International Journal of Multidisciplinary Research and Development 2015; 2(3): 760-762

International Journal of Multidisciplinary Research and Development

IJMRD 2015; 2(3): 760-762
www.allsubjectjournal.com
Received: 08-03-2015
Accepted: 29-03-2015
e-ISSN: 2349-4182
p-ISSN: 2349-5979
Impact Factor: 3.762

Take Vaishnavi V
(B.E Computer Engg.Pune University) PREC, Loni, Maharashtra, India.

Karle Gayatri D
(B.E Computer Engg.Pune University) PREC, Loni, Maharashtra, India.

Bhosale Vrushali S
(B.E Computer Engg.Pune University) PREC, Loni, Maharashtra, India.

Barde Kirtee G
(B.E Computer Engg.Pune University) PREC, Loni, Maharashtra, India.

S.D. Jondhale
Prof. (M.E Computer Engg.Pune University) PREC, Loni, Maharashtra, India.

Correspondence:
S.D. Jondhale
Prof. (M.E Computer Engg.Pune University) PREC, Loni, Maharashtra, India.

Location proof updating using location based services with privacy preserving

Take Vaishnavi V, Karle Gayatri D, Bhosale Vrushali S, Barde Kirtee G, S.D. Jondhale

Abstract
In today's world, the mobile devices are used to detect the current location of the person. This allows the users to cheat on their locations and try to access the restricted resources or the Data. In APPLAUS, we proposed A Privacy Preserving LocAtion proof Updating System in which, the Bluetooth enable mobile devices, generates the location proofs and updates to the location proof servers. The pseudonyms are used to maintain the location privacy from each other. We also developed user centric privacy model. In this model, which individual users evaluate their location privacy and decide whether and when to accept the location proof request. APPLAUS can be implemented within existing network infrastructure and also used Bluetooth enabled mobile devices. APPLAUS can effectively provide location proofs and preserves the location privacy.

1. Introduction

Nowadays, more location based applications and services require users to provide the location proof at a particular time. There are many kinds of location sensitive applications e.g. many applications which require location based access control such as a company may allow its employs information access only when employees or Boss can prove that they are in a particular department of office. Another one is police investigation, in which police forces are interested in finding out if a person was at a murder place at some time. The common theme across this location sensitive application is that they offer a benefit to the users to locate in a particular geographical area at a particular time. Thus, users get courage to cheat on their location.

Above location sensitive applications needs users to prove that they really at the claimed location. Most mobile devices are capable of finding the locations. This uses GPS data to be transmitted [3]. The location proofs are also generated using the photos and videos [3], but these takes lots of time for proof generation and the accuracy is not good enough and the location history cannot be verified. That's why the system becomes so much expensive and time consuming.

We propose, A Privacy Preserving LocAtion proof Updating System (APPLAUS), in which Bluetooth enabled mobile devices in range generates location proofs, which are uploaded to location proof server that can verify the trueness of each location proof. Only an authorized verifier can query and also retrieve location proofs from the server. We use periodically changed pseudonyms at each mobile device to maintain location privacy from each other and from the untrusted location proof server. We also developed user centric privacy model. In this model individual users evaluate their location privacy and decide whether and when to accept the location proof request.

2 Working Model:

In APPLAUS, mobile nodes communicate with neighboring nodes through Bluetooth, and communicate with the untrusted server through the cellular network interface. Based on different roles they play in the process of location proof updating, they are divided into Prover, Location Proof Server, Witness, Certificate Authority or Verifier. The message flow and architecture of APPLAUS is shown in Fig. 1.

Prover:

It is the node who needs to collect location proofs from its neighboring nodes. At time t, when a location proof is needed, the prover will firstly broadcast a location proof request to

its neighboring nodes. The prover will generate a dummy location proof, if no positive response is received. After receiving proof submit it to the location proof server.

Witness:
The nodes which agrees to provide location proof to prover,it becomes witness. The witness sends generated location proof to the prover.

Location proof server:
Our goal is to monitor real-time locations and to retrieve history location proof information if needed, a location proof server is responsible for maintaining and storing the location proofs history records. It directly communicates with the prover nodes. Because of pseudonym is used for the location proof and though server is untrusted and compromised it is impossible for the attacker to find the real location.

