International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Achieving Personalized Privacy and Compromised Conspiracy in Location Proof Updating System

Anusha.J.D[1], H.Packiaraj[2]

PG Student, Department of CSE, Loyola Institute Of Technology And Science,Nagercoil,India[1]

Email: anushaxvr@gmail.com[1]

Assistant Professor, Department of IT, Loyola Institute Of Technology And Science, Nagercoil, India[2],

Abstract- An alibi is a form of defense used in criminal procedure wherein the accused attempts to prove that he or she was in some other place at the time the alleged offense was committed. Today's location-sensitive service relies on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations. To address this issue, we propose A Privacy-Preserving Location proof Updating System in which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect from the untrusted location proof server. In order to defend against colluding attacks, we also present betweeness ranking-based and correlation clustering-based approaches for outlier detection. APPLAUS can be implemented with existing network infrastructure, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost. Extensive experimental results show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks In addition We propose two in-network aggregate location anonymization algorithms, namely, resource-and quality-aware algorithms. Both algorithms require the sensor nodes to collaborate with each other to blur their sensing areas into cloaked areas, such that each cloaked area contains at least k persons to constitute a k-anonymous cloaked area This helps the system to enable and provide high-quality location monitoring services for system users, while preserving personal location privacy.

Index Terms- ***Wireless sensor networks (WSN), source location, privacy, pseudonyms, colluding attacks.***

1. INTRODUCTION

Wireless sensor networks are network of small sensing devices, which collaborate with each other to gather process and communicate over wireless channel information about some physical phenomena. These self-organizing, highly robust and energy efficient networks can be excellent sentinels for monitoring underground mining, wildlife and various physical infrastructures such as bridges, pipelines, and buildings.

A WSN can be deployed in harsh environments to fulfil both military and civil applications. Basically, sensor networks are application dependent. Sensor networks are primarily designed for real-time collection and analysis of low level data in hostile environments. For this reason they are well suited to a substantial amount of monitoring and surveillance applications.

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks.

In Passive Attacks, the monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature. In Active Attacks, the unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack.

Location Based services take advantage of user location information and provide mobile users with various resources and services. Nowadays, more and more location based applications and services require users to provide location proofs at a particular time. For example, "Google Latitude" and "Loopt" are two services that enable users to track their friends' locations in real time. These applications are location-sensitive since location proof plays a critical role in enabling these applications

One common assumption when defining location privacy metrics is that one is dealing with attackers whose objective is to re-identify an

individual out of an anonymized data set. However, today's communication scenarios are more diverse. For instance, there are several entities involved in mobile location sharing between individuals.

Hence, in a communication relation with a service provider (e.g. SNS or network infrastructure) or with social contacts, an anonymity approach seems inadequate. Between each user and every single entity involved there is some level of trust and the identities are already known, at least to some extent. Hence, taking an anonymity approach for communication relations to peers or service providers (e.g. SNS or network infrastructure) seems to be inadequate.

In this paper, we propose A Privacy-Preserving LocAtion proof Updating System (APPLAUS), which does not rely on the wide deployment of network infrastructure or the expensive trusted computing module. In APPLAUS, Bluetooth enabled mobile devices in range mutually generate location proofs, which are uploaded to a untrusted location proof server that can verify the trust level of each location proof. An authorized verifier can query and retrieve location proofs from the server. Moreover, our location proof system guarantees user location privacy from every party.

We use statistically updated pseudonyms at each mobile device to protect location privacy from each other, and from the untrusted location proof server. We develop a 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 request. In order to defend against colluding attacks, we also present betweenness ranking-based and correlation clustering-based approaches for outlier detection. Extensive experimental and simulation
results based on multiple data sets show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks.

We propose two in-network aggregate location anonymization algorithms, namely, resource- and quality-aware algorithms. Both algorithms require the sensor nodes to collaborate with each other to blur their sensing areas into cloaked areas, such that each cloaked area contains at least k persons to constitute a k-anonymous cloaked area. Location monitoring refers to the system where the wireless sensor network nodes counts the number of sensors which are capable of detecting the objects present in their sensing areas. Third party always monitor the personal location which is becoming a privacy threat. To over come this we have proposed a method by using a series of routers to hide the client's IP address from the server. We propose a privacy-preserving location monitoring system for wireless sensor networks. In our system, we design two in-network location anonymization algorithms, namely, Cloaked Area Determination Algorithm and quality enhanced histogram algorithm. This helps the system to enable and provide high-quality location monitoring services for system users, while preserving personal location privacy. The Cloaked Area determination algorithm aims to minimize communication and computational cost. A quality enhanced histogram approach is used that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then, the estimated distribution is used to provide location monitoring services through answering range queries.

