ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

The Solution for Weak Identity in Privacy Preserving Location Proof Updating System

Pranali Pise[1]
Student
Department of Computer Engineering
G. S. Moze College of Engineering, Balewadi
Pune – India

Ratnaraj Kumar[2]
Professor,
Department of Computer Engineering
G. S. Moze College of Engineering, Balewadi
Pune – India

Abstract: The inspiration of this approach is to authenticate user's mobile device by protecting privacy of location proof. A person's location proof depends on user's mobile device position. Biometric authentication technique is proposed in order to avoid malevolent users from prevaricating their uniqueness. The location proofs are generated by co-located bluetooth enabled mobile devices. The working of our proposed system is similar to A Privacy Preserving Location proof Updating System (APPLAUS) [13]. In advance to it, the technique of biometric authentication is deployed for preventing the weak identity of mobile device. The history of the location proof of mobile devices is saved on an untrusted location proof server; therefore there is a possibility of attacks on data, which can expose the locations of genuine devices. Hence the major necessity is to preserve the privacy of each device by using multiple pseudonyms. Therefore to maintain security and privacy, our proposed system that is An Efficient Approach to a Location Proof Updating and Privacy Preserving System (AEALPUP2S) separates the sensitive biometric data from location history of mobile device. For extra security, the biometric information is stored in biometric encryption format.

Keywords: location proof; location privacy; identity privacy; unlinkability; biometric authentication.

I. Introduction

Any mobile network doesn't sustain a proper infrastructure and also insecure due to its broadcasting nature, which means, mobile nodes can connect or leave network at any time and location. The mobile device is used to discover the location of person. Location proof is the document that certifies the location of the person at a particular time in geographical area. By using location proof, mobile device offer services about nearest entities (i.e. nearby hospitals, airport, ATM, restaurants.).Location sensitive applications consist of Location based access control and Location aware routing. Location proof updating system is useful in providing a history of location proofs and identifying a geographical location of users.

At the first glance we think that idea of APPLAUS system is best; but after studying carefully, we observed that there is weak identity of mobile device is observed; weak identity means uniqueness of mobile device is lost. In simple words we can say that if someone's mobile is lost or stolen by anyone else in the system then there is a chance of misuse of device means it is very risky for that person in system. So, to avoid system from weak identity, we re-established the A Privacy Preserving Location proof Updating System (APPLAUS) [13] system by using biometric system with the name of An Efficient Approach to A Location Proof Updating and Privacy Preserving System (AEALPUP2S) with an addition of one extra feature that is Biometric Authentication. In our system, for obtaining location proof privacy, mobile nodes are satisfying some basic properties like Identity privacy which is an ability to hide the identity of the mobile node by using pseudonym. So the real identity of the user can't be traced by the malevolent node. Unlinkability property **which** is an ability to hide the relation of subsequent sessions of the mobile node from unauthorized entity. Location privacy which is an ability to prevent other parties from gaining one's current or past location. Also Biometric encryption which is untraceable biometric, as the biometric data provided by the user can not be reversible. Neither the key nor the biometric data can be retrieved from the stored template as biometric encryption binds securely the cryptographic key to the biometric data. Only a valid person can reconstruct key only if the accurate biometric sample is presented on verification [11], and lastly biometric authentication which is detection of the person by using their physiological and behavioral characteristics. Biometric identification is necessary to spot the mobile device used to generate location proof at particular time for the specified person [11].

To the best of our knowledge this is the first efficient and robust system which uses biometric Authentication. As biometric feature exchange is easily observed in future, so this system will be used in many areas for authentication purpose. The rest of the paper is organized as follows: Section II is the survey of related work of location privacy in various systems. Our system design is detailed in Section III. In Section IV, the implementation details are explained. Experimental results are presented in Section V. We conclude this paper at last and planned for future.

