International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.1, 2015

REVIEW ARTICLE

ISSN: 2321-7758

SURVEY BASED ON LOCATION PROOF TECHNIQUES TO AVOID COLLUSION RESISTANCE

THANIGAI ARASU. B[*1], RAMYA DORAI. D[2]

[1]PG Scholar, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India

[2]Associate Professor, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India

Article Received: 30/01/2015 | Article Revised on:10/02/2015 | Article Accepted on:14/02/2015

ABSTRACT

Location privacy is mainly considered to develop the application. The privacy should be more secure to protect the location from the anonymous user. The different methods and techniques are used to protect the location using LBS (Location Based Services). The locations proof are used to decide the current location of the user. The valuable features of the location proofs tell about accessing the location based services (LBS) by using mobile device. Location privacy is most important to keep their location more confidential. The privacy level should be maintained according to their spatial and temporal region. In this paper, its specifies detail survey about the various techniques that are well suited to preserve location privacy and location proofs.

Keywords: Location based services, Location proof, Location privacy and User location.

INTRODUCTION

Location privacy plays a vital role for mobile users who use location-based services provided by the third party Provider through mobile networks. A mobile network is not of highly secure due to broadcasting, because mobile nodes join the network and leave the network at any time and at any location. Mobile device provide user location based on location based services. User current location are updated using google loopt and latitude. Location-based services provide information based on the neighbouring nodes and offer location aware services. Geographical location data are collected in different methods using GPS systems such as IP address, or Wi-Fi network mapping. Location sensitive applications collects the location proof of the users current location and stores the data in datasets for further clarifications in the form of user location history. The location history is updated for the location proof, the information can be eavesdropped by adversaries. It may cause severe problems of location privacy for the user. Eavesdropping may be eradicated using authentication for providing location privacy. The nodes are the changing pseudonyms can be update using the history of the datasets for the privacy of the location proof. Here some survey paper specifies the location proof privacy of the users locations.

A. Location privacy in pervasive computing

Beresford, et al proposed as location-aware applications begin to track our movements in the name of convenience, how can we protect our privacy? This article introduces the mix zone-a new construction inspired by anonymous communication techniques-together with metrics for accessing user anonymity. It is based on frequently changing pseudonyms.

Advantages

- Improvements in secure
- Defend against Anonymous user

Disadvantages

- Anonymous Communication
- Not secure

B. Secure positioning of wireless devices with application to sensor networks

Capkun et al proposed the problem of positioning in wireless networks has been mainly studied in a non-adversarial setting. They have analyzed the resistance of positioning techniques to position and distance spoofing attacks. A mechanism for secure positioning of wireless devices, called verifiable multilateration was proposed. This mechanism can be used to secure positioning in sensor networks. This system was analyzed through simulations.

Advantages

- Defend against attacks
- Improvement in security

Disadvantages

- Distance spoofing attack,
- External attackers can modify(spoof) the measured positions and distances of wireless nodes

C. Enabling New Mobile Applications with Location Proofs

Stefan Saroiu, Alec Wolman et al proposed that the location is rapidly becoming the next "killer application" as location-enabled mobile hand held 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, 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. This paper describes a mechanism to implement location proofs, which present a set of six future applications that require location proofs to enable their core functionality.

Advantages

- Security and
- location proof is efficient

Disadvantages

- Issues in location proof
- security problem

D. A Social Network Based Patching Scheme for Worm Containment in Cellular Networks

Zhichao Zhu proposed that, cellular phone networks have begun allowing third-party applications to run over certain open-API phone operating systems such as Windows Mobile, Iphone and Google's Android platform. However, with this increased openness, the fear of rogue programs written to propagate from one phone to another becomes ever more real. This paper proposes a counter-mechanism to contain the propagation of a mobile worm at the earliest stage by patching an optimal set of selected phones. The counter-mechanism continually extracts a social relationship graph between mobile phones via an analysis of the network traffic. As people are more likely to open and download content that they receive from friends, this social relationship graph is representative of the most likely propagation path of a mobile worm. The counter mechanism partitions the social relationship graph via two different algorithms, balanced and clustered partitioning and selects an optimal set of phones to be patched first as those which have the capability to infect the most number of other phones. The performance of these partitioning algorithms is compared against a benchmark random partitioning scheme.

Advantages

- Defend against attack and worms
- Make rekliable and securable.

