Volume: 05, Issue: 02, Pages:1908-1912 (2013) ISSN : 0975-0290

Secure and Efficient Vertical Handover in Heterogeneous Wireless Networks

Muhammad Waseem Khan
Department of Computer Science, COMSATS Instituite of Information Technology, Wah Cantt
Email: muhammad.wasim1@gmail.com

ABSTRACT

Handover occurs when a wireless node switches from one network to another. One of the main requirements of this process is to make it secure by using reliable security mechanisms, but it can decrease performance as well. So it is very essential to maintain balance between security and performance during handover. Different handover security schemes that can provide reliable security as well as performance to a certain level will be discuss in this paper. The goal of this paper is to know, how to maintain balance between handover security and performance.

Keywords – **CAPWAP, EAP, HOCKEY, MIH, Mobile IP, Vertical Handover.**

Date of Submission : September 04, 2013 Date of Acceptance : October 10, 2013

I. INTRODUCTION

One of the main challenges that fourth generation wireless networks are facing now a days is to maintain network connectivity when a mobile user switches between two different networks[1]. The procedure of migration from one network to another is called handover. If the handover occurs between different networks then it is called vertical handover, but if it occurs within a single network then it is called horizontal handover. In this paper, emphasis will be on vertical handover. IEEE 802.21 Multimedia Independent Handover (MIH) is a standard that assist mobility across heterogeneous networks. Unfortunately, the IEEE 802.21 doesn't provide enough security[2]. So, in order to secure the handover process, strong security solutions must be implemented for heterogeneous networks to maintain security. Meanwhile, security mechanisms make the handover process more complicated in a wireless and mobile environment[3],[4]. Authentication and Authorization are essential to secure the user mobility, but it increase overhead during the handover phase[5]. Hence, in order to gain a balance between handover security and performance, several security schemes used for vertical handover will be discuss in this paper. Section 2 will cover different challenges related to vertical handover, current trends including existing security solutions and comparison between these security solutions. Section 3 contains the proposal of a balanced security mechanism to attain handover security and performance simultaneously. Section 4 presents conclusion.

II. CURRENT CHALLENGES, TRENDS, AND ISSUES

Secure handover management requires the transfer of essential user's credentials and related data between two access networks in a secure manner. However, existing security mechanisms add complexity and overhead to handover management. Hence, it is essential to achieve both efficiency and security at the same time. The trade-off among these two parameters will increase more when service provider is different from network provider[6]. In this condition, it is mandatory for wireless user to get authenticated both from network provider as well as service provider. In such scenario, AAA protocol is used for authentication, which is expensive, since home network is far away from visited network[7]. In order to handle such delays, which lead to performance degradation, different type of handoff management techniques has been proposed by the researchers to improve the handoff process. Mobile IP[8] is a macro-mobility scheme which manages the mobile node's movement between different networks. According to this scheme, mobile home agent updates the care of address (CoA) with mobile node's permanent address, whenever mobile node changes foreign network. Home agent receives the packets from correspondent node, encapsulates and tunneled the packets to visited network having mobile node's CoA, foreign agent will then de-capsulate and forwards them to the mobile node. Although Mobile IP solves the basic problem related to mobility, but it also increases delay, packet loss, and signaling cost as well.

MPA (Media-Independent Pre-Authentication)[9] is another secure and efficient handover scheme. It facilitates the mobile node to obtain target network's IP address, send or receive packets to target network, and complete binding update process before handover. In order to optimize handover after the discovery of target network, pre authentication and SA (security association) occurs between mobile node and authentication agent. Two keys derived from SA. Then, Pre configuration occurs to obtain nCoA when mobile node migrates to nPoA (new point of attachment), now mobile node can communicate with both oCoA and nCoA due to the establishment of tunnel. Binding update and data packets are transmitted using

Volume: 05, Issue: 02, Pages:1908-1912 (2013) ISSN : 0975-0290

tunnel. After completing binding update, mobile node deletes the tunnel and migrates to nPoA. Packet buffering which starts after the deletion of tunnel will stop when 'delete tunnel signal' is received. There are following Cons attach with MPA security scheme, i.e., MPA mechanism can't provide secure transport of messages, and MPA cause packet loss if handover occurs before the completion of binding update.

In MPA, packet loss can occurs if the mobile node starts handoff before the completion of MPA binding update procedure. Dynamic buffering scheme will buffer those packets and guarantee that oAR (old Access Router) will keep the packets sent from correspondent node to the mobile node with oCoA. After handover, oAR will forward those packets to mobile node through nAR.

FMIP (Fast Mobile Internet Protocol)[10] is another scheme to avoid from packet loss, it created a tunnel between mobile node and nAR to forward all packets with oCoA to nAR during handover process. After handover, nAR forward packets to the mobile node.

