IJRRECS/June 2014/Volume-2/Issue-6/2408-2413 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

MANAGING OF HIGH EFFECTIVENESS BY SAFE HANDOVER SYSTEM

S.Lakshmi Prasanna[1], A.Satchidanandam[2]

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

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

ABSTRACT:

To make available user anonymity, group signature-based protocols were introduced. To keep away from denial of service attack, several current hand over authentication methods merely necessitate a mobile node and an access point to be concerned in every protocol run. Existing schemes of group signature do make available revocable anonymity, however cannot congregate high effectiveness. A novel system of handover authentication called PairHand, was introduced which make use of pairing based cryptography to securely handover process and to decrease the communication as well as computation spending of the concerned entities. It necessitates two handshakes among a mobile node and an access point, and does not require broadcasting or verifying any certificate as in conventional public key cryptosystems. A handover process of authentication has to be computationally competent and speedy enough to preserve constant connectivity for mobile nodes and moreover Securities as well as privacy are severe concerns for handover authentication provision. A representative handover authentication situation involves entities such as: mobile nodes, authentication server and access points. Before entering network, a mobile node registers to authentication server, subsequently subscribes services and unites to access point for accessing network.

Keywords: Efficiency, security, privacy, Wireless networks, Cryptosystems.

1. INTRODUCTION:

A representative VANET comprises of trusted authority, huge number of vehicles which are equipped by means of wireless On-Board Units as well as several stationary Roadside Units. Trusted authority set up roadside units as well as registers vehicles all the way through granting consequential authentication keys. Each Roadside Unit receives and subsequently verifies traffic safety messages from On-Board Units [4]. Data transmission is expensive processes in wireless networks which send 1-bit over a wireless medium necessitate over 1000 times more energy than a particular 32-bit computation. To make available robust security, employing a digital signature scheme is widely recognized as the most effective approach for handover authentication. It is not proficient in communication, since the certificate has to be put out all along with digital signature since message propagates in system [8]. This leads to additional energy expenditure on mobile nodes. To validate each digital signature, corresponding receiver constantly takes two pricey signature verification processes. 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 [1]. The performance of the protocols possibly will get worse when number of revoked users is huge. All existing protocols of handover authentication fail to make available suitable security as well as efficiency guarantees. Users are hesitant to recognize such mobile service. It is absolutely significant to make available a resourceful handover authentication procedure for practical wireless networks. A novel system of handover authentication called PairHand, was introduced which make use of pairing based cryptography to securely handover process and to decrease the communication as well as computation spending of the concerned entities [11]. It merely requires two handshakes among a mobile node and an access point, and does not require broadcasting or verifying any certificate as in conventional public key cryptosystems. A competent batch signature verification system was projected in which each access

point can concurrently authenticate numerous received signatures.

2. METHODOLOGY:

To triumph over the geographical coverage bound of each access point and offer seamless access service in support of mobile nodes, it is imperative to include a competent handover procedure [3]. One significant component in the handover procedure is verification. Despite the knowledge put into practice, as revealed in fig1 a representative handover authentication situation involves entities such as: mobile nodes, authentication server and access points. Before entering network, a mobile node registers to authentication server, subsequently subscribes services and unites to access point for accessing network [14]. When mobile node moves from present access point into a new access point, handover authentication has to be performed at novel access point. All the way through handover authentication, novel access point authenticates mobile node to recognize and throw out any access demand by an unlawful user. A session key has to be established among the mobile node and the novel access point to make available privacy and reliability of the communication session. 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 [7]. Existing schemes of group signature do make available revocable anonymity, however cannot congregate high effectiveness. The privacy preserving method based on pseudonyms was adopted. When scheming Pair Hand, we uncover that nothing of the existing privacy conscious cryptographic primitives, for instance ring signature, blind signature, and group signature system, and go well with safety along with competence requirements [2]. Blind signature in addition to ring signature can merely make available unrestricted privacy, whereas PairHand demands

conditional privacy, and consequently, revocable anonymity. The modern effort quantitatively considered the storage space condition for preloading anonymous keys as well as connected certificates for enduring use [16]. Their results are achieved based on enumerating upper as well as lower bounds on pseudonym change period for upholding an acceptable extent of privacy. The preload-and-replenish system has been introduced by numerous researchers and works capably. Mobile nodes commonly encompass huge storage capability, rendering the preloading concerning a huge pool of pseudonyms from authentication server [12]. Since preloading process in handover authentication procedure entail a group of shorter-lived pseudonyms, the memory utilization is bounded by results.

