A Fast Handover Scheme between WiFi and WiMAX Networks

Hung-Min Sun[1], Shuai-Min Chen[1], Yao-Hsin Chen[1], Heng-Jeng Chung[1], I-Hung Lin[2]

[1]*Dept. of Computer Science, National Tsing Hua University, HsingChu, Taiwan, R.O.C*

[2]*Networks & Multimedia Institute, Institute for Information Industry, Taipei, Taiwan, R.O.C*

hmsun@cs.nthu.edu.tw

Abstract With the rapid development of wireless communication, mobile users are desirous to handover between different types of network interfaces. The IEEE 802.21 Draft Standard was proposed to integrate the Media Independent Handover (MIHs) between the wireless network interfaces, such as WiFi, WiMAX, 3GPP, and 3GPP2. It aims to provide completed handover architectures for the ubiquitous goal. However, the IEEE 802.21 Draft Standard may not hold the seamless roaming character and does not provide the security mechanism.

In this paper, we propose an efficient handover mechanism between WiFi and WiMAX networks to meet the seamless roaming character by reducing the authentication processes. In addition, the proposed scheme involves security mechanisms that guarantee the handover messages to be secure.

Keywords: 802.21, MIH, Handover, WiFi, WiMAX.

1. INTRODUCTION

In recent years, wireless technologies, such as WiFi [8] , WiMAX [9] , 3GPP [10] , 3GPP2 [11] have become more popular in our daily life. Users can connect to the Internet by using one of these wireless technologies. However, none of these network interfaces provides the mechanisms to handover between heterogeneous networks, i.e., vertical handover. On the other hand, users can not directly handover between different wireless technology interfaces since the media types are incompatible. Therefore, in order to solve this defect, the IEEE 802.21 Draft Standard [12] has been instituted to make vertical handover possible. The IEEE 802.21 Draft Standard presents Media Independent Handover Functions, called MIHFs. To optimize vertical handover, IEEE 802.21 Draft Standard provides link layer intelligence and other related network information upon upper layer. For this reason, any two wireless technology interfaces can exchange handover information via MIHF to achieve vertical handover. This can make handover between heterogeneous environments to be realizable. Moreover, the applications and services of wireless technology become more convenient and effective. Although IEEE 802.21 Draft Standard presents solutions for vertical handover, it does not include any security mechanisms in handover protocols. In other words, it still remains a critical problem when implements it. Moreover, it may not hold the seamless roaming character.

Since WiFi and WiMAX technologies are more popular than the others, the handover mechanisms between WiFi and WiMAX are demanding first. Therefore, we propose a secure and efficient vertical handover protocol between IEEE 802.11 Standard [13] (WiFi) and IEEE 802.16 Standard [5] (WiMAX) based on the IEEE 802.21 Draft Standard. Traditionally, a Mobile Station (MS) must re-authenticate with the target NAS (Network Access Server) when handovers from one network to another. In other words, the authentication process should be executed again and consequently is time consumed. Due to this defect, the proposed scheme enables mobile users to handover between two heterogeneous wireless networks without executing the entire authentication. Instead, the proposed scheme allows the mobile user to execute reduced authentication steps which greatly saves the time spent when handover occurred. In the meanwhile, the proposed scheme provides security functionality by adopting IP Security (IPSec) [17] [18] as the basis of the security infrastructure to protect handover information.

The main idea of the proposed scheme is to inherit the Master Session Key (MSK) from the serving network to candidate network by securely transferring the MSK. By means of re-using the MSK, the authentication processes at the candidate network can be reduced greatly. Besides, the proposed scheme applies IPSec to provide secure communication for some information of the handover process.

The rests of this paper are organized as follows. Section 2 describes the background knowledge of

IEEE 802.11, 802.16, and 802.21. Section 3 describes the proposed scheme. Section 4 gives the security and efficiency analysis. Finally, the conclusion is given.

