International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Analysis of Protective Mechanism in Roaming Network for Secure Communication

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

[1, 2] Department of Computer Science & Engineering, G.H. Raisoni College of Engineering. Nagpur, Maharashtra, India

Abstract: ***Roaming means the expansion of a wireless network service in an location that is different from registered home network. Roaming service provide mobile subscriber the capability to move from one access point to other for communication when it is out of the normal coverage area. Within the diverse network, providing protective and resourceful roaming service is difficult, because various networks have various protective policies and authentication protocols. Protective mechanism in roaming network for secure communication is presented in this paper. The scenario of denial of service attack is described and the preventive method against the attack is mention.***

Keywords: Roaming service, Resourceful, Protective mechanism, Denial of service Attack

1. Introduction

The rapid development in a range of mobile and wireless network technology enables mobile subscribers (MSs) to access Internet service anytime and anywhere[2][3]. The advancement in the wireless telecommunication is rapidly increasing, but the complementary nature of the existing network and interworking amoung them is difficult[4][21]. Within the heterogeneous network, guranting the secure and efficient roaming service is still difficult [6][7], because different network have different authentication protocols and security policies.

Roaming deals with the expansion of a wireless network service in an location that differs from registered home location. In other words, roaming is the capability for the cellular user or the mobile subscriber to mechanically make and receive voice calls for communication purpose, sharing of data, or have right to use other services, such as home data services, when travelling from one geographical coverage area to other geographical coverage area [1]. (CPAL) for roaming service, which provide universal secure roaming service mechanism for secure communication in roaming network[1]. A novel group signature technique is used by CPAL to provide an anonymous user linking function which can not only capably hide user's identities but also permit the authorized entities to associate all access information of the similar mobile subscriber not having information of the user's actual identity. In the existing secure roaming schemes the privacy preservation only equates with anonymity, i.e. hiding user's identities[1]. On the other hand this may not be appropriate for various privacy necessities.

There may be huge number of mobile user that needs to be revoked in the network anytime due to various reasons, e.g. when any prohibited or exceptional event occurs. Though the existing secure roaming scheme does not support this function, hence 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 service is important. Internet service providers (ISP) and cellular service provide Roaming service policies. Global System for Mobile Communications (GSM) and code division multiple access (CDMA) operators provide traditional cellular roaming services. Mobile/cellphone subscriber service packages are incorporated with wireless telecommunication roaming services for use outside local network area.

2. Related Work

For secure roaming service CPAL –Conditional Privacy Preserving Authentication with Access Linkability for Roaming Service, which provide multilevel privacy preservation mechanism for secure communication in the roaming network[1].CPAL uses the master linking key process for authentication purpose. Jiang and Shi [33], [34] propose some mutual authentication and key exchange methods in roaming network for secure communication. In [33] and [34], public key cryptography such as digital signature and Diffie– Hellman key exchange, is accepted on the basis of SC-based Schemes, which can further improve the security of roaming Service. Mainly existing roaming schemes for secure communication in roaming network can mainly be classified into three categories: symmetric-cryptosystem-based (SCbased), asymmetric-cryptosystem-based (AC-based), and hybrid schemes. The EAP-based authentication and key agreement protocols [28],[29],can also be called as SC-based secure roaming method are designed based on standard protocols [30], [31]. SC-based methods are widely used because they are well match with accepted protocols. Though this protocol require the relation between the foreign server and the home server, that may lead to the single point of failure [32], which require large authentication transmission overhead because of the large distance between the foreign server and the home server. The limitations of SC-based schemes have greatly encourage the research of AC-based schemes [11], [12], [22],[35], because AC-based schemes can supply more security, tough privacy preservation, and need less communication overheads. These benefits have led to the rapid raising popularity of the AC-based secure roaming methods. One of the important security belongings in the AC-based secure roaming schemes is tough user anonymity, which includes user anonymity and user untraceablility. The point that a privacy-preserving and user authentication scheme should fulfill the following requirements for secure communication in the roaming network: subscription validation, server authentication, key establishment, provision of user revocation function, user anonymity, and untraceablility. However, the existing privacy-preserving authentication methods 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 capability to anonymously link the access information from the user for statistical purposes. This may not be sufficient for different applications in the roaming service.

3. Possible Attacks in Roaming Network

Roaming mobile subscribers should be allowed to authenticate the foreign server they visit to stay away from potential deception and other malicious attacks.

