ISSN:0975-9646

A Survey on Privacy Preserving in Roaming Network

Kousalya.K[#1], Anitha.P ME[*2], Gowri.K[#3]

[#] *PG scholar Dept of CSE, Angel College Of Engineering And Technology, Tiruppur, Tamilnadu, India*
[*] *Assistant Professor, Angel College Of Engineering And Technology, Tiruppur, Tamilnadu, India*

Abstract -Wireless network is one of the important criteria for the roaming users while they travel across the networks. With the improvement of mobile technologies people often require privacy and security in roaming networks. Security and privacy preserving is vital one to transfer the data through network between two servers i.e. Home Server and Foreign Servers. In network, security and privacy problem in roaming network is because of limited number of bandwidth. User may travel across the network and want to protect the data like user ID, location information and secure data from one to other networks. This survey studies the existing approach of various roaming protocol to provide better security under roaming networks.

Keywords: ***Wireless technology, Mobile network, Roaming users, Data Privacy and Roaming Protocols.***

I. INTRODUCTION

With the tremendous growth of users in Wireless Technologies (WT), network size also increased. Providing security and privacy to these WT in network is most important factor. The most wireless technology here used is Mobile Technology (MT). Mobile technology is one of the progress factors on behalf of the people. People frequently require anonymity when they roam among the visited networks for their data. While roaming, preventing the resources from anonymous in network is a great issue and also identifying the anonymous in network after their attack requires more communication and computational cost, in recent computational capacity is limited under mobile terminology. To ensure connectivity for users roaming from one network to another, possibly provide roaming services in a secure and private manner [1].

Roaming service has to allow the MT users to use the WT services even when they take moves from one network to another i.e. home to foreign network. MT users may roam in different networks. Roaming service involves home server, foreign server and the MT user. MT users, who travel across different networks and access the home and foreign servers when their moves. For a harmless roaming service foreign server has to authenticate the user from the home server without knowing the data of the user. Foreign server just authenticate by only using the identity. Roaming services should be secure in location privacy, protect user data and provide strong user anonymity. This survey deals with the security and privacy of roaming networks.

They where many roaming protocols implemented for providing security and privacy like two-party, three-party protocols. In the two party protocols that do not access the home server (network). So we cannot trace the user. It has drawbacks in both the protocols it does not provide strong user anonymity and high computational cost. Three party protocols are implemented for accessing the home server. Currently three-party protocols focused for anonymous authentication [1, 2]. It requires open communication connection between home and foreign server (network). Open communication is not a possible one at every time without authentication process among them, hence home server may not be always online. In three-party it takes long time process in communication between them. For the privacy reason the above two protocol does not support well, other technique like roaming protocol based group signature with backward unlinkability [3] give a better security when compared to the above protocols. They were many approaches proposed to solve the privacy problem of mobile network they were showed in this survey.

II. LITERATURE REVIEW

Nowadays mobile technology and wireless network are interconnected together. Wireless transaction are done through Public atmosphere so no of attackers are increased. Limited no of bandwidth could not provide better security for the user due to the high communication and computational cost. Hence it is more disputes to propose security modules and protocols for defending wireless communication. We have reviewed and evaluated the security and privacy problem of existing research works and analyze the drawbacks of the many articles. This survey shows the existing proposed techniques and its varying.

Hyo Jin Jo et al, studied the existing three-party roaming protocol mechanisms and analyze the required assistance of the home servers, and also studied the two-party roaming protocols have weak security , weak anonymity, insecurity in the CK model, backward linkability, and leakage of the session key or inefficient operations. They were the problem in high authentication and revocation costs. Hence in two-party roaming protocols requires the revocation lists to revoke invalid users. A revocation list includes the revocation information associated with each Revoked User (RU). It uses group signature algorithms to authenticate users anonymously. However, these algorithms generally involve a high revocation cost, depending on the number of RU [2].