II. Literature Survey

H. Kido [1]in proposed an anonymous communication technique using dummies for locationbased services means a method of generating a fake location proof and mixing them with real location proof, so it becomes complicated for location based service providers to differentiate them.A.R. Beresford and Stajano in [2] projected a framework for frequently changing user's identity by the use of pseudonyms. Pseudonyms are used for hiding the original identity. B. Waters and Felten [3] proposed a device which allowed to obtain location proofs from a location manager and then submit these proofs to a verifier. Saroiu and Wolman [4] also have location providers which issues location proofs but it discloses the user's identity and also has no means to detect defrauds. As any nearby device can collect these beacons and use them to prove that it was within this area at the time specified in the proof. But there are some disadvantages like proof issuer will not know whether the recipient received location proof or not and also proofs are transferable and no strong security mechanism is implemented. In the proposed method of Kirkpatrick and Bertino [5], the location devices issue location proofs based on near field communication so there system provides pseudonimity alone.Lenders [6] discusses a geo tagging service that allows a content creator to get a location or time certificate for the content but it does not bind the content to its generator. A challenge response scheme is planned by Capkun and Hubax [7] which uses multiple receivers to estimate a wireless node location accurately using radio frequency propagation characteristics. Li and Ren [8] and Zhang [9] tried to provide source location privacy against traffic analysis attacks in wireless sensor networks by using dynamic routing and anonymous communications.

In A Privacy Preserving Location Proof Updating System APPLAUS architecture stands around three independent entities which are: Certification Authority and Verifier, the Location proof server, the prover and witness. APPLAUS is a location proof updating system in which co-located Bluetooth enabled mobile devices mutually generate location proofs and send updates to location proof server. When a device needs a location proof, it broadcasts a location proof request which contains its current pseudonym and his actual position. Once the proof is received and accepted by a neighbouring device (means witness), then the location proof is created for both the prover and witness by including the current pseudonym of the witness and the whole is hashed and signed by that witness and delivered to the prover. After that prover node is sending it to location proof server. At any time if verifier want to check location of any node, It ask to certification authority by giving original identity and time. Certification authority converts original identity into corresponding pseudonym and send it to the location proof server. Location proof server sends the location proofs to certification authority and at last it sends to the verifier. Verifer checks the collected location from certification authority with the claimed location of prover, If matches; then prover gets verified as legitimate node, otherwise not.

But there is one main drawback of weak identity of mobile device is observed as if provers mobile gets lost or is used by someone else, then it is dangerous for the system which is used in restricted resource access. So this drawback is rectified by our proposed system by using biometric authentication, so that no one can access restricted resources as biometric security is added. And the system is used by legitimate nodes only. Also the problem of neighbouring dishonest nodes gets reduced.

III. Proposed System Design

In our system, mobile nodes communicate with neighboring nodes by means of Bluetooth interface. The Cellular network interface is communication medium for untrusted location proof biometric server.

The mobile nodes are categorized as Prover node, Witness node, Location Proof Biometric Server, Certificate Authority and Verifier.

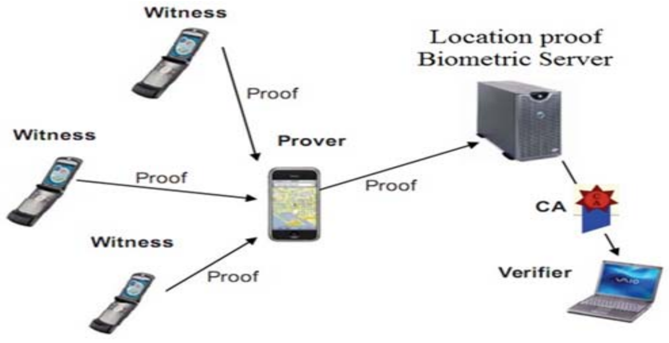


Fig 1. AEALPUP2S System Architecture

A. *Proof updating node (Prover):*

Node P is responsible for obtaining location proofs from its neighboring nodes. When location proof is needed at time t, the node P broadcast the location proof request to the neighboring nodes through bluetooth interface.

B. Mobile node (Witness):

A neighboring node agrees to give location proof for the node P. Neighboring nodes which agrees to share location proof and biometric identification are collected by node P and send it to the location proof server & biometric server respectively.

C. Location proof Biometric server:

As our goal is not only to check real-time locations but also to retrieve history of location proof information whenever it is needed. So, location proof Biometric server is necessary for storing the past records of the location proofs with the biometric data and the current time.. It communicates directly with the node P who submits their location proofs to a location proof server. The location proofs from neighboring nodes are stored as pseudonyms, even if the server is compromised; the opponent is unable to trace the location of the particular node at that particular time and the biometric data from the nearby nodes are stored as biometric encryption format, even if the server gets compromised adversary is not able to identify the identity of a particular node.