2. RELATED WORK

In this section, we will see the some of the related works providing location privacy using different approaches:

Location privacy is a particular type of information privacy that we define as the aptitude to prevent other parties from learning one's current or past location [4]. With pervasive computing, though, the scale of the problem changes entirely. Most likely you do not care if someone finds out where you were yesterday at a particular time, but if this someone could look over the history of all your past movements, recorded every second with sub meter precision, everyone might start to see things differently. Then they focus on the privacy aspect of using location information in pervasive computing applications. They do not essentially need to stop all access because some applications can use this information to provide useful services. But, we want to be in control and to keep our position secret but wanting social group to be able to locate us with privacy. So they build Privacy-protecting framework based on frequently changing pseudonyms. So users avoid being identified by the locations they visit [7]. In that they introduce the concept of mix zones and showing how to plot the problem of location privacy onto that of anonymous communication. Pseudonym is used to destroy the link between location information and user identity. Untraceability, by itself, may not be enough in pseudonym based approach. The provision of unlinkability is related to an aspect of privacy also referred as path privacy. Adversary has no coverage in silent mix zone [8]**.**Multiple pseudonyms for unlinkability prevent from correlation attacks.

Location proof of mobile node contains five fields: proof issuer, proof recipient, timestamp, geographical location, digital signature. In this case proof issuer is Wi-Fi access point.

Wi-Fi access points (AP) advertise its presence by broadcasting beacon signals to its surrounding area [5]. If the recipient needs the location proof then it extracts the beacon's sequence number and uses it for asking the location proof. The demand for a location proof contains the client's public key and the signed AP's sequence number. The client signs the sequence number to guard their reliability and to make it hard for others to masquerade as client devices. Then AP checks whether the signature is legitimate and whether the sequence number is current one. If the request is valid, the AP creates a location proof with a current timestamp and designates to the client. If the request is invalid then AP drops the request mutely. Another sensible consideration is making sure that APs are configured with the correct location coordinates. While it is cheap to provision APs with GPS to routinely determine their geo-location, most APs are situated in indoor environments where GPS does not work fine. One way to overcome this complexity is to provide the AP with an additional configuration interface for administrators. To point a location proof-enable AP, the administrator initially takes the AP outdoors and runs a setup program that uses GPS to establish the AP's location.

A location proof is an electronic form of article that certifies someone's bearing at a definite location at particular time [10]. A retroactive location proof is used to currently interact with a target application. A proactive location proof is collected for the future purpose, without having a goal application in mind. Cryptographic hashes and digital signatures are used for user anonymity. Location proof request is sent to the AP by the user, with granularity. If AP receives the request it generates nonce for itself and then sends the nonce to the user. Then user concatenates the received nonce with user nonce and signs them. At last AP creates a location proof which is enclosed by group signature which is finally send to user. The issuer gets the hash of the signature and its nonce. The hash in combination with the user's nonce serves for two purposes: First, they behave as a commitment by the user to her signature. Finally, it hides the user's signature and therefore his identity from the proof issuer. A dishonest user may collude with a malicious intruder. This is to launch a replay attack to acquire location proofs for a place where the dishonest user is no longer located. The task of the malicious intruder is to acquire further location proofs from the same proof issuer on behalf of the dishonest user, who is moved away. It's impossible for malicious intruder to succeed, that the proof issuer is going to re-use nonce. However, since each nonce is used only once, the malicious intruder cannot thrive.

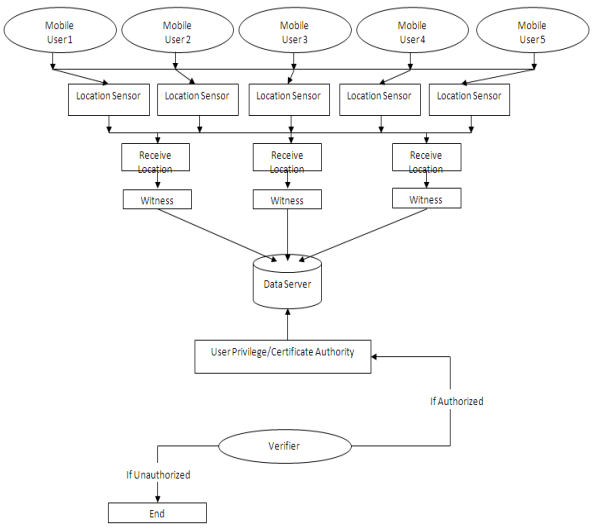
Personality identifiable information is being openly unknown as anonymity. Customizability means user can flexibly control the tradeoff between privacy protection and accuracy for LBS [13]. Customizable k-anonymity model for protecting privacy of location data works by, thrashing the location of a user within a cluster of k members. A third party is employed to gather the user's locations and classify them in some k-size sets. Then one of the members of the location set is chosen as the representative location of all those users. k-anonymity approach utilizes a trusted third party as an anonymizer, where the implementation could be based on a centralized or distributed architecture. The vital challenges in k-anonymity are to come across k-1 other users to keep the anonymity. Two other evils with k-anonymity approach are the reduction of accuracy and they require for a trusted third party.