Enhanced MPA (eMPA)[11] scheme is used to avoid the packet loss which occurs before the completion of binding update procedure during handover. It is based on two steps. Firstly, correspondent node or home agent of mobile node must reply with ACK whenever they receive the binding update message. Secondly, oAR and mobile node need to be modified such that, Mobile node will get the amount of BUAs that were not received yet, oAR will apply IPSec encapsulation technique to the packets sent to the mobile node with oCoA, and replace these packets with a new IP header and nCoA as the destination address, and After the completion of handover, mobile node will check if all BUA packets have been received and then confirm the deletion of IPSec tunnel to the oAR.

The flow of eMPA in figure 4[11] starts with acquisition of IP addresses of AA, CA, and AR. Proactive handover tunnel is established after the process of pre authentication. Then handover occurs, and delete PHT message will be sent to nAR. Here, if mobile node find out that all binding update acknowledgments are not received then it sends IP Sec tunnel message to oAR, which creates IPSec tunnel, meanwhile mobile node perform handover with nAR, during handover if oAR receive packets of mobile node with oCoA, it will forward them to nAR. After handover, nAR will forward BUA packets to mobile node, which it received from home agent, finally, mobile node will send delete IP Sec tunnel message to oAR. As compare to MPA, eMPA can reduce the time of forwarding packets and also reduce the loss of packets.

Security issues that are related to MIH message security are MIH access control, replay protection, and message integrity[12]. IPSec is one of the mechanisms used for data security, especially to protect those messages that run over IP protocols, i.e., IPv6. DTLS (Datagram Transport Layer Security) is another security scheme used to provide security especially for datagram protocols. IPSec and DTLS mechanisms consist on several steps including network information query, resource query, resource reservation, target layer 2 establishment (handover execution) and handover completion. IPSec and DTLS use separate mechanisms for authentication purposes, i.e., IKEv2 and DTLS authentication procedures. These mechanisms add latency in handover process because both schemes require multiple authentications, i.e., L2 authentication and MIH transport authentication simultaneously.

MIHSec[13] is another security mechanism used to reduce the latency overhead attach with IPSec and DTLS schemes. It removes MIH authentication process and use MSK (Master Session Key) to maintain key hierarchy. MIHSec security solution has some advantages, such as, MSK keys are use to maintain key hierarchy as well as to generate keys, it reduces the overhead introduced by multiple authentications in IPSec and DTLS, The handover latency is reduced by eliminating IKE/DTLS authentication procedures, and Confidentiality and message integrity is also achieved through MIHSec. The comparison among IPSec/IKEv2, DTLS, and MIHSec proves that MIHSec is best in order to reduce handover latency.

The Extensible Authentication Protocol (EAP)[14] enables client that request for network access and authentication server to implement authentication process. Authenticator is introduced between both authentication server and client; it passes on EAP messages between authentication server and client. It also distributes ciphering keys, which are used to encrypt data over access link. PANA (Protocol for carrying Authentication for Network Access) is used to enable EAP transportation over IP. PANA session is establish between client and PAA (PANA authenticator) after client discovers the PAA, negotiate parameters and granting of authorization. MSK and authorization lifetime are two parameters of a PANA session state.

PANA Session Transfer[14], also known as Context transfer can reduce the handover delay. After discovering new PAA, the old identifier and authentication token is transmitted. Authorization parameters are determined after authentication of mobile node by old PAA. The intermediate MSK will be sent to the new PAA which confirms successful authentication. These parameters are also used to start new PANA session as well.

Volume: 05, Issue: 02, Pages:1908-1912 (2013) ISSN : 0975-0290

In Make-before-break, mobile node will get configuration parameters for target access router; fulfill the requirement of access link recovery by installing whatever it requires, and adjust its future movement with the help of routing update. It allows mobile node to install PANA session at a target authenticator as well.

Context transfer has several differences and shortcomings as compare to other techniques, i.e., Authorization based on previous authenticator neglect the rule that AAA server[15] is the main entity to decide authorization, if an attacker compute intermediate MSK and determine unencrypted nonces b/w mobile node and authenticator, he can easily compute the new MSK, and the above solution also can't be deployable for inter domain handovers.

EAP has certain drawbacks as far as mobile scenario is concerned, i.e., EAP authentication takes a considerable time, and authentication mechanism is not efficient because frequent round trips are required from point of attachment to user's home domain.

Hence, a fast re-authentication scheme that involves local re-authentication server placed near the mobile user is very essential in such kind of environments.

EAP authentication requires several exchanges and iterative execution whenever a mobile peer migrate to new authenticator, if EAP server resides in peer's home domain, then it can be far away from authenticator, it will leads to signaling latency overhead as well.