A. Denial of service (DoS) Attack

With the help of compromised nodes this types of threads produce a malicious action that leads to some danger in security mechanism. The compromised routing is very difficult to detect in the presence of compromised nodes. When attacker attacks in the normal communication scenario the compromised route looks same as the normal route but results to some problems. for example:-A compromised node can take part in the communication but drops several packets that results in degradation in the quality of service being presented by network.

B. Malicious Node Attack

The basic concept behind the malicious node attack in the network is to insert itself in the active path from source to destination or to take of network traffic. In this type of attack, the attacker can create routing loops which in turn results in the formation of several congestion. The malicious node “X” can take of important data by placing itself between source “A” and destination “D” as shown in fig 1. “X” can also redirect the data packets exchanged between “A” and “D”, which leads to important end to end delay between “A” and “D”. Against routing and Path selection the attackers attacks in the malicious node attack scenario.

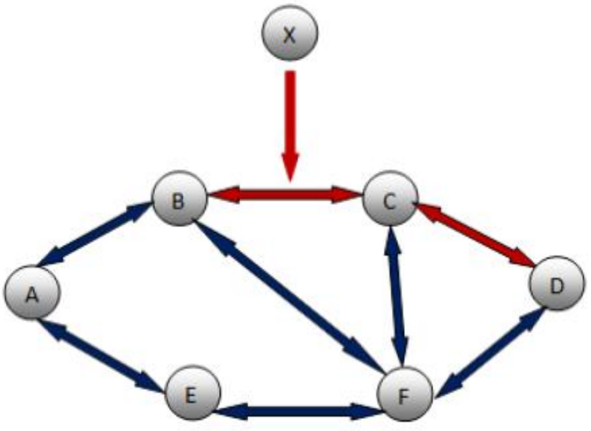

Figure1: Routing Attack by Malicious Node

4. Preventive Mechanism Against DoS Attacks

The roaming authentication protocol is incorporated with the message specific puzzles, the incorporation of message specific puzzles with authentication protocol can be done in the following way, when no evidence of attack is find by the foreign server i.e the predefined threshold is greater than the bogus access request, then it request with processes normally. On the other hand if it presumes itself of being attacked, then it will only perform expensive verification on access request carefully. The server then access the request by incorporating a unique puzzle into the beacon messages and then the solution of this puzzle should be attach to each access request message. When the solution comes exactly correct then only the server commits resource to process an access request.

The solution verification is the fast process but solving a puzzle requires a huge force search in the solution space. On the server resources the puzzles are deployed in conjunction with conventional time slots. Therefore to interrupt the normal communication service an attacker must have plentiful resource that will be able to punctually calculate a huge number of puzzle solution in line and with its sending rate of prohibited access request. In opposite to that although puzzles somewhat increase legitimate user’s working load when the server is under attack condition, but yet they are capable to obtain access to network despite of the presence of the attack.

5. Conclusion

With the progression of wireless communication the concept of roaming can be extended to the emerging paradigm of networking e.g. VANET and e-health, when this user want to access an foreign network which is different from the home network were the service was registered. CPAL can be applied to the access process security and privacy preservation, but doesn’t effectively resist the internal and external attack in the roaming network. Hence the paper deals with study of possible behavior of internal and external attack and their preventive method, this paper deals with lightweight secure and privacy preserving scheme to effectively resist denial of service attack in roaming network. Hence the overall performance of the roaming network is improved.

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] A. Al Shidhani and V. Leung, “Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers,” IEEE Trans. Dependable Secure Comput., vol. 8, no. 5, pp. 699–713, Sep./Oct. 2011.

[3] P. Taaghol, A. Salkintzis, and J. Iyer, “Seamless integration of mobile WiMAX in 3GPP networks,”

IEEE Commun. Mag., vol. 46, no. 10, pp. 74–85, Oct. 2008.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] 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.

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

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

[20] A. Juels and J. Brainard, “Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks,” *Proc. NDSS ’99*, 1999, pp. 151–65.

[21] 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.

[22] 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.

[23] M. Peng, Y. Liu, D. Wei, W. Wang, and H. Chen, “Hierarchical cooperative relay based heterogeneous networks,” IEEE Wireless Commun., vol. 18, no. 3, pp. 48–56, Jun. 2011.

[24] 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.

[25] 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.

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

[27] 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.

[28] 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

[29] 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.

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

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

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

[33] 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.

[34] 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.

[35] 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.