently extracted and replaced, in which case the smart devices need only provide the capability for reading from and writing to said equipment such as an SD card slot.

Costs are obviously higher for smart devices than for cell phones with traditional functions, and they provide stronger processing capabilities, more comprehensive functionality and the ability to store and handle greater amounts of data and information. This also means that losing a smart device is a greater loss to a consumer. The primary loss is the cost of purchasing a new device, though there are also risks associated with the data stored on the storage unit of the lost device. Said risks are characterized by the following: the risk of thedisclosure of private information or commercial secrets; and the risk of the destruction of data, such as audio-visual evidence can be deleted by other people resulting from losing the device.

Operating systems for mobile devices provide a lock screen function to prevent losses caused by losing a cell phone. Users can specify images and passwords that are required to unlock the screens so that it is difficult for other people to unlock them, making it impossible for them to use their devices. This is a preliminary form of protection for the data stored on the internal storage unit of the device, but naturally it cannot defend against cracking the locked screen by wiping the device. Privacy protection and

anti-theft applications can be installed on smart devices in the form of cell phone guard software. With these types of software users can set up passwords with respect to the running authority of designated data and applications. They also feature functions such as sending a text message to a designated number when a new card is installed in a phone; when said message is received, performing specific operations including, for example, a positioning application will proceed, and location information will be sent to a designated number, or a photograph will be taken and said photograph will be sent to a designated number, or a warning sound will be emitted when data on the phone is destroyed, etc.

In addition to anti-theft-related security issues, there are other cases where cell phones require security, such as unusual events related to the territory they are active in or their operational status. Said security functions may comprise warnings, monitoring or remote control in cases where a parent wishes to be made aware when her/his child's whereabouts no longer conform to the child's normal range of day-to-day activities. Alarms, data acquisition and remote control for devices are useful when users are caught in unusual circumstances and cannot operate their cell phones, such as during a kidnapping or following an accident. However, methods or devices with these sorts of alarm functionality that meets these requirements do not currently exist.

## BRIEF SUMMARY OF THE DISCLOSURE

The present invention solves the need for an alarm for a mobile device and controlling the mobile device remotely when the mobile device is lost or in an abnormal operational state or environment.

To realize said objective, the present invention provides a method for an alarm for a mobile device comprising the following:

storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data;

comparing the mobile device's current operating status data and the data stored on the storage unit to determine whether an abnormal event has occurred to the mobile device;

switching the mobile device into alarm mode if an abnormal event has occurred.

Optionally, in the step of storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data, said historical operating status data comprises the operating status data when the screen of the mobile device is in an unlocked state.

Optionally, in the step of comparing the current operating status data of the mobile device with the stored historical operating status data and/or the statistical analysis of the historical operating status data, said current operating status data comprises the operating status data when the screen of the mobile device is in a locked state.

Optionally, in the step of storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data, said operating status data comprises one or more of the following: hardware data, location data and communication service application data. Said hardware data comprises the locked status of the screen and/or the motion status of the mobile device; said location data comprises one or more of the following: the identification data for the cell the mobile device is resident in, the access point of the connected WiFi and the GPS positioning data for the current location; and saidcommunication service application data comprises the call log for the mobile device and/or the text message log. The statistical analysis of said location data comprises one or more of the following: the time duration corresponding to the ID data for the cell the mobile device is resident in, the time duration corresponding to the connection to the WiFi access point, and the time duration corresponding to the GPS positioning data for the current location.

Optionally, in the step of comparing the current operating status data of the mobile device with the stored historical operating status data and/or the statistical analysis of the historical operating status data, said current operating status data comprise one or more of the following: hardware data, location data and communication service application data. Said hardware data comprises the locked status of the screen and/or the motion status of the mobile device; said location data comprises one or more of the following: the ID data for the cell the mobile device is resident in, the access point of the connected WiFi and the GPS positioning data for the current location; and said communication service

application data comprises the call log for the mobile device and/or the text message log. Said statistical analysis of said location data consists of one or more of the following: the time duration corresponding to the ID data for the cell the mobile device is resident in, the time duration corresponding to the connection to the WiFi access point, and the time duration of the mobile device in the area corresponding to the location data as determined by the GPS positioning.