3PFH is another authentication mechanism which executed between EAP peer, authenticator, and EAP server. Boot Strapping phase consists on derivation of a key from key hierarchy, it will happens when mobile get access network access for the first time. 3PFH assumes that K_{AS} is shared between peer and server, whereas K_{BS} has been shared between authenticator and EAP server. Fig 2(a)[16] shows the case in which EAP peer share a key between local server and EAP authenticator under same server, and Fig 2(b)[16] is the case when peer go for authentication belongs to a local server with whom peer doesn't share any key.

The multilayer pseudonym architecture improves privacy during bootstrapping and fast re-authentication phases. Requirements of this process are including user anonymity and un-traceability. According to this architecture, permanent identity is not enough for mobile user to get recognized during network access, but also has assigned three types of pseudonyms including Bootstrapping Pseudonym, Home Fast Pseudonym, and Visited Fast Pseudonym. BP used during EAP authentication and has only one instance at any time, HFP used in fast re-authentication process which includes fast re-authentication server, and VFP is selected by the peer when performs handover with a new authenticator.

Fig 3[16] represents a four layer pseudonym graph; first layer is of PI (Permanent Identity), and remaining layers consists of three different pseudonyms. Relationships exist between pair of pseudonyms as well. Intra-layer relationship is the relationship exists between pseudonyms of same layer, whereas inter-layer relationship exists between pseudonyms of different layers. Hence relationship exists between all layers depicts transitive relationship as well. The problem occurs if eavesdropper find the value of new pseudonym during distribution, and relate it with previous pseudonym, then he can get access to the graph of relationships as well. So, privacy enhanced BP and privacy enhanced FP is introduced to avoid from such problems. EAP-EXT method is introduced which support privacy related operations during BP phase.

Local Administrative Domain (LAD)[8] with localized optimization is another mechanism to gain a balance between security and performance because it is easy to enhance the performance and handover security at the same time by implementing optimization within administrative domain. With the help of EAP-AKA and ERP re-authentication mechanism, less security signaling is required, which decrease latency overhead as well. EAP-AKA and ERP done the process of re-authentication without involving home server, it require only one RTT between mobile node and local server to complete re-authentication process, hence it results a good performance as well. Overall handoff completion time reduces with the help of local AAA operation. Energy consumed during security and mobility signaling reduces with the help of Proxy Mobile IP. Bandwidth of wireless link will increases rapidly with the help of EAP-AKA and EAP re-authentication mechanisms.

CAPWAP (Control and provisioning of wireless APs)[17]play a role of central authority and manage all APs. WLAN deployment is split into two parts: Fat AP, implements IEEE 802.11 protocol and Thin AP implement lower portion of MAC and PHY layer. Authentication and Access Control reside on AC (Access Controller) allow clients to connect any WTP (Wireless Termination Point). After initial authentication, session key is deliver to AC using CAPWAP. After mobile node discovers new WTP, AC runs a 4-way handshake in order to deliver new traffic key.

HOKEY (Handover Keying)[17, 18] supports handover from one AP to another AP belong to different network and also roaming b/w different operators. Since, Credentials are stored at the local server, so Authentication process become fast, and local HOCKEY server, co-located with visited n/w AAA server get keys using AAA protocols.

In IEEE 802.11r[17], the initial AP acts as an authenticator, communicate with AAA server. After that each AP interacts with initial AP rather than directly with AAA server. The important property of IEEE 802.11r is key management and key transfer protocol between R0kh (R0 key holder), since it holds PMKR0 and R1kh (R1 key holder), since it holds PMKR1.

HOKEY is the only scheme that can support domain level keys and is the only handover scheme supporting inter-enterprise routing. CAPWAP is simple at application level, since it can use PMK; reside at centralized AC to derive multiple traffic keys. Handoff process time of

Volume: 05, Issue: 02, Pages:1908-1912 (2013) ISSN : 0975-0290

CAPWAP, HOCKEY, and IEEE 802.11r are 85us, 130us, and 70us respectively.

In order to reduce the EAP authentication latency during handover, many protocols have been proposed including security context transfer, i.e., security context keys are transfer to target BS from service BS, Key hierarchy is used to reduce authentication delay by utilizing new key hierarchy designed for handover keying purpose, and Kerberos style ticket use Kerberos to distribute keys to target authenticator. A new ticket-based HO authentication scheme based on IEEE 802.16m[19], i.e., Multicast and Broadcast Service (MBS) reduce handover delay without using TGS. This scheme allows only the legitimate MS to access IEEE 802.16m network.

III. DISCUSSION

In order to reduce the latency overhead of authentication process, HOCKEY as a localized re-authentication mechanism within an access domain should be used. It consists of a collection of sub-nets, network entities, and AAA database under a common administration. This approach eliminates the latency overhead coming from multiple rounds of authentication exchanges between a mobile node and its home network. Optimization can be implemented in the domain to enhance the performance and handover security. When a mobile node leaves its home network and enters into LAD, handover occurs and this handover will be handled by the responsible local domain. When the mobile node changes its access point, i.e., point of attachment within the LAD, localized handover mechanism will be used to provide a good level of security and performance.

