HIP-based Handover Mechanism under MIH Architecture in Heterogeneous Wireless Networks

Shih-Jung Wu
Department of Innovative Information and Technology
Tamkang University
I-lan County, Taiwan R.O.C.
e-mail: wushihjung@mail.tku.edu.tw

Che-Yu Yang
Department of Information Management,
China University of Technology,
Taipei, Taiwan
Email: cyyang@cute.edu.tw

***Abstract*—In this paper, we offers a HIP-based vertical handover scheme under MIH architecture in heterogeneous wireless network. Many diversity wireless access technologies are offering in Next Generation Wireless Networks (NGWN). In NGWN, the integration of wireless access network will be accomplished by seamless handover which contains many challenges i.e. service mobility, vertical handover, common authentication, unified accounting/billing, security mechanisms, QoS and service provisioning, etc. Toward this direction, our research aims to provide a complete integration of heterogeneous network architecture and support a fit mobility management for network to seamless handover. We focus on simulation about vertical handover execution for WiMAX to WiFi scenario. Our idea can modify defects of Mobile IP and SIP. And it provides internet users always best connection. Moreover, we hope to contribute our research to beyond 4G wireless networks.**

Keywords- MIH; HIP; Mobility Management; Heterogeneous Wireless Networks, Handover

I. INTRODUCTION

The future generation of mobile networks will consist of multiple wireless access technologies such as WiMAX, WLAN and cellular systems seamlessly integrated. In the future, wireless devices will have multiple heterogeneous interfaces, so mobile users will be able to roam across these heterogeneous wireless networks with uninterrupted active connections. When a mobile users moves from one wireless access network to another, a network service exchanging will exactly happen. In order to enhance the experience of mobile users by facilitating handovers between heterogeneous wireless networks, the IEEE 802.21 Working Group does an effort to ratify the Media Independent Handover (MIH) [1] standard. The MIH framework offers the common interface and provides link layer and other related network information to upper layers. Moreover, mobility management is one of the most important issues in the mobile communication, and it affects efficiency of the whole mobility network apparently. The reaching of mobility can be implemented though handover and mobility management protocol, containing Session Initiation Protocol (SIP) at application layer and Mobile IP (MIP) at network layer. Meanwhile, the protocol can improve the efficiency that heterogeneous wireless network integrated. However, using SIP needs more handover message. And, MIP causes communication delay and triangle routing. Opposing to SIP and MIP shortcomings [11, 13], Host Identity Protocol (HIP) [2] defined by Internet Engineering Task Force (IETF) has emerged as a feasible solution for service mobility. One problem with the current Internet architecture is that the IP address describes both the host topological location in the network, and the host identity. The HIP is one proposal to solve this semantic overloading of IP addresses. HIP introduces a new cryptographic namespace, the Host Identity namespace. The location information, i.e. the IP address, is used only for routing purposes, not for identifying the host. Moreover, each time the mobile users change access network, they must be authenticated and authorized to access resources in the new access network. For this reason, Diameter Protocol [5] is developed by the IETF to provide an AAA (Authentication, Authorization, and Accounting) related mechanism. It has several advantages, compared to earlier AAA protocols. For instance, RADIUS offers improvements in the areas of reliability, security, scalability, and flexibility. Diameter Protocol includes base protocol and various application protocols, such as NAS (Network Access Server) Application, Mobile IP, CMS (Cryptographic Message Syntax security) and so on.

This paper offers a heterogeneous mobile integrated architecture and a HIP-based vertical handover scheme which utilities MIH in heterogeneous wireless network. In addition, the Diameter Protocol is used for authentication of registered users. The rest of the paper is organized as follows. Section II describes related work. Section III introduces a new heterogeneous mobile integrated architecture. Section IV proposes vertical handover scheme between WiMAX and WiFi. Finally, section V presents the conclusions and future works.

