World Applied Sciences Journal 34 (10): 1351-1356, 2016
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2016.1351.1356

Advanced Location Tracking and Privacy Preserving with Secure Positioning and Location Proof Udating

C. Amuthadevi and R.S. Pratheeba

Department of Computer Science and Engineering,
Adhi College of Engineering and Technology, Kanchipuram Tamilnadu, India

Abstract: Tracking the locations of a particular person or devices plays a crucial role in many real time applications. Current mobile devices use either Bluetooth or Wi-Fi for connectivity and makes tracking as possible with minimum cost of computation and consumption of power. Location proof verification and privacy preserving are the two important criteria in the location sensitive/based applications. This work proposes an location proof updating method by using 'APPLAUS' – A Privacy Preserving LocAtion proof Updating System combined with 'SPINE' -Secure Positioning In sensor Networks Algorithm for location proving, to avoid colluding attacks and preserve the privacy of the source. Experiments were done with few witness nodes and both the witness nodes pseudonym and location are encrypted by public key encryption. The performance of APPLAUS and SPINE are evaluated by Trust level and proof delivery ratio.

Key words: Location proof updating system · APPLAUS · Privacy Preservation · SPINE Algorithm

INTRODUCTION

Location based services (LBS) were emerged in 1990's and initially proposed for emergency related services. Practically it was implemented by Federal Communication Commission in 1996 in US [1]. LBS use real time environment from mobile phones to provide the details such as nearby restaurants, coffee shops, etc [2]. LBS have 5 components. They are: service provider's software application, mobile network for transmitting data and requests for service, a content provider to supply the user by means of geo-specific information, a positioning component like GPS and the end user's mobile device. It is a software application for an IP-capable mobile device that knows where the mobile device is located. It may be a query-based and provide the end users with useful information such as "Where is the nearest ATM?.

Privacy of the location information is connected with controlling the access to individual's current location and past locations. For this purpose pseudonyms are changed frequently [3]. By using mobile device "location proof" tells about accessing the LBS. Individual user can decide whether to accept location proof for a particular time or afterwards. Also user can calculate the location privacy levels [5]. In the Location Proof Updating System adversaries can eavesdrop the location information. Eavesdropping can be prevented by using Public Key Cryptography. For identity privacy, by using pseudonyms the identity of the node is hidden. Multilateration can be used to find the position of nodes from a set of reference points whose positions are already known/identified. This can be based on the distances measured between the reference points and the device. Verifiable Multilateration is used for secure positioning in a variety of systems in the presence of adversaries [4]. Mobility management defines the mobile user's movement and its location in the network.

Bluetooth technology is similar to a client-server architecture. In this context, connection initiator is a client and one who receives the connection is termed as server. If Bluetooth is used by single device at a particular time, then it is called as point-to-point communication. It uses radio frequency for the communication [4]. Bluetooth devices within the range mutually generate location proofs. And that proofs are uploaded to a untrusted location proof server. Server can verify the trust level of each location proof. The prover broadcasts a location proof request to its neighboring nodes via Bluetooth [5].

Corresponding Author: C. Amuthadevi, Department of Computer Science and Engineering, Adhi College of Engineering and Technology, Kanchipuram Tamilnadu, India.

LBS applications are mostly used in hospitals for improving the efficiency and reduce expenditure. It works on RTLS and WI-Fi technology for indoor locations. LBS is used in many hospitals designed for indoor navigation, tracking staff and patients, location-based messaging, management of asset, location analytics and in integrating with other clinical systems [3]. One implication of this technology is that data about a subscriber's location and historical travels is maintained and controlled by network operators, including mobile carriers and mobile content providers. Mobile content providers and application developers are a concern. Some of the applications of LBS are,

Google Latitude: To track the neighbours' locations in real time "Google Latitude" and "Loopt" are used. It provide an on/off switch and allows to place in a particular location. The Location obfuscation techniques which slightly change the location of the users to provide their real location as confidential. But they still represent their position and LBS provider gives services.

Information Services: Location-based information services define the information in the digital distribution based on device location, specificity of time and user behavior. This is one of the most popular and earliest implementation types of LBS using both pull and/or push services.

Starting from 2001 the communication between mobile client and server was operated with SMS, than MMS. The user could ask the server with simple questions such as the address of the nearest parks or ATM centre. Wireless network operators provided these services. The information is commonly stored in external providers with wireless internet through smartphone apps (Yelp, Yellow Pages, Gas Buddy). The aim of data and information given by service provider is very comprehensive and it contain local street map, variety of locations (restaurants, gas stations, cafes, stores, pharmacies, hospitals, services, touristic attractions etc.)

