International Journal on Applications in Information and Communication Engineering
Volume 5 : Issue 2: December 2019, pp 25 – 32 www.aetsjournal.com ISSN (Online) : 2394 - 6237

SECURING WIRELESS DEVICES USING LOCATION BASED SERVICES

GOWRISHANKAR . R , T.MANIVEL

Abstract— Mobile Tracker Free lets locate a mobile phone and have a history of GPS positions. Retrieve the GPS position of the phone every hour with the date, longitude, latitude and location address. It can set the interval time to 15 minutes instead of 1 hour. View GPS location on Google Map. Retrieve position via mobile network if GPS is disabled. To locate the phone, it must emit at least the roaming signal to contact the next nearby antenna tower, but the process does not require an active call. Mobile positioning, which includes location based service that discloses the actual coordinates of a mobile phone bearer, is a technology used by telecommunication companies to approximate where a mobile phone, and thereby also its user (bearer), temporarily resides. The more properly applied term locating refers to the purpose rather than a positioning process. Such service is offered as an option of the class of location-based services which uses GPS. The Latitude and longitude of the mobile phone's location is searched by the Mobile phone. It sends the data to the Internet through Network socket with a particular IP address. Thus the data reaches the terminal with the particular IP address.

Index Terms: Data mining,Feature selection, Feature clustering, Semi-supervised, Affinity propagation

I.INTRODUCTION

Location-Based Services (LBSs) are one of the most important components in mobile Online Social Networks (mOSNs) which provides information and entertainment service based on the geographical position of the mobile device. LBS have experienced explosive growth in recent years, particularly leveraging the fast development of mobile technology and the cloud computing. In LBS, the location of a device, representing one of the most important contextual information about the device and its owner, is exploited to develop innovative and value-added services to the users' personal context. Many individual, commercial, and enterprise-oriented LBSs are already available and have gained popularity. Various LBS applications have been proposed, such as location-based mobile advertising to mobile phone users. In E-health systems, LBS can also be applied to allow access to patient records outside the hospitals by doctors with location based access technology. There are also many examples of LBS including mobile check-in games like Foursquare, social networks like Loop, and location-enabled applications like Google Maps. Analysts project the revenues for LBS to grow from 2.8 billion in 2010 to hit 10.3 billion by 2015. With the increasing popularity of LBS, the privacy concerns on users' locations have been raised. Because the location tracking capability of mobile devices has been improved greatly, user's personal information such as the position and preference will be leaked and vulnerable to improper use. As a result, it violates user's privacy and impedes the development of various LBS applications.

Mobile information society is developing rapidly as mobile telecommunications moves from second to third generation technology. The Internet and its services are coming to wireless devices. The convergence of content and technology is deepening and the market is being reorganized. Different actors want to preserve their place in the mobile digital economy. Location-based services and personal navigation are parts of mobile multimedia services. Personal navigation is a service concept in which advanced mobile telecommunications allow people find out where they are, where they can find the products and services that they need and how they can get to a destination.

R.Gowrishankar , Assistant Professor , Department of Information Technology , Muthayammal Engineering College.

T.Manivel , Assistant Professor , Department of Information Technology , Muthayammal Engineering College.

II. LITERATURE REVIEW

1)A Field Study of Run-Time Location Access Disclosures on Android Smartphones

Author: Huiqing Fu, Yulong Yang, Nileema Shingte, Janne Lindqvisty, Marco Gruteser

Smartphone users are increasingly using apps that can access their location. Often these accesses can be without user's knowledge and consent. For example, recent research has shown that installation-time capability disclosures are ineffective in informing people about their apps' location access. In this paper, we present a four-week field study (N=22) on run-time location access disclosures. Towards this end, we implemented a novel method to disclose location accesses by location-enabled apps on participants' smart phones. In particular, the method did not need any changes to participants' phones beyond installing our study app. We randomly divided our participants to two groups: a Disclosure group (N=13), who received our disclosures and a No Disclosure group (N=9) who received no disclosures from us. Our results confirm that the Android platform's location access disclosure method does not inform participants effectively. Almost all participants pointed out that their location was accessed by several apps they would have not expected to access their location. Further, several apps accessed their location more frequently than they expected. We conclude that our participants appreciated the transparency brought by our run-time disclosures and that because of the disclosures most of them had taken actions to manage their apps' location access.

