

A New Mechanism for Fast Handover between Heterogeneous Networks

Myoung Ju Yu *, Seong Gon Choi*

*College of Electrical & Computer Engineering, Chungbuk National University, 410 Seongbong-ro, Heungdeok-gu, Cheongju, Chungbuk 361-763, South Korea

mju@cbnu.ac.kr, sgchoi@cbnu.ac.kr

Abstract— This paper proposes a new handover mechanism between WiMAX and WLAN networks. It can support low latency by simplifying re-authentication process during handover. The proposed scheme allocates MA ID (Mobile Agent Identifier) as AAA key during initial connection establishment to WiMAX or WLAN. The MA ID plays a role as general AAA key which enables the MN to access to all ANs (Access Networks) connected with core network. During handover, a MN requests access with the MA ID and each AN allows the MN to access without additional key allocation. This paper verifies that the proposed scheme has lower handover latency than the existing one via numerical analysis.

Keywords—Heterogeneous Networks, WiMAX, WLAN, Handover, Authentication

I. INTRODUCTION

The demand for next generation wireless systems, which support seamless worldwide communication and various multimedia services, is increasingly accelerated along with the rapid development of mobile terminal and wireless technology. Recently, the issue of interworking between heterogeneous networks is on the rise to offer seamless services at anytime, anywhere independently of the access technologies and service providers to users [1].

The wide range of 3G system, high speed and low cost of WLANs, WiMAX having broadband support, to provide continuous services among these ANs, there must be intelligent intermediate architecture to integrate these technologies to provide best services for the users as well as operators. Accordingly, many interworking studies are in progress [2]-[7]. Especially, 3G system-WLAN interworking has been studied widely [2]-[4]. WiMAX-WLAN interworking is just about to be invigorated, relatively [5]-[7].

ITU-T SG13 has progressed Y.MM-WAW (Mobility Management for Interworking between WiMAX and WLAN) which describes mobility management architecture between WLAN and WiMAX where each AN is operated by different service provider. The Y.MM-WAW includes signal flows on connection establishment, roaming and handover as well as functional architecture for WiMAX-WLAN interworking [5].

Generally, when a MN (Mobile Node) enters a new type of network, it firstly detects a movement, changes a data link, registers to the new network, processes authentication, and

connects to the services. These processes cause heavy burdens due to its time-taken operations and overheads. Especially, as each heterogeneous network deploys its own authentication mechanism, the MN should be re-authenticated whenever it handovers. Authentication delays can be associated with handover latency, which directly affect the QoS (Quality of Service) of applications running on a MN. To support seamless service, handover between heterogeneous networks should be performed with little delay. The Y.MM-WAW has the foregoing problem.

In this paper, to solve the above-mentioned problem of the Y.MM-WAW, we propose a new handover mechanism between WiMAX and WLAN networks which simplifies re-authentication process during handover by allocating MA ID as general AAA key in case of initial connection establishment. Each AN recognizes the role of the MA ID in advance. So, when the MN with the MA ID requests access to new AN, the network allows the MN to access after checking the MA ID. Accordingly, signalling for AAA key creation and exchange can be substantially reduced compared to existing mechanism. For performance analysis, we evaluate handover latency based on analytical model [8]-[10]. The numerical results show that the proposed scheme outperforms the existing one.

The remainder of this paper is organized as follows. Section II introduces the related works about WiMAX-WLAN interworking and authentication process in IEEE802.1x. Next, Section III presents the proposed scheme and Section IV shows the performance analysis and results. Finally, Section V concludes this paper.

II. RELATED WORKS

This section introduces WiMAX-WLAN interworking and authentication process in IEEE802.1x as the related works. We describe network and signal flows for WiMAX-WLAN interworking and, representatively, authentication methods in IEEE802.1x [5], [11].

A. WiMAX-WLAN Interworking

1) Network Configuration

Figure 1 shows network environment for interworking between WiMAX and WLAN. In Figure 1, ANs such as WiMAX and WLAN are connected to NGN core network. As

the NGN is responsible for supporting MN's mobility, it should be able to provide mobility regardless of different access technologies when a MN moves between heterogeneous ANs and thus needs to have functions such as AAA, charging, etc for interworking between WiMAX and WLAN [5].