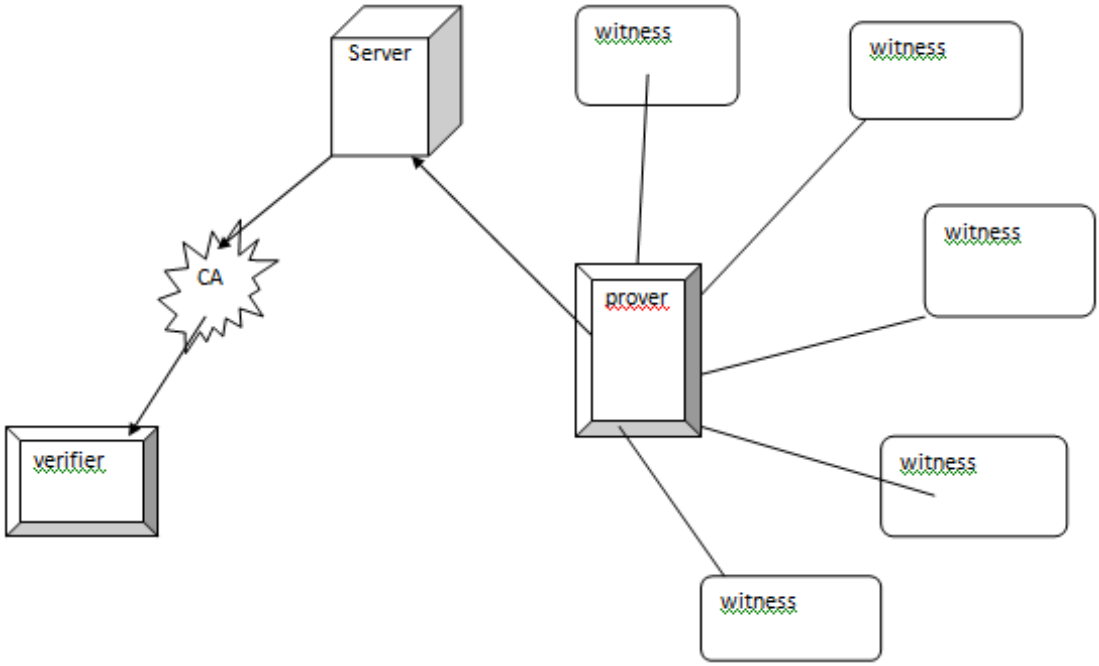

Fig 1: Architecture of APPLAUS

Certificate Authority:
An independent trusted third party is run an online CA. Every mobile node registers with the CA and get allocated by a set of public/private key pairs. CA only knows the mapping between the real identity and pseudonyms. It acts as a bridge between the location proof server and verifier. Location proof is forwarded from the server to the verifier.

Verifier:
In a specific time a verifier who is authorized is verifies location. The verifier has close relationship with the prover. e.g., friends or colleagues, which are trusted to have authorization.

2.1 Input:
Login ID and Password, Request for Location Proof

2.2 Output:
We get a verified and correct Location proof

3 Algorithms:

A. Algorithm 1: Location proof updating scheduling for the prover

Input: Updating parameter m

1. Generate N distinct parameter m_1, m_2,…., m_N
2. for each pseudonym i, do
3. while current timestamp t, follows poison distribution with m_i , do
4. send location proof request
5. If request is accepted then
6. submit location proof
7. else
8. generate and submit dummy proof
9. end if
10. end while
11. end for

Explaination of Algorithm:
The location proof server contains all history about location proofs and if attackers compromise this server, he will obtain complete coverage and track the nodes through network. So, the location proof updating server needs scheduling for prover and witness. Hence information related to location of individual node is not revealed.
Suppose, a node has number of different pseudonyms which changes periodically, each pseudonym updates location proof with the help of poisson distribution in inter-updated intervals, then A single node follows poisson distribution with different parameters of pseudonym which are pre-determined. Poisson distribution has property of pseudonym unlinkability and strong source location unobservability.
In algorithm 1, pre-defined updating parameter m shows how location proofs are updated frequently. If sometimes no location proof is generated at the updating time, then it follows scheduled Poisson distribution and a dummy proof is generated and submitted. The dummy proof is same as real location proof and impossible for attacker to reveal.

Algorithm 2: Scheduling of the location proof updates at witnesses side

Input: Incoming time t of location proof exchange request

1. Calculate location privacy loss D when assuming the incoming request is accepted
2. D > € , € is predefine location privacy loss threshold then
3. Deny location proof exchanged the request
4. If Else
5. Accept location proof exchange request
6. End if

Explaination of Algorithm:

Privacy of witness may vary depends on time and location. When it exchanges location proof. User centric [3] location privacy uses a distributed technique to protect its privacy level [6]. In this, each mobile node locally monitors location privacy. The average location privacy where measure by a wide network. In this system, location privacy of a node accumulates over time. Each mobile monitors its privacy level and decides when to accept location proof request, after then it calculates a privacy loss. In this way, a node has control the period of time over location is tracked.

4. Advantages:

1. We use multiple pseudonyms to preserve location privacy.
2. We also develop a user centric location privacy model in which individual users evaluate their location privacy levels in real time.
3. We use statistically changed pseudonyms for each device to protect source location privacy from each other, and from the untrusted location proof server.

Conclusion

In this paper, we proposed a privacy preserving location proof updating system in which neighboring Bluetooth enable mobile will generate location proof and updated to the location proof server. Pseudonym is used for device to protect privacy of location from each other and untrusted server.

References

1. APPLAUS: A Privacy Preserving Location Proof Updating System for location- based services
2. Toward privacy preserving and collusion resistance in a location proof updating system
3. B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.C. Herrera,A.M. Bayen, M. Annavaram, and Q. Jacobson, “Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring,” Proc. ACM MobiSys, 2008.
4. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, “Location-Based Trust for Mobile User-Generated Content: Applications Challenges and Implementations,” Proc. Ninth Workshop Mobile Computing Systems and Applications, 2008.
5. M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, “Caravan: Providing Location Privacy for VANET,” Proc. Embedded Security in Cars (ESCAR) Workshop, 2005.
6. 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.