2)A Framework for Location Privacy in Wireless Networks

Author: Yih-Chun Hu Helen J. Wang

Though an increasing number of wireless hotspots and mesh networks are being deployed, the problem of location privacyhas been ignored. When a user's location privacy is compromised, an attacker can determine where the user is, and use this information, for example, to stalk or blackmail the user. In existing systems, a user's location can be easily inferred from the signal strengths of packets transmitted from her fixed address. Even if an attacker cannot decode packet contents and addresses, he can correlate different transmissions using a model of the user's movement. In this paper, we argue that location privacy must be a first-class citizen in the design of a wireless communications system. We build a transaction-based wireless communication system in which transactions (a single request-response exchange between two nodes) are unlinkable; that is, they cannot be correlated. We find that it is even possible to support real-time session-based services such as Voice-over-IP on top of transaction primitives, though with weaker privacy properties. We also identify a number of challenges in providing location privacy in the areas of routing, incentives for multi-hop forwarding, and user- and application-driven tuning of the privacy-performance tradeoff.

3) Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking

Author: Marco Gruteser and Dirk Grunwald

Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. *Anonymity* can provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service providers' requirements for safeguarding private information. However, guaranteeing anonymous usage of location-based services requires that the precise location information transmitted by a user cannot be easily used to re-identify the subject. This paper presents middleware architecture and algorithms that can be used by a centralized location broker service. The adaptive algorithms adjust the resolution of location information along spatial or temporal dimensions to meet specified anonymity constraints based on the entities that maybe using location services within a given area. Using a model based on automotive traffic counts and cartographic material, we estimate the realistically expected spatial resolution for different anonymity constraints. The median resolution generated by our algorithms is 125 meters. Thus, anonymous location-based requests for urban areas would have the same accuracy currently needed for E-911

services; this would provide sufficient resolution for way finding, automated bus routing services and similar location-dependent services.

4) Enabling New Mobile Applications with Location Proofs

Author: Stefan Saroiu, Alec Wolman

Location is rapidly becoming the next "killer application" as location-enabled mobile handheld devices proliferate. One class of applications that has yet-to-emerge are those in which users have an incentive to lie about their location. These applications cannot rely solely on the users' devices to discover and transmit location information because users have an incentive to cheat. Instead, such applications require their users to prove their locations. Unfortunately, today's mobile users lack a mechanism to prove their current or past locations. Consequently, these applications have yet to take off despite their potential. This paper presents location proofs – a simple mechanism that enables the emergence of mobile applications that require "proof" of a user's location. A location proof is a piece of data that certifies a receiver to a geographical location. Location proofs are handed out by the wireless infrastructure (e.g., a Wi-Fi access point or a cell tower) to mobile devices. The relatively short range of the wireless radios ensures that these devices are in physical proximity to the wireless transmitter. As a result, these devices are capable of proving their current or past locations to mobile applications. In this paper, we start by describing a mechanism to implement location proofs. We then present a set of six future applications that require location proofs to enable their core functionality.

5) GPS-free positioning in mobile ad hoc networks

Author: Srdjan, Capkun, Maher Hamdi, Jean and Pierre Hubaux

We consider the problem of node positioning in ad hoc networks. We propose a distributed infrastructure free positioning algorithm that does not rely on GPS Global Positioning System Instead the algorithm uses the distances between the nodes to build a relative coordinate system in which the node positions are computed in two dimensions. Despite the distance measurement errors and the motion of the nodes the algorithm provides sufficient location information and accuracy to support basic network functions. Examples of applications where this algorithm can be used include Location Aided Routing and Geodesic Packet Forwarding. Another example are sensor networks where mobility is less of a problem. The main contribution of this work is to define and compute relative positions of the nodes in an ad hoc network without using GPS. We further explain how the proposed approach can be applied to wide area ad hoc networks.