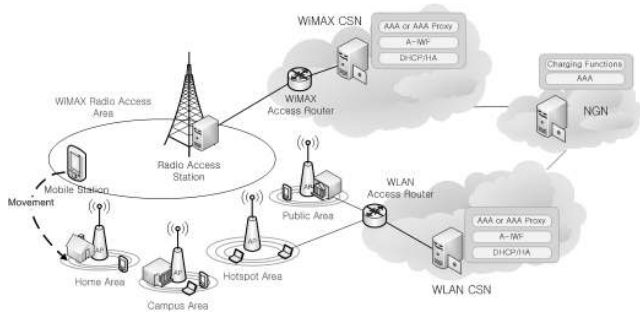


Figure 1. Network environment for WiMAX and WLAN Interworking

The WiMAX network contains a number of WiMAX ARs (Access Router) and BSs (Base Station). Each WiMAX AR is connected to BSs in WiMAX radio access area. The WiMAX network supports DHCP (Dynamic Host Configuration Protocol), HA (Home Agent), AAA or AAA proxy functions, A-IWF, etc for interworking with other networks. The WiMAX AR controls BSs and supports IP mobility for a MN moving within a WiMAX AR and between different WiMAX ARs. Therefore, it supports L3 mobility functions. The BS controls radio resources and supports L2 mobility between different BSs by interworking with WiMAX AR [5].

The WLAN network contains a number of WLAN ARs and APs (Access Point). Each WLAN AR is connected to APs in wireless access area. WLAN network supports DHCP, HA, AAA or AAA proxy functions, A-IWF, etc for interworking with other networks. The WLAN AR interworks with APs and supports L3 mobility by MN's movement. The AP is responsible for connecting a MN to different ANs [5].

2) Connection Setup in WiMAX and WLAN

Figure 2 shows the WiMAX connection establishment as follows. Firstly, the MN connect to the WiMAX AN and establishes the WiMAX connection based on the detail procedure which refers to [6]. And then the MN authenticates with the NGN using PKMv2 and EAP-TLS/TTLS/CHAPv2/AKA, etc and registers with the 802.16 network. After that, the MN establishes the service flows using DSA Request/Response and also completes data path registration with the ASN. L3 connection process can be divided into network-based mobility and host-based mobility [5].

The MN sends a DHCP Discover message to discover a DHCP server for host IP configuration. In network-based mobility, the mobility client in ASN G/W, for example MAG in PMIPv6, is triggered to initiate registration procedure. And then the MA sends AAA Request message to AAA server and receives AAA Response message from. After that, the MA responds with the Registration Request message. Once the

MN-MA security is validated, the MA assigns an IP for the MN. If this is the initial entry for the MN, the MA creates a binding cache for the MN. At this point mobility tunnel is established between the ASN G/W and the MA. After that, the MN and ASN G/W exchange DHCP Offer, DHCP Request and DHCP ACK messages. In host-based mobility, after IP configuration process, the MN performs registration procedure [5].

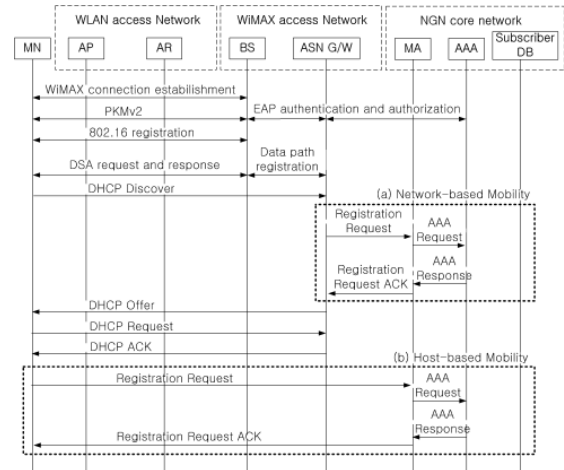


Figure 2. Connection Establishment to WiMAX

Figure 3 indicates the WLAN connection establishment as follows. First of all, the MN establishes 802.11 association with the AR and authenticates with the NGN using 802.1X/EAPOL and various EAP methods such as EAP-TLS and EAP-AKA. 802.12X port is unblocked in AR by handshaking between MN and AR. Like the preceding, L3 connection process can be divided into network-based mobility and host-based mobility. Also, it follows the same procedure as indicated in Figure 2 [5].

