ANALYSIS OF SECURITY ROAMING NETWORK AND PRIVACY PRESERVING MECHANISM

Ashwini A. Lokhande[1], Sonali U. Nimbhorkar[2]

[1]*Dept. of Computer Science & Engineering, G.H. Raisoni College of Engineering, Nagpur*
[2]*Dept. of Computer Science & Engineering, G.H. Raisoni College of Engineering, Nagpur*

Abstract

The Progression in various wireless network, such as roaming network which enables mobile subscriber to enjoy internet service anytime anywhere. Seamless roaming over wireless networks is highly desirable to mobile users, but ensuring the security and efficiency of this process is challenging. The communication systems in roaming services have special requirements and vulnerabilities, and therefore deserve special attention. Privacy-preserving authentication mechanism for Roaming services is presented in this paper. CPAL resists various security threats and provides more flexible privacy preservation compared to the existing schemes. The challenges which are unique to roaming service are discuss. The resistance against the denial of service attack in roaming service is describe.

Keywords:-*Roaming network, Privacy preserving, Authentication mechanism, CPAL, Denial of service Attack.*

----------***----------

1. INTRODUCTION

With the Progression in various mobile and wireless networks, including universal mobile telecommunication systems, wireless local area networks, roadside-to-vehicle communication systems [1], and satellite networks, ubiquitous computing becomes a reality. Users can access network services anywhere and anytime. However, within the heterogeneous networks, ensuring the secure and efficient roaming service is still difficult [4], [5], because different networks have different security policies and authentication protocols. Subsequently, any secure roaming scheme committed for only one type of network technology cannot fulfill the security needs from the heterogeneous networks.

In heterogeneous networks, user privacy preservation has become an important and challenging issue in the roaming service, and has been widely considered by researchers. In most existing secure roaming schemes, the privacy preservation only equates with anonymity, i.e., hiding users' identities. However, this may not be suitable for diverse privacy needs in real world [6], [7]–[9].

Moreover, there may be a large number of mobile users that need to be revoked in the network anytime due to various reasons, e.g., when any illegal or exceptional events occur. However, the existing secure roaming schemes [9], [10] do not support this function. This will significantly increase the burden of the home authentication server and potentially reduce the efficiency of the whole network. Therefore, efficient user revocation for dynamic membership in the secure roaming services is important. The General roaming scenario for wireless networks for communication is shown in Fig. 1. It involves three parties: a roaming user *U*, a visited foreign server *V*, and a home server *H* of which *U* is a subscriber. Normally, *V* and *H* have a roaming agreement, So *U* can access its subscribed services through *V* when *U* is in a foreign network administered by *V*. Before *U* can access resources provided by *V*, an appropriate authentication process between *U* and *V* must be carried out. This process is of great importance.

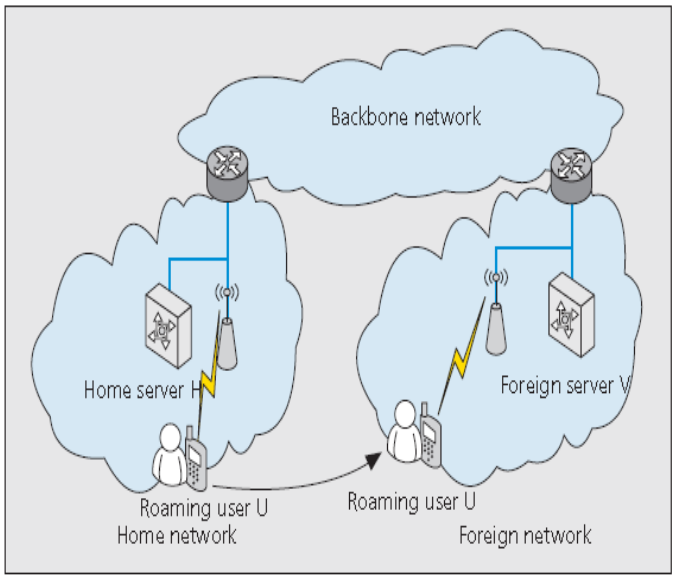

Fig 1 Overview of roaming services

2. RELATED WORK

The existing roaming schemes for secure communication can mainly be classified into three categories: symmetric-cryptosystem-based (SCbased), asymmetric-cryptosystem-based (AC-based), and hybrid schemes. The SC-based secure roaming schemes,such as EAP-based authentication and key agreement protocols [26],[27], are designed based on standard protocols [28], [29]. SC-based schemes are mostly accepted because they are compatible with standard

