Analysis of Security, Privacy and Efficiency Aspects of Handover Authentication Protocol for Wireless Sensor Networks

Iqbaldeep Kaur
Associate Professor
Computer Science & Engineering,
Chandigarh Engineering College,
Landran, Punjab, India
Iqbaldeepkaur.cu@gmail.com

Harnain Kour
M. Tech. Research Scholar,
Computer Science & Engineering,
Chandigarh Engineering College,
Landran, Punjab, India
nainbani1@gmail.com

Dr. Amit Verma
Professor and Head, Head of Department
Computer Science& Engineering,
Chandigarh Engineering College,
Landran, Punjab, India
dramit_verma@yahoo.com

Abstract— In the recent years, technology in the field of wireless network and mobile devices has abruptly growing. This growing technology provokes the need to enhance the security, privacy and efficiency of wireless sensor networks. To capture this need, handover authentication protocol is introduced that enables the mobile nodes to securely & efficiently roam from one access point to another in wireless sensor network. As wireless sensor network is easily susceptible to vulnerable attacks, so there is the need to design an efficient authentication protocol that can transfer the data with more security, privacy and efficiency over the mobile nodes. In this research work, we have presented the existing approaches on handover authentication protocol in wireless network. The presented work discusses the aspects of security, privacy and efficiency in handover authentication protocol.

Keywords— Handover Authentication Protocol, Wireless Network, PairHand Protocol, HashHand Protocol, Cryptography

I. INTRODUCTION

In today's advanced technology, handheld mobile gadgets and wireless communication have a great influence on human's day to day life in various aspects [1]. Due to low cost solution for various real life challenges, wireless sensor networks are growing rapidly. Wireless sensor networks need no any kind of infrastructure, is rigid to maintain security, can be employed for environment monitoring and quick deployment low cost solution. Figure 1 shows the structure and various elements of wireless sensor network. In WSN, main role is played by resource sensor nodes to sense the neighbor node data and transfer to base stations. Due to some constraints of sensor node in WSN like storage, computation, power etc. the preferred method is multi-hop communication where large number of nodes exists. Due to infrastructure-less mobile nodes in WSN, there are some main concerns regarding the efficiency, privacy and security of communication [2]. So, there is need of proper authentication of data along with the node information.

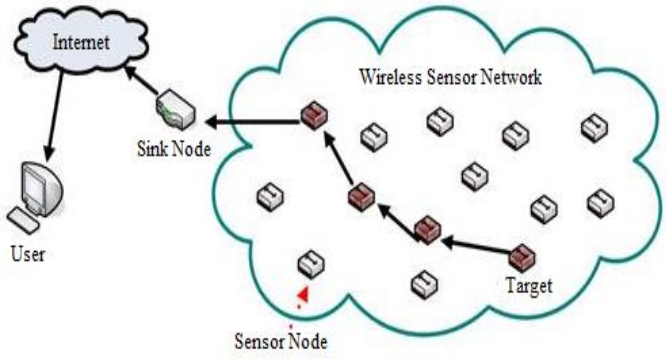

Figure 1: Wireless Sensor Network

Authentication can be defined as the procedure that ensures the authentic identity of nodes and their data transformation from authentic source. Authentication can be defined one way, mutual, three way and implicit authentication [3]. Authentication mechanisms in WSN can be categorized on the following basis.

- Dynamic, static and both aspects
- Cryptographic methods with public key (asymmetric method) and shared key (symmetric method)

- Authentication of broadcast, multicast and uni-cast messages

Authentication mechanism feature provide precaution against impression, replay attacks and forgery attacks [4]. There can be various types of attacks in wireless sensor networks like acknowledgement spoofing, HELLO flood attacks, selective forwarding, denial of service attacks etc. It is not easy to identify each type of attack & unauthorized user access but some new authorization protocols are proposed that are efficient in WSN security, privacy & efficiency aspects. As per the security aspects of WSN, there are different challenges & requirements related to freshness, integrity, authorization, availability, non repudiation, data confidentiality and authentication [5].