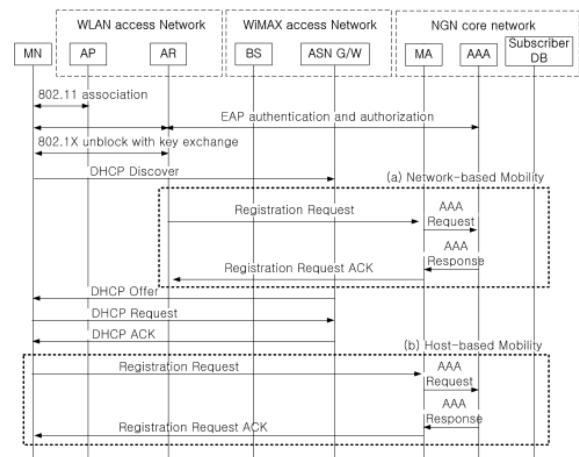


Figure 3. Connection Establishment to WLAN

B. Authentication in IEEE802.1x

IEEE802.1x was designed to provide higher layer authentication mechanisms to L2. Basically IEEE802.1x has three entities such as Supplicant, Authenticator (AP or AR),

AAA server. The Supplicant can be considered as the IEEE802.1x station desiring to join the network. The Authenticator is the device that controls the access; in a WiMAX/WLAN network it can be the IEEE802.16 BS or the ASN G/W and IEEE802.11 AP or AR. The AAA server makes the authentication decision, for example, the RADIUS server [11].

IEEE802.1x executes the mutual authentication through one of EAP (Extensible Authentication Protocol) methods, including EAP-TLS, EAP-AKA, and so on. As EAP is part of the PPP (point-to-point) protocol the protocol used is called EAPOL (EAP over LAN). The EAPOL messages of concern for IEEE802.11 are listed as follows [11]-[12].

- EAPOL-Start: Determines if there is an authenticator. Used by sending this message to a special group multicast to MAC address reserved for 802.1x authenticator. Response is an EAPOL-Identity Request in EAPOL-Packet.
- EAPOL-Key: Authenticator sends encryption keys to the Supplicant.
- EAPOL-Packet: A container for transferring EAP messages on LAN.
- EAPOL-Logoff: Disconnection message.

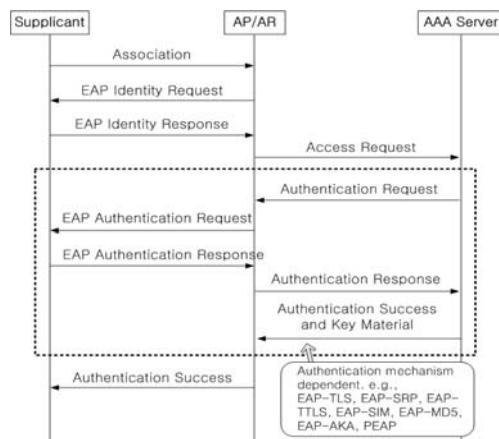


Figure 4. IEEE802.1x message sequence

Unfortunately, re-authentication procedure in EAP framework which causes long time latency is a well-known bottleneck existing for a long time [12].

III. FAST HANDOVER MECHANISM BETWEEN WiMAX AND WLAN NETWORKS

This section presents general AAA key and the detailed procedures for fast handover between WiMAX and WLAN.

A. General AAA key for fast handover

For fast handover, we focus on re-authentication should be executed whenever a MN handover to new type of network. The re-authentication delays can cause heavy latency during handover. The proposed scheme uses MA ID as general AAA key to reduce handover latency by simplifying re-authentication procedure of existing scheme, [5]. The MA ID, identifier of MA located in core network, presents the

authority to access to all ANs connected with core network. It is allocated to the MN in case of initial connection establishment to WiMAX or WLAN. When the MN moves to new AN, it requests access to the network with the MA ID. As each AN recognizes the role of the MA ID in advance, the networks check the MA ID and allow the MN to access. Compared to the existing scheme [5], as the MA ID is general AAA key which can be applied to both WiMAX and WLAN, the MN that already has the MA ID does not need to execute AAA key creation and exchange when it accesses to new network. Accordingly, signalling for AAA key creation and exchange can be substantially reduced.