Navigation: Navigation services allowing location in the real geographical position of a mobile device using one of the available positioning systems and then get direction and/or user navigation to required location including vehicles, crafts and pedestrians. The LBS approach gives advantage over mobile navigation software using data stored in the memory of a mobile device, because it potentially gives user to access real-time data. The disadvantage of large volumes of data wanted to be transferred over wireless network is decreasing as many network operators provide unlimited or less priced data transfer.

Location Based Social Media: Social media have been popularized on the Internet and have become increased research topic. Social networks such as Myspace, Facebook and Twitter, have changed the path how people communication and maintain relations among friends, colleagues, peers or also a family. The development and omnipresence of location-awared mobile devices give social media as a possibility to divide location with content created users. There are different models of networks based on content created users. Many LBSNs use elements of gamification to attract audiences and create motive for users. Another ways to attract users are often coupons otherwise discounts used in pull or push way.

Mobile Location-Based Gaming: Today Growing trend among LBS in world is Mobile Location Based Gaming (MLBG). Elements of traditional open-air field games is being linked by MLBG (e.g. Hide-and-seek, Paper Chase) with noval technologies available on mobile devices including technologies using positioning, fast speed internet with wireless, image recognition and augmented reality among others. MLBG is defined as a location-based game that can run on a mobile device and by using a communication channel, the game exchanging information with a server or other players.

Related Works: The first identified piece of privacy legislation was England's 1361 Justices of the Peace Act, which legislated for the eavesdroppers arrest and stalkers. The Fourth Amendment to the US Constitution announces officially as citizens' right to privacy and in 1890 US Supreme Court Justice Louis Brandeis demonstrated that "the right to be left alone" is one of the fundamental rights of a democracy. The 1948 Universal Declaration of Human Rights denotes that everyone has a privacy rights at home, with family and in correspondence. Although many people clearly consider their lack of interruption of a fundamental right, relatively few can give an exact definition of the term [3].

Location-sensitive service based on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide false evidence by cheating on their locations. To refer this

issue, A Privacy-Preserving LocAtion proof Updating System (APPLAUS) in which mobile devices with Bluetooth enabled which generate location proofs and send updates to a location proof server. Oftenly changed pseudonyms are used by the mobile devices to source location privacy protection from each other nodes and from the untrusted location proof server. In this approach user-centric location privacy model is developed in which evaluation of their location privacy levels of individual users and decide whether and when the location proof requests are accepted. Colluding attacks can be avoided by using betweenness ranking-based and correlation clustering-based approaches. APPLAUS with existing network infrastructure can be implemented and can be easily deployed in mobile with Bluetooth enabled platform. By doing this little computation or power cost are made [6].

The wireless communication pervasiveness recently gave mobile ad hoc networks (MANET) a significant researcher's attention, because of its innate capabilities of instant communication for many time and missionning critical applications. However, in civilian and military environments make advantages of networking give vulnerable to security threats. Support for an lack of understanding in MANET is a statistically independent to security critical challenge. A new unknown authentication protocol for mobile ad hoc networks enhanced with a distributed reputation system. To provide mechanisms prevent a real identity of communicating nodes with an ability of avoid identified attacks is the main ability. The distributed reputation system is included for a trust management and behavior of malicious node detection in the network. The end to end authentication of anonymous is conducted in three-pass handshake based on an asymmetric key and symmetric key cryptography. Secure and multiple anonymous data channels are established After successfully finished authentication phase. The anonymity is randomly chosen guarantied by pseudonyms owned by a user. The network nodes are publicly identified and are users' independent pseudonyms [7].

A Smoke Screen is a system that provides flexible and power efficient mechanisms for node's privacy management. "Clique" signals are broadcasted which can only be interpreted by other trusted nodes. It enables sharing between social relations and broadcasting opaque identifiers (OIDs), which can be able to resolv an identity by a trusted broker and enables sharing between strangers. as they can be pre-computed with acceptable storage costs computing these messages is power-efficient [8].

The problem of wireless networks positioning has been originally studied in a non-adversarial technique. The resistance of techniques using positioning is to avoid position and distance spoofing attacks. A method used for secure positioning of wireless devices, that is Verifiable Multilateration. Then only able to show how this method can be used to secure positioning in sensor networks [5].

Here a feeling-based privacy model is used. This model allows a user to express his/her privacy requirement by giving a public region, in which the user will feel easily if the region is reported as his/her location. The public region popularity, measured using entropy based on its footprints of visitors' inside in it, is then take as the user's desired level of privacy protection. With this model presented a new technique that allows a user's location information that is to be reported more accurate while giving him correct location privacy protection. The novel technique supports trajectory cloaking and it can be used in application scenarios where frequent location updates make along a trajectory that cannot be detected. In addition to calculating the effectiveness of the proposed method under various conditions via simulation, also implemented an experimental based system for location privacy-aware uses of location-based services. An anonymous location make known for an LBS may be correlated with restricted spaces to find a possible set service requestors [9].