6) GPS-less Low Cost Outdoor Localization for Very Small Devices

Author: Nirupama Bulusu, John Heidemann, Deborah Estrin

Incrementing the physical world through large networks of wireless sensor nodes, particularly for applications like marine biology, requires that these nodes be very small, light, un-tethered and unobtrusive, imposing substantial restrictions on the amount of additional hardware that can be placed at each node. Practical considerations such as the small size, form factor, cost and power constraints of nodes preclude the use of GPS(Global Positioning System) for all nodes in these networks. The problem of localization, i.e., determining where a given node is physically located in a network is a challenging one, and yet extremely crucial for many applications of very large device networks. It needs to be solved in the absence of GPS on all the nodes in outdoor environments. In this paper, we propose a simple connectivity-metric based method for localization in outdoor environments thatmakes use of the inherent radiofrequency (RF) communications capabilities of these devices. A fixed number of reference points in the network transmit periodic beacon signals. Nodes use a simple connectivity metric to infer proximity to a given subset of these reference points and then localize themselves to the centroid of the latter. The accuracy of localization is then dependent on the separation distance between two adjacent reference points and the transmission range of these reference points. Initial experimental results show that the

accuracy for 90% of our data points is within one-third of the separation distance.

7) Localized Algorithms In Wireless Ad-Hoc Networks: Location Discovery And Sensor Exposure

Author: Seapahn Meguerdichian, Sasa Slijepcevic, Vahag Karayan, Miodrag Potkonjak

The development of practical, localized algorithms is probably the most needed and most challenging task in wireless ad-hoc sensor networks (WASNs). Localized algorithms are a special type of distributed algorithms where only subsets of nodes in the WASN participate in sensing, communication, and computation. We have developed a generic localized algorithm for solving optimization problems in wireless ad-hoc networks that has five components: (i)data acquisition mechanism, (ii)optimization mechanism, (iii)search expansion rules, (iv)bounding conditions, and (v)termination rules. The main idea is to request and process data only locally and only from nodes who are likely to contribute to rapid formation of the final solution. The approach enables two types of optimization: The first, guarantees the fraction of nodes that are contacted while optimizing for solution quality. The second provides guarantees on solution quality while minimizing the number of nodes that are contacted and/or amount of communication. This localized optimization approach is applied to two fundamental problems in sensor networks: *location discovery* and *exposure*-based coverage.

8) Location Based Authentication: A New Approach towards Providing Security

Author: Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil

Identifying communicating entities i.e. "users" is today's need. The process of identifying these entities accurately is known as authentication. The conventional authentication mechanisms are based on three factors: knowledge, possession and biometrics. The geographical position of a user is an important attribute that can be used to authenticate a user. In this paper, we are trying to explain how location can be used as one of the credentials to give access to data only to legitimate user. This technique is relatively new approach towards information security.

9) Location Tracking in a Wireless Sensor Network by Mobile Agents and Its Data Fusion Strategies

Author: Yu-Chee Tseng, Sheng-Po Kuo, Hung-Wei Lee, and Chi-Fu Huang

The wireless sensor network is an emerging technology that may greatly facilitate human life by providing ubiquitous sensing, computing, and communication capability, through which people can more closely interact with the environment wherever he/she goes. To be context-aware, one of the central issues in sensor networks is location tracking, whose goal is to monitor the roaming path of a moving object. While similar to the location-update problem in PCS networks, this problem is more challenging in two senses: (1) there are no central control mechanism and backbone network in such environment, and (2) the wireless communication bandwidth is very limited. In this paper, we propose a novel protocol based on the mobile *agent* paradigm. Once a new object is detected, a mobile agent will be initiated to track the roaming path of the object. The agent is mobile since it will choose the sensor closest to the object to stay. The agent may invite some nearby slave sensors to cooperatively position the object and inhibit other irrelevant (i.e., farther) sensors from tracking the object. As a result, the communication and sensing overheads are greatly reduced. Our prototyping of the location-tracking mobile agent based on IEEE 802.11b NICs and our experimental experiences are also reported.

