ISSN:2320-0790

An International Journal of Advanced Computer Technology

Privacy Preserving Location Proof Updating System

Dhinesh Kumar S.[1], A. Jesudoss[2], D. Saravanan[3]

[1] PG Student, Sathyabama University

[2] Assistant Professor, Faculty of Computing, Sathyabama University

[3] Assistant Professor, Faculty of Computing, Sathyabama University

Abstract: Location-sensitive service broadcasting on user's mobile devices to discover the current location. A privacy preserving Location proof updating system(APPLAUS),which does not rely on the wide deployement 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. An authorized verifier can query and retrieve location proofs from the server.Moreover,our location proof system guarantees user location privacy from every party.Bluetooth enabled mobile devices in range mutually generate location proofs.CA used to be the bridges between the verifier and the location proof server..

Keywords: Location-based check, location proof, location confidentiality, fictitious name, collude attack

I. INTRODUCTION

LOCATION-BASED Services, the user can take advantage of the location information, and provide a variety of resources and services to the mobile users. These days, more and more applications and services based on the location of the specified time, the need to provide customers with the location standards. For example, "Google Latitude" and "Loopt" real-time, to allow the two services to keep track of their friends' locations. Plays a key role in the creation of these applications from the location that the location -sensitive applications. There are many types of location -sensitive applications. There is a category of location -based access control. For example, a hospital, doctors or nurses in hospital does not have a separate room only allow access to patient information [4]. Location -sensitive applications in that they really are (or have) to prove to customers. Knowing that most of the mobile users the ability to devices, applications and services, some consumers from fraud and provide their current or past locations is the lack of a secure system. Possible solutions to a wide open location system , GPS, 1 which allows users to calculate their position , but it is to use the flow of information is unidirectional , there is a back channel from the GPS receiver to the satellites , the system computed the location of the user, find , and do not know that anyone Service access . Sensing the level of the raw GPS implicitly and automatically gives its users the location privacy. Cellular service providers in real-time tracking services that will help to verify the positions of mobile users, the accuracy is not good enough and proven history. In this paper, we rely on the deployment of a network infrastructure or expensive, it is a wide range of trusted computing module to update privacy -preserving location proof system (APPLAUS), propose. APPLAUS, Bluetooth mutual trust level for each location to verify that the burden of proof, which are uploaded to the server in an untrusted location proof of the location standards, the product range of mobile devices. Verifier to query the server to return to the location from which the authorized standards. In addition, our proof of the location of each party to ensure that the user location privacy. We protect the privacy of each other, especially in the location from fruit updated every mobile device to use pseudonyms, and UN Goodwill location proof from the server . Therefore, the performance of many applications the use of pseudonyms is concerned is just as good as using real identities. Obviously, the pseudonyms used in the past, nicknamed linked directly to the new nickname should be produced. Their place in the privacy of individual users, in real time, we evaluated the levels of development of the model as a user- centric location privacy and that a location -proof and to decide when to accept the request. Colluding to the attacks, the correlation for the ranking based and outlier detection, we also present the clustering -based approaches.

II. RELATED WORK

A.PSEUDONYM

Commonly used in many networks, we can set up the credentials for mobile devices run by an independent trusted third-party certificate authority (CA) are considered. Nicknamed the location of privacy, I M public / private key pairs of the network before entering the preloading of each mobile node is registered with the CA to protect the process. I used the pen to serve as the node's public key. Do not want to be tracked by the application; a user will want to use every visit to the various pseudonyms. Then the user, as they state, if you have a lot of applications to provide good services , but also a set of preferences, access to a variety of pseudonyms , the application can easily map the pseudonyms of the same user, this is to be expected . Different from any other nickname is the nickname of the state is therefore the application for the user is required to ensure that. There are two main problems. The first, (the user's pseudonyms in general) for a given user, and then store the rest of the parts of the application should be supplied in an anonymous manner. Second , the program user to customize the map to the two pairs are the same , so we are small, random variations cannot be able to determine that it might have to add . Operational semantics, and therefore could affect them negatively, while important, however, insignificant variations, may be a significant disadvantage observer. We protect the privacy of the location of multiple pseudonyms are used , ie, the mobile nodes periodically reducing the ability to link their long-term , that can be used to sign messages to change the nickname . Remove spatial relationship of their location, quiet, close to the mobile nodes and zones [1], [2], or by using the name of the coverage areas of coordination [5]. Without loss of generality, we require each node according to its privacy from time to time to change the pseudonyms.

B.MIX ZONES

We consider a continuous part of a road network, such as a whole city or a district of a city. We assume that the adversary installed some radio receivers at certain points of the road network with which she can eavesdrop th communications. On the other hand, outside outside the range of her radio receivers, the adversary cannot hear the communications. Thus, we divide the road network into two distinct regions: the observed zone and the unobserved zone. Physically, these zones may be scattered, possibly consisting of many observing *spots* and a large unobserved area, but logically, the scattered observing spots can be considered together as a single observed zone.