2. RELATED WORKS

2.1. IEEE 802.11

The first version of the IEEE 802.11 Standard was released in 1997. However, it is not completed until IEEE 802.11a Standard is set up in 1999. So far, IEEE 802.11 Standard has many different versions and the most popular ones are 802.11a [1] , 802.11b [2] and 802.11g [3] .

The IEEE 802.11 Standard adopts Wired Equivalent Privacy (WEP) [1] to authenticate the mobile station and the NAS. However, WEP was found security weaknesses [14] . Recently, the IEEE 802.1x Standard [6] specifies a stronger and more secure authentication method, PACP (Port Access Control Protocol). PACP adopts EAP (Extensible Authentication Protocol) [15] to generate Master Session Key (MSK) to guarantee the secrecy. PACP will use the generated key iterated. In addition, EAP-TLS [15] which is a kind of the EAP provides a secure mechanism and negotiates a secure PMK (Pair-wise Master Key) between the MS and NAS. PMK can be used to derive other keys to encrypt the transmitted messages between the AP and MS.

2.2. IEEE 802.16

In the progress of IEEE 802.16 Standard, the IEEE 802.16d Standard [4] was proposed in 2004. It is generally called “fixed WiMAX” (fixed Worldwide Interoperability for Microwave Access), created by WiMAX Forum [9] , but it does not support for mobility. The second standard is IEEE 802.16e Standard [5] , proposed in 2005. It is introduced to support for mobility, and is, therefore, called “mobile WiMAX”. Consequently, the IEEE 802.16e Standard is supported for mobile environment.

The authentication processes and key management protocol of IEEE 802.16e Standard is Privacy Key Management protocol version 2 (PKM_{v2}) [5] . It also adopts EAP method to generate MSK and PMK, which are used for MS and BS to communicate securely.

2.3. IEEE 802.21

To optimize handovers between heterogeneous environments, the IEEE 802.21 Draft Standard [12] has been specified in 2008. It provides link layer information and other related network information upon upper layer. It makes vertical handover possible. Since the IEEE 802.21 Draft Standard provides a solution of vertical handover, it improves the user experience of mobile devices. Mobile users can handover among different wireless network interfaces freely by launching the handover processes. Till now, mobile users should handover manually by disconnecting with the serving network and then connecting with a candidate network, independently. This inconvenience reveals the importance of vertical handover.

The IEEE 802.21 Draft Standard has the MIH functions, which provide the following services: (a) media-independent event service (MIES), (b) media-independent command service (MICS), and (c) media-independent information service (MIIS). The MIES provides event reporting corresponding to dynamic changes in link quality, link status, and link characteristics. The MICS enables users to manage and control link behaviors. The MIIS provides detail information about serving and neighboring networks. It will indicate which candidate network is suitable for the user to handover.

3. THE PROPOSED SCHEME

The proposed scheme focuses on the handover between WiFi and WiMAX. Therefore, we assume there are two RADIUSs servers. One belongs to the WiFi network, named R_{11}, and the other belongs to the WiMAX network, named R_{16}. In addition, we assume that a MS has registered at one wireless environment, and is preparing to handover to another wireless environment. The overall handover processes are classified into three phases and are described as follows.

3.1. Handover from WiFi to WiMAX

Initial Phase

At the beginning, a MS has registered and been authenticated with R_{11} by performing PACP. After executing the authentication process, R_{11} and the MS will share a master session key, MSK. R_{11} will relay the MSK to AP for further access between AP and the MS. See figure 1.

Once the handover occurred, the preceding handover steps will be transferred first, such as measurement report, information query, link going down indication, scan for candidate network, resource availability check, target notification, resource reservation and establish new L2 connection. Due to the insensitiveness of these information, we do not encrypt them.