protocols. However, they require the interaction between the foreign server and the home server, which may lead to the single point of failure [30], and induce large authentication transmission overhead because of the long distance between the foreign server and the home server. Jiang and Shi [31], [32] propose several mutual authentication and key exchange schemes for roaming services. In [31] and [32], public key cryptography such as digital signature and Diffie– Hellman key exchange, is adopted on the basis of SC-based Schemes, which can further enhance the security of roaming Service. The limitations of SC-based schemes have greatly stimulated the research of AC-based schemes [9], [10], [20],[33], because AC-based schemes can provide more security, stronger privacy preservation, and require fewer communication rounds. These advantages have led to the recent increasing popularity of the AC-based secure roaming schemes. One of the important security properties in the AC-based secure roaming schemes is strong user anonymity, which includes user anonymity and user untraceablility. They point that a privacy-preserving and user authentication scheme should satisfy the following requirements for communication in the roaming network: server authentication, subscription validation, provision of user revocation function, key establishment, user anonymity, and untraceablility. However, the existing privacy-preserving authentication schemes for roaming service used for communication cannot provide anonymous user linkability that makes the authorized entities, e.g., FN operators or service providers; have the ability to anonymously link the access information from the user for statistical purposes. This may not be enough for diverse applications in the roaming service.

3. CHALLENGES AND REQUIREMENTS OF SECURE ROAMING SERVICES

Many security and efficiency challenges exist in roaming services, mainly due to the resource constraints of mobile users, the authentication delay constraint, and the demanding security requirements of roaming applications.

A. **Server Authentication:** Roaming users should be allowed to authenticate the foreign server they visit to avoid potential deception and other malicious attacks.

B. **Subscription Validation:** A visited foreign network must authenticate mobile users to ensure their legitimacy.

C. Provision of User Revocation: Services to a roaming user should be terminated once its subscription period ends.

D. **Key Establishment:** A session key should be established between a roaming user and a visited foreign server to protect subsequent data exchanged between them.

E. **Low Computation Complexity and Communication cost:** A mobile user is generally constrained in terms of power, processing capability, and storage space. The degree of the resource limitation is different for various mobile devices (e.g., laptop PC, smart phone, PDA). Therefore, a roaming authentication process should be computationally efficient. At the same time, such a process should be fast enough to maintain persistent connectivity for mobile users.

F. **Basic User Anonymity and Non-Traceability:** A user should be anonymous, and its activities must not be linkable by eavesdroppers. Non-linkability means that an adversary cannot link the communication activities of a particular user together and thus establish the user's profile.

G. **Attack Resistance:** The roaming protocol should have the ability to resist various attacks in wireless networks (e.g., denial of service [DoS] attack, replay attack, deposit case attack) such that it can be applied in the real world.

4. RESISTANCE AGAINST DOS ATTACKS

To prevent the DoS attack, in roaming network for communication have suggested that the message-specific puzzles of [18] can be Incorporated into current roaming authentication protocols (e.g., [11-16]) in the following way. When a foreign server finds no evidence of the attack (e.g., the arrival rate of bogus access requests is less than a predefined threshold), it Processes access requests normally (i.e., indiscriminately). However, when it suspects itself of being attacked, it only performs expensive verification on access requests selectively. In particular, the server attaches a unique puzzle into the beacon messages and requires the solution of the puzzle to be attached to each access request message. The server commits resources to process an access request only when the solution is correct.

In general, solving a puzzle requires a brute force search in the solution space, while solution verification is very fast. Additionally, puzzles are deployed in conjunction with conventional time-outs on server resources. Thus, in order to create an interruption in services, an adversary must have abundant resources to be able to promptly compute a large enough number of puzzle solutions in line with its sending rate of illegal access requests. In contrast, although puzzles slightly increase legitimate users' computational load when the server is under attack, they are still able to Obtain network access regardless of the existence of the attack.