In this paper, various existing research methods on the security, efficiency & privacy aspects of handover authentication protocol in WSN are presented. Handover authentication protocol [6] ensures the secure transmission of data for registered Mobile Nodes (MN) on Authentication Server (AS) from one Access Point (AP1) to second Access Point (AP2) by establishing a session key between the MN and AP2. But there are various challenges & issues in the design of handover authentication protocol related to efficiency, privacy and security due to limited power & processing capabilities of MNs and time bound handover process. Also various kinds of attacks like Denial of Service (DoS) attacks is there that interrupt the privacy and security of data. The presented paper discusses the existing work on handover authentication protocol.

Rest of the paper is presented in the following manner. Section II presents the basic concept of handover authentication protocol. Section III discusses the existing work on handover authentication protocol in WSN with some key features. Section IV concludes the paper with some future directions.

II. HANDOVER AUTHENTICATION PROTOCOL

Handover Authentication Protocol enables the mobile nodes to successfully switch from the base station to another without any service loss during data transmission from base station in wireless networks [7]. The key elements of handover authentication protocol are Authentication Server (AS), Access Point (AS) and Mobile Node (MN). Initially, each MN is registered on AS with their identity and generated a secret key. Then, MN can connect with any AP using the authentic secret key and identity. Whenever, MN switch from one AP1 to another AP2, then AP2 authenticate MN and a session key is generated between the MN and AP2. This complete process is known as handover authentication protocol as shown in figure 2.

Wireless networks are easily vulnerable to attacks due to non-existence of any physical network connection. So, privacy, efficiency & security are the major concerns in this protocol. A typical handover authentication protocol should meet the security, efficiency & privacy requirements of attack resistance, provision of user revocation, conditional privacy preservation, user anonymity & untraceability, key establishment, server authentication and subscription validation.

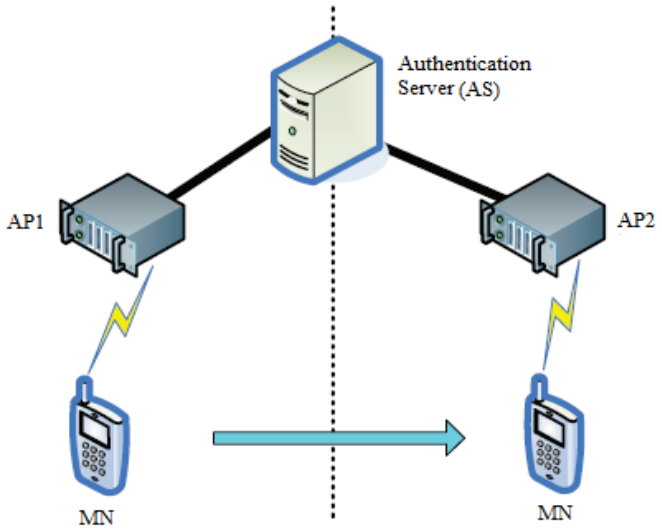

Figure 2: Handover Authentication Protocol

III. EXISTING WORK ON HANDOVER AUTHENTICATION PROTOCOL

This section explores the existing work on Handover Authentication Protocol in Wireless Sensor Network. Handover Authentication Protocol is analysed on the basis of security, privacy and efficiency aspects. Different authors have used different approaches in handover authentication protocol. The analysis of these different research methods is also shown in table I.

He et al. (2012a) [8] have proposed a novel PairHand approach based on Handover Authentication Protocol. In PairHand approach, Bilinear Pairing based cryptographic security process is used that shows better efficiency due to incorporation of batch signature verification process. There is the requirement of only two handshakers b/w mobile node & access point for verification and does not need other kind of public key cryptosystems. Also there is no any requirements of group signature, ring signature or blind signature approach. PairHand protocol only supports the conditional privacy based user revocation. PairHand protocol is also resistance from DoS attacks as it supports light weight verification polynomial based approach. PairHand protocol shows efficient performance results as compare to smart card based authentication method, chameleon hashing and Priauth protocol.

