An Approach to Authenticate user's Mobile device and to Preserve Privacy towards Location Proof(A2MP2LP)

[1]Senthilguru S, [2]Blessed Prince P

[1]Post Graduate Scholar
Department of Information Technology, Karunya University
Coimbatore, Tamilnadu-641114, India

[2]Assistant Professor (SG),
Department of Information Technology, Karunya University
Coimbatore, Tamilnadu-641114, India

Abstract

The purpose of this approach is to authenticate user's mobile device and to preserve privacy towards location proof.A person's location proof depends on the user's mobile device position. Biometric authentication technique was proposed in order to avoid malicious users from prevaricating their identity. The location proofs are generated by co-located Bluetooth enabled mobile devices. The working of our proposed system is similar to Privacy-Preserving Location proof Updating System (APPLAUS) [14]. To prevent the weak identity of mobile device, the technique of biometric authentication was deployed. 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 the data, which can expose the location of legitimate devices. Hence the major necessity is to preserve the privacy of each device by using multiple pseudonyms. Therefore to maintain security and privacy the proposed system's (A2MP2LP) architecture separates the sensitive biometric data from the history of the device location. For extra security the biometric information is stored in biometric encryption (BE) format. A2MP2LP explains the biometric authetication and perserving privacy towards location proof method.

Keywords: *Location privacy, location proof, Biometric authentication, Mobile networks,biometric encryption.*

1. Introduction

Mobile Networks does not maintain infrastructure and insecure due to its broadcasting nature. In MANET, at any time and at any location mobile nodes can join and leave the network [16]. The mobile device is used to find the location of the person. Location proof is document that certifies the location of the person at particular time in the geographical area. By using Location proof, mobile device provide services about nearest entities (i.e. Nearby ATM, Restaurants, airports, etc.,). Location sensitive applications are based on location proof generated by the user's mobile device. Location sensitive applications includes [10][11] Location based access control, Location aware routing, etc., Location proof updating system helpful in providing a history of location proofs and identifying a geographical location of users. To obtain the location privacy mobile nodes are anticipated to satisfy some or all of the basic properties given below: [12]

Location privacy: It's defined as the facility to prevent other parties from acquisition one's current or past location.

Identity privacy: It's defined as the ability to hide the identity of the mobile node by using pseudonym. So that the real identity of the user can't be traced by the malicious node.

Un linkability: No unauthorized entity (adversary) should be able to relate subsequent sessions of the mobile node.

Biometric authentication: It is defined as an identification of the person by using their physiological and behavioral characteristics. Biometric identification is required to identify the mobile device used to generate location proof at particular time for the specified person [17].

Biometric encryption (BE): It's defined as the untraceable biometric because the biometric data provided by the user can't be reversible. Neither the key nor the biometric can be retrieved from the stored template because BE bind securely the cryptographic key to the biometric. Only a legitimate person can re-create key only if the accurate biometric sample is presented on verification [17]. The attackers can be classified according to the scope; nature and behavior of attacks are follows: [13].

Table 1: Different types of attackers

Passive attacker	Participate eavesdropping message in communication

Active attacker	Prevent the packets to be delivered to the destination
Inside attacker	Authenticate member of the group
Outside attacker	Intruders
Local attacker	To the limited radio range, but many local attackers join to perform attacks over the network
Malicious attacker	They didn't get any benefit on attacking

2. Related Work

Beresford and Stajano [1] proposed a framework to frequently change a user's identity through pseudonyms. Kido [2] proposed a technique by generating a dummy location data and mixing them with real location data, so that it becomes difficult for the Location Based Service providers to differentiate them. In the method proposed by Waters and Felten [3] a device is allowed to obtain location proofs from a location manager (LM) and submit the proofs to a verifier.

Kirkpatrick and Bertino [4] have dedicated location devices (LDs) issue location proofs based on Near-Field Communication where this sytem provides pseudonimity alone. Saroiu andWolman [5] also have APs issue location proofs but it reveals the user's identity and also has no means to detect cheats.

Lenders et al. [6] describe a geotagging service that allows a content creator to obtain a location/time certificate for the content but it does not bind the content to its generator. A challenge-response scheme is proposed by Capkun and Hubax [7] which use multiple receivers to estimate a wireless node location accurately using RF propagation characteristics. Through dynamic routing or anonymous authentication, Li and Ren [8] and Zhang et al. [9] tried to provide source location privacy against traffic analysis attacks.