Optionally, said cell ID data includes the cell ID (aka "cell identity"), the location area identification (LAI) and the routing area identification (RAI); and said WiFi access point information includes the service set identifier (SSID) or the basic service set identifier (BSSID).

Optionally, the following steps are performed in whole or in part to determine whether an abnormal event has occurred:

the screen of the mobile device is not unlocked within a first designated period of time;

the current operating status data when the screen of the mobile device is in a locked state does not appear in the historical operating status data and/or the statistical analysis of the historical operating status data stored when the screen was in an unlocked state within a second designated period of time.

Optionally, the period of time measured within said first designated period of time is the time elapsed since the mobile device was turned on, and the period of time measured within said second designated period of time is the time elapsed since the mobile device was turned on.

Optionally, the following operations are performed in whole or in part once the mobile device is switched into alarm mode:

one or more of the following are sent to a designated contact: a location, a photograph which has been taken, or predetermined alarm data;

an operation is performed according to instructions received from a designated contact.

Optionally, said instructions include one or more of the following: uploading, deleting, encrypting data or emitting an alarm sound.

Optionally, in addition to storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data, the date and time of the historical operating status data are stored, and the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data stored prior to a third designated period of time are deleted.

The present invention also provides an apparatus for an alarm for a mobile device comprising a storage unit, an alarm control unit and an operating status data acquisition unit. The operating status data acquisition unit acquires the current operating status data from the mobile device. The alarm control unit analyzes the data acquired by the operating status data acquisition unit and stores it in the storage unit, and then compares the mobile device's current operating status data and the data stored on the storage unit to determine whether an abnormal event has occurred to the mobile device. The device is switched into alarm mode if an abnormal event has occurred.

Optionally, the apparatus further includes a settings unit for configuring a designated time and/or emergency contacts and outputting said designated data to the storage unit for storing.

In the present invention the current operating status data of the mobile device is compared with the stored historical operating status data and/or the statistical analysis of the historical operating status data to determine whether an abnormal event has occurred. This is advantageous because an alarm message will be sent out when the mobile device is lost or misplaced, or when the user cannot operate it. Conditions for triggering an alarm are kept secret, which is particularly advantageous under certain circumstances.

## BRIEF DESCRIPTION OF THE DRAWINGS

The summary of the present invention given above and the specific embodiments given below are better understood when reviewed together with the drawings. It should be clarified that the drawings act only as examples of the present invention for which patent rights are being sought. Reference numbers in the drawings are used to indicate the same or similar elements.

Figure 1 is a schematic flow chart of Embodiment 1 of the present invention; and

Figure 2 is a schematic diagram of Embodiment 2 of the present invention.

## DETAILED DESCRIPTION

The detailed characteristics and features of the present invention given in the embodiments below are sufficient to allow anyone skilled in the art to understand the technical content of the present invention and to implement it. The specification, claims and drawings of the present invention allow those skilled in the art to readily understand the objectives and features of the present invention.

The description of at least one of the exemplary embodiments given below is explanatory only, and does not restrict the present invention and its application or use.

The present invention solves the need for an alarm for a mobile device and controlling the mobile device remotely when the mobile device is lost or in an abnormal operational state or environment.

### EMBODIMENT 1

Figure 1 is a schematic flow chart of Embodiment 1 of the present invention.

Step 1 (101): Determine whether the screen is in an unlocked state. If it is, perform Step 2. If not, perform Step 3.

Step 2 (103): Store the current operating status data as the historical operating status data for the mobile device, and/or update and store the statistical analysis of the historical operating status data, then complete said update process.

Step 3 (105): Compare the current operating status data of the mobile device with the stored historical operating status data and/or the statistical analysis of the historical operating status data to check for abnormalities in the current operating status data for the mobile device. Perform Step 4 if there are any abnormalities. If not, complete the update to the operating status.

Step 4 (107): Switch into alarm mode.

The historical aspect of the historical operating status data refers to data from prior to the present moment, though it may also further include data from the present moment as well. Similarly, the stored historical operating status data comprises the operating status data or the statistical analysis of said data from prior to the present moment, though it may also further include current operating status data and the updated statistical analysis of the current operating status data. Once the current operating status data is saved it turns into historical operating status data or a portion of the statistical analysis of the operating status data.