He et al. (2012b) [9] further enhanced the existing PairHand protocol in handover authentication method. Authors have identified the weakness in the existing PairHand approach and fixed the security issues without the loss of any other feature. In existing PairHand protocol, there was the problem related to cryptography based session key corresponding to pseudonym. This problem would be resolved if cyclic group order 'q' and hash function signature key $H_2(M_i)$ will be non coprime. So, In this enhanced PairHand protocol, the order of cyclic multicative group G_T and cyclic additive group G is initially fixed. In this way, enhanced PairHand protocol has fixed the weakness of existing PairHand protocol.

Tsai et al. (2013) [10] have proposed the concept of bilinear pairing based handover authentication protocol that adapt the pseudonyms to give user anonymity. The proposed concept also provides user unlinkability as there is only the authentication server AS that knows the identity of mobile node MN. This bilinear pairing approach is based on random oracle model and shows the security against the denial of service attacks. To evaluate the efficiency and security aspects of bilinear pairing, it is compared with enhanced PairHand protocol which is also a type of handover authentication protocol. Overall proposed concept shows efficient results also in terms of computational costs as compare to enhanced PairHand protocol.

He et al. (2013c) [11] have proposed the Handauth based approach that adds the privacy aspects in existing handover authentication protocol. In privacy terms, Handauth protocol provides session key establishment and user authentication. Authors have mentioned the various features for Handauth protocol like attack resistance, dynamic user revocation, easily scheduled revocation, access point authentication, access service expiration management, AAA server anonymity, conditional privacy preservation, forward secure user revocation, untraceability of user and their anonymity. Authors have used AVISPA tool for the security analysis of proposed Handauth protocol. Authors have used the parameters of communication overhead and authentication latency for performance evaluation. Handauth protocol shows efficient results as compare to SFRIC and Chameleon hashing protocols for the considered parameters.

Lee and Bonnin (2013) [12] have proposed a novel authentication approach of handover optimized ticket based authentication scheme. In this protocol, mobile node can reuse the credentials provided by authentication server during the handover access of different access point networks. The reuse of authentication credential simplifies the handover authentication and reduces the handover latency. To analyze the performance of proposed HOTA approach parameters of handover failure probability, packet loss and handover latency were considered and shows efficient performance as compare to older approach for PMIPv6 protocol. The proposed HOTA approach is analyzed with formal BAN logic authentication method.

Wang and Hu (2014) [13] have presented the existing work on PairHand based handover authentication protocol. Further, authors have proposed an improved PairHand protocol by analyzing the security weakness in existing PairHand approach. In improved PairHand approach, captured signatures are reduced by introducing linear combination method for key recovery attack. With the same pseudo-ID attacker can easily detect the private key of mobile node. So, improved PairHand approach use the random oracle model and provides both the authentication and semantic security aspects. From the evaluated results, authors have shown the greater efficiency and security with secret key size of Improved PairHand approach as compare to original PairHand protocol and Tsai et al.'s Bilinear pairing based authentication protocol.

Mapoka et al. (2015) [14] have proposed HOISKA approach for the high mobility mobile multicast. HOISKA is handover optimized authentication scheme based on independent session key per access network. Authors have developed this approach for decentralization of multi-service group key chain management scheme. HOISKA entail the reuse of initial issued access credentials to mobile nodes for the multicast multi-services. Due to decentralization of authentication functions in wireless networks, handover authentication process becomes easy and efficient. Authors have compared the performance of HOISKA with EAP-TLS based on the parameters of handover latency and authentication cost. In this comparative analysis, HOISKA shows lesser handover blocking probability and handover delays as compare to EAP-TLS.

Kumar and Om (2015) [15] have proposed a fast authentication approach for the wireless local area networks. The considered protocol supports fast handover as it is based on mutual authentication that there is no any requirement of access from authentication server for mobile nodes due to use of two way handshake protocol. Proposed concept is analyzed on the basis of authentication delay and transmission cost. Based on these parameters, proposed fast authentication protocol shows efficient results as compare to PairHand protocol and SFRIC approach.