10) Location-based Trust for Mobile User-generated Content: Applications, Challenges and Implementations

Author: Vincent Lenders, Emmanouil Koukoumidis, Pei Zhang and Margaret Martonosi

The recent explosion in shared media content and sensed data produced by mobile end-users is challenging well-established principles and assumptions in data trust models. A fundamental issue we address in this paper is how to establish

some trust level in the authenticity of content created by untrusted mobile users. We advocate a secure localization and certification service that allows content producers to tag their content with with a spatial timestamp indicating its physical location. At the same time, however, our approach preserves the privacy of producers by not exposing their identity to the potential content consumers. We provide a list of existing and possible applications that would profit from such a secure localization service and sketch possible implementations of the service, highlighting advantages and drawbacks.

11) Secure positioning of wireless devices with application to sensor networks

Author: Srdjan C˘apkun and Jean-Pierre Hubaux

The problem of positioning in wireless networks has been mainly studied in a non-adversarial setting. In this work, we analyze the resistance of positioning techniques to position and distance spoofing attacks. We propose a mechanism for secure positioning of wireless devices, that we call Verifiable Multilateration. We then show how this mechanism can be used to secure positioning in sensor networks. We analyze our system through simulations.

12) Secure Verification of Location Claims

Author: Naveen Sastry, Umesh Shankar and David Wagner

With the growing prevalence of sensor and wireless networks comes a new demand for location-based access control mechanisms. We introduce the concept of secure location verification, and we show how it can be used for location-based access control. Then, we present the Echo protocol, a simple method for secure location verification. The Echo protocol is extremely lightweight: it does not require time synchronization, cryptography, or very precise clocks. Hence, we believe that it is well suited for use in small, cheap, mobile devices.

13) Short Paper: Location Privacy: User Behavior in the Field

Author: Drew Fisher, Leah Dorner and David Wagner

Current smartphone platforms provide ways for users to control access to information about their location. For instance, on the iPhone, when an application requests access to location information, the operating system asks the user whether to grant location access to this application. In this paper, we study how users are using these controls. Do iPhone users allow applications to access their location? Do their decisions differ from application to application? Can we predict how a user will respond for a particular application, given their past responses for other applications? We gather data from iPhone users that sheds new light on these questions. Our results indicate that there are different classes of users: some deny all applications access to their location, some allow all applications access to their location, and some selectively permit a fraction of their applications to access their location. We also find that apps can be separated into different classes by what fraction of users trust the app with their location data. Finally, we investigate using machine learning techniques to predict users' location-sharing decisions; we find that we are sometimes able to predict the user's actual choice, though there is considerable room for improvement. If it is possible to improve the accuracy rate further, this information could be used to relieve users of the cognitive burden of individually assigning location permissions for each application, allowing users to focus their attention on more critical matters.

14) TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones

Author: William Enck Peter Gilbert and Byung-Gon Chun

Today's smartphone operating systems frequently fail to provide users with adequate control over and visibility into how third-party applications use their private data. We address these shortcomings with TaintDroid, an efficient, system-wide dynamic taint

tracking and analysis system capable of simultaneously tracking multiple sources of sensitive data. TaintDroid provides realtime analysis by leveraging Android's virtualized execution environment. TaintDroid incurs only 14% performance overhead on a CPU-bound micro-benchmark and imposes negligible overhead on interactive third-party applications. Using TaintDroid to monitor the behavior of 30 popular third-party Android applications, we found 68 instances of potential misuse of users' private information across 20 applications. Monitoring sensitive data with TaintDroid provides informed use of third-party applications for phone users and valuable input for smartphone security service firms seeking to identify misbehaving applications.