B. Handover between WiMAX and WLAN

We represent message flows for handover between WiMAX and WLAN which simplify re-authentication signalling by using general AAA key, the MA ID.

1) Handover from WLAN to WiMAX

Figure 5 shows message flow for handover from WLAN to WiMAX. When a MN which was connected with WLAN moves to WiMAX, it tries to access WiMAX AN.

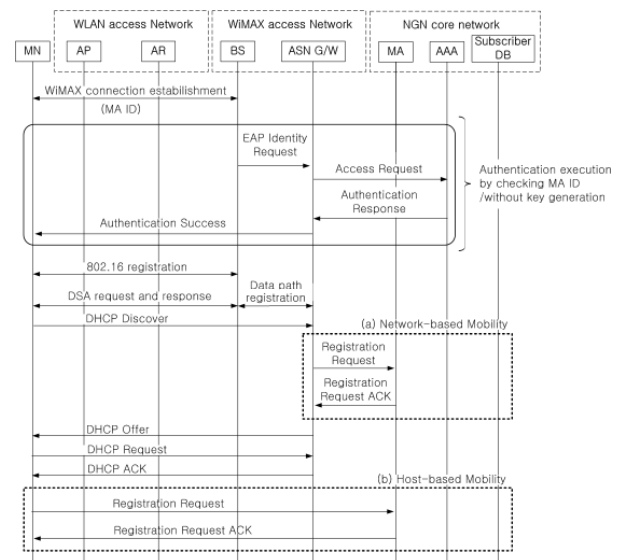


Figure 5. Handover from WLAN to WiMAX

1. The MN establishes the WiMAX connection with MA ID which receives via connection establishment with WLAN. The MN sends the MA ID to BS.
2. The BS requests authentication with the MA ID. WiMAX AN and AAA server check the MA ID and then authorize the MN to access without key creation and exchange. The MN authenticates with the NGN using PKMv2 and EAP-TLS/TTLS/CHAPv2/AKA, etc.
3. The MN registers with the 802.16 network.
4. The MN establishes the service flows using DSA Request/Response and also completes data path registration with the ASN G/W.

5. The MN sends DHCP Discover message to discover a DHCP server for host IP configuration.

The following steps from 6 to 8 are only valid for network-based mobility.

6. The ASN G/W is triggered to initiate registration procedure. It sends Registration Request message to the MA. The same NAI is used during this EAP authentication procedure is used in this Registration Request message.
7. The MA responds to the ASN G/W with the Registration Request ACK message. Once the MN-MA security is validated, the MA assigns an IP for the MN. Also, the MA updates the binding cache for the MN. At this point, mobility tunnel is established between the ASN G/W and the MA.
8. The ASN G/W sends DHCP Offer message to the MN.
9. The MN responds to the first DHCP Offer message received with DHCP Request message to the ASN G/W along with the address information received in the DHCP Offer.
10. The ASN G/W acknowledges the use of this IP address and other configuration parameters by sending DHCP ACK message.

The following steps from 11 to 12 are only valid for host-based mobility.

11. The MN initiates registration procedure. It sends Registration Request message to the MA. The same NAI is used in this Registration Request message.
12. The MA responds to the ASN G/W with the Registration Request ACK message. The MA assigns an IP for the MN and updates the binding cache for the MN.

2) Handover from WiMAX to WLAN

Figure 6 shows message flow for handover from WiMAX to WLAN. When a MN which was connected with WiMAX moves to WLAN, it tries to access WLAN AN.