3. Architecture

Using Bluetooth interface mobile nodes communicate with neighboring nodes, and cellular network interface is communication medium for untrusted location proof server and biometric server.

Depending on roles they are categorized as Prover, Witness, Location Proof Server, Biometric Server, Certificate Authority or verifier

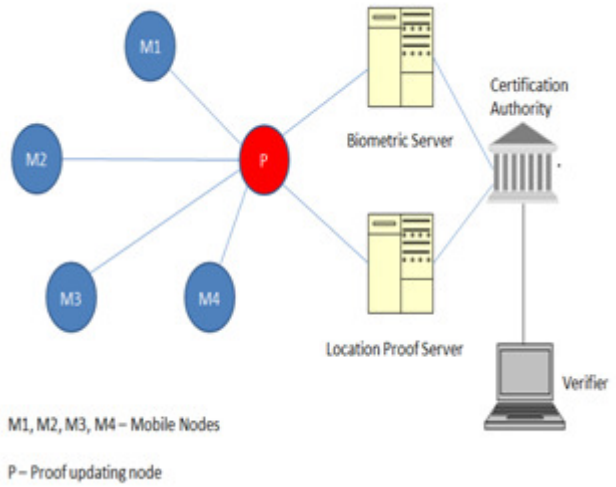

Fig1. Architecture of A2MP2LP

3.1 Proof updating node

Node P is responsible for obtain location proofs from its neighboring nodes. The node P broadcast the location proof request to the neighboring nodes at time t through Bluetooth.

3.2 Mobile node

An adjacent node agrees to provide location proof for the node P. The nodes which agree to share the location proof and biometric identification are collected by node P and send it to location proof server & biometric server respectively.

3.3 Location proof server

As our goal is to monitor real-time locations and also to retrieve history of location proof information whenever it is needed, a location proof server is essential for storing the historical records of the location proofs. It communicates directly with the node P who submits their location proofs to the location proof server. The location proofs from the nodes (M1, M2, M3, and M4) are stored as pseudonyms, even if the server is compromised; the adversary is unable to track the location of the particular node at the particular time.

3.4 Biometric server

Node P communicates straight to the biometric server and submits the biometric data and the current time. The biometric data from the nodes (M1, M2, M3, and M4) are stored as biometric encryption format, even if the server is

compromised adversary is unable to identify the identity of the particular node.

3.5 Certificate authority

It is commonly used term in the most of the networks, here we consider as online CA which is maintained by an independent trusted third party. The mobile nodes which are registered with the CA pre-load a pair of public/private key before entering into the registered network. Real identity and pseudonyms are mapped by CA, which works as a bridge between the location proof server and the verifier. CA retrieve location proof, biometric data from the location proof server, biometric server respectively and it forwards to the verifier.

3.6 Verifier

A third-party agent which is authorizes to verify a mobile nodes (M1, M2, M3 and M4) location, within a particular time period. The verifier must be close relationship with the node P, e.g., friends or colleagues, to be trusted for gaining authorization.

4. Protocol

If node P wants to collect location proofs at particular time t, by using Bluetooth location proofs are collected from the neighboring nodes within its range. Mobile node uses multiple pseudonyms for different communication.

1. The node P broadcasts a location proof request through Bluetooth, according to its update scheduling to its neighboring nodes. The broadcast request contain the node P's current pseudonym, and random number for that session.

2. Mobile nodes in range of the node P will decide whether to accept the location proof request according to the privacy metric. That is each node will have different privacy levels according to the spatial and temporal region. Once the request is accepted then it creates the location proof for the both nodes and provides the biometric data in form of BE to the node P.

3. The location proof and biometric data is received by the node P and its responsible to deliver the location proof and biometric data to the suitable server respectively. The packet contains the Node P's pseudonym and random number. The location proof is signed and hashed by the mobile nodes (M1, M2, M3..,) and it's encrypted by respective server's public key. So eavesdropping communication and altering the message is not possible for attacker and also the node P can't delay the location proof.