An adversary has same credentials as legitimate mobile user. So the real event source can be eavesdropped by the adversary [9]. The local adversary and global adversary can analyze the traffic, to find what information is passed by the user by traffic analysis. Event source unobservability, which tells as local and global adversary cannot predict the real event occurrence, even if it's manageable to collect all the information passing through the network. Event source unobservability is process of choosing dummy traffic to hide the real event sources. Add dummy traffic to the real event by add some proxies that proactively filter dummy message on their way to destination. Proxy based and tree based filtering are used in event source unobservability preserving privacy solution for sensor networks, maximally reduce the network traffic while increasing delivery ratio with sacrificing privacy level.

There is a spectacular increase in the location based services this includes that of the foursquare or the yelp that contains a number of services [14]. Most of the services rely on the users for the correct location. But suppose there is a enticement user, then the users lie about that location. With the location proof architecture a users location, services proof is being collected so as to validate. Here everyplace is being introduced with the user's privacy of high concern along with that it can detect cheating users who collect the proofs where they are not located. everyplace integrated with yelp has proved to provide optimal privacy .

3. PROPOSED WORK

In this paper, we propose A Privacy-Preserving Location proof Updating System (APPLAUS), which does not rely on the wide deployment of network infrastructure or the expensive trusted computing module.



In APPLAUS, Bluetooth enabled mobile devices in range mutually generate location proofs, which are uploaded to an untrusted location proof server that can verify the trust level of each location proof.

An authorized verifier can query and retrieve location proofs from the server. Moreover, our location proof system guarantees user location privacy from every party. More specifically, we use statistically updated pseudonyms at each mobile device to protect location privacy from each other, and from the untrusted location proof server. We develop a 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 request. In order to defend against colluding attacks, we also present between's ranking-based and correlation clustering-based approaches for outlier detection.

In WSN, the location privacy can be improved when compared with the existing location based services. In this we can store the previous location history and also accuracy and efficiency can also be improved.

3.1 USER REGISTRATION

The initial registration process normally involves requesting for registration on the network, authentication of the user by the network, registration of the user and informing the home location register (HLR) of the users current whereabouts.

Fig no 2: User Registration

3.2 WITNESS

Once a neighboring node agrees to provide location proof for the prover, this node becomes a witness of the prover. The witness node will generate a location proof and send it back to the prover.

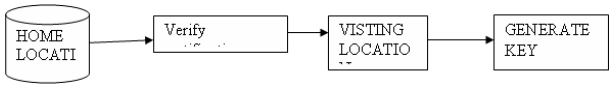


Fig no 3: Witness

3.3 VERIFIER

Verifier is a third-party user or an application who is authorized to verify a prover's location within a specific time period. The verifier usually has close relationship with the prover.

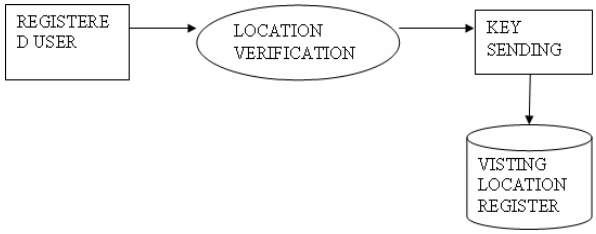


Fig no 4:Verifier

4. ALGORITHM

The Cloaked Area determination algorithm aims to minimize communication and computational cost. A quality enhanced histogram approach is used that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then, the estimated distribution is used to provide location monitoring services through answering range queries. The effectiveness of proposed detection system is evaluated and influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined.

The above proposed algorithms minimizes the communication and computational cost, size of the cloaked areas and also maximizes the accuracy of the aggregate locations reported to the server.