Preserving privacy under personal location is one of the greatest issues in wireless network. They where many approach proposed for the privacy preserving policy under personal location. In many research articles they

focus only on anonymization of location techniques but failed to preserve privacy under the network. Some privacy policy may cause data leakage problem because of inefficient algorithms. Many approaches were implemented, which failed to prevent the internal data misuse and privacy preserving policy [2].

Yan Sun, Thomas F. La Porta and Parviz Kermani proposed a Location-Based Services System (LBSs) for location sharing in social networks. LBS system is used to secure the privacy of the user locations. It secures a user identity and locality within basic mobile communication services. This paper focuses on following aspects: User should be control the access to location information at different levels of granularity and with different levels of user control, user has to define the group of entities that are allowed to access its location information and the main goal of location information is to provide intelligent services to the other users and servers. LBS support location privacy control by the user. It supports user control and scalability. It provides Instant Messaging service for server and clients [3].

Yan Sun et al approaches is based on offering members of the location information group keys (GKs) that enables them to decrypt the location information. For this GK management this paper proposes a Rebalancing algorithm to maintain rekeying performance with GK management. This article supports the free coupling through a network, thus permit third-party control. This paper provides a protocol like suitable key distribution, Multimedia Internet Keying (MIKEY), and Logical Key Hierarchy (LKH) protocol. These protocols are used to maintain hierarchical location information dissemination for flexible location privacy control for effective message delivery and group management complexity. Hence it does not support the multicast communication. And they were computational cost is also high. They were user anonymity problem from this approach [3].

Monitoring personal location under untrusted server may cause the privacy problem for the user in wireless sensor network. For this issue Chi-Yin Chow, Mohamed F. Mokbel, and Tian propose a preserving-privacy location monitoring system to provide better security to the user. Chi-Yin Chow et al propose a two in-network algorithm, which are *resource* and *quality-aware* algorithms used to protect the location information of the user [4]. Both these algorithms are well established in k-anonymity privacy model to indistinguishable among k person's aggregate locations. Each aggregate location is a cloaked area. This approach provides a high quality for monitoring services for the locations of system user. Hence this approach provides a high quality location monitoring. The resource-aware algorithm is one which is used to reduce communication and computational cost, while the quality-aware algorithm is used to reduce the size of cloaked areas in order to generate more accurate aggregate locations. Here they use spatial Histogram model to analyze the aggregate locations from sensor node to estimate the monitored objects. Hence this approach reduces the quality of monitoring services; it requires high quality services for larger areas and less privacy protection.

Chunlin Jiang , Weijia Jia and Ke Gu proposed a anonymous authentication protocol based on anonymous proxy signature for wireless communication systems. With the rising number of wireless network with numerous users requires anonymous authentication while roaming among different areas in different networks. Roaming user does not like to identify and tracker their own information to other user, they also want to secure their information while roaming from home network to foreign network [5].

Chunlin Jiang et al proposed five properties for strong anonymity they were (a*) Server Authentication*: a user is confident on their identity of the visited server. (b) *Subscription Validation*: Visited server validates the identity of the home server of the user. (c) *Key Establishment*: Random session key is established by the user and the visited server which the key is only known to them. In this case, the home server should not acquire the session key. (d) *User Anonymity*: By this anonymity no one can tell the identity of the user (e) *User Untraceability*: no one is able to identify any previous protocol runs which have the same user involved including the visited server [5]. So it is hard to tackle these issues because of limited computation and limited storages.