4. For location proofs of a particular node an authorized verifier can request to the Certification Authority (CA) along with the real identity and a time interval. The certificate authority performs authentication of the verifier in the first step followed by the conversion to corresponding pseudonym from its real identity within a specific time interval and collects its location proof from the location proof server. It will also verify the identity of the mobile node by checking the data in the biometric server at that requested time interval. If both the identities match, the authentication and location proof are valid. Certificate Authority will gather queries from k different mobile nodes and send them out at a time rather than satisfy the request of a single node, in order to preserve the relation among pseudonym and location server.

5. Hashed location is returned instead of original location by the location proof server to the Certificate Authority and the Certificate Authority sends this location to the verifier. For determining whether the claimed location is authentic, the verifier equates the hashed location with the claimed location accessed from the prover. Prover sends it biometric encrypted data to CA and it performs the matching between the sample in the biometric server at a particular time the location proof server determines the hash of each location and it identifies the person's identity.

5. Simulation Result

NS2 is discrete-event network simulator, primarily used in research. The objective of the ns-2 project is to make an open simulation environment for networking research that will be preferred inside the research community.

Table 2. Simulation Parameters

Simulation Area	500m X 500m
Simulation Time	500 sec
Routing Protocols	Aodv
Number of Nodes	50
Node placement	Random
Mobility Models	Random Walk and Random Waypoint
Interface	Bluetooth(BNEP)

Power consumption is calculated based on the amount of energy consumed by the nodes during each status.

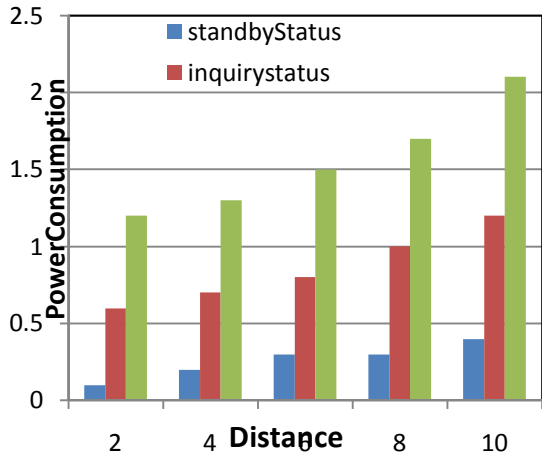

Fig. 2 Power consumption graph for different Bluetooth status

Power consumption can be defined as the total amount of power needed for the communication between the nodes. Bluetooth has mainly 3 states: proof exchange status, inquiry status and standby status. Standby status receives the incoming signals without responding to them. They have the least power consumption when compared to the other two. Inquiry status sends the location proof requests for the neighboring nodes. Proof exchange status responds to the location proof updating requests. This has the highest power consumption with the inquiry status having moderate power consumption. The graph plotted here has the distance in the x-axis and power consumption in the y-axis. Power is measured in milli watts (mW) and the distance is measured in meters.

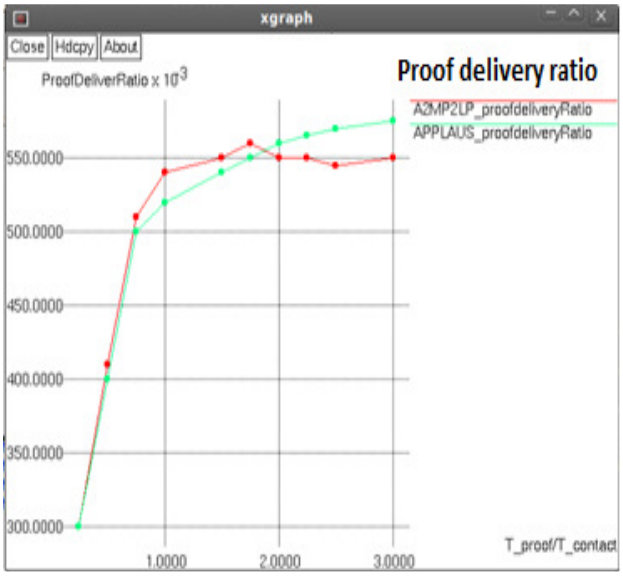

Fig 3. Proof delivery ratio

The percentage of location proof message that is successfully uploaded to the location proof server is termed as the proof delivery ratio. The required interval between two location proof updates is T-proof and T-contact in the mean value of the real node contact interval. Y-axis has the proof delivery ratio and X-axis is marked with T-proof/T-contact. By analyzing the graph, the proof delivery ratio is more or less similar even though in the proposed work the device biometric authentication is an added feature.