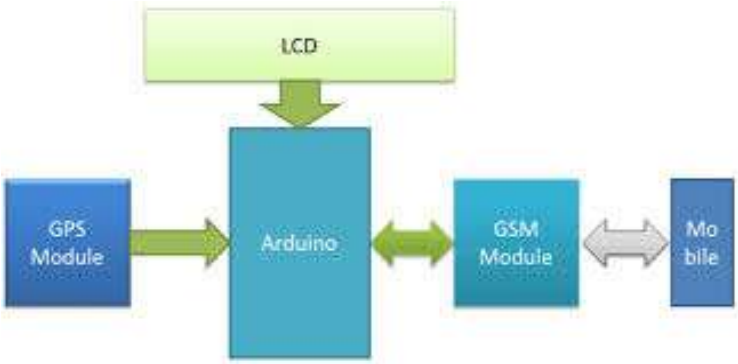
15) The Active Badge Location System

Author: Roy Want, Andy Hopper, Veronica Falcao and Jonathan Gibbons

A novel system for the location of people in an office environment is described. Members of staff wear badges that transmit signals providing information about their location to a centralized location service, through a network of sensors. The paper also examines alternative location techniques, system design issues and applications, particularly relating to telephone call routing. Location systems raise concerns about the privacy of an individual and these issues are also addressed.

