Designing Secure Architecture for Preserving Privacy in MANET Mobile Sensing

Miss. Snehal G. Sarode **Dr. V.M.Thakre**

Abstract **:- Fourth-generation wireless networks may require an integration of mobile ad hoc networks (MANET) into external network to enhance the flexibility of the communication and roaming. This phenomenon is well-suited for commercial and military applications which yield additional benefit of roaming. However, integration of MANET with external network iposes a serious security challenge for communication because of open and distributed nature of the ad hoc network. In this paper, a secure privacy preserving architecture has been proposed to provide privacy and security for data communication in wireless mobile ad hoc networks. This architecture includes the concept of observer obscurity to provide privacy and security for the genuine nodes and to exclude misbehaving nodes in the network. The proposed architecture is designed based on the k-times anonymous authentication and onion routing - a cryptography concept which supports for anonymous communication.**

Keywords **: Location privacy, Mobile Ad Hoc Networks.**

I. INTRODUCTION

Recent extensive media reports about Google and Apple's smart phones (i.e., Android phones and iPhones) being able to store and gather users' location data have attracted national attention. The privacy concerns from mobile users on location data have significant impact on usage and development of location based service applications and systems. Location based service (LBS) is a type of service where the information is provided based on a mobile user's geographical location. L*ocation privacy* is "the ability to prevent other parties from learning one's current or past location." Therefore, addressing a user's *diverse* and *dynamic* privacy requirements which may depend on his location would be necessary for location privacy protection.

A number of localization and ranging techniques for wireless networks enables networking functions (i.e., position-based routing) to enable location related applications (e.g., access control, data harvesting). The mechanisms rely on GPS, high speed hardware, directional antennas, robust statistics or spread spectrum techniques using spreading codes[1]. Location privacy has been a serious concern for mobile users who use location-based services provided by the third party provider via mobile networks[2]. Recently, there have been tremendous efforts on developing new anonymity or obfuscation techniques to protect location privacy of mobile users.

II. BACKGROUND

Researchers have proposed a number of localization and ranging techniques for wireless networks [1].An efficient implementation of the protocols remains a challenge, however, since almost all of them rely on ToA ranging and generally assume fast processing hardware at the prover (except in the case of ultra sound implementations, which are limited in range)[2]. The method equally well using any kind of ranging, even low-cost RSSI based methods [3]. The approach to secure localization relies on a set of covert base stations. Covert base stations can be realized by hiding or disguising static base station or by the random motion of mobile base stations[4].

Location privacy has been a serious concern for mobile users who use location-based services provided by the third party provider via mobile networks. Recently, there have been tremendous efforts on developing new anonymity or obfuscation techniques to protect location privacy of mobile users..According to [5], the strategies in protecting location privacy can be divided into four categories:
Regulatory approaches,Privacy policy based approaches,Anonymity based approaches, Obfuscation based approaches

A new distance bounding protocol[6] is proposed based on ultrasound and radio wireless communication where proposal to make use of multiple base stations to narrow down the area in which the nodes lie is described. In [7], the authors propose a mechanism called "packet leashes" that aims at preventing wormhole attacks by making use of the geographic location of the nodes (geographic leashes), or of the transmission time of the packet between the nodes (temporal leashes).

The remainder of this paper is organized as follows: In section III, we present the previous work done. Section IV discusses the existing methodologies and section V discusses the analysis. The proposed methodology is explained in Section VI. The outcomes and results are discussed in Section VII. The conclusion and future work are given in section VIII and Section IX respectively.

III. PREVIOUS WORK DONE

A distance bounding protocol is proposed that can be used to verify the proximity of two devices connected by a wired link. A technique called verifiable multilateration [1] is proposed, based on distance-bounding, which enables a local infrastructure to verify locations of the nodes. It is further shown that technique can be extended for secure localization of a network of sensors.

To protect location privacy, many approaches have been proposed [2]. To measure the location privacy, two

metrics, where one is based on entropy and the other is based on anonymity set s, are also proposed [3]. Another approach is the aforementioned approach [4] where a user's location will be reported as a two-dimensional spatial cloaking area where at least $k-1$ other users are also in the same area[5].

Location-sensitive applications[6] require users to prove that they really are (or were) at the claimed 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 [7] is to build a trusted computing module on each mobile device to make sure trusted GPS data is generated and transmitted. Although cellular service providers have tracking services that can help verify the locations of mobile users in real time, the accuracy is not good enough and the location history cannot be verified. For example, a solution[8] is proposed which is suitable for third-party attestation, but it relies on PKI and the wide deployment of WiFi infrastructure.

In the last decade, a number of indoor localization systems [9] were proposed, based notably on infrared ,ultrasound, received radio signal strength and time-of-flight radio signal propagation techniques. These localization techniques were then extended and used for localization in sensor and ad hoc networks Recently, a number of secure distance and location verification have been proposed.