III. THE LOCATION PROOF UPDATING SYSTEM

In this section, we prove the updating of the location of the structure, protocol, and how to achieve privacy in their location to prove the location of the mobile nodes APPLAUS introduced updating schedule.

A-Architecture

In APPLAUS, mobile nodes communicate via Bluetooth to the neighboring nodes, and unreliable by the cellular network interface communicating with the server. They are in the process of updating the location proof online on different roles, they Prover, the witness, the location proof server, the certificate authority or assorted verifier. Architecture and the message entered APPLAUS.

Prover: node to its neighboring nodes needs to collect from the location standards. T the time needed for a location proof, prover Bluetooth to transmit the request to its neighboring nodes, the proof of a location. Get any positive response, prover dummy location proof server product and the location proof submit.

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.

Server Location Proof: Our goal is not only

Monitor real-time conditions, but again Evidence needed information on the history of the location, a Evidence of the need for server space to store Evidence, the history of the place. PROVER their location and the nodes communicate directly with submission standards. Identify the source location parameters such as pseudonyms, use, evidence is unreliable servers in the sense that even though it is compromised and monitored by attackers, it is impossible for the attacker to reveal the real source of the location proof.

Certificate authority: usually use a lot of Networks, which is run by an independent third we consider an online CA. CA and pre-load the network before entering the public / private key pairs, each mobile node in the register set. CA real identity and pseudonyms (public keys) to know the mapping, and ensures that the only party that acts as a bridge between the server and the location proof. From the server back to the location proof and ensures that it is ahead of it.

Verifier: a third-party user or an application who is authorized to verify a prover's location within specific time period. The verifier usually has close relationship with the prover, e.g., friends or colleagues, to be trusted enough to gain authorization.

IV. THE LEVEL OF PRIVACY PROVIDED BY THE MIX ZONE

(By changing pseudonyms) to quantify the level of privacy provided by the mix zone, there are various metrics. In making the decision described above, our model is a natural metric is the probability of success of the adversary. Is the probability of success, then mix zone and changing pseudonyms are ineffective. On the other hand, if the adversary is less probability of success, then the tracking system is difficult and ensures privacy shows the impact of the nickname in the location privacy.

V. COLLUDING ATTACKS

And the location privacy of the location of the joint problems of proof in [33] has been studied, but the fear of colluding attack is still an open issue. Two nodes collude with each other to create bogus location standards, this is a threat. C1 is an honest node from San Francisco to New York City (NYC) to prove that she was in need, for example, she said, New York City. Generally location tag, she bogus location standards for the design of such attacks may be another colluding node C2 and colluders world location traces, as well as the time and identify the location and tested the stability of the interaction between the moving trajectories. No matter what their real identities of the first system, we witness the number of nodes required to obtain a prover to consider the statistical initial solution. As we know, at a certain point the location proof server contains information about the number of pseudonyms. Prover enough to find this information to peers or peer is always the same on the basis of some of the statistical methods used to assess whether it is about not finding.

VI. EVALUATION

A- APPLAUS NETWORK IN SOCIAL FIELD

APPLAUS server in the network, users can make use of its services on a primary level was registered. In response, the server, the user ID of a user. Each mobile node in the network before entering the public / private key pairs, which is composed of a set. The user back to the server at the end of the Bluetooth device name and device ID are stored. After the user is logged in to a friendship, and he finds the name of the new users will be forwarded to the social network. He requested that his account of the user's request will be presented to the user with a third party. Deny the request to the third-party user in the network, and can accept a friendship