Said method illustrates the process for one instance of an operating status update. There are multiple causes for triggering an update, which can be classed as periodic or event-triggered.

An example of a periodic update is when said process is performed once every 10 minutes. An event-triggered update for the mobile device triggers the aforementioned process when the following events occur: the device is turned on, the device is turned off, the screen is unlocked, the screen is locked, cell update, location area update or router area update occurs in a cellular communication network, the mobile device accesses a WiFi network or disconnects form a WiFi network, the GPS is turned on or off, there is a change to the GPS positioning data, a telephone call is made or received, and a text message is sent or received.

Said operating status data includes hardware data, location data and/or communication service application data. There are multiple metrics for analyzing the location data. Examples include the duration or the frequency that the mobile device is resident in a given cell or connects to a given WiFi access point during a designated period, such as over a 7-day or 30-day period; the stored cell ID and the LAI, and the stored duration or frequency of residence corresponding to them; or the stored SSIDs of the WiFi access points and the stored duration or frequency of connections corresponding to them. The residence duration in the location data area can also be analyzed and stored. The area where the location data, such as PGS positioning data, is derived from can be determined using various methods. For example, the latitude and longitude of the given location data can be defined as a center with a radius of 1 km. When the latitude and the longitude of the mobile device's GPS location data is located

less than 1 km from said center it is deemed to be within said area, and the residence time for the mobile device at any position within 1 km of said center is assigned to the area corresponding to said center. The shape of said area can also be a polygon formed by multiple location data.

The screen in Step 2 is in an unlocked state. When the mobile device acquires the current resident cell ID it will also acquire the access point's SSID if it gains WiFi access. The frequency number which has been stored will be increased by 1 if said cell ID or SSID is found in the stored statistical analysis. Within this statistical analysis there is a corresponding relationship between the frequency and the residence or connection duration. If said cell ID or SSID is not found, then said cell ID or SSID is stored and the frequency number is stored as 1. Said stored data can further include the status of the screen as unlocked.

In Step 3 the methods for checking for abnormalities in the current operating status data for the mobile device including the following: if the current cell ID, LAI, SSID and the current location data area appear in the stored data, then the current operating status data is deemed to be normal. However, if the current cell ID, LAI, SSID and location data area have not been stored when the screen is in a locked state, then the current cell ID, LAI, SSID and location data area are stored, the screen status corresponding to them is stored as locked, and the corresponding frequency number is designated as 1. Otherwise, "1" is added to the frequency number corresponding to the current cell ID, LAI, SSID and location data area when the screen is in a locked state. When the frequency number for the current cell ID, LAI, SSID current location data area is lower than the designated frequency number, e.g., it is at 50, it is determined to be normal. If not, then the current operating status data is deemed to be abnormal.

In Step 3 there are multiple ways of determining whether there are any abnormalities in the current operating status data. For example, a first designated period can be 24 hours. The continuous locked state of the screen is then measured, and if it exceeds said first designated period it will be deemed abnormal. In another example, the current operating status data can be analyzed with the screen in a locked state, and if the stored operating status data with the screen in an unlocked state does not appear for a continuous period that exceeds a second designated period, such as 24 hours, then it will be

deemed abnormal. For example, while the screen was in an unlocked state, if for a continuous period of 24 hours the mobile device has not accessed the WiFi access point that was previously accessed or the cell in which it was resident, then it will be deemed abnormal.

The shorter said first and second designated periods are, the more beneficial they are in promptly sending out alarm data, though the false alarm rate will also be higher.

In Step 3 the mobile device's communication service application data can be used to determine whether there is any abnormality. For example, the calls made or received for the mobile device or the contacts who have sent text messages are stored, and the corresponding communication frequency and the date of the latest communication are recorded. Statistical results occurring before a third designated period are deleted, for example, 150 days, and the contacts are listed in the order based on the frequency of communication, from largest to smallest. When determining whether an abnormality has occurred, a check is made to see if any one contact out of the first N of said list of contacts, for example the first 50, has communicated with the mobile device within the most recent second designated continuous period. If yes, then the status is deemed normal, otherwise it is deemed abnormal. The communication service application data may also be determined abnormal by checking to see if communication has been made by a designated emergency contact within the second designated continuous period of time. For example, a user's parents' telephone number may be designated as the emergency contacts, and the device will be switched into alarm mode if no contact has been made with the parents within 24 hours.