IV. EXISTING METHODOLOGIES

1.Secure localization in sensor networks with mobile base stations

In this method rely on mobile base stations[1]. It is shown how mobile base stations can be used to secure localization and to verify the locations of sensor nodes. It is assumed that the sensors compute their locations through one of the non-secure localization algorithms.The authority has a number of mobile base stations (similar to data mules), that know securely their locations (e.g., through secure GPS). These mobile base stations can be single-purpose or multi-purpose, and therefore can be used for only position verification or also for data collection and other tasks. The mobile base stations share a secret key with each sensor. The protocol relied on the assumption that the covert base station is hidden, whereas all communication between the node and the localization infrastructure is performed through the public base station. Here, position verification is performed through mobile base stations.

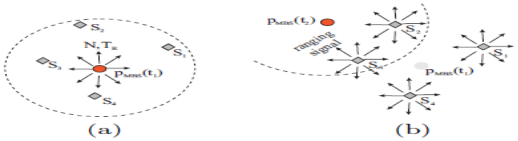

Fig 1: Position verification in sensor networks

2. The Location Proof Updating System

The location proof updating architecture[2] and how mobile nodes schedule their location proof updating to achieve location privacy in APPLAUS is introduced. 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 categorized as Prover, Witness, Location Proof Server, Certificate Authority or Verifier.

The architecture and message flow of APPLAUS is shown in Fig

.

- Prover: 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: As the goal is not only to monitor real-time locations, but also to retrieve history location proof information when needed, a location proof server is necessary for storing the history records of the 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.

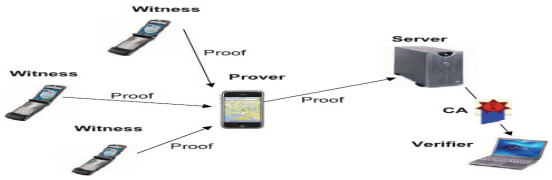

Fig. 2.Location proof updating architecture and message flow.

When a prover needs to collect location proofs at time t, it executes the protocol in Fig. 3 to obtain location proofs from the neighboring nodes within its Bluetooth communication range. Each node uses its M pseudonyms PM as its identity throughout the communication.

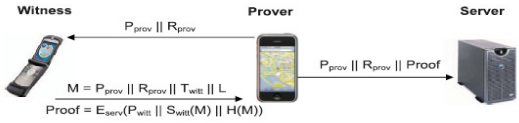

Fig 3: Location proof updating protocol

3. LBS Model

A general model is assumed for location-based services[3] where there are three critical components:mobile users, trusted location anonymization server, and location based service providers. See Fig. for illustration.

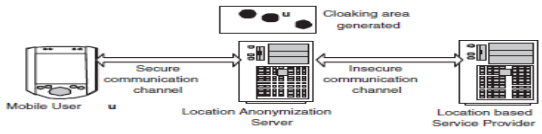

Fig 4: LBS model

In this model, a mobile user uisends a location based service request to the trusted anonymization server, which includes location data (x, y), timestamp information t, as well as privacy requirement r. Hereafter, (ui, x, y, t, r) are used to represent such request. During this step, user authentication and message encryption can be performed to provide security protection. After the anonymization server gets the request message, it will perform location anonymization (generating a clocking area $c$which covers the user's location (x, y)) to provide location privacy protection, then the anonymized location information (the cloaking area c) will be sent to the location based service providers for the services. In this model, location privacy of a mobile user refers to his exact location.

V. ANALYSIS AND DISCUSSION

Node localization does not require communication from the base stations to the mobile nodes: the base stations locate mobile nodes measuring signal reception times at each base station. This is why method ofSecure localization in sensor networks with mobile base stations [1] is well suited for secure localization with hidden base stations. But In the proposed protocol, node location privacy is not preserved. However, this protocol can be enhanced to include public base station authentication which prevents an attacker from challenging the node and from requesting from it to send localization signals disclosing its location. Other attacks are possible on node's location privacy.

APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks. Location proof updating system reduces the accuracy of location information along spatial and/or temporal dimensions. It also has the property of pseudonym unlinkability and statistically strong source location unobservability. Also the robustness of APPLAUS such as defending against traffic analysis and statistical testis evaluated[2].

For the location proof and location privacy the threat of colluding attack is still an open issue. For example, when a dishonest node C1 from San Francisco needs to prove herself in New York City (NYC), she can have another colluding node C2 to generate bogus location proofs for her, with location tag of New York City. Generally speaking, such attacks can be identified by looking into the location traces and examining the interactions between colluders as well as the time and location consistency along the moving trajectory[2].

An optimization problem is formalized for cloaking area generation, called L2P2 problem, which aims to find the cloaking areas with minimum sizes such that diverse privacy requirements are still satisfied [3]. When more LBS requests are involved, the computation of common user sets are affected by more cloaking areas. Other services, such as, people tracking and social networking, need both the identity of the user as well as his exact location. This problem is discussed and the solution is given in the proposed methodology.