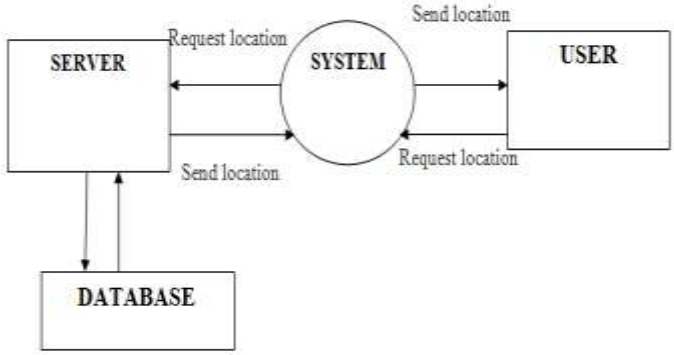
III.PROJECT DESCRIPTION

A. ARCHITECTURE DIAGRAM

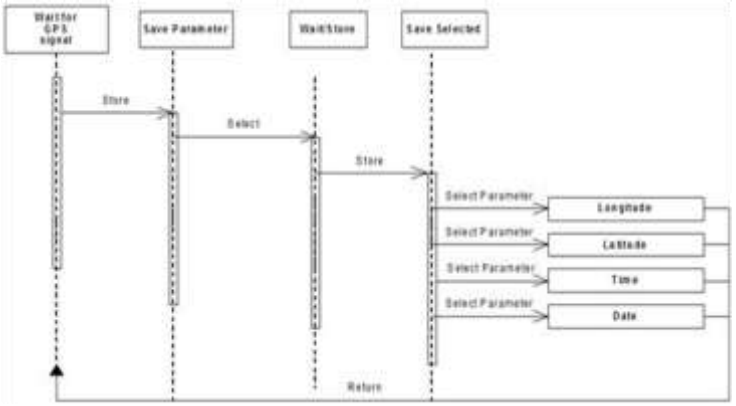


B.UML Diagrams

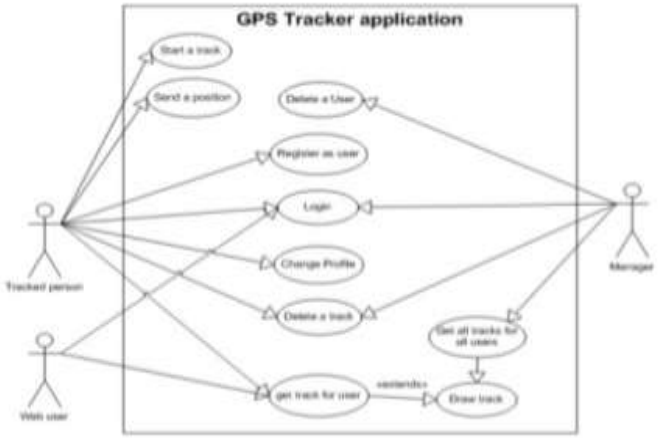
Data Flow Diagram



Sequence Diagram



Use case Diagram



IV. MODULE DESCRIPTION

A. Enhanced Security Provider Module

We observe that the identity of the same querying user is linkable by the location service provider in the friends' location query of previous works Although multiple fake identities have been inserted for each user in these systems, friends' queries from the same user will be linked because of the same friend set. As a result, this security vulnerability will potentially help the location service provider identify which record is true in the location database and make location dummies useless.

In addition, with the real fake identity, the location service provider can obtain the friend relations and locations even if some of them are dummies. More seriously, if we consider multiple queries without location updates, the location service provider is able to finally obtain the topological structure of the social network and launch multiple attacks.

Aiming at fixing this security issue, we propose a new system by introducing a new architecture with multiple location servers. More specifically, all location information will be stored in each location server. When a request of friends' locations is submitted from a user, this set will be divided into multiple subsets, and each subset will be sent to a location server, respectively. In this way, friends' location queries from the same user will be different from the point view of each location server with enough high probability. As a result, these queries cannot be linked to the same user, and improved privacy has been achieved in this new system.

B. Location Sharing Module

In the location-sharing system of mOSNs, users communicate with the location service and social network server. The user's location service is provided by LS, and the social network service is provided by SOSN. The users can submit two types of queries, nearby friends' locations and strangers' locations. In general, the location-sharing mechanism consists of three phases, which are described as follows.

(i) User registration. Two kinds of registration are required for users:

(ii) Registration at the social network server and

(iii) Registration at location servers. (a) Users are required to register their personal information for the LBS at SOSN. Specifically, they need to provide the information of their profiles and individual preferences, which will be kept by the social network server. (b) Users also need to register their pseudoidentity and specified access control policy at the LSs through SOSN in an anonymous way.

(iv) Location updates. Users need to update their location information at the location servers if their locations change. The new location information will be stored and updated at the location servers for location services.

(v) Location query. There are two kinds of queries supported in the system, which are the following. a) Friends' location query. When a user wants to know his/her nearby friends' current locations, he/she queries the social network service provider and LBS providers and receives the location information of friends whose specified access control setting is satisfied by the querying user. b) Strangers' location query. When a user wants to get nearby strangers' current locations, he/she queries the social network service provider and LBS providers and receives the location information of someone whose specified access control setting is satisfied by the user

C. IoT Network Threat Model

Different trust assumptions will be defined over the entities involved in the system:

1) the users are assumed to be dishonest and would try to access the location information outside the scope of their access privileges.

2) The social network server is assumed to be "honest-but-curious," i.e., the social network server will follow our proposed protocol but try to find out as much sensitive information as possible. For example, it may want to extract the users' location information from the interactive communications.

3) The location server is also supposed to be "honest-but-curious." It will also honestly follow our protocols and try to get some users' sensitive information such as the friend list. Note that, in our security model, the adversary is not allowed to control both the social network server and the location servers. In other words, the social network server and the location servers are not allowed to collude and get the information that they have not owned individually. This security assumption is also specified in past systems. This assumption is reasonable because it is unlikely that two service providers operated by independent organizations can be controlled by the same adversary..

V. CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

This Mobile Tracking System has been designed and developed and works properly. It is very efficient; user can easily use this application. Any people can track any mobile location any time using this application. The application is free of cost and does not require any additional device. We have tested in different Android phones and different browsers it works smoothly.