3. SCHEMING OF HANDOVER AUTHENTICATION SYSTEM:

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 usually constrained in terms of power as well as processing ability [5]. A handover process of authentication has to be computationally competent. Such a process has to be speedy enough to preserve constant connectivity for mobile nodes. Securities as well as privacy are severe concerns for handover authentication provision. The entire existing protocols of handover authentication are focussed to not many safety attacks such as users are intensely anxious about their privacy-related data for instance the individuality, position, as well as roaming route [15]. By means of Denial-of-Service attacks, opponent can weaken assets of access point and authentication server and provide them less competent of serving lawful mobile nodes. Such attacks are categorized into categories. The usual method of executing handover authentication necessitates an access point towards unconditionally forward any access demand, applicable or unacceptable, to authentication server, an opponent can effortlessly launch denial of service attacks on authentication server all the way through an access point [10]. To keep away from denial of service attack, several current hand over authentication methods merely necessitate a mobile node and 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 [6]. 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 [13]. Regardless of requirement and significance, no research was conducted to tackle this attack within handover authentication.

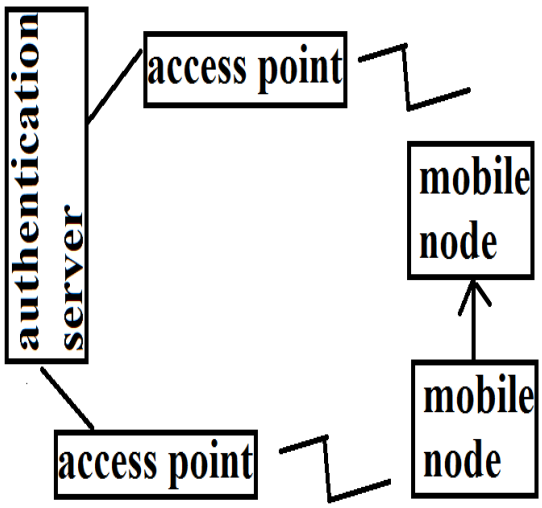

Fig1: An overview of Handover authentication

4. CONCLUSION:

Blind signature in addition to ring signature can merely make available unrestricted privacy, whereas PairHand demands conditional privacy, and consequently, revocable anonymity. By means of Denial-of-Service attacks, opponent can weaken assets of access point and authentication server and provide them less competent of serving lawful mobile nodes. The entire existing protocols of handover authentication are focussed to not many safety attacks such as users are intensely anxious about their privacy-related data for instance the individuality, position, as well as roaming route. Since preloading process in handover authentication procedure entail a group of shorter-lived pseudonyms, the memory utilization is bounded by results. When scheming Pair Hand, we uncover that nothing of the existing privacy conscious cryptographic primitives, for instance ring signature, blind signature, and group signature system, and go well with safety along with competence requirements. When mobile node moves from present access point into a new access point, handover authentication has to be performed at novel access point. The verification impediment incurred in the protocols in support of every access request is linearly proportional to the revoked user's number.

REFERENCES:

[1] U.S. Department of Transportation, National Highway Traffic SafetyAdminstration, Vehicle Safety Communications Project, Final Repot,2006

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

[3] J. Choi, S. Jung, Y. Kim, and M. Yoo, "A fast and efficient handoverauthentication achieving conditional privacy in V2I networks," LNCS5764. Springer, pp. 291–300, 2009

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

[5] C. Blundo, et al., "Perfectly-secure key distribution for dynamic conferences,"in Advances in Cryptology-Crypto 1992, LNCS 740, PP. 471–
486.

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

[7] C.-C. Chang, C.-Y. Lee, and Y.-C. Chiu, "Enhanced authenticationscheme with anonymity for roaming service in global mobility networks,"
Computer Commun., vol. 32, no. 4, pp. 611–618, 2009

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

[9] K. C. Barr and K. Asanovi, "Energy aware lossless data compression,"ACM Trans. Comput. Syst., vol. 24, no. 3, pp. 250–291, 2006.

[10] M. Scott, Multiprecision Integer and Rational Arithmetic C/C++ Library(MIRACL). Published by Shamus Software Ltd., http://www.shamus.ie/.

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

[12] 3rd Generation Partnership Project, 3GPP Specification: 3GPP TS33.102, 3G Security, Security Architecture, Dec. 2002.

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

[14] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," J.Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

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

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