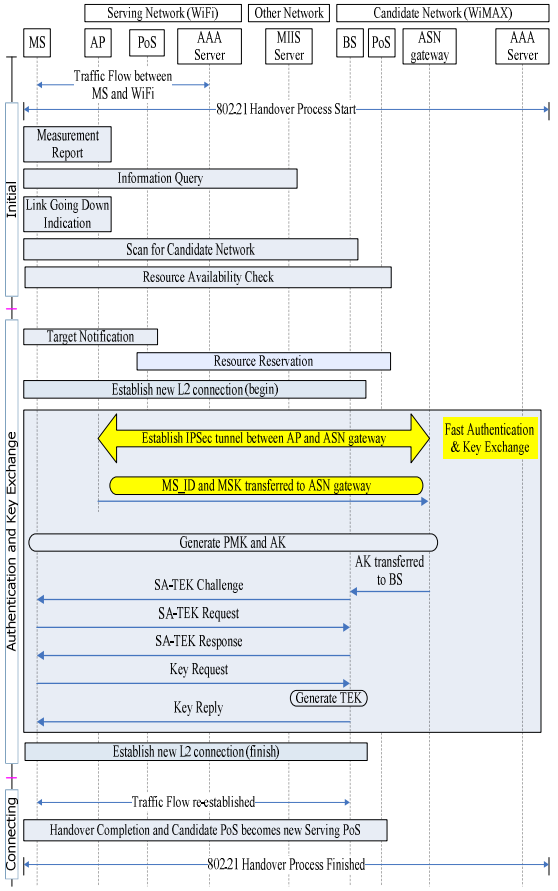

Figure 1. Handover flow chart from WiFi to WiMAX

Authentication and Key Exchange Phase

WiFi and WiMAX have their own authentication and key exchange mechanisms. The IEEE 802.16 Standard adopts PKM_{v2} [5] while IEEE 802.11 Standard adopts PACP [6] . However, both of the PKM_{v2} and PACP execute EAP [6] [15] to generate a Master Session Key. MSK is used for generating and deriving the other session keys, such as PMK, AK, TEK, KEK, PTK and GTK to protect successive transferred messages. In other words, MSK is the most important key used by PKM_{v2} and PACP. Nevertheless, generating MSK through EAP method consumes the most of time at authentication and key exchange phase. When a MS requests for handover, the MSK used in the serving network will be transferred to the candidate network. By re-using the prior MSK, the EAP method can be omitted.

After executing the preceding handover steps, AP and ASN gateway mutually establish an IPSec Tunnel. With the using of IPSec Tunnel, AP and ASN gateway can securely communicate with each other. Then AP transfers the MSK used in WiFi network to the ASN gateway of WiMAX network via the IPSec Tunnel. After that, the sub-keys such as Pairwise Master Key (PMK) and Authentication Key (AK) can be generated by the MS and the ASN gateway as well as PKM_{v2} done. Then, ASN gateway sends the AK to the BS for generating TEK. Since WiMAX directly adopts the MSK used in WiFi, it needs not to execute the entire PKM_{v2}. It just executes the rest steps of the PKM_{v2} and may achieve the seamless character.

Connecting Phase

Finally, “Establish new L2 connection” is finished, and the traffic flow is re-established. Now, the whole handover from WiFi to WiMAX is completed. The MS has successfully handovered to the WiMAX network. The candidate PoS becomes new serving PoS.

3.2. Handover from WiMAX to WiFi

Initial Phase

At the beginning, a MS has registered and been authenticated with R_{16} by performing PKM_{v2}. After executing the authentication process, R_{16} and the MS will share a master session key, MSK. R_{16} will relay the MSK to ASN gateway for generating other keys, such as AK and TEK used between BS and the MS. See figure 2.

Once the handover occurred, the preceding handover steps will be transferred first, such as measurement report, information query, link going down indication, scan for candidate network, resource availability check, target notification, resource reservation and establish new L2 connection. Due to the insensitiveness of these information, we do not encrypt them.