IV. CONCLUSION

To understand the interaction between performance and handover security, I analyze different security schemes that can provide handover security as well as performance to some extent. Comparison between these schemes depicts that security and performance during handover process are interrelated. In order to seek a balance between handover security and performance, local administrative domain with localized security optimization using HOCKEY mechanism is proposed to promote handover performance. I intend to extend my research work in the field of vertical handover in order to improve performance and provide sufficient security simultaneously.

ACKNOWLEDGEMENTS

I acknowledged COMSATS Institute of Information Technology, Pakistan to support us in this work.

REFERENCES

[1] K. Meriem, *et al.*, "An intelligent handover management system for future generation wireless networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, 2008.

[2] A. A. Muhammad Sharif, Mudassar Raza,Waqas Haider, "A Novel Wormhole Detection Technique for Wireless Ad Hoc Networks," *Int. J. Advanced Networking and Applications*, vol. 3, pp. 1298-1301, 2012.

[3] M. S. Bilal Ahmad Khan, Mudassar Raza,Tariq Umer,Khalid Hussain,Aman Ullah Khan, "An Approach for Surveillance Using Wireless Sensor Networks (WSN)," *Journal of Information & Communication Technology*, vol. 1, pp. 35-42, 2007.

[4] M. M. Muhammad Sharif, Waqas Haider,Mudassar Raza, "Priority Based Congestion Control Routing in Wireless Mesh Network," *Int. J. Advanced Networking and Applications*, vol. 3, pp. 1147-1151, 2011.

[5] G. Karopoulos, *et al.*, "Survey of secure handoff optimization schemes for multimedia services over all-IP wireless heterogeneous networks," *IEEE Communications Surveys and Tutorials*, vol. 9, pp. 18-28, 2007.

[6] W. Haider, *et al.*, "The Realization of Personalized E-Learning platform based on 3G Mobile phone and NGN control frame work for SIP based IP Networks," *Research Journal of Recent Sciences ISSN*, vol. 2277, p. 2502.

[7] K. H. Faraz Ahsen, Nyla Khadam,Muhammad Sharif,Noor Zaman, "Conservation of flow with Lossy Channel in Wireless Mesh Network," *Journal of Information & Communication Technology*, vol. 1, pp. 10-20, 2007.

[8] Y. Ding, "Securing Handover in Wireless IP Networks," M.Sc, Department of Computer Science, UNIVERSITY OF HELSINKI, Helsinki, 2009.

[9] A. Dutta, *et al.*, "Media-independent pre-authentication supporting secure interdomain handover optimization," *Wireless Communications, IEEE*, vol. 15, pp. 55-64, 2008.

[10] D. S. Nursimloo, *et al.*, "A two-layered mobility architecture using fast mobile IPv6 and session initiation protocol," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, p. 24, 2008.

[11] L.-H. Yeh, *et al.*, "An enhanced media-independent pre-authentication framework for preventing packet loss," in *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*, 2010, pp. 284-288.

[12] W. Jeong-Jae, *et al.*, "Secure media independent handover message transport in heterogeneous networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[13] G. Li, *et al.*, "Secure Access Authentication for Media Independent Information Service," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, 2010.

[14] D. B. Brahim Gaabab, Jean-Marie Bonnint, "Authentication Optimization for Seamless Handovers," presented at the IEEE, France, 2007.

Volume: 05, Issue: 02, Pages:1908-1912 (2013) ISSN : 0975-0290

[15] M. SONG, *et al.*, "A secure fast handover scheme based on AAA protocol in mobile IPv6 networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, pp. 14-18, 2008.

[16] F. Pereniguez, *et al.*, "Privacy-enhanced fast re-authentication for EAP-based next generation network," *Computer Communications*, vol. 33, pp. 1682-1694, 2010.

[17] T. Clancy, "Secure handover in enterprise WLANs: capwap, hokey, and IEEE 802.11 R," *Wireless Communications, IEEE*, vol. 15, pp. 80-85, 2008.

[18] X. Zheng and B. Sarikaya, "Handover keying and its uses," *Network, IEEE*, vol. 23, pp. 27-34, 2009.

[19] A. Fu, *et al.*, "A fast handover authentication mechanism based on ticket for IEEE 802.16 m," *Communications Letters, IEEE*, vol. 14, pp. 1134-1136, 2010.

Authors Biography

Muhammad Waseem Khan is a student of MS (Computer Science) at COMSATS Institute of Information Technology, Wah Campus, Pakistan. He has completed his Bachelor degree from COMSATS Institute of Information Technology, Lahore in 2010. His areas of interest are Image Processing, Information Security and Mobile Computing.