IJRRECS/July 2014/Volume-2/Issue-7/2803-2807 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

ACCOMPLISHING OF QUALIFIED PRIVACY BY HANDOVER SYSTEM

Sangapu Hazarathaiah[1], U.Ramya Sree[2]

[1]**M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthaasurengi (V), Patancheru (M), Hyderabad, T.S, India**

[2]**Assistant Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India**

ABSTRACT:

The complete existing protocols of handover authentication are engaged to not many security attacks as users are extremely anxious concerning their privacy-related information. A handover procedure of authentication has to be computationally skilled and such a procedure has to be prompt enough to protect constant connectivity for mobile nodes. All existing protocols of handover authentication fail to make available suitable security as well as efficiency guarantees. Scheming of a handover authentication procedure is not an effortless mission. Novel system of handover authentication called PairHand, was set up which utilize pairing based cryptography to firmly handover process and to reduce communication plus computation spending of concerned entities. When designing Pair Hand, we discover that not anything of existing confidentiality aware cryptographic primitives, such as ring signature, blind signature, as well as group signature system, and go well with safety all along with capability requirements.

Keywords: Security attacks, Cryptographic primitives, Pair Hand, Mobile nodes, Handover authentication.

1. INTRODUCTION:

To overcome geographical coverage bound of every access point and put forward seamless access service for mobile nodes, it is very important to include a capable handover procedure. Securities and privacy are strict concerns for provision of handover authentication. A novel system of handover authentication called PairHand, was set up which utilize pairing based cryptography to firmly handover process and to reduce communication plus computation spending

of concerned entities. The system simply necessitates two handshakes between a mobile node as well as an access point, and does not necessitate broadcasting or else validation of any certificate like in systems of conventional public key cryptosystems. One important constituent in handover procedure is confirmation. In spite of information put into exercise, as shown in fig1 a representative handover authentication circumstance entails mobile nodes, authentication server as well as access points [1]. All through handover authentication, new access point validates mobile node to distinguish and discard any access demand by an illegal user. When designing Pair Hand, we discover that not anything of existing confidentiality aware cryptographic primitives, such as ring signature, blind signature, as well as group signature system, and go well with safety all along with capability requirements. Earlier than entering network, a mobile node records to authentication server, afterwards subscribe services moreover unite towards access point for accessing network. When mobile node moves from present access point into a new access point, handover authentication has to be performed at novel access point. The preload-and-replenish system has been introduced by numerous researchers and works capably [2][3]. Mobile nodes commonly encompass huge storage capability, rendering the preloading concerning a huge pool of pseudonyms from authentication server. As preloading procedure in handover authentication process involves a collection of shorter-lived pseudonyms, the memory exploitation is enclosed by results.

2. METHODOLOGY:

The complete existing protocols of handover authentication are engaged to not many security attacks for instance users are extremely anxious concerning their privacy-related information such as the individuality, position, in addition to roaming route [4][5]. To avoid denial of service attack, quite a lot of current hand over authentication means just requires a mobile node as well as an access point to be concerned in every protocol run. The access point needs to carry out costly cryptographic process to make sure the legitimacy of the sender. This checking is exploited by opponent to make an additional type of denial of service attack. Specifically, it can introduce fake access requests into networks, compel the access points that accept such messages to carry out

costly verifications, and ultimately weaken their resources. Regardless of requirement and significance, no research was conducted to tackle this attack within handover authentication. Novel system of handover authentication called PairHand, was set up which utilize pairing based cryptography to firmly handover process and to reduce communication plus computation spending of concerned entities. Scheming of a handover authentication procedure is not an effortless mission. There are two most important realistic issues demanding the design. Initially efficiency desires to be measured. A mobile node is typically controlled in terms of power in addition to processing ability [6][7]. A handover procedure of authentication has to be computationally skilled and such a procedure has to be prompt enough to protect constant connectivity for mobile nodes. Securities in addition to privacy are strict concerns for handover authentication prerequisite.