VI. PROPOSED METHODOLOGY

The secure privacy-preserving architecture in wireless mobile ad hoc networks is designed to provide security and privacy for the nodes either in ad hoc networks or in the internet during data communication. There are three entities, i.e. the mobile nodes in ad hoc network, mobile gateway and regular nodes in the fixed network. The system model for the proposed architecture is depicted in Figure

Fig 5: System Architecture

The proposed method contains the following modules:

1. Configuration module

The configuration module has two faces such as the initial setup and the user registration. During the initial setup phase, the MG generates agroup key (public/secret key pair) and sends announcement with group public key during gateway advertisement.

2.Watchdog module: The main function of the watchdog module is to overhear the packet transmission and collect usefulinformation about network behaviors, such as packetforwarding, dropping and tampering

3. Decision making module: This section describes the process of estimating thetrust, judging the reputation and how the mobilenodes are categorized as trusted/outlier and genuine/malicious.

4 Report module: Any user who identifies an outlier or malicious user in the network can act as an Observer and categorize him/her as a misbehaving user. Then the Observer can report to the other users in the network a maximum of one time per reason per misbehavior type.

VII. OUTCOMES AND RESULTS

A secure privacy preserving architecture will provide privacy and security for data communication in wireless mobile ad hoc networks. This architecture includes the concept of observer obscurity to provide privacy and security for the genuine nodes and to exclude misbehaving nodes in the network.

VIII. CONCLUSION

The proposed architecture addresses the privacy and security issues in mobile ad hoc networks when it is integrated with the

fixed network to access the internet. The architecture adapts the modules such as watchdog, trust estimation and reputation in order to monitor and determine the mobile nodes trust and reputation. Based on these factors,an observer decides the node state and reports to the other users in the network if it is a misbehaving node (outlier or malicious). The proposed architecture has its own importance inmobile ad hoc networks in the integrated environment.

IX. FUTURE SCOPE

The proposed architecture is suitable for a constrained number of mobile nodes. If the number of mobile nodes exceeds the threshold in a network, then the mobile node energy consumption is comparatively high. So, the scalability factor needs to be considered in addition with existing concepts in the future.

REFERENCES

1. SrdjanCapkun, Kasper Bonne Rasmussen, Mario Cagalj, Mani Srivastav,"*SecureLocation Verification With Hidden and Mobile Base Stations"*, IEEE Transaction on Mobile Communications, Vol 7,Issue 4,PP 1-14, April 2008.
2. Yu Wang,DingbangXu, Xiao He, Chao Zhang,,Fan Li, Bin Xu,"*L2P2: Location-aware Location Privacy Protection for Location-based Services"*,INFOCOM, 2012 Proceedings IEEE, 978-1-4673-0775-8/12, pp.1996,2004,March 2012
3. Zhichao Zhu, Student Member, IEEE, and GuohongCao,"*Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System*",IEEE TRANSACTIONS ON MOBILE COMPUTING,VOL. 12, NO. 1, pp 51-64,January 2013
4. J Qaddour, R Barbour, *Evolution to 4G wireless: problems, solutions, and challenges* (Paper presented in the 3rd ACS/IEEE international conference on computer systems and applications, Cairo, Egypt, 2005), pp. 78–I
5. D Axiotis, T Al-Gizawi, K Peppas, E Protonotarios, F Lazarakis, C Papadias, P Philippopoulos, *Services in interworking 3G and WLAN environments.* IEEE WirelCommun. 11(5), 14–20 (2004)
6. M Lott, M Siebert, S Bonjour, D von Hugo, M Weckerle, *Interworking of WLAN and 3G systems.* IEE Proc Comm. 151(5), 507–513 (2004)
7. N Komninos, DD Vergados, C Douligeris, *A two-step authentication framework for mobile ad hoc networks.* China Commun J. 4(1), 28–39 (2007)
8. K El Defrawy, G Tsudik, *Privacy-preserving location-based on-demand routing in MANETs*. IEEE J Sel Area Comm. 29(10), 1926–1934 (2011)
9. A Loay, K Ashfaq, G Mohsen, *A survey of secure mobile ad hoc routing protocols*. IEEE CommunSurv Tutorials. 10(4), 78–93 (2008)
10. P Jianli, P Subharthi, J Raj, *A survey of the research on future internet architectures.* IEEE Commun Mag. 49(7), 26–36 (2011)

AUTHOR'S PROFILE

Dr. V.M. Thakare was born in Wani, Maharashtra in 1962. He was worked as Assistant Professor for 12 Years at Professor Ram Meghe Institute of Technology & Research, Badnera and P.G.Department of Computer Science, S.G.B. Amravati University, Amravati. Currently he is working as Professor & Head in Computer Science from last 9 years, Faculty of Engineering & Technology, Post Graduate Department of Computer Science, SGB Amravati University, Amravati. He has published 110 papers in various National & International Conferences & 30 papers in various International journals. He is working on various bodies of Universities as a chairman & members. He has guided around 400 more students at M.E / MTech, MCA M.S &M.Phil level. He is a research guide for Ph.D. at S.G.B. Amravati University, Amravati. His interest of research is in Computer Architecture, Artificial Intelligence and Robotics, Database and Data warehousing & mining