

Phone theft detection & continuous tracking with user profile recording using android

Senguttuvan S¹, R.Senthamarai¹, K.Pushpavathi²

¹Department of Computer Applications, Faculty of Computer Applications, Aarupadai Veedu Institute of Technology, Paiyanoor, Chennai-603104.

²Vinayaka Missions University, Salem, India

*Corresponding author: E-Mail: sengutt0sellur@gmail.com

ABSTRACT

Mobile computing offers significant benefits for organizations that choose to integrate the technology into their fixed organizational information system. The emergence of powerful portable computers, along with advances in wireless communication technologies, has made mobile computing a reality. In the Existing System, Lots Of Applications Are Developed To Track A Smart Phone But Still It Is Not That Comfort In Finding The Exactly. We Have To Manually Report To The Customer Of The Mobile To Block The Imei Number Of The Phone. In The Proposed System, Android Application Is Deployed With Initial Registration Of Alternative Mobile Number. If The Phone Is Stolen And Sim Card Is Not Changed, Original User Will Send Sms Through A Normal Phone Or Through An Application Deployed In Another Android Phone To Track And Verify The Location Of The Theft Mobile. The Application Will Track The Theft Phone. In The Modification Part, We Are Implementing Both The Logic Of Tracking The Theft Phone With Changed Sim Card & Not Changed Sim Card. Thief Photo Is Captured By Automatic Camera Initiation And Voice Is Recorded And Uploaded In The Server. Both The Location And Voice Are Sent As Sms Alert To The Alternative Mobile Number Of The Original User. Thief Photo Is Mailed To E Mail Id Of Original User. Location & Alert Sms Are Sent To The Alternative Number Even If Interest Is Not Available.

KEY WORDS: Location tracking, Android, Smart Phone, Context, Tracking.

1. INTRODUCTION

Recently, location privacy has become a topic of concern largely due to the proliferation of GPS devices, web location services, WLAN, and cell ID based positioning technologies. The ability to locate a wireless device for beneficial reasons has been looked into by several researchers. Localization can be passive or active. In passive localization, the users do not carry any device (having radiofrequency transmitter) but in active localization the users carry devices. In active localization, users may know about their or others' (depending on the application and privacy policy) location with the help of some basic components like mobile devices, mobile communication network, service provider like the Global Positioning Service (GPS) and Geographical Information System (GIS) etc. Even a cell phone without a GPS unit can send location information to the operator by using radio signal transmission of the base station. Different localization principles that may be applied to gain position information with respect to an object to be tracked include: Network-based. Wireless Internet have made localization easier and more effective. Since smart handhelds have a variety of sensors like accelerometer, compass, gyro etc, it is possible to make tracking systems not only location aware but also context aware. Location is a part of context but context also encompasses conditions like if the user is moving, if he is taking turns etc. Gathering context helps to better track an individual especially for surveillance. For instance, if the device is stolen, it would be easy to predict the exact location of the device at some future time instant if the context (including location) of the device is known at the current time instant. Moreover context information can be utilized to minimize network data transfer for these kinds of applications. For example, if the device is static or moving slowly there is no need of sending updates to the tracker device frequently. However effectiveness of context sensing depends on various other conditions like if the user is carrying the device in his/her pocket or holding the device in hand etc.

Related Works: This section explains some of the works of other authors related to tracking of Android devices. In (Dar, 2013), the authors have designed an application to track Android devices when lost. The application installed on the device discovers the current geographical position either from GPS or Network-Service-Provider and transmits its details to the web-application via Internet. But in this application the owner of the lost mobile handset can track the phone as long as the mobile number is not changed. If the mobile number is changed, the application will not work. Another concern is Web Server. The application only stores the coordinates, from which it is really difficult to track the locality of the position. From this work it is not clear whether the application has to be kept running when the phone is not lost and also what triggers the application to run for transmitting the current position to the web application if the application is not running.

Proposed System: In the PROPOSED SYSTEM, Android Application is deployed with initial registration of Alternative Mobile number. If the phone is stolen, Original user will send SMS through a Normal phone or through an Application deployed in another Android phone to Track and verify the location of the theft Mobile. If the Thief changes the SIM card immediately Location details are sent to the alternative Phone number of the original User. In

the MODIFICATION part, both the logic of tracking the Theft Phone with SIM Card & Theft Phone with changed SIM Card is tracked continuously. Thief Photo is captured by automatic Camera Initiation and Voice is recorded and uploaded in the server. Both the Location and Voice are sent as SMS Alert to the Alternative Mobile number of the Original User.

