ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (650-653), Month: April - June 2015, Available at: www.researchpublish.com

Protecting Sensitive Files from Unauthorized Network Users Based On Location Proof Criteria

[1]Midhun Das, [2]Rasheeda Z Khan

[2]Head of Department, [1,2] Dept. Of ISE, Shree Devi Institute of Technology, Mangalore, India

Abstract: **Today's location-sensitive service depends on user's mobile device to determine the current location. This leads malicious users to access restricted resource by cheating on their locations. To resolve this, proposed A Privacy-Preserving Location proof Updating System (APPLAUS) in which collocated Wi-Fi enabled systems mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the systems to protect source location privacy from each other, and from the untrusted location proof server. Also developed user-centric location privacy model where the individual users evaluate their location privacy levels and decide whether and when to accept location proof requests. APPLAUS can be implemented with existing network infrastructure, and can be easily deployed in Wi-Fi enabled systems with low power cost. Further experimental results show that APPLAUS can effectively provide location proofs, significantly provide source location privacy, and it detects colluding attacks.**

Keywords: **Location-based service, location proof, location privacy, pseudonym.**

1. INTRODUCTION

Location privacy is an important security issue. Lack of location privacy can expose significant information about the traffic carried on the networks and the physical world entities. This paper focuses on source-location privacy schemes through routing to randomly selected intermediate node before the message is transmitted to the SINK node [1]. A model based on the concept of the mix zone, characterize the tracking strategy of the adversary in this model, and introduce a metric to quantify the level of privacy enjoyed by the vehicles. Also introduced a metric to quantify the level of privacy enjoyed by the vehicles in this model [2]. A mechanism for secure positioning of wireless devices, that called as Verifiable Multilateration. It focus on sensor network positioning and propose SPINE, a system for Secure Positioning In sensor NEtworks. This system is based on Verifiable Multilateration and ensures secure positioning of sensors in the presence of adversaries [3]. It introduce more efficient algorithms based on a new accumulation technique that integrates well with traversal algorithms solving the single-source shortest-paths problem. The range of networks for which betweenness centrality can be computed is thereby extended signicantly [4]. When a user's location privacy is compromised, an attacker can determine where the user is, and use this information, for example, to stalk or blackmail the user. So that location privacy must be a first-class citizen in the design of a wireless communications system. We build a transaction-based wireless communication system in which transactions are unlinkable [5]. The "distance bounding" technique solves the problem by timing the delay between sending out a challenge bit and receiving back the corresponding response bit. It can be integrated into common identification protocols. The technique can also be applied in the three-party setting of "wallets with observers" in such a way that the intermediary part can prevent the other two from exchanging information, or even developing common coinflips. [6].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (650-653), Month: April - June 2015, Available at: www.researchpublish.com

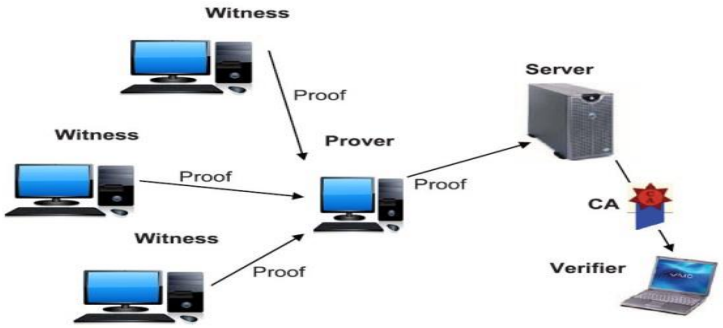

Fig. 1: Location proof updating architecture and message flow.

It can be summarized as follows:

- Proover: the node who needs to collect location proofs from its neighboring nodes.
- Witness: Once a neighboring node agrees to provide location proof for the prover, this node becomes a witness of the prover.
- Location proof server: It is necessary for storing the history records of the location proofs. It communicates directly with the prover nodes who submit their location proofs.
- Certificate authority: As commonly used in many networks, we consider an online CA which is run by an independent trusted third party.
- Verifier: a third-party user or an application who is authorized to verify a prover's location within a specific time period.

2. PRELIMINARIES

2.1 Pseudonym:

Here we consider an online certification Authority (CA) which is run by independent trusted third party. These are commonly used in many networks. Probes are used for system nodes to discover their neighbors. This is due to the broadcast nature of the wireless communication. When a node say i, receives a probe from another node, it checks the certificate of the public key of sender and the physical identity, e.g., Bluetooth MAC address. Thereafter the signature of the probe message is verified by i. A security association is established, if any confidentiality is required.

2.2 Threat Model:

Assume that an adversary aims to track location of a system node. An adversary can have the same credential as a system node. We assume that adversary is internal, passive, and global. Internal means that the adversary is able to compromise or control individual system and then communicate with others to explore private information. Also there is a chance for individual devices may collude with each other to generate false proofs. By passive, we assume that adversary cannot perform active channel jamming, mobile worm attacks or other attacks such as denial-of-service attacks, since these attacks are not related to location privacy. By global, we assume adversary can monitor and analyze all the traffic in its neighboring area or can also monitor all the traffic around the server. The adversary can thus treated as a set of malicious system nodes in the network. We need to properly design and arrange the location proof records in the untrusted server so that no private information related to individual users will be revealed even after it is compromised. Thus the problem we address in this paper consist of collecting set of location proofs for each node and further protect the location privacy of peer nodes from each other or even from the untrusted location proof server to prevent other parties from learning a nodes past and current location information.