The analysis of social networks is essentially done by the betweenness centrality index, but costly to compute. Now, the fastest known algorithms able to do in Ø(n3) time and Ø(n2) space, where n is the number of actors in the nodes of network. By the fast-growing need to compute centrality indices is motivated on large, but very sparse, networks, noval algorithms for betweenness are explained in this paper. It require Ø(n + m) space and able to run in Ø(nm) and Ø(nm + n2 log n) time on unweighted network and weighted networks, respectively, where m is the number of links. An required tool for the analyzing of social networks are centrality indices on the graph vertices.

They are developed rank of the actors according to their position in the network of nodes and interpreted as the importance of actors embedded in a social network structure. Many centrality indices are based on the concept of shortest paths linking actors pairs, measuring, e.g., the average distance from other actors, or the ratio of shortest paths an actor lies on. Many network-analytic studies depends at least in part on an calculation of these indices. With the increasing practicality of electronic collection of data and, of course, the emergence of the

Web, there is a equal increasing demand for the calculation of centrality indices on networks of nodes with thousands of actors. Several concept of centrality originating from analyzing of social network are in use to determine the structural importance of Web pages [10].

MATERIALS AND METHODS

Applaus: This system does not use the existing network infrastructure and expensive trust based models. It uses the mobile devices which communicate about their location by Bluetooth, an untrusted server is used for location proof storage and an authorized proof verifier is used for verification of location proof [11]. Each mobile device exchange its location information to its neighborhood device based in its requirement and privacy consideration.

In this work, a Central Authority system is used for maintain the credentials for each registered mobile device. Pseudonym approach is used and each registered node k gives set of private and public key pairs at the time of registration. Here, public key is called as pseudonym of node k. The corresponding private key is used to sign the messages digitally. Usually location finding and exchange of location information are done by sending probe messages. When a mobile device receives probe message from other device, it checks the sender's public key and Media Access Control (MAC) address. Then digital signature of the probe message is verified by the receiving mobile device. Then receiving device decides about exchange of the location.

Whether to accept the location proof from a particular node, Threshold based verification method is used. It finds the mobile nodes which create false location proofs. Trust level (or) security level is calculated by the following equation.

$$TL_{node} = \frac{N\ proof}{N\ nighbor}$$

where N proof is the number of proofs collected from the neighbors and N-neighbor is the number of neighbor nodes within the predefined range. For a node, if the trust level is less than the threshold, then it is considered as dishonest node.

Prover with SPINE Algorithm: The proposed secure positioning algorithm(SPINE) is one of the centralized algorithm which is based on distance bounding and verifiable-multilateration. Node-centric positioning system refers that a node computes its position from public base stations with identified locations. Internal attacks are caused because the attacker simply lies his/her position that was computed. It is simply called as node centric. This algorithm is executed in two phases: (i) the distance bounds able to be measured with neighbours and (ii) the position of the nodes are computed, by collecting distance bounds from the central authority [3].

In this secure positioning system two nodes take part. They are a reference node set and sensor nodes set with identified locations. Communication between nodes and verifiers take place using radio transmissions. The bidirectional communication can be possible. The nodes of the sensor have able to measure distance but not having GPS receivers. Measuring of nodes can be done by time-of-arrival otherwise round-trip time with the help of radio signals. Few delays can be bounded by the nodes.

An authority who operates the network, controls the membership of the network and a unique identity of each node to be assigned. Symmetric cryptographic keys are to be generated by each node and any task required to be accomplished to secure its communications. Secrete keys can be established by all the nodes of the network. This is achieved by preloading all keys into network of the nodes.

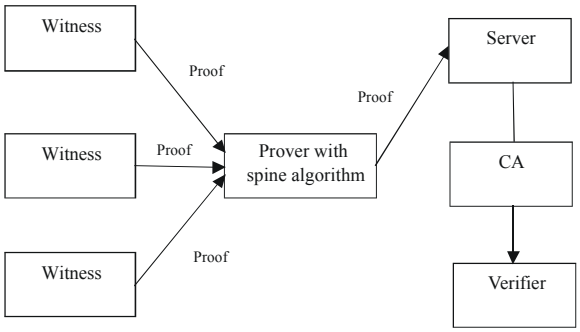

Fig. 1: Proposed Architecture

Each mobile node plays different role in the location proof updating process. The roles are specified in the Figure 1. Prover is a node that wants to collect the location proofs from the nearer nodes. When a location proof is required, the prover broadcast request for location proof to its neighboring nodes via Bluetooth. If the positive response is not received, the prover creates 'dummy location proof' and send to the location proof server. The nodes who accept to share the location proof with the prover is called as 'witness' of the prover. The witness node can make a location proof and forward to the prover.