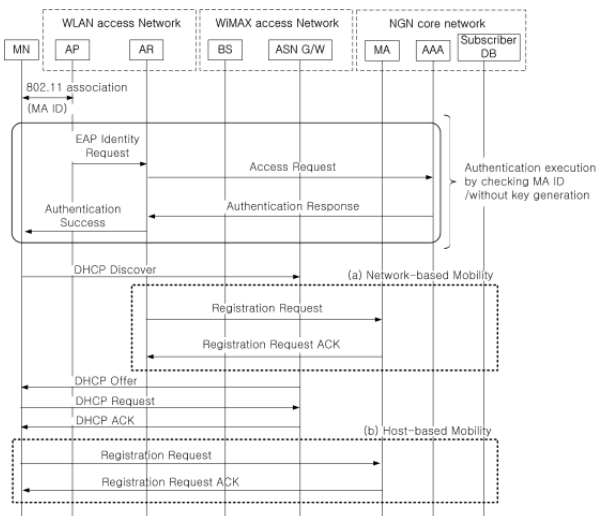


Figure 6. Handover from WiMAX to WLAN

1. The MN establishes WLAN association with MA ID which receives via connection establishment with WiMAX. The MN sends the MA ID to AP.
2. The AP requests authentication with MA ID. WLAN AN and AAA server check the MA ID and then authorize the MN to access without key creation and exchange. Likewise, the MN authenticates using PKMv2 and EAP-TLS/TTLS/CHAPv2/AKA, etc.

The following steps are the same with handover from WLAN to WiMAX in Figure 5.

IV. PERFORMANCE ANALYSIS AND NUMERICAL RESULTS

This section presents the performance analysis for the existing and proposed scheme. We compare the proposed scheme with the conventional thing, [5] in terms of handover delay when a MN moves between heterogeneous networks.

The handover latency is defined as the time interval during which a MN cannot receive and transmit any packet due to the handover procedure. That is, it is an interval from the time the MN loses the L2 connection with the old BS until the time the MN receives or transmits packets by the new IP address through the new BS [13].

The network topologies are based on [5]. Also, we only consider the processing time of network element in terms of handover latency because we assume the transmission time is same for two schemes. For performance analysis, we use M/M/1 queuing model, and the total processing time of each network element depends on the number of layers.

According to [8]-[10], let M_x be the set of messages processed in a network element x , and the utilization of a network element x , ρ_x , is obtained by

$$\rho_x = \sum_{l \in M_x} (\lambda_l / \mu_l) \quad (1)$$

Where λ_l and μ_l are the mean arrival rate and the mean service rate of messages of type l . We assume that the mean arrival rate of message l is equal for all messages in a network element. This assumption implies

$$\lambda_l = \lambda_x \text{ for all } l \in M_x \quad (2)$$

where λ_x is the mean arrival rate of any message in network element x . From Eq. (1) and (2), the mean sojourn time of message l in a network element x , σ_l , is obtained by

$$\sigma_l = 1 / \{\mu_l (1 - \rho_x)\} \text{ with } l \in M_x \quad (3)$$

We define the total service time in a network element x , s_x .

$$s_x = \sum_{l \in M_x} (1 / \mu_l) \quad (4)$$

That is, s_x is the time that is spent to process all messages arriving in the network element x during each scenario. The total service time in each scenario, S , is then expressed as

$$S = \sum_{x \in E} s_x \quad (5)$$

where E is the set of network elements. Therefore, the total service time for each scheme is presented in Table 1. (a) $s_{L2_{Req}}$: packet service time of MAC layer. (b) $s_{L3_{Req}}$: packet service time in MAC and network layers.

TABLE 1. EXPRESSION FOR TOTAL SERVICE TIME (S)

Scheme		Expression
Network-based Mobility	Existing-WiMAX	$3(s_{L3_{Req}} + s_{L3_{Res}}) + 12s_{L2_{Req}} + 14s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}$
	Existing-WLAN	$3(s_{L3_{Req}} + s_{L3_{Res}}) + 10s_{L2_{Req}} + 12s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}$
	Proposed-WiMAX	$3(s_{L3_{Req}} + s_{L3_{Res}}) + 8s_{L2_{Req}} + 9s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}$
	Proposed-WLAN	$3(s_{L3_{Req}} + s_{L3_{Res}}) + 6s_{L2_{Req}} + 7s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}$
Host-based Mobility	Existing-WiMAX	$4(s_{L3_{Req}} + s_{L3_{Res}}) + 13s_{L2_{Req}} + 15s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}$
	Existing-WLAN	$4(s_{L3_{Req}} + s_{L3_{Res}}) + 11s_{L2_{Req}} + 13s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}$
	Proposed-WiMAX	$4(s_{L3_{Req}} + s_{L3_{Res}}) + 9s_{L2_{Req}} + 10s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}$
	Proposed-WLAN	$4(s_{L3_{Req}} + s_{L3_{Res}}) + 7s_{L2_{Req}} + 8s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}$

We assume that the processing time of each layer's header in a network element is in proportion to that of IP header, and that the database (DB) processing delay in Table 2 is same as the processing time of IPv6 header. We derive the processing delay in each layer from the processing time of each layer's header [8], [10], and the service time in each network element according to element type can be calculated as Table 2.

