IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue I, December 2014
ISSN: 2394 - 6598

LOCATION IDENTITY SYSTEM FOR SECURE AND DEFEND AGAINST COLLUDING ATTACKS

C.SATHYA
PG SCHOLAR -CSE DEPT
M.I.E.T. ENGG. COLLEGE ,TRICHY.
sathyacs91@gmail.com

Dr.V.CHANDRASEKAR M.Tech.,Ph.D.,
PROFESSOR-CSE DEPT
M.I.E.T. ENGG.COLLEGE,TRICHY.

ABSTRACT—Users mobile device to determine the current location and it sends location information to other users. It makes possible for cheat on the users location by malicious users. In this paper it is proposed A Privacy Preserving Location Proof Updating System (APPLAUS) to create location proof information and updates to the location proof server. Sometimes pseudonyms are changed by the user nodes to protect location privacy from malicious users and from the un trusted location proof server. To develop user-centric location privacy model in which entity users to estimate their location privacy levels and make a decision for when to accept the location proof requests. With the aim of preserve against colluding attacks, present between's ranking-based and correlation clustering-based approaches for outlier detection. APPLAUS can effectively provide location proofs, secure for key generation, extensively preserve the user's location privacy, and successfully discover colluding attacks. To avoid time delay using the TTL Algorithm, this algorithm will avoid time delay by fixing the time value for content and protect the network from the malicious users, if any user is fake while fake their proof that user will be filtered from the network, they cannot access the network.

I. INTRODUCTION

LBS can access, combine, and transform contextual information, and more specifically location information, in order to personalize the service provided to the user. For instance, LBS can be used for resource discovery (e.g., finding the closest room from my position), path-finding (e.g., computing the shortest route to a gas station), real time social applications (e.g., informing me about the presence of my friends in the area) or location-based gaming (e.g., playing with the nearest competitor). A location proof is an electronic form of document that certifies someone's occurrence at a certain location at some point in time. A location proof architecture is a mechanism with which mobile users can obtain location proofs from proof issuers and with which applications can verify the validity of these proofs.

Location based applications have existed for several years verify the correctness of a user's original location is a challenge that has only recently gained attention in the research area. Existing architectures for the generation and verification of such location proofs have limited flexibility. Role based access control is not always sufficient in restricting access to confidential information. Online social networks allow users to form social groups based on their geographical locations.

Location-sensitive applications require users to prove that they really are at the original locations. Although most mobile users have devices capable of discovering their Locations, some users may cheat on their locations and there is a lack of secure mechanism to provide their current or past locations to applications and services. One possible solution is to build a trusted computing module on each mobile device to make sure trusted GPS data is generated and transmitted.

II. LITERATURE REVIEW

Saroiu and Wolman [1] proposed in this paper location proofs that enables the appearance of mobile applications and need "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 to mobile devices. It can provide location proofs to unknown users by uploading real encounter location to the untrusted server while

IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue I, December 2014
ISSN: 2394 - 6598

maintaining location privacy. Xu and Cai[2] propose feeling–based model for location privacy protection in the location based services. This model allows a service to express user privacy requirement by requesting that the location is disclosed on user must be atleast as popular as spatial region such as shopping mall. Identifying such a region is called a public region for privacy evaluated is much more sensitive than specifying a number of K as in the traditional K-anonymity model.

The technique [3] to introduce a new entity for user location systems, the mix zone, which is analogous to a mix node in communication systems. Privacy of location information is about controlling access to this user information. It do not necessarily want to stop all access because some applications can use this information to provide useful services. A mix zone is defined to be a spatial region in which a mobile node does not support its location. When there are multiple nodes inside the same mix zone [4] they exchange their pseudonyms.

In vehicular communications also introduce some privacy risk by making it easier to track the physical location of vehicles. These vehicles are using pseudonyms that they change with some frequency. A mix zone is defined to be a spatial region in which a mobile node does not report its location. When there are multiple nodes inside the same mix zone, they exchange their pseudonyms. Supporting proactive location proofs[5] are challenging because these proofs might enable proof issuers to track a user or they violate a user's location privacy by revealing more information about a user's location than strictly necessary to an application.

III. PROPOSED METHODOLOGY

In this paper, to propose A Privacy-Preserving Location proof Updating System (APPLAUS), this does not rely on the broad use of network infrastructure or the exclusive trusted computing module. In APPLAUS, Bluetooth enabled mobile devices in certain range mutually produce location proofs, which are uploaded to a untrusted location proof server that can verify the trust level of each location proof.