Karim El Defrawy, and Gene Tsudik approaches, in most network, communication is based on long term basic (addresses) for privacy conscious in Mobile Ad-Hoc Networks (MANET) is risky under tracking nodes by eavesdropping based on their identifiers by outsider and threat appear from malicious insiders, for this issues karim et al proposed on-demand (re-active) location-based anonymous routing protocol PRISM. Privacy-friendly Routing in Suspicious MANETs (PRISM) is primarily varying from all previous anonymous on-demand MANET routing protocols [6]. PRISM use location-centric for communication paradigm, it is used to ensure integrity of routing messages in preventing node tracking. In this case less information for short term means better privacy, for this method it uses an Adhoc On-demand Distance Vector (AODV). It is a distance-vector to hides the MANET topology. This approach achieves privacy and security beside both outsider and insider attacker. From karim et al there is inherent trade-off between privacy and session duration in location-centric mobile communication. It support only for short term addressing but failed in long term process, for this trade-off this paper proposed group-based Reference Point Group Mobility Model (RPGMM) [6].

Jiang et al. proposed an anonymous user authentication method using smart card for roaming service in global mobile networks [7]. This method guarantees the security preserve that are offered by the authors embrace. It contains three phases, i.e. registration phase, login and authentication phase and password update phase and shares a unique long-term key. This method use quadratic residue assumption for authentication scheme, which is very efficient. This method shows to be a very better candidate authentication protocol for approval in observe and in fact insecure against the stolen-verifier attack and cannot resist replay attack. It does not attain perfect forward secrecy. It fails to offer protection against a

strong repeat attack and also computation and communication cost is high, vulnerable to denial of service attack [7]. Most of the researchers have only concentrate on data transmission process and fails to provide privacy and security one. If it provides security means they were less no. of security for the transmission data.

III. PRIVACY AND SECURITY

Privacy protection is especially meaningful and challenging in such an environment. Privacy protection for the roaming user is one of the increasing factors for people that care about their privacy. A roaming user's privacy is like a movement model, extracting information, network usage habit, etc. should be protected from possible enemy intend to break users' privacy [8]. Protecting the privacy of the roaming user in wireless network have to solve the following problems have to protect the user identity, user data, user location information and user likability between the home and foreign server.

a. User Identity

Each user has a unique Identity (ID) for the transferring the information through wireless communication. It is maintained by the ID proxy server [9, 14]. It is an independent service provider this manages the service of the user using separate user ID. Communication device can directly communicate with the proxy server using HTTP protocol. It contains two components i.e. mobile device identification: it helps to check the original user by identifying their name, address, phone no and the home server ID. Then the second component is checking the accessing of the data to that mobile user. So only the users have secure data in wireless communication.

b.Data privacy

Data privacy protections aims privacy of the user data which is collected by a network and queries posted to a network to allot privacy to the user data [10]. Data privacy is under two scenario (i) External adversary and (ii) internal adversary. External adversary: protect the network eavesdrops communication and where in internal adversary protect the access to encryption keys of the two servers (i.e. Home & Foreign server). For data privacy in roaming networks they were used ciphertext anonymity in many research articles. Ciphertext anonymity in one which does not contains identity of both the sender and the receiver information. Here we use Signcryption scheme to provide a better privacy with the ciphertext anonymity property for the user under that two servers (Home & Foreign).

c. Location privacy

Location privacy is especially important in Wireless Network. Location event or the location information is one of the primary concerns from the adversary. Location privacy is under two adversaries: (i) Local adversary and (ii) Global adversary. Local adversary: is able to monitor traffic under limited area of the network at a time. Where as in Global adversary: able to monitor whole network at a time. Accessing Location privacy must be controlled by the user so only they can securely travel in one to another server in network. User must characterize a set of entity to allow access to its location information this provides intelligent services to the attackers [11, 12].

d. Home Server and Foreign Server

Home server (HS) and Foreign Server (FS) have roaming agreements so only user can access the data in wireless network [8]. User wants to access the data while their roaming means he/she has a proper registration and authentication process so only FS server allow the data during their roaming. In this case Security assessment is one of the important for their data so only user may travel across the networks User privacy like movement pattern, network usage habit etc. should be protected from potential adversary through roaming protocols [13].