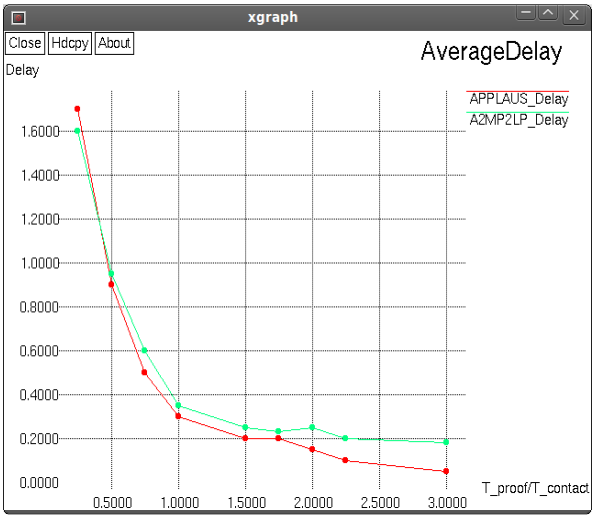

Fig 4. Average delay

There is always a time delay between the time when a location proof update is needed and when the location proof message has reached the location proof server. This time difference is coined as average delay. Y-axis consist of the delay and X-axis is marked with T-proof/T-contact. By analyzing the graph, the average delay is same as the APPLAUS.

5.1 Privacy Vs biometric device Authentication

Device authentication is needed to provide user identity. The biometric information and location information of the mobile device users are stored in two different servers in order to prevent single point failure. Thus both the privacy and authentication are achieved.

6. Conclusion

In location proof updating system, authentication is necessary because mobile devices are used to update location proof for the specific person. Location privacy to device can be achieved by using multiple pseudonyms for the communication and location proof updating purpose. APPLAUS protocol is developed to protect against

location privacy from both outsider and insider attacks using cryptographic encryption scheme. But the APPLAUS lacks device authentication and this is rectified by using **A2MP2LP** protocol for updating biometric information along with location proof. **A2MP2LP** satisfy the main objectives of preserving privacy towards location proof and authenticating the device owner.

References

[1] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing, 2:46–55, January 2003.
[2] H. Kido, Y. Yanagisawa, and T. Satoh. An anonymous communication technique using dummies for location-based services. In Proc. of IEEE Int'l Conf. on Pervasive Services (ICPS2005), 2005.
[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] M. S. Kirkpatrick and E. Bertino. Enforcing Spatial Constraints for Mobile RBAC Systems. In Proc. SACMAT 2010, pages 99-108.
[5] S. Saroiu and A. Wolman. Enabling New Mobile Applications with Location Proofs. In Proc. HotMobile '09, pages 1-6.
[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, pages 60-64.
[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] Emmanouil Magkos, Cryptographic Approaches forPrivacy Preservation in Location-Based Services
[12] S. Saroiu and A. Wolman. Enabling new mobile applications with location proofs. In ACM HotMobile, 2009.
[13] Efficient Detection of Sybil Attack based on CryptographyinVANET, International Journal of Network Security & Its Applicarions, Nov 2011
[14] Z. Zhu and G. Cao. Applaus: A privacy-preserving and collusion resistance in location proof updating system IEEE INFOCOM 2011
[15] Yu Wang and Dingbang Xu. L2P2: Location-aware Location Privacy Protection for Location-based Services, INFOCOM, 2012 Proceedings IEEE
[16] Senthilguru and Blessed prince. A survey on preserving privacy towards location proof, IJARCET vol 2, no2, 2012
[17] Ann Cavoukian, The Relevance of Untraceable Biometricsand Biometric Encryption, Wiley publishers.

Authors

Senthilguru S has done Btech in Information Technology from Karunya University 2011 and is now doing his final year Mtech in Network and Internet Engineering from Karunya University, Coimbatore. The main areas of interest include Privacy towards location proof in MANETs, cloud computing

Blessed prince p is currently working as Assistant Professor in Karunya University, Coimbatore. He had completed her M.E. He has area of interest in pervasive computing. He is life time member of CSI and ISTE.