3. AN OVERVIEW OF EXISTING HANDOVER STRATEGIES:

To provide robust protection, employing a digital signature system is extensively recognized as the major successful approach in support of handover authentication. It is not capable in communication, as certificate was to extinguish all along with digital signature since message propagates in system. This leads to additional energy expenditure on mobile nodes. To validate each digital signature, corresponding receiver constantly takes two pricey signature verification processes [8]. This is because the certificate desires to be genuine as well. To make available user anonymity, group signature-based protocols were introduced. User revocation listing desires to be dispersed across complete network in a well-timed manner. The verification impediment incurred in the protocols in support of every access request is linearly proportional to the revoked user's number. The performance of the protocols possibly will get worse when number of revoked users is huge. A competent batch signature verification system was projected in which each access point can concurrently authenticate numerous received signatures. All existing protocols of handover authentication fail to make available suitable security as well as efficiency guarantees. The conventional method of performing handover authentication is to allow novel access point contact authentication server

who proceed as a sponsor for vouching that a mobile node is its lawful subscriber [9]. It will sustain additional computation as well as communication impediment; particularly authentication server is regularly positioned in a distant location. For mutual authentication as well as key establishment, the entire protocols devoid of communicating with authentication server necessitate not less than three handshakes among the mobile node and the novel access point while previous protocols necessitate not less than four handshakes between three entities. Existing schemes of group signature do make available revocable anonymity, however cannot congregate high effectiveness. The privacy preserving method based on pseudonyms was adopted. Users are hesitant to recognize such mobile service. It is absolutely significant to make available a resourceful handover authentication procedure for practical wireless networks. Blind signature besides ring signature can merely provide unobstructed confidentiality, while PairHand demands conditional privacy, as well as revocable anonymity. The present attempt quantitatively measured the storage space circumstance for preloading anonymous keys plus connected certificates for durable use. Their results are attained based on specifying upper with lower bounds on pseudonym change time for maintenance of tolerable scope of privacy.

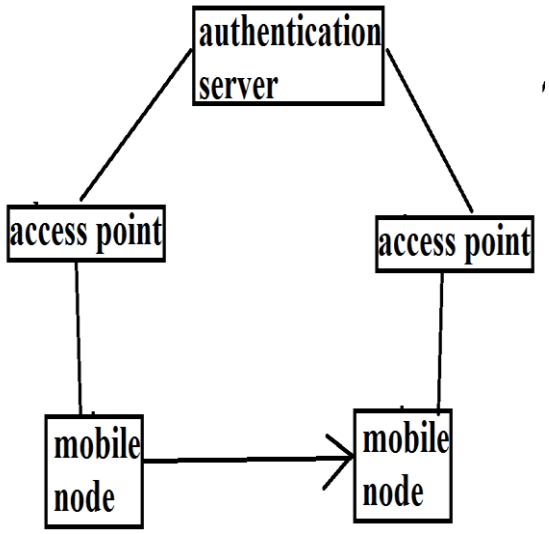

Fig1: An overview of Handover authentication

4. CONCLUSION:

To avoid denial of service attack, quite a lot of current hand over authentication means just requires a mobile node as well as an access point to be concerned in every protocol run. Regardless of requirement and significance, no research was conducted to tackle this attack within handover authentication. The conventional method of performing handover authentication is to allow novel access point contact authentication server who proceed as a sponsor for vouching that a mobile node is

its lawful subscriber. All through handover authentication, new access point validates mobile node to distinguish and discard any access demand by an illegal user. Novel system of handover authentication called PairHand, was set up which utilize pairing based cryptography to firmly handover process and to reduce communication plus computation spending of concerned entities. In spite of information put into exercise, a representative handover authentication circumstance entails mobile nodes, authentication server as well as access points. Scheming of a handover authentication procedure is not an effortless mission. As preloading procedure in handover authentication process involves a collection of shorter-lived pseudonyms, the memory exploitation is enclosed by results. For mutual authentication as well as key establishment, the entire protocols devoid of communicating with authentication server necessitate not less than three handshakes among the mobile node and the novel access point while previous protocols necessitate not less than four handshakes between three entities.

REFERENCES

[1] Y.-P. Liao and S.-S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol. 31, no. 1, pp. 24–29, 2009.

[2] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118–1123, 2009.

[3] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," Computer Commun., vol. 34, no. 3, pp. 367–374, 2011.

[4] J. Choi and S. Jung, "A secure and efficient handover authentication based on light-weight Diffie-Hellman on mobile node in FMIPv6," IEICE Trans. Commun., vol. E-91B, no. 2, pp. 605–608, 2008.

[5] Y. Kim,W. Ren, J. Jo, M. Yang, Y. Jiang, and J. Zheng, "SFRIC: a secure fast roaming scheme in wireless LAN using ID-based cryptography," in Proc. ICC 2007.

[6] J. Choi, S. Jung, Y. Kim, and M. Yoo, "A fast and efficient handover authentication achieving conditional privacy in V2I etworks," LNCS 5764. Springer, pp. 291–300, 2009.

[7] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," IEEE Commun. Lett., vol. 14, no. 1, pp. 54–56, 2010.

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

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