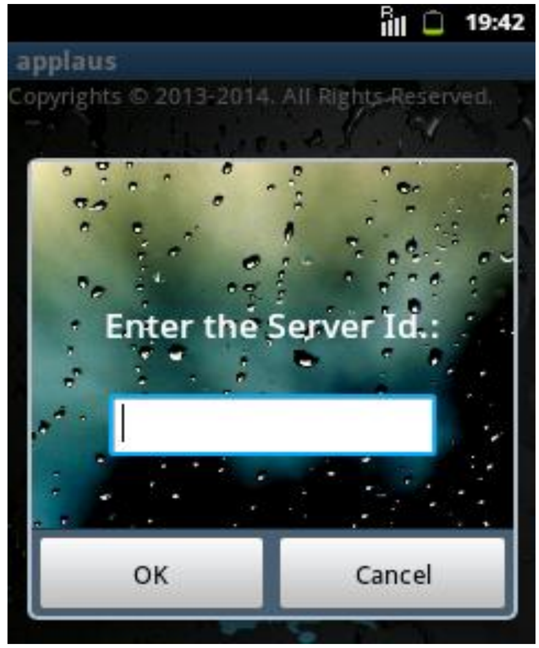

Fig. 1 Applaus apk

Fig. 2 User Registration

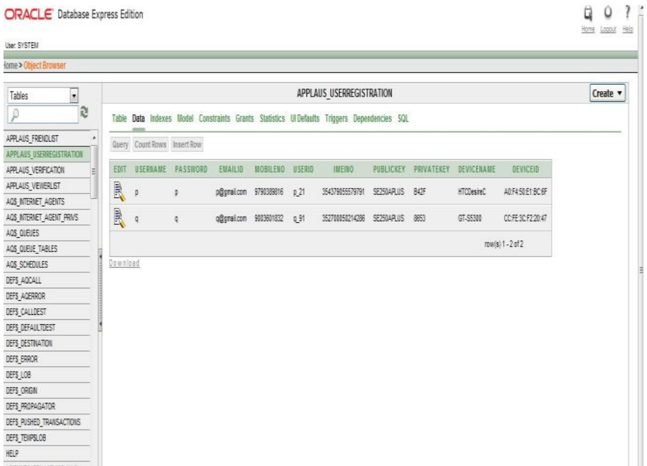

Fig. 3 User Registration Data

B. RESULTS OF LOCATION PROOF UPDATING SYSTEM

Time T from its neighboring nodes need to collect the location standards prover, Bluetooth to transmit the request to its neighboring nodes, the proof of a location. The request of the prover's nickname (prover's mobile Bluetooth device name, device id . , User information) and are randomly generated . Agrees that once the location for the prover to a neighboring node, the node becomes a witness to the prover. Witness in a position to prove the product node and sends it back to the prover. Witness turns his GPS and his current latitude and longitude positioning the product, and then sends its response back to the prover. Response prover's nickname, prover of the randomly generated number, name of the witness and the witness's has a randomly generated number. Get any positive response, prover dummy location proof server product and the location proof submit. This information will be seen as a map model verifier.

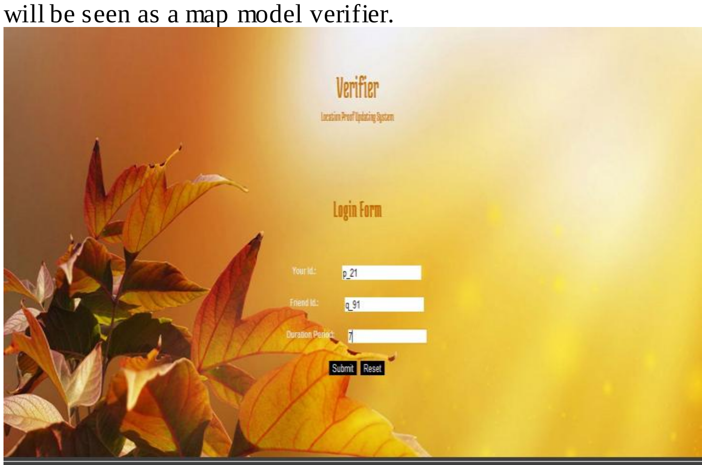

Fig. 4 Location Proof Updating System

VII. CONCLUSION AND FUTURE WORK

In this paper, we collocated Bluetooth standards for each product and the proof of the location of mobile devices is uploaded to the server, to protect the privacy of APPLAUS updating the location proof system proposed. We protect each other from the source location privacy for each device to use pseudonyms statistical turned, and cannot rely on proof from the server location. Their place in the privacy of individual users, in real time, we also evaluated the levels of development of the model is a user-centric location privacy and privacy levels based on their location and to decide when to accept a position in the proof of the conversion request . The best of our knowledge, this is the first work location evidence and the location privacy problem in the joint

REFERENCES

[1] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, "Caravan: Providing Location Privacy for VANET," Proc. Embedded Security in Cars (ESCAR) Workshop, 2005.

[2] D.Saravanan, Dr.S.Srinivasan, "Data Mining Framework for Video Data", In the Proc.of International Conference on Recent Advances in Space Technology Services & Climate Change (RSTS&CC-2010), held at Sathyabama University, Chennai, November 13-15, 2010.Pages 196-198

[3] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy," Proc. Fifth ACM Workshop Privacy in Electronic Soc., 2006.

[4] Y. Li and J. Ren, "Source-Location Privacy Through Dynamic Routing in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2010.

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

[6] 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.

[7] Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing 3(1), 46–55 (2003)

[8]. Beresford, A., Stajano, F.: Mix Zones: User privacy in location-aware services. In: Proceedings of First IEEE International Workshop on Pervasive Computing and Communication Security (PerSec) 2004, a workshop in PerCom (2004)

[9] D.Saravanan, Dr.S.Srinivasan, "Video Image Retrieval Using Data Mining Techniques "Journal of Computer Applications, Volume V, Issue No.1. Jan-Mar 2012. Pages39-42. ISSN: 0974-1925.

[10]H. Chan, A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, page 197. IEEE Computer Society, May 2003.

[11]A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Security and Privacy, 2003.

[12] Jesudoss A. and Subramaniam, N.P., "A Taxonomy of Authentication Techniques for Web Services", International Journal of Engineering Research & Technology, Vol. 3, Issue 1, Jan. 2014, pp.271-275.

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

[14] D.Saravanan, Dr.S.Srinivasan, " A proposed New Algorithm for Hierarchical Clustering suitable for Video Data mining.", International journal of Data Mining and Knowledge Engineering", Volume 3, Number 9, July 2011.Pages 569.