In Step 4 the operation for switching into alarm mode comprises encrypting the data stored on a storage apparatus and sending an alarm message to an emergency contact. A text message will then be sent from the emergency contact's number containing instructions, and the device will perform operations given in said instructions, which may include encryption, deletion, taking a photograph, sending out an alarm, uploading data, establishing the position of the device or uploading location data.

One advantage of the present embodiment is that the mobile device will be switched into alarm mode when the user has not unlocked the mobile device for a long period of

time and has not sent or received messages or calls from designated contacts, and/or the mobile device appears to be outside of the normal daily geographical range of the user for a long period of time. This is advantageous because an alarm message is sent out when the mobile device is lost or misplaced, or when the user cannot operate the mobile device. The conditions for triggering an alarm are kept secret, which is particularly advantageous for alarms required in certain environments.

## EMBODIMENT 2

As shown in Figure 2, Embodiment 2 provides an apparatus for an alarm for a mobile device of the present invention. The alarm apparatus for a mobile device comprises a settings unit 201, a storage unit 203, an alarm control unit 205 and an operating status data acquisition unit 207.

The settings unit 201 is used to configure the designated period of time and the emergency contacts of Embodiment 1 and to output the settings data to the storage unit 203 to be stored.

The operating status data acquisition unit 207 acquires the current status data from the mobile device including location data, communication service application data and screen lock status data.

The alarm control unit 205 analyzes and stores the data acquired by the operating status data acquisition unit to the storage unit 203. It also determines whether the current operating status is abnormal using the data stored in storage unit 203. If it is abnormal the mobile device will be switches into alarm mode.

The advantages of the present invention are that it incorporates the user's daily habits, such as which contacts the user typically communicates with, which cell the device is normally resident in, which areas it generally appears in and how often the phone is unlocked and used, to determine whether anything is unusual about the current status of the mobile device. If the circumstances are deemed abnormal then the device will be switched into alarm mode. The traditional technology simply judges whether a password has been entered incorrectly for a given number of times or whether a SIM card has been changed before it determines that a device should be

switched into alarm mode. Even though the method of the present invention delays putting the mobile device into alarm mode longer than the traditional technology, the conditions for triggering an alarm are secret, which is particularly advantageous under certain circumstances such as if the user is kidnapped and held for a long period of time and cannot operate a mobile device.

The embodiments of the present invention are given in the aforementioned sequence in order to distinguish between their respective points of emphasis. The same or similar parts appearing in all of the embodiments will be readily apparent. The descriptions of the apparatus disclosed in the embodiments is comparatively brief because the methods given in the different embodiments all correspond to each other, therefore the nature of the apparatus will be readily apparent in those parts of the embodiments which refer to the methods.

The preferred embodiments of the present invention disclosed above do not limit the present invention. Those skilled in the art can make changes or modifications to it without departing from the spirit and scope of the present invention, therefore the claims of the present invention shall define the designated scope of protection for the present invention.

What is claimed is:

1. A method for an alarm for a mobile device, comprising the following:

storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data;

comparing the current operating status data of the mobile device with the stored historical operating status data and/or the statistical analysis of the historical operating status data to determine whether an abnormal event has occurred;

switching the mobile device into alarm mode if an abnormal event has occurred.

2. The method of claim 1, wherein, in the step of storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data, said historical operating status data comprises the operating status data when the screen of the mobile device is in an unlocked state.

3. The method of claim 1, wherein, in the step of comparing the current operating status data of the mobile device with the stored historical operating status data and/or the statistical analysis of the historical operating status data, said current operating status data comprises the operating status data when the screen of the mobile device is in a locked state.

4. The method of claim 1, 2 or 3, wherein, in the step of storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data, said historical operating status data includes one or more of the following: hardware data, location data and communication service application data.

5. The method of claim 4, wherein said hardware data comprises the locked status of the screen and/or the motion status of the mobile device; said location data comprises one or more of the following: the ID data for the cell that the mobile device is resident in, the access point of the connected WiFi, the GPS positioning data for

the current location; and said communication service application data comprises the call log for the mobile device and/or the text message log.