TABLE 2. SERVICE TIME IN NETWORK ELEMENT

Service Time	Value
$s_{L2_{Req}}$	2.59 ms
$s_{L2_{Res}}$	0.65ms
$s_{L3_{Req}}$	10 ms
$s_{L3_{Res}}$	2.5ms

Given that the reference arrival rate of a message at a network element for each scenario is λ , we define the effective call arrival rate, λ_x^{eff} , of a message.

$$\lambda_x^{eff} = \lambda / s_x \quad (6)$$

From Eq. (3) and (6), the total processing time of each scheme is presented in Table 3, where n is the hop number between access and core network elements. We assume that n is 5 and evaluate the handover latency of each scheme.

TABLE 3. EXPRESSION FOR TOTAL SERVICE TIME (S)

Scheme		Expression
Network-based Mobility	Existing-WiMAX	$\{3(s_{L3_{Req}} + s_{L3_{Res}}) + 12s_{L2_{Req}} + 14s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}\} / (1-\lambda)$
	Existing-WLAN	$\{3(s_{L3_{Req}} + s_{L3_{Res}}) + 10s_{L2_{Req}} + 12s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}\} / (1-\lambda)$
	Proposed-WiMAX	$\{3(s_{L3_{Req}} + s_{L3_{Res}}) + 8s_{L2_{Req}} + 9s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}\} / (1-\lambda)$
	Proposed-WLAN	$\{3(s_{L3_{Req}} + s_{L3_{Res}}) + 6s_{L2_{Req}} + 7s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}\} / (1-\lambda)$
Host-based Mobility	Existing-WiMAX	$\{4(s_{L3_{Req}} + s_{L3_{Res}}) + 13s_{L2_{Req}} + 15s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}\} / (1-\lambda)$
	Existing-WLAN	$\{4(s_{L3_{Req}} + s_{L3_{Res}}) + 11s_{L2_{Req}} + 13s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}\} / (1-\lambda)$
	Proposed-WiMAX	$\{4(s_{L3_{Req}} + s_{L3_{Res}}) + 9s_{L2_{Req}} + 10s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}\} / (1-\lambda)$
	Proposed-WLAN	$\{4(s_{L3_{Req}} + s_{L3_{Res}}) + 7s_{L2_{Req}} + 8s_{L2_{Res}} + (n-1)s_{L3_{Req}} + (n-1)s_{L3_{Res}}\} / (1-\lambda)$

Figure 7 and 8 present the handover latency for network-based mobility and host-based mobility in case of handover between WiMAX and WLAN. In Figure 7, we can see the proposed scheme's handover latency is lower than the existing one in case of network-based handover. Similarly, Figure 8 shows the proposed scheme has lower handover latency than the existing thing in host-based handover. It is because the re-authentication signalling during handover can be reduced by using general AAA key.

