Mobile Tracking for Theft Protection

Aqsa Chappalwala [1], Sohel Patel [2], Mohammad Sohail Shaikh [3], Ashfaq Shaikh [4]

[1, 2, 3] *B.E Students, Department of Information Technology, M.H.Saboo Siddik College of Engineering, Mumbai University, Mumbai, India.*

[4] *Assistant Professor, Department of Information Technology, M.H.Saboo Siddik College of Engineering, Mumbai University, Mumbai, India.*

Abstract

Although the powerful functions of smartphones provide much convenience for users, it causes a great damage because of loss and theft. The smartphone usage among people is increasing rapidly and hence its theft is also increasing. In this paper, we propose a software model to track the stolen smartphones. It can also be used in case when the device is misplaced but not stolen. The user will be able to find the position of the device using GPS system or network services which will provide geographical location of the device. But the location tracking isn't just enough as the person who has stolen it, can move from one place to another, so the proposed software model will also capture the image of the person. The location details along with the image of the person will be mailed to the registered email address. Moreover, if the person replaces the SIM card of the device with his own SIM, then a message will be sent automatically to the registered number from this new SIM card, thus revealing the identity of the device stealer.

Keywords - Theft protection, device tracking, GPS, location tracking, android.

1. Introduction

A smartphone offers a variety of features such as calling, mobile payments, music, camera, GPS, Internet and more. Worldwide, smartphone sales surpassed 41 million units in the third quarter of 2009, a 12.8% increase from the third quarter of 2008, according to Gartner, Inc. [1]. Suppressing all other traditional communication purpose, smartphones are now at the peak of popularity in their usage of accessing the internet which includes mail access, social networking, mobile shopping and mobile banking. Although the powerful functions of smartphones provide much convenience for users, it also causes a great damage because of loss and theft. For example, a lost smartphone could be used for international calls by the smartphone finder and the personal information stored in the smartphone could be exposed to the finder. Hence, internet and GPS can be used as an important tool for finding the phone in case when it is lost or stolen. Few surveys [2][3], about mobile theft in various countries has been studied. This claims the need of an intelligent application to be run in mobile to eradicate mobile theft and track the mobile even if the SIM is changed and/or phone is reset/formatted.

2. Proposed Model

The proposed model is divided into client and server architecture. The client side will have the tracking software running on it whereas the server will have the database consisting of details related to the smartphone.

2.1. Client End

The client runs on the smartphone. The client software will monitor the remote database each time the device is connected to the internet, to check if the "stolen bit" corresponding to the IMEI number of the device, is set to "true" or not. The significance of the "stolen bit" is that it can take only 2 values that is "true" or "false". The value "true" is an indication to the client that the device has been stolen, whereas the value "false" indicates that the device is not stolen. Moreover, to hide the presence of the existence of the client on the device, it will be implemented as a service running in the background, so the stealer of the device will have no idea that there is some tracking process being carried on the device.

2.2. Server End

The server end is implemented using PHP and MySQL database. The database which will store the details of the registered smartphones such as its IMEI, contact number, email id, location details, picture, stolen bit, etc. corresponding to a device. The access to this remote database is provided to both, the software as well as to the owner of the device. Once, the device is stolen, the owner can manually update the stolen bit corresponding to the IMEI number of the device to "true" in the database, using the interface implemented in PHP. The following figure explains the working of the entire model, when the user uses the smartphone for the very first time and registering the device into the remote database.
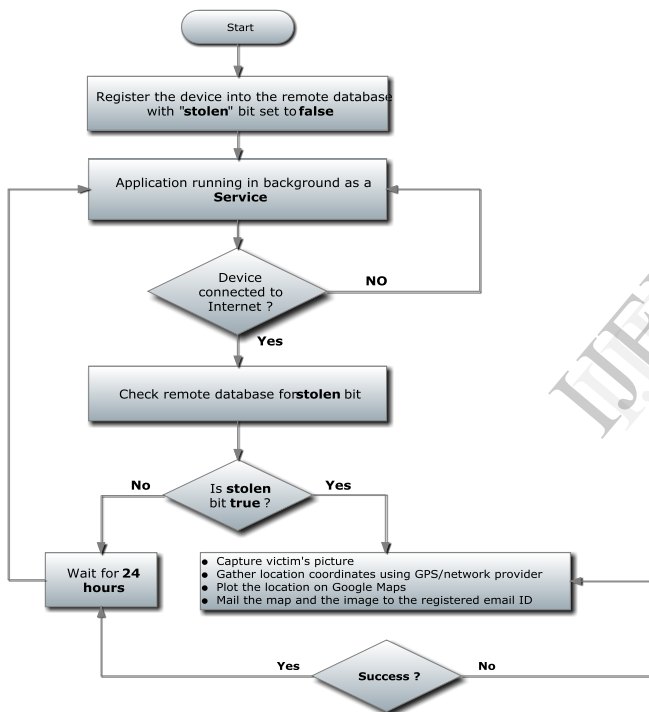

Figure 1.0 : Working of the proposed model.

3. The Proposed Algorithm

The algorithm of the proposed model has been given below:

Step 1: Start the device. Enter the email id and contact number.

Step 2: Connect to the internet using Wi-Fi or mobile data.

Step 3: The IMEI of the device along with the email id and contact number is registered into the remote database and stolen bit is set to "false".