Our Work: Our goal is to design a smart phone-based context tracking service that can be used to track context of a handheld device including location and state. This can be used to identify lost or stolen smartphones from any other handheld device. The proposed system has two components; one is the server module that provides the location and context upon request from a client. The server module has to be installed in the device being tracked. It should be preconfigured (offline) with two

Passwords

System Password: Used to authenticate a user who can configure the default client device. It is also used to authenticate user requesting to stop context tracking service.

SMS Password: This is used to authenticate client that requests for starting context tracking service. The client module can be in any other device that can initiate the tracking service through SMS (Short Message Service). If the client module is in an Android device then Google Map can be used to show the locality of the tracked device (server).

Here a sensor called ‘accelerometer’ has also been used to detect whether the phone having the server module is moving or not. If the device is moving fast, location updates are needed to be sent more frequently. It might happen that the phone (having the server component) is stolen and the SIM card of the phone is removed. But if the phone is re-boot two notification messages to the default preconfigured client device. One of these two messages contains the phone number of the new SIM card which is inserted and another message will contain the current location of the lost phone. These two messages are always shared whenever the server is reboot or a new SIM card is inserted into the phone. Moreover if the client is installed in another smart hand held device, current location of the server can be shown on Google Map which is more user friendly than only receiving the text message with the location information.

Implementation: The system is implemented in Java in Android SDK. We call the system Mobile Police. This works in two phases described below.

Online Phase: In this phase context tracking occurs. It is initiated by an SMS sent from any client (may not be the default one) in the format When the server module installed in the phone receives the SMS, the application will divide this message into two substrings. The first part “START LSERVICE” works as a command and the second part is checked for authentication against the SMS password stored in the database of the server device. If these conditions are satisfied, context tracking gets started in background of the server device. The SMS will be sent from the lost mobile in the following

format: “JU001

My mobile’s current location is :

Latitude :<current_latitude>

Longitude :<current_longitude>

Location :<current_location>

Device moved >= 100m”



Figure.1. Registration form



Figure.2. Registration form

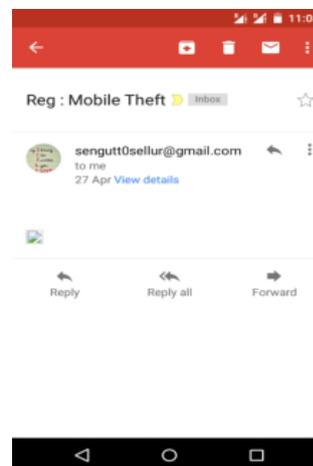


Figure.3. Online Phase

2. CONCLUSION

In this paper, a context tracking service is designed and implemented that can be used to track context of individuals and hence can be applied to locate lost/stolen smart phones or users if he/she is struck in trouble tracks the location through the network not by using hungry GPS and senses user context through accelerometer Location updates are sent based on the context of the device Tracking can be remotely triggered from any device that may not have Android Operating system.

ACKNOWLEDGEMENT

This paper is done for MCA Department of Computer Applications Aarupadai Veedu Institute of Technology College Vinayaka Missions University, Salem, India.

REFERENCES

- Bahl P, Padmanabhan V, Enhancements to the RADAR user locat system, Microsoft Research, 2000.
- Dar NA and Khan AA: A Devices: An Implementation of Services and Web-services in Mathematics & Computing Systems, 54, January-June 2013.
- Freudiger J, Manshaei MH, Hub Parkes JB, Non-cooperative Location Pr theoretic Analysis. In ACM Conference o Communications Security, 2009.
- Henniges R, Current approx Service-Centric Networking - TU-Berlin, 2012
- Kuppusamy KS, Senthil Rafor R, Remote Access and ProtecShort Message Service, IComputer Science, EngineTechnology (IJCSIT), February 2012.
- Wilson J, Patwari N, See Tracking Using Variance-B Networks, IEEE Transaction, 10(5), 2001, 612-621