6. The method of claim 5, wherein the statistical analysis of said location data comprises one or more of the following: the time duration corresponding to the ID data for the cell the mobile device is resident in, the time duration corresponding to the connection to the WiFi access point, and the time duration corresponding to the GPS positioning data for the current location.

7. The method of claim 1, 2 or 3, wherein, in the step of comparing the current operating status data of the mobile device with the stored historical operating status data and/or the statistical analysis of the historical operating status data, said current operating status data comprise one or more of the following: hardware data, location data and communication service application data.

8. The method of claim 7, wherein said hardware data comprises the locked status of the screen and/or the motion status of the mobile device; said location data comprises one or more of the following: the ID data for the cell the mobile device is resident in, the connected WiFi access point and the GPS positioning data for its current location; and said communication service application data comprises the call log for the mobile device and/or the text message log.

9. The method of claim 8, wherein the statistical analysis of said location data comprises one or more of the following: the time duration corresponding to the ID data for the cell the mobile device is resident in, the time duration corresponding to the connection to the WiFi access point, and the time duration corresponding to the GPS positioning data for its current location.

10. The method of claim 1, wherein the following steps are used in whole or in part to determine whether an abnormal event has occurred:

the screen of the mobile device is not unlocked within a first designated period of time;

the current operating status data when the screen of the mobile device is in a locked state does not appear in the historical operating status data and/or the statistical analysis of the historical operating status data stored when the screen was in an unlocked state within a second designated period of time.

11. The method of claim 6, wherein the period of time measured within said first designated period of time is the time elapsed since the mobile device was turned on, and the period of time measured within said second designated period of time is the time elapsed since the mobile device was turned on.

12. The method of claim 1, wherein the following operations are performed in whole or in part once the device is switched into alarm mode:

one or more of the following are sent to a designated contact: a location, a photograph which has been taken, or designated alarm data;

an operation is performed according to instructions received from a designated contact.

13. The method of claim 8, wherein said instructions comprises one or more of the following: uploading, deletion, encrypting data or emitting an alarm sound.

14. The method of claim 1 or 2, wherein, in addition to storing the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data, the date and time of the historical operating status data are stored and the historical operating status data for the mobile device and/or the statistical analysis of the historical operating status data stored prior to a third designated period of time are deleted.

15. An apparatus for an alarm for a mobile device comprising a storage unit, an alarm control unit and an operating status data acquisition unit,

the operating status data acquisition unit for acquiring the current operating status data from the mobile device;

the alarm control unit for analyzing the data acquired by the operating status data acquisition unit and storing it in the storage unit, and then comparing the mobile device's current operating status data and the data stored on the storage unit to determine whether an abnormal event has occurred to the mobile device, and switching the mobile device into alarm mode if an abnormal event has occurred.

16. The apparatus of claim 15, further comprising a settings unit for configuring a designated time and/or emergency contacts and outputting said designated data to the storage unit for storing.