He et al. (2015d) [16] have identified the some security challenges in enhanced PairHand protocol. Authors have identified that existing protocol bears the problem of private key compromisation. To overcome this security issue, authors

have proposed an ID based signature protocol (IBS). This protocol increases some computational costs but overcomes the security challenges of enhanced PairHand protocol. IBS protocol shows efficient results as compared with PairHand protocol on the basis of security and efficiency aspects.

He et al. (2015e) [17] have proposed a novel HashHand named handover authentication protocol. Initially, authors have presented the standard aspects required for efficient & secured handover authentication protocol. Further they analyzed the existing protocol for security and efficiency aspects. They have also analyzed the well known PairHand authentication protocol and identified some security threats. Authors have proposed HashHand protocol by adding the merits of PairHand protocol, eliminating security vulnerability and introducing session key update mechanism. In HashHand protocol, security is maintained by features of key update, server authentication, subscription validation and key establishment. Overall HashHand protocol maintains security and shows efficient results as compare to PairHand protocol.

TABLE I
Analysis of Existing Handover Authentication Protocol

Authors & Year	Method Used	Compared with	Key Features
Lee and Bonnin (2012) [8]	Handover Optimized Ticket based Authentication Scheme (HOTA)	BAN logic authentication method	• Mobile node can reuse the credentials provided by authentication server during the handover access of different access point networks. • Parameters of handover failure probability, packet loss and handover latency were considered and shows efficient performance as compare to considered approach for PMIPv6 protocol.
He et al. (2012a) [9]	PairHand approach	Smart Card based Authentication method, Chameleon Hashing and Priauth Protocol	• Bilinear Pairing based cryptographic security process. • Incorporation of batch signature verification process. • Protocol is also resistance from DoS attacks as it supports light weight verification polynomial based approach.
He et al. (2012b) [10]	Enhanced PairHand protocol	PairHand Protocol	• Identified the security weakness in the existing PairHand approach. • Order of cyclic multicative group G_T and cyclic additive group G is initially fixed.
Tsai et al. (2013) [11]	Bilinear Pairing based handover authentication	Enhanced PairHand protocol	• Adapt the pseudonyms to give user anonymity. • Provides user unlinkability. • Based on random oracle model.
He et al. (2013c) [12]	Handauth Protocol	SFRIC and Chameleon Hashing Protocol	• Provides session key establishment and user authentication.

			• AVISPA tool is used for the security analysis.
Wang and Hu (2014) [13]	Improved PairHand protocol with linear combination	PairHand protocol and Tsai et al.'s Bilinear Pairing based authentication protocol	• With the same pseudo-ID attacker can easily detect the private key of mobile node. • Use the random oracle model. • Provides both the authentication and semantic security aspects.
Mapoka et al. (2015) [14]	HOISKA approach	EAP-TLS approach	• Approach for the high mobility mobile multicast. • Decentralization of multi-service group key chain management scheme.
Kumar and Om (2015) [15]	Fast Handover Authentication Approach	PairHand protocol and SFRIC approach	• Based on mutual authentication. • Proposed concept is analyzed on the basis of authentication delay and transmission cost.
He et al. (2015d) [16]	ID based signature protocol (IBS)	PairHand protocol	• Identified that existing protocol bears the problem of private key compromisation. • Protocol increases some computational costs but overcomes the security challenges of PairHand protocol.
He et al. (2015e) [17]	HashHand Protocol	PairHand protocol	• HashHand protocol adds the merits of PairHand protocol, eliminating security vulnerability and introducing session key update mechanism. • Security is maintained by features of key update, server authentication, subscription validation and key establishment.

IV. CONCLUSION

There are different protocols of wireless sensor network that can provide authentication of wireless networks. Handover authentication protocol has attracted the researchers due to their efficient and security aspects of handover mobile node communication approach.

In this paper, we have presented the work of different researchers to improve the security, privacy and efficiency aspects of handover authentication protocol. Different authors have presented their work in their prospective with different comparison parameters. Here, the approaches of HOTA, PairHand approach, Enhanced PairHand approach, Handauth, HashHand, IBS approach, HOISKA and bilinear based approach. The analysis evaluation of the work is also presented. After many improvements, HashHand is the more efficient protocol in the field of Handover Authentication Protocol as compare to other protocols.