2.3 Location Privacy Level:

Here we use multiple pseudonyms to provide location privacy. We assume that each node changes its pseudonyms from time to time depending on its privacy requirement. Here we introduce a mix zone. If the node changes its pseudonym at least once during a time period, this refers to a mix-zone and a mix of its identity and the location occurs. The mix-zone becomes a confusion point for adversary.

2.4 Protocol:

- The prover broadcast a location proof request to its neighboring nodes through Wi-Fi according to its update scheduling. The request should contain the prover's current pseudonym P_{prov}, and a random number R_{prov}.
- Witness decides when to accept the location proof request according to its witness scheduling. Once agreed, it will generate location proof for both prover and itself send proof back to the prover. This location proof includes the prover's pseudonym P_{prov}, prover's random number R_{prov}, witness's current time stamp T_{witt}, witness's pseudonym P_{witt}, and their shared location L.
- After receiving the location proof, prover is responsible for submitting this proof to the location proof server. The message includes prover's pseudonym P_{prov} and random number R_{prov}, or its own location for verification purpose.
- An authorized verifier can query the CA for location proofs of specific prover. The CA first authenticates the verifier, then converts real identity to its corresponding pseudonyms during that time period and then retrieves their location proofs from the server. In order not to expose correlation between pseudonyms to the location server, CA will always collect enough queries from k different nodes before a set of queries are sent out.
- The location proof server returns hashed location rather than real location to the CA, who then forwards to the verifier. The verifier compares the hashed location with the claimed location acquired from the prover to decide the claimed location is authentic.

3. SCHEDULING LOCATION PROOF UPDATES

It is necessary to schedule the location proof so that it need to properly design and arrange the location proof updating schedules for both prover and witness so there will be no source location information related to individual user is revealed even if the server is compromised.

When the witness nodes exchange information of location proofs the location privacy of nodes varies depending on the time and the location. Thus it is necessary to protect the location privacy in a user-centric manner so that each user can decide when and how to protect their location privacy. The user-centric location privacy follows a distributed approach and each system node monitors location privacy level over time.

A network wide metric measures the average location privacy but may ignore some nodes due to low location privacy levels. However, the user centric approach is more scalable and can maintain location privacy at higher levels. In our model, the location privacy of a node may observed over time. It depends on the distribution diversity of last pseudonym and its previous pseudonyms before the last successful pseudonym get changed. Each system node monitors and measures its own location 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 then calculates the privacy loss between the next scheduled updating time and the current updating time. In this way, a node has the capacity to control the time period over which its location is tracked.

Under our attack model, an adversary can easily understand a constant rate distribution and its mean by statistic test through the history of location proof records. Since it is difficult to guarantee the perfect event unobservability while providing low latency, we choose statistically strong source location unobservability in order to achieve low latency and high privacy.

4. PERFORMANCE ANALYSES

In this section, a thorough experimental evaluation of the feasibility of deploying APPLAUS such as the computation and the storage constraint, power consumption, and the proof exchange latency. The performance of APPLAUS is also evaluated by the use of simulation technique.

4.1 Privacy evaluation:

Here we deals with the robustness of APPLAUS such as defending against traffic analysis and statistical test. We cannot prevent the attacker from using any statistical analysis tool. For the attacker, the hypotheses of the test are:

- H_0—the two pseudonyms belong to the same source.

- H_1—the two pseudonyms belong to different source.

Suppose when the attacker makes a decision, there are some risks to get wrong decision. The decision is called as detection, if H_0 is accepted when it is actually true. If H_0 is in fact true, accepting H_1 is a false negative. On the other hand, if H_1 is in fact true, accepting H_0 is a false positive. False positive has no negative effect on privacy since taking two different pseudonyms as the same would not help identifying the real source. We focus on false negative which indicates the percentage of cases that has not been detected by the attackers. Here we use computation time and successful detection ratio inorder to measure the efficiency and effectiveness for detecting colluding nodes.

5. CONCLUSION

In this paper, we proposed privacy-preserving location proof updating system called APPLAUS, where collocated Wi-Fi enabled systems mutually generate location proofs and upload to the location proof server. Also we use statistically changed pseudonyms for each system to protect source location privacy from each other, and from untrusted location proof server. We developed a user-centric location privacy model where the individual users evaluate their location privacy levels and decide whether and when to accept location proof request. Here we addresses the joint problem of location privacy and location proof. Thorough analysis investigating privacy and location proofs guarantees of proposed schemes is given, and experiments on the real-time location show that provides source location privacy and collusion resistant.

REFERENCES

[1] Li, Yun, and Jian Ren. "Source-location privacy through dynamic routing in wireless sensor networks." INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.

[2] 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.

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

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

[5] Hu, Yih-Chun, and Helen J. Wang. “A framework for location privacy in wireless networks.” In ACM SIGCOMM Asia Workshop. 2005.

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

About The Authors:

Midhun Das[1] completed the Bachelor’s Degree in Computer Science and Engineering from Visvesvaraya Technological University (VTU). Currently pursuing masters in Computer Network Engineering from SDIT, Mangalore.

Rasheeda Z Khan[2] received Master Degree in Computer Science and Engineering from NITTE. She is currently working as Head Of Department in the Department of Information Science and Engineering, Shree Devi Institute of Technology.