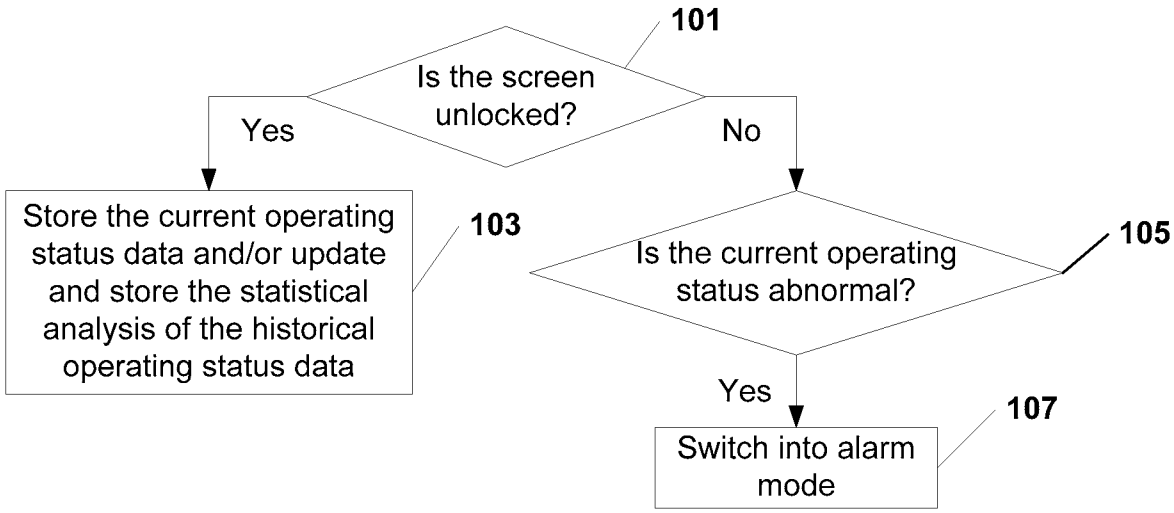


*Figure 1*

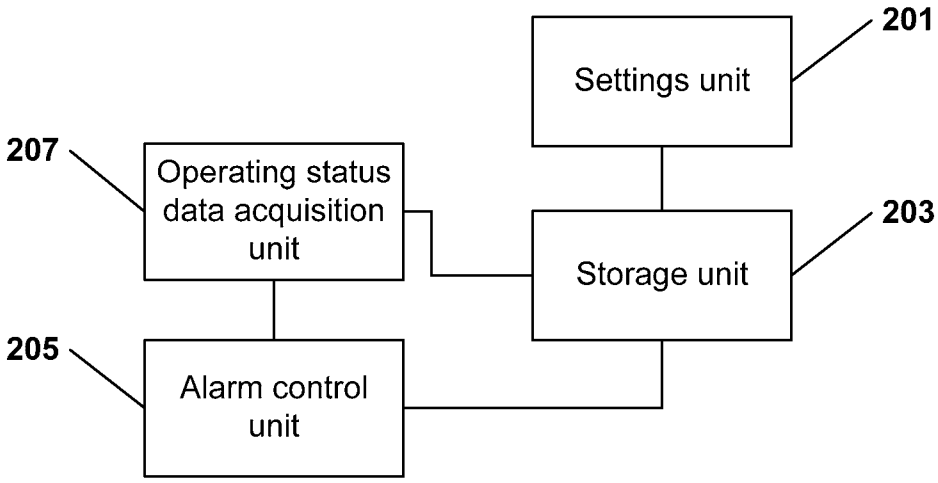


*Figure 2*

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2013/089511**

**A. CLASSIFICATION OF SUBJECT MATTER**

H04M 1/725(2006.01)i; G08B 19/00(2006.01)i

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)

H04M, H04W, H04Q, G08B

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)

CNABS,CNTXT, CNKI,VEN: phone, telephone, abnormal, different, alert, alarm, warm, lock, unlock

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| PX | CN 103428335 A (XI'AN WINGTECH ELECTRONIC TECHNOLOGY CO., LTD.) 04 December 2013 (2013-12-04)<br>see the abstract, description, paragraphs [0014]- [0046] and figure 1 | 1-16 |
| X | CN 101778353 A (HUAWEI DEVICE CO., LTD.) 14 July 2010 (2010-07-14)<br>see the abstract, description, paragraphs [0018]- [0093] and figures 1-4 | 1-16 |
| A | CN 102946468 A (GUANGDONG OPPO MOBILE COMMUNICATION CO., LTD.) 27 February 2013 (2013-02-27)<br>see the whole document | 1-16 |
| A | JP 2012244435 A (FUJITSU LTD.) 10 December 2012 (2012-12-10)<br>see the whole document | 1-16 |

☐ Further documents are listed in the continuation of Box C. ☑ 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 |
|---|---|
| **28 April 2014** | **09 June 2014** |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| **STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA(ISA/CN)**<br>**6,Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088 China** | **CHEN,Junru** |
| Facsimile No. **(86-10)62019451** | Telephone No. **(86-10)62089549** |

**INTERNATIONAL SEARCH REPORT**
Information on patent family members

International application No.
**PCT/CN2013/089511**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| CN 103428335 A | 04 December 2013 | None | |
| CN 101778353 A | 14 July 2010 | None | |
| CN 102946468 A | 27 February 2013 | None | |
| JP 2012244435 A | 10 December 2012 | None | |