D. Certification Authority:

It is commonly used in the most of the networks; here we consider the certificate authority which is maintained by an independent trusted third party. The mobile nodes which are registered with certificate authority, preload a pair of public and private key before entering to the registered network. The real identity and pseudonyms are mapped by certificate authority only, as no one knows the relation between real identity and pseudonym. Also it works as a bridge between the location proof server and the verifier. The certification authority retrieves location proof, biometric data from the location proof server and biometric server respectively and then at last it forwards to the verifier.

E. Verifier:

A trusted third party agent, which authorizes to validate a mobile nodes location, within a particular time period. The verifier must have a close relationship with the node P, which means friends or colleagues, to be trusted for gaining authorization.

Separation of privacy knowledge is achieved in our system. That means the knowledge of privacy information is separately distributed to the location proof biometric server, the certification authority, and verifier. Thus, each party has partial knowledge only. Privacy property of our protocol is achieved by the separation of privacy knowledge it means the location proof biometric server only knows pseudonyms and locations and biometric data, the CA only knows mapping between the real identity and its pseudonyms, while the verifier only knows the real identity and its authorized locations. So, the attackers are not able to learn a user's location information without integrating all the knowledge. So, compromising either party of the system does not disclose the privacy information.

The nodes in the system should be registered to the Certificate Authority (shows in following figure, prover node's registration) for joining in system. Mobile node i with a set of M public and private key pairs. After registration to the CA. K_i^{Pub} serve as the pseudonyms of node i and K_i^{prv} enable node i for digitally sign the messages.When prover node P wants to collect location proofs at particular time t, then it broadcast the location proof request for location proofs to neighboring nodes within its bluetooth range. All mobile node uses multiple pseudonyms for different communication.

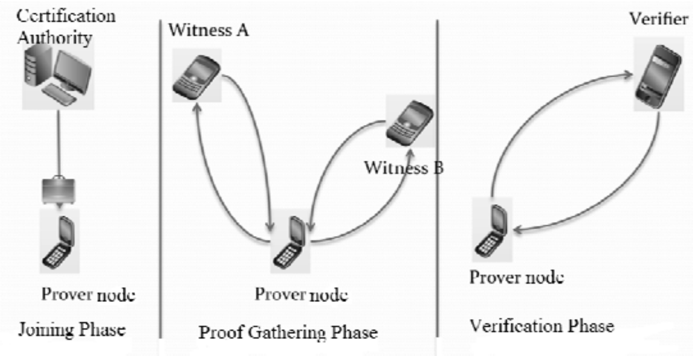


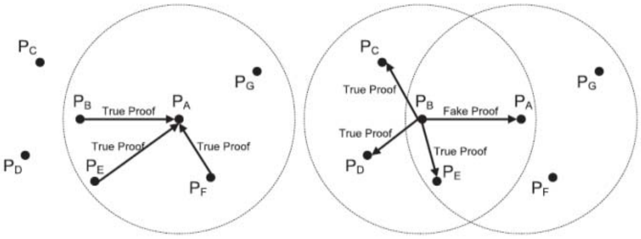
Fig 2. Registration,Gathering,verification procedures

The broadcast request contains the node P's current pseudonym and random number for particular session. Mobile nodes in range of prover will decide whether to accept the location proof request or not, according to the privacy metric. As each neighboring node will have different privacy levels according to spatial and temporal region. Once the request gets accepted, it creates the location proof for both the nodes and provides the biometric data to the prover. The location proof and biometric data is received by the prover and it is responsible for delivering it to the location proof biometric server. The packet contains the prover's current pseudonym and random number for that particular session and the location proof with biometric data which is signed and hashed by the mobile nodes and it is again encrypted by respective server's public key. So, eavesdropping of communication and altering the message is impossible for the attacker and also the prover node can't deny the location proof. The location proofs are stored with pseudonym so the server doesn't know the real identity of the location. The location proof server determines the hash of each location for hiding it from certification authority.