V. FUTURE SCOPE

In this paper, our main focus was the analysis of different security, privacy and efficiency aspects of handover authentication protocols in wireless sensor network. Different authors presented their work in well efficient manner. But there is the further need of improvement in the security as mobile nodes are easy to vulnerable for the outer attacks. More efficient approaches can be proposed by considering mutual handshake authentication process with their security check of ID authentication of mobile node and session keys.

REFERENCES

[1]. Cairncross, Frances. *The death of distance: How the communications revolution is changing our lives*. Harvard Business Press, 2001.

[2]. Sen, Jaydip. "A survey on wireless sensor network security." *arXiv preprint arXiv:1011.1529* (2010).

[3]. Wong, Kirk HM, Yuan Zheng, Jiannong Cao, and Shengwei Wang. "A dynamic user authentication scheme for wireless sensor networks." In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, vol. 1, pp. 8-pp. IEEE, 2006.

[4]. Rajeswari, S. Raja, and V. Seenivasagam. "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks." *The Scientific World Journal* 2016 (2016).

[5]. Vaidya, Binod, Jorge Sá Silva, and Joel JPC Rodrigues. "Robust dynamic user authentication scheme for wireless sensor networks." In *Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks*, pp. 88-91. ACM, 2009.

[6]. Islam, S. K., and Muhammad Khurram Khan. "Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks." *International Journal of Communication Systems* (2014).

[7]. Jing, Qi, Yuqing Zhang, Anmin Fu, and Xuefeng Liu. "A privacy preserving handover authentication scheme for EAP-based wireless networks." In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pp. 1-6. IEEE, 2011.

[8]. He, Daojing, Chun Chen, Sammy Chan, and Jiajun Bu. "Secure and efficient handover authentication based on bilinear pairing functions." *IEEE Transactions on Wireless Communications* 11, no. 1 (2012a): 48-53.

[9]. He, Daojing, Chun Chen, Sammy Chan, and Jiajun Bu. "Analysis and improvement of a secure and efficient handover authentication for wireless networks." *IEEE Communications Letters* 16, no. 8 (2012b): 1270-1273.

[10]. Tsai, Jia-Lun, Nai-Wei Lo, and Tzong-Chen Wu. "Secure handover authentication protocol based on bilinear pairings." *Wireless personal communications* 73, no. 3 (2013): 1037-1047.

[11]. He, Daojing, Jiajun Bu, Sammy Chan, and Chun Chen. "Handauth: Efficient handover authentication with conditional privacy for wireless networks." *IEEE Transactions on Computers* 62, no. 3 (2013c): 616-622.

[12]. Lee, Jong-Hyouk, and Jean-Marie Bonnin. "HOTA: Handover optimized ticket-based authentication in network-based mobility management." *Information Sciences* 230 (2013): 64-77.

[13]. Wang, Weijia, and Lei Hu. "A secure and efficient handover authentication protocol for wireless networks." *Sensors* 14, no. 7 (2014): 11379-11394.

[14]. Mapoka, Trust T., Simon J. Shepherd, Raed Abd-Alhameed, and K. O. Anoh. "Handover Optimised Authentication Scheme for High Mobility Wireless Multicast." In *15th International Conference on Computer Modelling and Simulation (UKSim2015)*. 2015.

[15]. Kumar, Amit, and Hari Om. "A Secure Seamless Handover Authentication Technique for Wireless LAN." In *2015 International Conference on Information Technology (ICIT)*, pp. 43-47. IEEE, 2015.

[16]. He, Debiao, Muhammad Khurram Khan, and Neeraj Kumar. "A new handover authentication protocol based on bilinear pairing functions for wireless networks." *International Journal of Ad Hoc and Ubiquitous Computing* 18, no. 1-2 (2015d): 67-74.

[17]. He, Daojing, Sammy Chan, and Mohsen Guizani. "Handover authentication for mobile networks: Security and efficiency aspects." *IEEE Network* 29, no. 3 (2015e): 96-103.