Location proof server monitors the real time locations of mobile devices and used to get back the history of location proofs. The server is untrusted (i.e. even this

server is compromised by the attackers; real sources of location proof/witness cannot be traced. A central authority system is given by trusted third party works as independent. It acts as an intermediate/ communicator between the verifier and the server used for location proof, knows the pseudonyms and access the location proof and send to the verifier. A verifier is an application/user and authorized to verify the location of the prover.

RESULTS AND DISCUSSION

As Bluetooth technology is used for location information communication, mobile devices within the range of 10 m are used for fast updation with reduced cost of power. Ten witness nodes are generated and they are in moving state in the ad-hoc network. Then based on the user centric approach, nearby nodes are selected.

Table 1: Experimental Setup

Information Communication	Bluetooth technology
Number of Mobile Devices	10
Distance	10 m
Number of Witness nodes	10
Prover node	1
Selection Method	Random
Encryption	Public Key Cryptography (RSA)

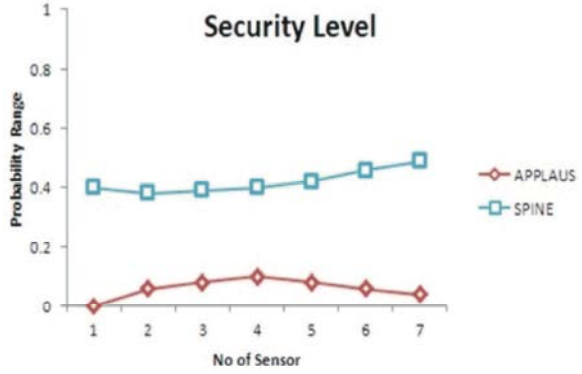

Fig. 2: Security Level

Fig. 3: Proof Delivery Ratio

Results are evaluated based on the trust level or security level and proof delivery ratio which are mapped from 0 to 1. The value 1 represents proof given by prover node is exactly correct. The trust system is implemented by threshold method.

From the Figure 2, it is observed that SPINE has the highest probability range when the number of sensor increases.

Proof Delivery ratio is the ratio of number of correctly identified locations to the number of reported locations. The Figure 3 shows the proof delivery ratio of APPLAUS and SPINE Algorithms. SPINE has the highest probability range when the number of sensor increases and it reaches near to 1.

CONCLUSION

As many of the applications need location based services, privacy preserving and location proof algorithms are implemented in the proposed work with few number of mobile nodes. Two algorithms APPLAUS and SPINE were used. Results proved that SPINE gave better performance in terms of trust level and proof delivery ratio than APPLAUS.

REFERENCES

1. Muthu, Vinothkumar, Einstein and Subala, 2013. "AASLTU: An Advanced System for Location Tracking and Updating", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, 3(3).
2. Pranali Pise and Ratnaraj Kumar, 2014. "A Review on Privacy Preserving in Location Proof System," International Journal of Advanced Research in Computer Science and Software Engineering, 4(1):.
3. Alastair, R. Beresford and Frank Stajano, "Location Privacy in Pervasive Computing, " IEEE CS and IEEE Communications Society.
4. Khairullah, M.D., Md. Habibur Rahman and S.M. Hasanul Banna, 2012. "BlueAd: A Location based Service using Bluetooth, " International Journal of Computer Applications (0975-8887), 43(15).
5. Srdjan Capkun and Jean-Pierre Hubaux, "Secure positioning of wireless devices with application to sensor networks,".
6. Zhichao Zhu and Guohong Cao, 2013. "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System, " IEEE Transactions on Mobile Computing, 12(1).

7. Tomasz Ciszkowski and Zbigniew Kotulski, “ANAP: Anonymous Authentication Protocol in Mobile Ad hoc Networks, ”.
8. Landon P. Cox, Angela Dalton and Varun Marupadi, “Smoke Screen: Flexible Privacy Controls for Presence-Sharing, ”.
9. Toby Xu, Ying Cai, “Feeling-based Location Privacy Protection for Location-based Services,”.
10. Ulrik Brandes, “A Faster Algorithm for Betweenness Centrality,”.
11. Zhichao Zhu and Guhhong Cao, 2013. “Toward Privacy Preserving Collusion Resistance in a Location Proof Updating System”, IEEE Transactions on Moblile Computing, 12(1).
12. Srdjan, C. Apkun and Jean-Pierre Hubaux, 2006.” Secure Positioning in Wireless Networks”, IEE Journal on Selected Areas in Communications, 24(2).