For location proof of any node for verification purpose, an authorized verifier can request to Certification Authority along with real identity and time interval. On location request to prover from verifier, the real identity and its location is known to the verifier in prover's claim. The certification authority first carry out authentication of the verifier, followed by converting the real identity to its corresponding pseudonym within a specific time interval and collects its hashed location proof from location proof biometric server. It will also verify the identity of mobile node by checking the data in the location proof biometric server at that requested time interval. As prover stores its biometric encrypted data to certification authority and then it performs the matching between the sample in the biometric server with it. If both the identities match, the authentication and location proof are valid. Hashed location is returned instead of original location, from location proof server to the Certificate Authority. And then certification authority sends this location to the verifier. For determining claimed location is authentic, the verifier equates the hashed location with claimed location accessed from the prover. And at last prover gets verified as legitimate node or not.

IV. Implementation Details

We implemented our An Efficient Approach to a Location Proof Updating and Privacy Preserving system in java. By using Java(TM) platform, Micro Edition Software Development Kit 3.0, as it is a state of the art toolbox for developing mobile applications. Also we use Connector flow Net Beans IDE 7.2.1 as the Net Beans IDE is an integrated development environment available for Windows for mobile applications using the Java platform. So we use it for creating web applications such as verifier and certification authority and also java applications such as Encryption, Decryption and Hashing. In addition to it, we used biometric encryption algorithms for the biometric data and also used RSA for digital signatures because it has faster verification speed. We also done threshold (threshold value taken as0.5) based verification for colluding attacks and countermeasures as shown in following figure.



(a) Normal case (b) Colluding case

Fig 3. Threshold based verification.

In Threshold based verification, in first case (Fig. 3a), prover node PA request for location proof to nodes (PB,PE,PF and PG). Trust level of node PA can be calculated as how many node accept location proof among all neighboring nodes. So, trust level of node PA=N proof /N neighbors=3/4=0.75, which is greater than predefined threshold (which is 0.5) so, all nodes should be considered as legitimate nodes. In other case, (Fig.3b) PA tries to claim its location in class 1 with his colluders although he is not in class 1. PB is PA's colluder and witness. So Trust level of PA =1/4 = 0.25, which is less than predefined threshold value so, PA is detected as malicious.

V. Result Evaluations

TABLE I
Comparison with the Previous System

No.	Comparison with the Previous System		
	Features	APPLAUS	AEALPUP2S
1.	Identity Privacy	Yes	Yes
2.	Location privacy	Yes	Yes
3.	Separation of privacy knowledge	Yes	Yes
4.	Biomertic proofs	No	Yes
5.	Authentication	No	Yes

Above table shows that our proposed system AEALPUP2S is having somewhat same features; in addition to it Biometric Authentication is also achieved in our system, so as to increase privacy and authentication as compared with existing system APPLAUS.

The following graph shows Threshold based verification means value 1 states legitimate node and 0 states malicious node.