5. IMPLEMENTATION RESULTS

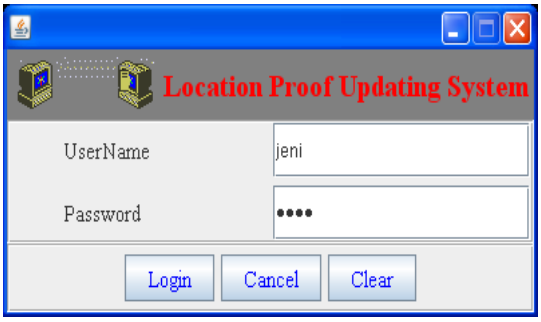


Fig no 5: User login

The login form used to create authorized user in a secure manner. It provided unique ID to each user and only the authorized users can use it. The login form contains all the authorized users.

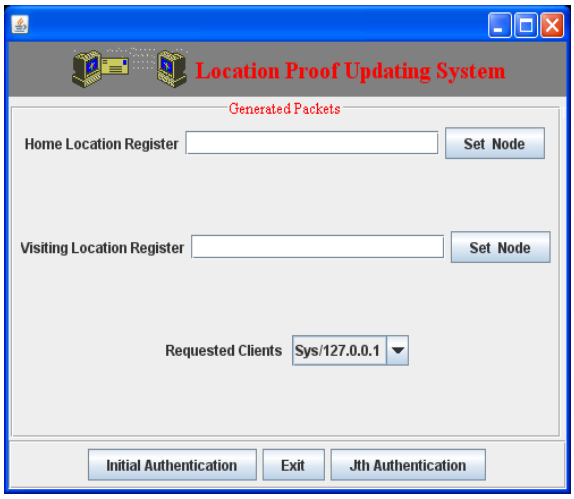


Fig no 6: Authentication

.

The home location register and the visiting location register are set and the location is verified based upon the information provided.

6. CONCLUSION

In this paper we propose a privacy-preserving location proof updating system called APPLAUS, where collocated Bluetooth enabled mobile devices mutually generate location proofs and upload to the location proof server. We use statistically changed pseudonyms for each device to protect source location privacy from each other, and from the untrusted location proof server.

We also develop a 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. To the best of our knowledge, this is the first work to address the joint problem of location proof and location privacy. To deal with colluding attacks, we proposed betweenness ranking based and correlation clustering-based approaches for outlier detection.

Extensive experimental and simulation results show that APPLAUS can provide real-time location proofs effectively. Moreover, it preserves source location privacy and it is collusion resistant. We also propose a fast mutual authentication and key exchange scheme for mobile communications. The scheme is designed for mutual authentication between a mobile user and the system

7. REFERENCES

[1]. Efficient Detection of Sybil Attack based on Cryptography in VANET, International Journal of Network Security & Its Applicarions, Nov 2011

[2]. Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless
Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[3]. A.R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Security and Privacy, 2003.

[4]. S. Saroiu and A. Wolman. Enabling new mobile applications with location proofs. In ACM HotMobile, 2009

[5]. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi. Locationbased trust for mobile user-generated content: applications, challenges and implementations. In ACM HotMobile, 2008.

[6]. M. Li, R. Poovendran, K. Sampigethaya, and L. Huang. Caravan: Providing location privacy for vanet. In Proceedings of the Embedded Security in Cars (ESCAR) Workshop

[7]. L. Butty´an, T. Holczer, and I. Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. Security and Privacy in Ad-hoc and Sensor Networks.

[8]. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao. Towards event source unobservability with minimum network traffic in sensor networks. In ACM WiSec, 2008.

[9]. W. Luo and U. Hengartner. Proving your location without giving up your privacy. In ACM HotMobile, 2010.

[10]. Emmanouil Magkos Cryptographic Approaches forPrivacy P reservation in Location-Based Services

[11]. Z. Zhu and G. Cao. Applaus: A privacy-preserving and collusion resistance in location proof updating system IEEE INFOCOM 2011.

[12]. B. Gedik and L. Liu. A customizable k-anonymity model for protecting location privacy. In *IEEE ICDCS*, 2005.

[13]. Wanying luo and urs hengartner. VeriPlace: A Privacy-Aware Location Proof Architecture

[14]. Yu Wang *and* Dingbang Xu. L2P2: Location-aware Location Privacy Protection for Location-based Service , Apr.–Jun. 2006.

[15] U. Brandes, "A Faster Algorithm for Betweenness Centrality," J. Math. Sociology, vol. 25, no. 2, pp. 163-177, 2001

[16] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc. Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '93), 1994.

[17] L. Buttya´n, T. Holczer, and I. Vajda, "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, 2007.

[18] S. Capkun and J.-P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," Proc. IEEE INFOCOM, 2005.

.