IV OUTCOMES OF SURVEY

- We have studied the security and privacy issues in roaming network and analyze the problem of various research articles.
- Wireless communications are more vulnerable to various kinds of network attacks.
- Most of the researchers concentrate only on data transmission but failed to concentrate on user privacy and security issues.
- They were security problem while transferring the data between the networks.
- Most wireless transactions are done through public atmosphere so they were insecurity problem through unknown person.
- Through roaming networks they were problem under Two-factor authentication and the key establishment in roaming protocol.
- Privacy problem due to high revocation cost.
- Eavesdropping and malicious attackers are raised due to increased no of networks.
- Authentication method using smart card for roaming service fails to protect against strong repeat attack.
- They were problem under strong privacy because of high computational and communication costs.
- They were the problem in high authentication and revocation costs

V. CONCLUSION

In this survey, we have presented an overview of privacy and security in roaming networks. With the advancement of mobile technologies, wireless networks have become widely available and interconnected together. While at the same time providing a stronger security and privacy protection for roaming users is most vital one. In this survey we have studied the efficiency of existing protocols and showed the result of the privacy in roaming protocol. The problem arises because of low bandwidth channels. Hence limited processing resources of wireless devices make it even more challenging to design security in wireless communication. For the best of our knowledge roaming protocol based group signature with backward unlinkability give a better security and privacy when compared to other techniques.

REFERENCES

[1] JIANG Chunlin, JIA Weijia, GU Ke and XU Ning, "Anonymous Authentication without Home Server in Mobile Roaming Networks." *Chinese Journal of Electronics* 22.2 (2013).

[2] Hyo Jin Jo, Jung Ha Paik, and Dong Hoon Lee, "Efficient Privacy-Preserving Authentication in Wireless Mobile Networks". IEEE trans. Mobile computing july 2014.

[3] Y. Sun, T. La Porta, and P. Kermani, "A flexible privacy enhanced location-based services system framework and practice," *IEEE Trans. Mobile Comput.*, vol. 8, no. 3, pp. 304–321, Mar. 2009.

[4] C.Y Chow, M.F.Mokbel, and T. He, "A privacy-preserving location monitoring system for wireless sensor networks," IEEE *Trans. Mobile Comput.*, vol. 10, no. 1, pp. 94–107, Jan. 2011.

[5] Chunlin Jiang, Weijia JIA and Ke GU, "An Anonymous Wireless Authentication Protocol Based on Proxy Signature". Trans. 2012.

[6] Karim El Defrawy, and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs" *IEEE Trans 201*.

[7] Jiang, Q., Ma, J., Li, G., & Yang, L. (2012). An Enhanced Authentication Scheme with Privacy Preservation for Roaming Service in Global Mobility Networks. Wireless Personal Communications".

[8] Wan, Zhiguo, Kui Ren, and Bart Preneel. "A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks."*Proceedings of the first ACM conference on Wireless network security*. ACM, 2008.

[9] Annavaram, Murali, Quinn Jacobson, and John P. Shen. "Hangout: A Privacy Preserving Location Based Social Networking Service." (2009).

[10] Kur, Jırı. "Privacy preserving protocols for wireless sensor networks."

[11] Iyer, KB Priya, and V. Shanthi. "Study on Privacy Aware Location based Service." *Journal of Scientific and Industrial Research* 72.5 (2013): 294-299.

[12] Gedik, Bugra, and Ling Liu. "Protecting location privacy with personalized k-anonymity: Architecture and algorithms." *Mobile Computing, IEEE Transactions on* 7.1 (2008): 1-18.

[13] Myles, Ginger, Adrian Friday, and Nigel Davies. "Preserving privacy in environments with location-based applications." *IEEE Pervasive Computing* 2.1 (2003): 56-64.

[14] Q. Han, Y. Zhang, X. Chen, H. Li, and J. Quan, "Efficient and robust identity-based handoff authentication in wireless networks," in *Proc. 6th Int. Conf. Network and System Security*, Fujian, China, 2012, pp. 180–191, LNCS 7645.