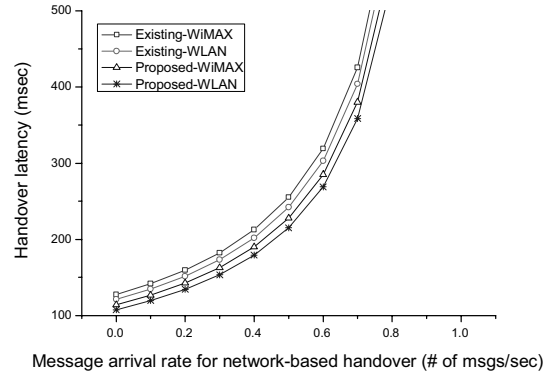


Figure 7. Network-based Handover Latency Time vs. Handover Rate

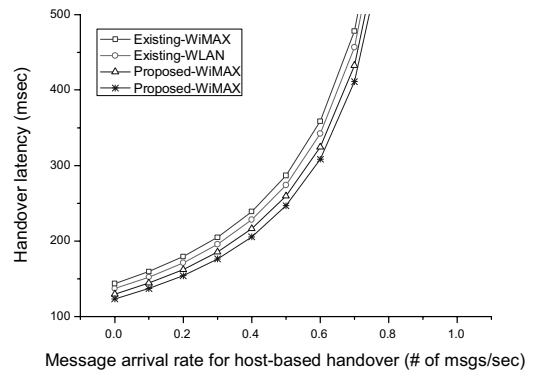


Figure 8. Host-based Handover Latency Time vs. Handover Rate

V. CONCLUSIONS

This paper proposes a new handover mechanism between WiMAX and WLAN networks which simplifies re-authentication process during handover by allocating MA ID as general AAA key when a MN initially connects to a network. The proposed scheme can substantially reduce re-authentication signalling during handover compared to existing thing. For the performance comparison, we calculated handover latency of two schemes using M/M/1 queuing system. As a result, we verified the proposed method shows lower handover latency than the existing thing.

In the future, we will consider the performance evaluation regarding various factors except to handover latency and define more correct parameter values.

ACKNOWLEDGMENT

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency). (NIPA-2010-(C1090-1011-0013))

CORRESPONDING AUTHOR

Seong Gon Choi (sgchoi@cbnu.ac.kr)

REFERENCES

- [1] M. J. Yu, S. G. Choi, "New Mechanism for Global Mobility Management based MPLS LSP in NGN," *FGCN2010*, Dec. 2010.
- [2] 3GPP, "3GPP system to Wireless Local Area Network (WLAN) Interworking," 3GPP TS29.234 ver. 8.0.0, Dec. 2008.
- [3] 3GPP, "Mobility between 3GPP WLAN Interworking and 3GPP systems," 3GPP TS24.327 ver. 8.0.0, Dec. 2008.
- [4] A. K. Salkintzis, G. Dimitriadis, D. Skyrianoglou, N. Passas, N. Pavlidou, "Seamless Continuity of Real-Time Video across UMTS and WLAN Networks: Challenges and Performance Evaluation," *IEEE Wireless Communications*, Vol. 12, pp. 8-18, June 2005.
- [5] J. M. Lee, S. G. Choi, "Mobility Management for Interworking between WiMAX and WLAN," *ITU-T NGN-GSI*, ver. 0.6, Sep. 2010.
- [6] WiMAX Forum, "WiFi-WiMAX Interworking," *WiMAX Forum*, Dec. 2009.
- [7] V. K. Gondi, N. Agoulmine, "Secured Roaming over WLAN and WiMAX Networks," *BcN'07*, pp. 1-12, May 2007.
- [8] M. J. Yu, J. M. Lee, T. M. Um, W. Ryu, B. S. Lee and S. G. Choi, "A New Mechanism for Seamless Mobility based on MPLS LSP in BcN," *IEICE TRANS. COMMUN.*, Vol. E91-B, pp.593-596, Feb. 2008.
- [9] Hyejeong Lee, Jee-Young Song, Dong-Ho Cho, "An Integrated Mobility Management Scheme in IPv6 based Wireless Networks," *VTC 2004*, Vol. 5, pp. 2748-2752, May 2004.
- [10] ESP (EMERGING STANDARDS AND PROTOCOLS), <http://www.xillinx.com/esp/wired/optical/collateral/mpls.pdf>.
- [11] Anand R. Prasad, Neeli R. Prasad, "802.11 WLANs and IP Networking: Security, QoS and Mobility," *Artech House*, April 2005.
- [12] H. M. Sun, Y. H. Lin, S. M. Chen, Y. C. Shen, "Secure and fast handover scheme based on pre-authentication method for 802.16/WiMAX infrastructure networks," *TENCON2007*, pp. 1-4, Oct.. 2007.
- [13] Jui-Hung Yeh, Jyh-Cheng Chen, Prathima Agrawal, "Fast Intra-Network and Cross-Layer Handover (FINCH) for WiMAX and Mobile Internet," *IEEE TRANSACTIONS ON MOBILE COMPUTING*, Vol. 8, pp. 558-574, April 2009.