5. CPAL:-DESIGN GOALS

Design goal to develop a CPAL (Conditional Privacy – Preserving Authentication Mechanism) for roaming service is as follows.

A. **Strong Anonymous Access Authentication:** First, the proposed scheme should provide strong anonymous access authentication. Specifically, it requires that authentication messages, which are interacted by the MS and the VAS, have not been altered during the transmission, i.e., if the adversary A forges and/or modifies the authentication messages, the malicious operations should be detected. Meanwhile, the identity of the MS cannot be revealed to adversary A or the VAS.

B. **User Tracking on a Disputed Access Request:** An important and challenging issue for roaming service with efficient privacy preservation is to maintain traceability for all the access messages in the presence of the anonymous access authentication. Without the tracking function, the above anonymous access authentication can only prevent an outside attack, but cannot deal with an inside one. For instance, an inside attacker could launch a Denial of Service (DoS) attack or impersonation attack, provided with no traceability by the HAC. In a DoS attack, the adversary sends a large number of fake access messages to jam the channel or to consume the rare computation resources of the VAC; while in an impersonation attack, the adversary actively pretends to be another MS to send false access request messages.

C. **Anonymous User Linking:** In order to provide CPAL, i.e., anonymity can be flexibly or elaborately controlled according to the corresponding requirements, the network operators or service providers that are authorized by the HAC or MS can acquire MS's statistics on the usage of services, while MS's identity will not be revealed.

D. **Efficient User Revocation for Dynamic Membership:** Due to some reasons (e.g., the subscription period of a user has expired or a user's secret key has been compromised), an efficient user revocation function should be proposed, especially for dynamic membership. That means the user revocation function can revoke a group of users simultaneously, which makes the whole scheme more flexible and efficient. Meanwhile, CPAL can provide a universal secure roaming service. That means the proposed CPAL and its signaling flows can be used in any roaming scenario regardless of the type of networks that the MS is visiting. Moreover, the proposed CPAL scheme should meet all security requirements in previous schemes.

6. CONCLUSION

Roaming services in wireless networks provide people with attractive flexibility and convenience for communication. A set of mechanisms to complement existing work for defending against DoS attacks, efficient authentication, flexible roaming in mobile contexts is describe here. CPAL-Condition Privacy Preserving Authentication with Access Linkability resists various security threats and provides more flexible and elaborate privacy preservation including user tracking, anonymous user linking, joining, and revocation function for dynamic membership.

REFERENCES

[1] Chengzhe Lai, , Hui Li, Xiaohui Liang, Rongxing Lu, Kuan Zhang, , and Xuemin Shen, ―CPAL: A Conditional Privacy- Preserving Authentication With Access Linkability for Roaming Service‖ IEEE internet of things journal, vol. 1, no. 1, february 2014.

[2] Y. Soh, T. Quek, M. Kountouris, and H. Shin, "Energy efficient heterogeneous cellular networks," IEEE J. Sel. Areas Commun., vol. 31, no. 5, pp. 840–850, May 2013.

[3] Huang, X. Hong, and M. Gerla, "Situation-Aware Trust Architecture for Vehicular Networks," *IEEE Communication.. Mag.*, vol. 48, no. 11, 2010, pp. 128–35.

[4] A. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," IEEE Security. Privacy, vol. 11, no. 2, pp. 55–62, Mar./Apr. 2013.

[5] D. He, C. Chen, J. Bu, S. Chan, and Y. Zhang, "Security and efficiency in roaming services for wireless networks: Challenges, approaches, and prospects,"IEEE Communication. Mag., vol. 51, no. 2, pp. 142–150, Feb. 2013.

[6] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. IEEE INFOCOM, 2008, pp. 1229–1237.

[7] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy preserving opportunistic computing framework for mobile-healthcare emergency," IEEE Trans. Parallel Distribute. Syst., vol. 24, no. 3, pp. 614–624, Mar. 2013.

[8] X. Liang, X. Li, H. Luan, R. Lu, X. Lin, and X. Shen, "Morality-driven data forwarding with privacy preservation in mobile social networks," IEEE Trans. Technol., vol. 61, no. 7, pp. 3209–3221, Sep. 2012.