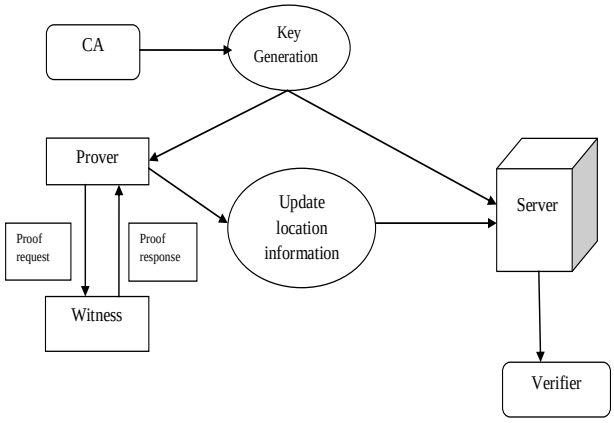

Fig. 1. Location Proof Updating System

Every mobile node registers with the Certificate Authority and generate a public or private key for protect the user location information. Prover node(initiation node) is initiate the location information and update the location proof server. This node is sends location proof request with prover identification to neighboring nodes. Witness nodes(neighbor nodes) are decide whether and when to accept the location proof requests using user centric privacy model. If no positive response is received the prover node will generate a fake location proof and submit it to the location proof server. The witness node will create a location proof information and send it back to the prover. The prover collects the location information from the neighbor nodes for confidentiality. Location Proofs are stored as pseudonyms so it is impossible for malicious users to reveal the real source of the location proof. Certificate Authority is to check the entered node is trusted it forwards to the location proof server. The verifier is close relationship to the prover, so it is check the prover location within a specific time period.

Betweenness is defined as the number of shortest paths from all vertices to all others that pass through node. It is noticed of which is the most affected node in the entire network(i.e., who interconnects with most others). Nodes are ordered in the priority based with the betweenness. Each node gives ranks these pseudonyms in the network. In this ordered which node is the lowest betweenness is only connected to one or few neighbors. So these nodes are consider the outliers among all the nodes and it also likely as a colluding attackers.

Correlation clustering approach only considers two location proofs correlated if they occurred at the same time. A node may have to wait for a time period

until its next location proof updating cycle. If the time delay between two location proofs is not too large, it should still consider them correlated. Correlation clustering algorithm on a temporal weighted graph to rule outlier clusters which is measured as suspicious location proofs.

To detect if two pseudonyms belong to the same source, the attacker can check whether the two probabilistic distributions of location proof updating time intervals from the two pseudonyms are identical. APPLAUS can provide location proofs to third-party by uploading real encounter location to the untrusted server while maintaining location privacy.

Identify the fake users those who submit the fake proof or those who misbehave the proof. Fake proof are categories into fake users and Normal proof are categories into normal users. Fake user originalities are categories into fake and status into week and normal user originalities are categories into good and status into normal. Identify the users whether they are Normal users or fake users. And monitoring the details whether normal user or fake user and maintain the details separately to protect the network. In case any fake user occurs they cannot access the network for security purpose.

Each mobile node monitors and measures its own privacy level in real time and decides whether and when to accept a location proof exchange request. After receiving a location proof exchange request, it calculates the privacy loss between the next scheduled updating time and the current updating time. Using a long-term pseudonym for each user does not provide much privacy even if the same user gives out different pseudonyms to different applications to avoid colluding attacks. Source node fixes the TTL Value along with Packets to the destination. Packets travel to the destination node through intermediate nodes with TTL Value. When packets reach the destination, TTL value will be check whether time lapse or not. If time lapse packets will be drop automatically or else packets reaches the destination whatever expect.

IV. CONCLUSION

In this paper it was proposed to location proof updating system and generate key for each node, so every nodes hiding the location information from malicious users. APPLAUS can provide location proofs effectively and it preserves source location privacy and collusion resistant. It defend against colluding attacks using betweeness ranking based and correlation clustering approach. So users location information is protected and restrict from attackers.

REFERENCES

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

[2] T.Xu and Y.Cai, "Feeling-Based Location Privacy Protection for Location-Based Services," Proc. 16th ACM Conf. Computer Comm. Security (CCS), 2009.

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

[4] 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.

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

.

[7] M.Shao, Y.Yang, S.Zhu, and G.Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, 2008.

[8]T.Jiang, H.J.Wang, and Y.C. Hu, "Location Privacy in Wireless Networks," Proc. ACM MobiSys, 2007.

[9]Z.Zhu and G.Cao, "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-Based Services," Proc. IEEE INFOCOM,2011