Authentication and Key Exchange Phase

WiFi and WiMAX have their own authentication and key exchange mechanisms. The IEEE 802.16 adopts PKM_{v2} [5] while IEEE 802.11 adopts PACP [6] . However, both of the PKM_{v2} and PACP execute EAP [6] [15] to generate a Master Session Key. MSK is used for generating and deriving the other session keys, such as PMK, AK, TEK, KEK, PTK and GTK to protect successive transferred messages. In other words, MSK is the most important key used by PKM_{v2} and PACP. Nevertheless, generating MSK through EAP method consumes the most of time at authentication and key exchange phase. When a MS requests for handover, the MSK used in the serving network will be transferred to the candidate network. By re-using the prior MSK, the EAP method can be omitted.

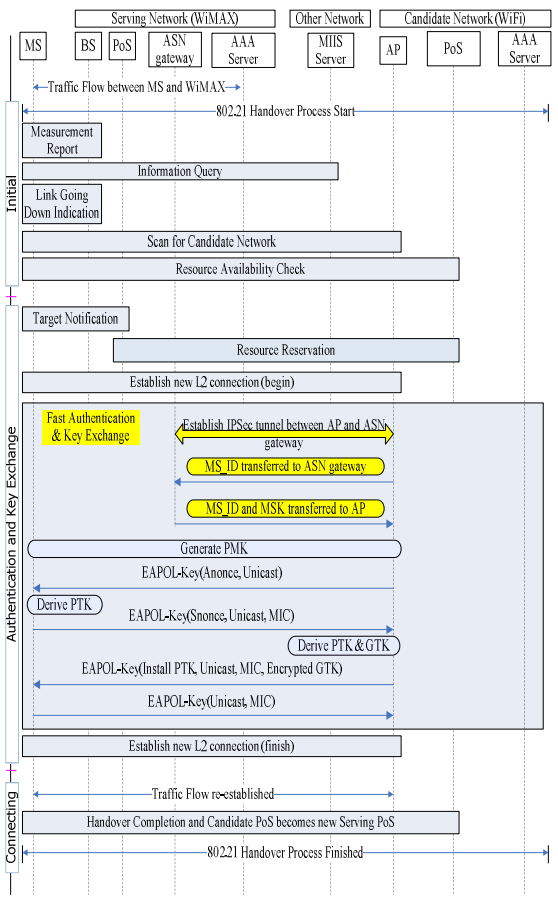

Figure 2. Handover flow chart from WiMAX to WiFi

After executing the preceding handover steps, AP and ASN gateway mutually establish an IPSec Tunnel. With the using of IPSec Tunnel, AP and ASN gateway can securely communicate with each other. Then AP first transfers the identity of the MS, i.e., MS_ID to inform the ASN gateway to transfer the corresponding MSK. After that, the sub-keys such as PMK, PTK and GTK can be generated by the MS and the AP with 4-way handshakes as well as PACP done. Since WiFi directly adopts the MSK used in WiMAX, it needs not to execute the entire PACP. It just executes the rest steps of the PACP and may achieve seamless character.

Connecting Phase

Finally, "Establish new L2 connection" is finished, and the traffic flow is re-established. Now, the whole handover from WiMAX to WiFi is completed. The MS has successfully handovered to the WiFi network. The candidate PoS becomes new serving PoS.

4. SECURITY AND EFFICIENCY ANALYSIS

In the IEEE 802.21 Draft Standard, it tends to provide the mechanisms of vertical handover and tries to meet the seamless requirement. However, it does not provide any security infrastructure [12] . In addition, the seamless character is a goal it would like to achieve, instead of what they have done. Hence, the proposed secure and efficient handover authentication scheme can conquer these two problems.

4.1. Security Analysis

The proposed scheme adopts IPSec in IP layer. IPSec is a collection of some protocols, such as IKE_{v2} [7] and it is originally designed for the security consideration. On the other hand, there is no security mechanism at the latest version of the IEEE 802.21 Draft Standard, the combination of IPSec and IEEE 802.21 Draft Standard will be one of the appropriate solutions. With the using of IPSec, the system provides the security functionality to assure the secrecy and confidentiality. Hence, the most important secret key MSK can be transferred securely in which we do not worry about forgery attack or sniffing attack.