[9] Yang, Q. Huang, D. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," IEEE Trans. Wireless Communication.., vol. 9, no. 1, pp. 168–174, Jan. 2010.

[10] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," IEEE Trans. Wireless Communication.., vol. 10, no. 2, pp. 431–436, Feb. 2011.

[11] G. Yang, D. S. Wong, and X. Deng, "Anonymous and Authenticated Key Exchange for Roaming Networks," *IEEE Trans. Wireless Communication..*, vol. 6, no. 9, Sept. 2007, pp. 3461–72.

[12] Z. Wan, K. Ren, and B. Preneel, "A Secure Privacy-Preserving Roaming Protocol based on Hierarchical Identity- based Encryption for Mobile Networks," *Proc. ACM WiSec '08*, 2008, pp. 62–67.

[13] Yang *et al.*, "Universal Authentication Protocols for Anonymous Wireless Communications," *IEEE Trans. Wireless Communication..*, vol. 9, no. 1, Jan. 2010, pp. 168–74.

[14] D. He *et al.*, "Privacy-Preserving Universal Authentication Protocol for Wireless Communications," *IEEE Trans. Wireless Communication..*, vol. 10, no. 2, Feb. 2011, pp. 431–36.

[15] D. He *et al.*, "Secure and Efficient Handover Authentication based on Bilinear Pairing Functions," *IEEE Trans. Wireless Communication..*, vol. 11, no. 1, Jan. 2012, pp. 48–53.

[16] D. He *et al.*, "Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks," *IEEE Trans. Computers*, published online 27 Dec. 2011.

[17] D. He *et al.*, "Strong Roaming Authentication Technique for Wireless and Mobile Networks," *Int'l. J. Communication. Systems*, published online 4 Jan. 2012.

[18] A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," *Proc. NDSS '99*, 1999, pp. 151–65.

[19] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Communication..*, vol. 17, no. 5, Oct. 2010, pp. 56–62.

[20] M. Chuang, J. Lee, and M. Chen, "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," IEEE Syst. J., vol. 7, no. 1, pp. 102–113, Mar. 2013.

[21] Z. Wan, K. Ren, and B. Preneel, "A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks," in Proc. 1st ACM Conf. Wireless Network. Security, 2008, pp. 62–67.

[22] Y. Kim, W. Ren, J. Jo, Y. Jiang, and J. Zheng, "SFRIC: A secure fast roaming scheme in wireless LAN using ID-based cryptography," in Proc. IEEE ICC, 2007, pp. 1570–1575.

[23] Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," IEEE Trans. Wireless Communication.., vol. 12, no. 3, pp. 1018–1025, Mar. 2013.

[24] A.Menezes, P. V. Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC press, 2010.

[25] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy preserving aggregation scheme for secure smart grid communications," IEEETrans. Parallel Distribute. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[26] C. Fan, Y. Lin, and R. Hsu, "Complete EAP method: User efficient and forward secure authentication protocol for IEEE 802.11 wireless LANs," IEEE Trans. Parallel Distribute. Syst., vol. 24, no. 4, pp. 672–680,Apr. 2013

[27] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Trans. Wireless Communication.., vol. 4, no. 2, pp. 734–742, Mar. 2005.

[28] D. Zhang, "3GPP TS 33.401 V12.5.0, 3GPP System Architecture Evolution (SAE); Security Architecture," Sep. 2012.

[29] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for Third Generation Authentication and Key Agreement (EAP-AKA), IETF RFC 4187," Jan. 2006.

[30] K. Dooley, Designing Large Scale LANs. Sebastopol, CA, USA: Reilly Media, 2009

[31] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," IEEE Trans. Wireless Communication.., vol. 5, no. 9, pp. 2569–2577, Sep. 2006.

[32] M. Shi, H. Rutagemwa, X. Shen, J. Mark, and A. Saleh, "A service-agent based roaming architecture for WLAN/Cellular integrated networks," IEEE Trans. Veh. Technol., vol. 56, no. 5, pp. 3168–3181, Sep. 2007.

[33] J. Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," IEEE Trans. Wireless Communication.., vol. 12, no. 3, pp. 1018–1025, Mar. 2013.