FUTURE ENHANCEMENT

Mobile apps receive GPS location and store into web server database, web application is use to create user profile and track mobile phone's location.

References

[1] Dr.E.Punarselvam ,S.Gopi " Effective and Efficient traffic scrutiny in sweet server with data privacy" in the link " http://www.aetsjournal.com/journal_issues/Effective-And-Efficient-Traffic-Scrutiny-In-Sweet-Server-With-Data-Privacy.pdf ".

[2] Manav Singhal & Anupam Shukla. "Implementation of Location based Services in Android using GPS and Web Services". International Journal of Computer Science Issues (2012), ISSN: 1694-0814.

[3] Ch. Radhika Rani, A. Praveen Kumar, D. Adarsh, K. Krishna Mohan, K.V.Kiran. " LOCATION BASED SERVICES IN ANDROID". International Journal of Advances in Engineering & Technology (2012), ISSN: 2231-1963.

[4] Radhika Kinage, Jyotshna Kumari, PurvaZalke, Meenal Kulkarni. "Mobile Tracking Application". International Journal of Innovative Research in Science, Engineering and Technology (2013), ISSN: 2319-8753.

[5] Prof. Seema Vanjire, Unmesh Kanchan, Ganesh Shitole, Pradnyesh Patil. "Location Based Services on Smart Phone through the Android Application". International Journal of Advanced Research in Computer and Communication Engineering (2014), ISSN: 2278-1021.

[6] Mahesh Kadibagil and Dr. H S Guruprasad. "Position Detection and Tracking System". International Journal of Computer Science and Information Technology & Security (2014), Vol. 4, No. 3.

[7] Abid Khan & Ravi Mishra, ―GPS – GSM Based Tracking System‖, International Journal of Trends and Technology, ISSN: 2231 – 5381, Volume 3, Issue 2, 2012

[8] Rodrigo R. Oliveira, Felipe C. Noguez, Cristiano A. Costa, Jorge L. Barbosa & Mario P. Pardo, ―SWTRACK: An Intelligent Model for Cargo Tracking based on off-the-shelf Mobile Devices‖, ELSEVIER – Expert Systems with Applications 40 (2013) 2023 – 2031

[9] Zechun Huang, Dingfa Huang, Zhu Xu & Zhigen Xu, ―GPS Vehicle Positioning Monitoring System Integrated with CORS and Mobile GIS‖, ELSEVIER - Procedia Environmental Sciences 10(2011)2498–2504

[10] Tushar Saxena, Deepak Kumar, J.S. Jadon, ―A Literature Study of Various Satellite Navigation Systems with Reference to Their Signalling Scheme‖, International Journal of Research Aspects of Engineering and Management, ISSN: 2348-6627, Vol. 1, Issue 1, FEB 2014

[11] Katina Michael & Roger Clarke, ―Location and Tracking of Mobile Devices‖, ELSEVIER - Computer Law & Security Review 29(2013) 216-228.

[12] Hassan I. Mathkour, ―A GPS Based Mobile Dynamic Service Locator system‖, Applied computing and informatics(2011) 9,95-106

[13] Changsheng Cai & Yang Gao, ―Precise Point Positioning Using Combined GPS and GLONASS Observations‖, Journal of Global Positioning Systems (2007), Vol.6, No.1: 13 – 22.

[14] U. Bareth and A. Kupper, "Energy-Efficient Position Tracking in Proactive Location-Based Services for Smartphone Environments," 2011 IEEE 35th Annual Computer Software and Applications Conference, Munich, 2011, pp. 516-521.

[15] Y. Ozen, O. Ozdemir and N. Bandirmali, "Android based energy aware real-time location tracking system," 2015 Seventh International Conference on Ubiquitous and Future Networks, Sapporo, 2015, pp. 842-844.

[16] P. A. Shinde and Y. B. Mane, "Advanced vehicle monitoring and tracking system based on Raspberry Pi," Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on, Coimbatore, 2015, pp. 1-6.