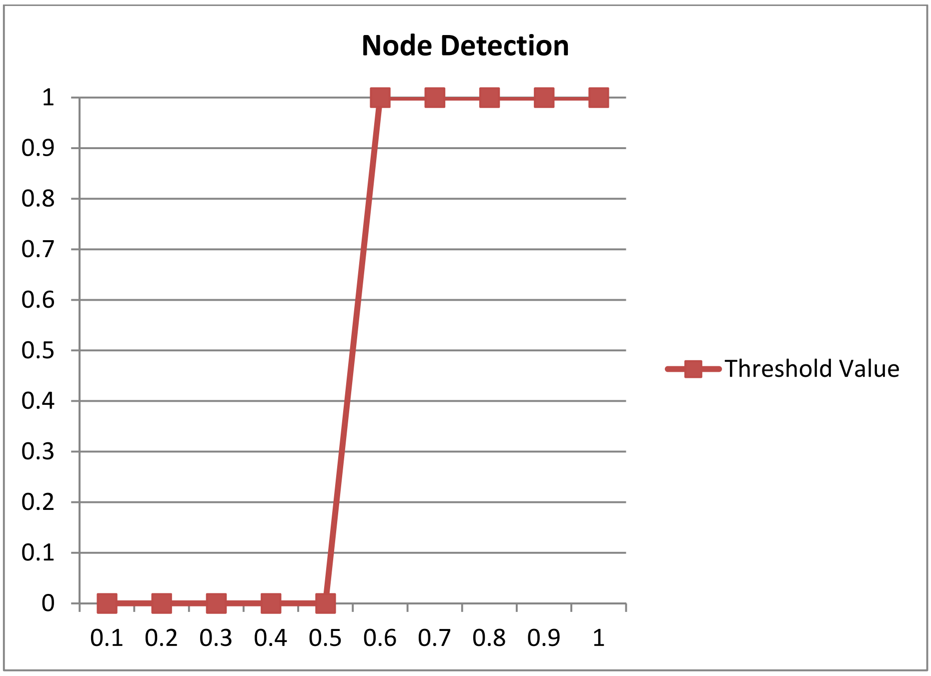


Fig 4. Graph calculated on trust level

VI. Conclusion

This paper presents a new location proof updating system, with authentication technique. The existing system APPLAUS lacks device authentication and this is rectified by using our AEALPUP2S system by updating biometric information along with location proof. As authentication is necessary for mobile devices for update location proof for the specific person. Significantly, our solution further improves user privacy protection by satisfying the main objectives of preserving privacy towards location proof and authenticating the device owner.

The experimental results indicate that our method can increase privacy and authentication remarkably. We plan to extend the proposed solutions to support future mobile devices having biometric data exchange, which can be usual in future, with the rapid change of technology. So, our approach will be used in real time environment also experiments the corresponding performance of our mechanisms in future life.

Acknowledgement

I am thankful to my guide and HOD of computer dept. Prof. Ratnaraj Kumar sir for his suggestions, valuable guidance, comments, support for preparing this paper.

References

1. H. Kido, Y. Yanagisawa, and T. Satoh. An anonymous communication technique using dummies for locationbased services. In Proc. of IEEE Int’l Conf. on Pervasive Services (ICPS2005), 2005.
2. A. R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing, January 2003.
3. B. Waters and E. Felten. Secure, Private Proofs of Location. Technical Report TR-667-03, Department of Computer Science, Princeton University, January 2003.
4. S. Saroiu and A. Wolman. Enabling New Mobile Applications with Location Proofs. In Proc. HotMobile 2009.
5. M. S. Kirkpatrick and E. Bertino. Enforcing Spatial Constraints for Mobile RBAC Systems. In Proc. SACMAT 2010.
6. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi.Location-based Trust for Mobile User-generated Content:Applications, Challenges and Implementations. In Proc.HotMobile '08.
7. S. Capkun and J.P. Hubaux, “Secure Positioning of Wireless Devices with Application to Sensor Networks,” Proc. IEEE INFOCOM, 2005.
8. Y. Li and J. Ren, “Source-Location Privacy Through Dynamic Routing in Wireless Sensor Networks,” Proc.IEEE INFOCOM, 2010.
9. Y. Zhang, W. Liu, and W. Lou, “Anonymous Communications in Mobile Ad Hoc Networks,” Proc.IEEE INFOCOM, 2005.
10. W. Luo and U. Hengartner. Proving your location without giving up your privacy. In ACM HotMobile, 2010.

11. Ann Cavoukian, “The Relevance of Untraceable Biometricsand Biometric Encryption”, Wiley publishers.

12. Efficient Detection of Sybil Attack based on CryptographyinVANET, International Journal of Network Security and Its Applicarions, Nov 2011

13. Towards Privacy Preserving and Collusion Resistance in a Location Proof Updating System Zhichao Zhu, Student Member, IEEE, and Guohong Cao, Fellow, IEEE Transactions on Mobile Computing, Vol. 12, no. 1, January 2013

14. Pranali Pise and Prof. Ratnaraj Kumar ,Pune University, India “A Review on Privacy Preserving in Location Proof System”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.

15. Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci. A social network based patching scheme for worm containment in cellular networks. IEEE INFOCOM 2009

16. T. Xu and Y. Cai. Feeling-based location privacy protection for locationbased services. In ACM CCS, 2009.

17. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao. Towards event source unobservability with minimum network traffic in sensor networks.In ACM WiSec, 2008

18. T. Xu and Y. Cai. Exploring historical location data for anonymity preservation in location-based services. In IEEE INFOCOM, 2008

19. M. Shao, Y. Yang, S. Zhu, and G. Cao. Towards statistically strong source anonymity for sensor networks. In IEEE INFOCOM, 2008.