Regards with the reduced authentication and key exchange phase, we omit the EAP processes to decrease the handover duration. It can greatly save the time to achieve the seamless character. Although we skip the EAP processes, the candidate network can trust the authenticity of the MS by securely communicating with the serving network through IPSec Tunnel. In other words, the candidate network trusts the authenticity of MSK that the serving network sent. In addition, we use the prior generated MSK immediately, the other keys can be generated from the reduced PKM_{v2} or PACP protocols. Consequently, the proposed scheme keeps the security requirements of PKM_{v2} and PACP.

4.2. Efficiency Analysis

With the key exchange of MSK, MS can handover to the candidate network faster. The document of IEEE 802.21 Draft Standard figures out that when a MS handovers to a new network environment, the MS should execute a complete authentication processes and key exchange operations of PACP or PKM_{v2}, respectively. However, the connection will break down temporally. Although the IEEE 802.21 Draft Standard provides the mechanisms of aspects of QoS towards enabling seamless mobility, the MIHF alone still can not guarantee the seamless mobility [12] . Thus, the original handover of IEEE 802.21 Draft Standard will result in seamless problems. Fortunately, the proposed scheme reduces the complicated authentication and key exchange processes and may

provide the feature of seamless connection.

5. CONCLUSIONS

In the IEEE 802.21 Draft Standard, there is no security mechanisms been applying to. Moreover, the vertical handover mechanisms may not hold the seamless character. In this paper, we propose a secure and efficient handover mechanism between WiFi and WiMAX. The proposed scheme accomplishes vertical handover between WiFi and WiMAX wireless networks, and reduces the authentication and key exchange processes of IEEE 802.21 Draft Standard.

For the security aspect, the proposed scheme adopts IPSec to provide security protections during the vertical handover process and in this scheme we keep the original security level for the existing wireless networks. On the other hand, for the time efficiency aspect, the proposed scheme does not need to re-execute the whole steps of the authentication and key exchange processes. Consequently, it could hold the features of seamless character.

6. ACKNOWLEDGE

This study is conducted under the “III Innovative and Prospective Technologies Project” of the Institute for Information Industry which is subsidized by the Ministry of Economy Affairs of the Republic of China.

REFERENCE

[1] IEEE 802.11 Standard, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, 1999.

[2] IEEE 802.11b Standard, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, 1999.

[3] IEEE 802.11g Standard, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, 2003

[4] IEEE Standard 802.16d-2004: Air Interface for Fixed Broadband Wireless Access Systems, Oct 2004.

[5] IEEE Standard 802.16e-2005: Air Interface for Fixed Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, Feb 2006.

[6] IEEE Standard 802.1x-2004: IEEE Standard for Local and metropolitan area networks, Port-Based Network Access Control, December 2004.

[7] C. Kaufman, Ed., “Internet Key Exchange (IKEv2) Protocol,” *IETF RFC 4306*, December 2005

[8] WiFi: http://www.wi-fi.org/

[9] WiMAX forum: http://www.wimaxforum.org/home/

[10] 3GPP: http://www.3gpp.org/

[11] 3GPP2: http://www.3gpp2.org/

[12] IEEE P802.21/D11.0, “Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services”, May 2008.

[13] The IEEE 802.11 Standard: http://www.ieee802.org/11/index.shtml

[14] H. R. Hassan, Y. Challal, “Enhanced WEP: An efficient solution to WEP threads,” *Wireless and Optical Communications Networks 2005, WOCN2005*, Second IFIP International Conference.

[15] IEEE Standard 802.11-2007: IEEE Standard for Information technology, Telecommunications and information exchange between systems, Local and metropolitan area networks, Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007

[16] Krishna Sankar, Sri Sundaralingam, Darrin Miller, Andrew Balinsky, "Cisco Wireless LAN Security, Chapter 7 EAP Authentication Protocols for WLANs" , 2004.

[17] R. Atkinson, "Security Architecture for the Internet Protocol," IETF RFC 1825, Aug. 1995.

[18] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol,” IETF RFC 2401, November 1998.