Step 4: Client software is running in the background of the device as a Service.

Step 5: Check the value of the stolen bit in the remote database corresponding to the IMEI of the device.

Step 6: If stolen bit is "false", continue to run in background and perform another check after 24 hours. If stolen bit is set to "true", gather current location co-ordinates of the device, the SIM card number, capture the photo using front camera(if the device has one), plot the location co-ordinates on Google Maps, send a text message to the registered contact number (if SIM card has changed) and email all the data to the registered email id.

4. Functionalities Provided by the Software

The proposed software model has a number of different ways in addition to location tracking, which adds up to the effectiveness and efficiency of the tracking process. These features have been enlisted:

4.1 Location tracking using GPS

The Global Positioning System (GPS) is a satellite-based navigation system made up of a network of 24 satellites placed into orbit by the U.S. Department of Defence. GPS was originally intended for military applications, but today it is used for a wide variety of applications. There are no subscription fees or setup charges to use GPS. Today's GPS receivers are extremely accurate to within 15 meters on average [4]. Taking advantage of this accuracy, we are incorporating GPS functionality in this software to detect the location of the stolen smartphone accurately. In the user segment the GPS receivers, such as the ones being integrated in most smartphone today, receive those signals and can use a minimum of 4 signals to calculate a three-dimensional location based on the signals' propagation delays.

4.2 Location tracking using Network Provider

Network-based techniques utilize the service provider's network infrastructure to identify the location of the handset. The advantage of network-based techniques (from a mobile operator's point of view) is that they can be implemented non-intrusively, without affecting the handsets. The accuracy of network-based techniques is

both dependent on the concentration of base station cells [5]. The Network Provider determines location based on availability of cell tower and WiFi access points and the results are retrieved by means of a network lookup. However, location tracking using network provider is not preferable due to its low accuracy but there is no harm in using it as a complementary tracking mechanism along with GPS [6]. Similar to WiFi positioning, cellular network positioning (Cell-Id positioning) uses a unique identifier of the base stations consisting of the mobile country code (MCC), the mobile network code (MNC), the id of the cell tower (CID) and its according location area identifier (LAI). That unique ids have to be related to a reference position like a GPS position fix. With these unique identifiers, a mobile phone can lookup the currently received base stations in a database via an IP-based network connection in order to retrieve the location. Since reception areas of base stations are much larger than those of WiFi hotspots, Cell-Id positioning is very inaccurate but consumes little energy due to the fact that mobile phones make measurements about nearby base stations anyways quite frequently for handover or location management. In summary, it can be stated that a clear advantage of WiFi positioning in comparison to GPS is that it is also suitable for indoor positioning and has moderate power consumption, but on the other hand, it is not as accurate [7].

4.3 Image capture using front camera

The location tracking mechanisms helps in serving their own unique purpose to determine the location of the stolen smartphone. To provide an additional help in tracking the stealer of the smartphone, the software will capture the image of the stealer using the front camera (if the device has one on it). The existence of this functionality will provide an additional benefit over location tracking.

4.4 Sending a text-message to the registered number

Text based messaging is most common in mobile devices, in which people can communicate with each other using short messaging service (SMS). The SMS is sent from one mobile device to another using SIM card services. This functionality adds effectiveness to the above three functionalities. The advantage of sending a text message from the stolen smartphone is that, we will be able to get the identification number of the SIM card of the stealer, so that we can easily trace the identity of the owner of that SIM card. However,

tracking of identity using the SIM number is not possible manually, but it requires some legal process.

4.5 Unique identification of device using IMEI number

The International Mobile Station Equipment Identity (IMEI) number is a unique 15-digit number allotted to each and every mobile phone. The IMEI number is used by a GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network. For example, if a mobile phone is stolen, the owner can call his or her network provider and instruct them to "blacklist" the phone using its IMEI number. This renders the phone useless on that network and sometimes other networks too, whether or not the phone's SIM is changed.

5. Conclusion

Mobile tracking for theft protection with the proposed approach has been presented in this paper. The efficiency and effectiveness of tracking depends upon the accuracy of the GPS hardware that is used on the device. The proposed software will consume very less memory and less battery power. The system can be used in any android device which has an IMEI number, and a GPS system. The most important advantage of the proposed software is that it will be embedded in the system ROM, so that it will never die even if the device is hard reset or formatted. The location can be effectively tracked using GPS and/or network provider. Additional details such as photo of the stealer can also be captured. A text message can also be sent when the SIM card is changed.

6. References

[1] http://www.gartner.com/it/page.jsp?id=1224645.
[2] Survey about mobile theft in USA : http://www.symantec.com/about/news/release/article.jsp?prId=20110208_01.
[3] Survey about mobile theft in India : http://asiarelease.asia/norton-survey-reveals-1-in-2-indians-is-avictim-ofmobile-phone-loss-or-theft/.
[4] http://en.wikipedia.org/wiki/Global_Positioning_System.
[5]http://en.wikipedia.org/wiki/Mobile_phone_tracking#Network-based.
[6] http://en.wikipedia.org/wiki/Mobile_phone_tracking.
[7] Simulating Power Consumption of Location tracking algorithms, 2012 IEEE 36th International Conference on Computer Software and Applications.
[8] http://en.wikipedia.org/wiki/Global_Positioning_System.