Disadvantages

- Malicious file and attacks
- Lack security in cellular communication

E. APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services

Zhichao Zhu and Guohong Cao proposed Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. This approach allows the user to cheat by having his device transmit a fake location, which might enable the user to access a restricted resource erroneously or provide bogus alibis. A Privacy-Preserving LocAtion proof Updating System (APPLAUS) in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and update to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. To develop user-centric location privacy model in which individual users evaluate their location privacy levels in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels.

Advantages

- Makes reliable communication
- Security enhanced
- Defend against attacks

Disadvantages

- Not privacy & secure
- Malicious file and attackers
- Stolen information

CONCLUSION

This paper compares many location techniques and models about the location proofs of changing pseudonyms, current and past history of location to avoid the fake location of the users and also preserves the location privacy. APPLAUS techniques are used more efficiently to provide location proof and preserve the location with collusion resistant. The survey paper specifies the usage of the location privacy and the effectiveness with collusion resistant are described from the above mentioned papers. The techniques provide the users to protect the location from unauthorized users.

REFERENCES

[1]. Buttya,L , Holczer,T & Vajda,I (2007), 'On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs', Proc. Fourth European Conf. Security and Privacy in Ad-Hoc and Sensor Networks.

[2]. Capkun,S & Hubaux, JP (2005), 'Secure Positioning of Wireless Devices with Application to Sensor Networks,' Proc. IEEE INFOCOM.

[3]. Cox, LP, Dalton, A & Marupadi, V (2007), 'Smokescreens: Flexible Privacy Controls for Presence-Sharing,' Proc. ACM MobiSys

[4]. Freudiger,J, Manshaei, MH, Hubaux, JP & Parkes, DC (2009), 'On Non-Cooperative Location Privacy: A Game-Theoretic Analysis,' Proc. 16th ACM Conf. Computer and Comm. Security (CCS).

[5]. Hoh,B, Gruteser,M, Herring,R, Ban,J, Work,D, Herrera,JC, Bayen,AM, Annavaram,M & Jacobson,Q (2008) 'Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring,' Proc. ACM MobiSys.

[6]. Lenders,V, Koukoumidis,E, Zhang,P & Martonosi,M, (2008), 'Location-Based Trust for Mobile User-Generated Content: Applications Challenges and Implementations,' Proc. Ninth Work- shop Mobile Computing Systems and Applications.

[7]. Li,Y & Ren,J, (2010), 'Source-Location Privacy Through Dynamic Routing in Wireless Sensor Networks,' Proc. IEEE INFOCOM.

[8]. Luo,W & Hengartner,U (2010), 'Proving Your Location Without Giving Up Your Privacy,' Proc. ACM 11th Workshop Mobile Computing Systems and Applications (HotMobile '10).

[9]. Manweiler,J, Scudellari,R, Cancio,Z & Cox,LP (2009), 'We Saw Each Other on the Subway: Secure Anonymous Proximity-Based Missed Connections,' Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile '09).

[10]. Manweiler,J, Scudellari,L & Cox,LP (2009), 'SMILE: Encounter- Based Trust for Mobile Social Services,' Proc. ACM Conf. Computer and Comm. Security (CCS).

[11]. Rhee,I, Shin,M, Lee,K & Chong,S (2007), 'On the Levy-Walk Nature of Human Mobility,'Proc. IEEE INFOCOM.

[12]. Saroiu,S & Wolman,A (2009), 'Enabling New Mobile Applications with Location Proofs,' Proc. ACM 10th Workshop Mobile Computing Systems and Applications (Hot Mobile'09).

[13]. Shao,M, Yang,Y, Zhu,S & Cao,G (2008), 'Towards Statistically Strong Source Anonymity for Sensor Networks,' Proc. IEEE INFOCOM.

[14]. Yang,Y, Shao,M, Zhu,S, Urgaonkar,B & Cao,G (2008), 'Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks,' Proc. First ACM Conf. Wireless Network Security (WiSec).

[15]. Zhu,Z & Cao,G (2011), 'APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-Based Services,' Proc. IEEE INFOCOM.

[16]. Zhu,Z, Cao,G, Zhu,S, Ranjan,S & Nucci,A (2009), 'A Social Network Based Patching Scheme for Worm Containment in Cellular Networks,' Proc. IEEE INFOCOM.