II. RELATED WORKS

A. *Media Independent Handover (MIH) and Host Identity Protocol (HIP)*

Media Independent Handover (MIH) was introduced by IEEE and intended to facilitate handover and interoperability among IEEE 802 technologies, including wire and wireless network. And, it also supports handover between IEEE 802 and non-IEEE 802 technologies. The user can set up the network environment by its profile, and then select the proper network environment by enabling the network selection mechanism. The MIH Function offers three types of services: MIES (Media-Independent Event Service), MICS (Media-Independent Command Service) and MIIS (Media-Independent Information Service). MIH works as follows, when the event happens in the layer 2 of different network technologies (e.g., signal decay), it can transmit to the upper layer through MIES. And the upper layer (e.g., SIP, MIP, HIP and so on) can transmit the command (e.g., switching access interface) to the lower layer through MICS as well. The user devices and the network systems can offer related information (e.g., network topological) to the lower layer or the upper layer through MIIS. Furthermore, the MIH provides a unified interface between the link layer users in the mobility-management protocol stack and existing media-specific link layers, such as those specified by 3GPP, 3GPP2 and IEEE 802 family of standards.

In the current Internet, the host is identified by using the Internet Protocol (IP) addresses. The IP address describes both the host topological location in the network, and the host identity. The dual operation of the IP address causes problems when the host has to change its IP address due to mobility. The host has to disconnect all its connections and build them up again with the new IP address. The location information changes, but it should not affect the identity information of the host (mobility). Furthermore, the host may wish to be associated with more than one home network, but it may need to use a different IP address per various home networks (multi-homing). The IETF (Internet Engineering Task Force) is working on multiple similar solutions to meet the new requirements (mobility & multi-homing). One of these efforts is The Host Identity Protocol (HIP) [3, 10].

HIP proposed a new namespace, called the Host Identity namespace. Each Host Identity is unique and separated from the IP address. It provides a convenient and efficient way to address hosts regardless of their location. In HIP, a pair of self-generated public and private keys provides the Host Identity. There are two main representations of the Host Identity, the full Host Identifier (HI) and the Host Identity Tag (HIT). The HI is a public key and directly represents the identity. Since there are different public key algorithms that can be used with different key lengths, the HI is not good to be used as a packet identifier in HIP. Consequently, a hash of the HI, the HIT, becomes the operational representation. The HIT has the length of an IPv6 address. Another representation of the Host Identity, the Local Scope Identifier (LSI), has the length of an IPv4 address. Fig. 1 shows the methods of identifying a host.

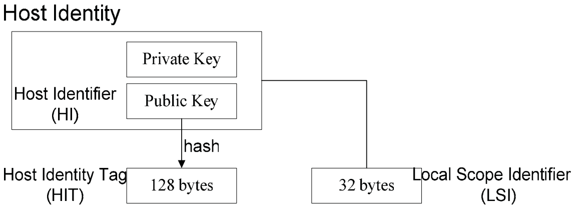


Figure 1. Methods of identifying a host.

A Host Identifier (HI), a name in the Host Identity namespace, represents a statistically globally unique name. In HIP, public key of an asymmetric key pair is used as the HI. Correspondingly, the host is defined as the entity that holds the private key from the key pair. This has the advantage that the HI can authenticate HIP packet and protect man-in-the-middle attacks. Thus Rivest-Shamir-Adelman (RSA) public key algorithm must be supported by HIP and Digital Signature Algorithm (DSA) should be supported too.A Host Identity Tag (HIT) is a 128-bit representation for a Host Identity. It is created by taking a cryptographic hash through the original HI. Using the HIT has two advantages. First, its fixed length makes the protocol easier to manage and code. Second, it presents the identity in a consistent format to the protocol. In the HIP packet exchange, the HIT is used to identify a sender or a receiver and it is unique as long as it is being used. A Local Scope Identifier (LSI) is a 32-bit localized representation of a Host Identity. The LSI has the same length as IPv4 addresses and can be used by the legacy IPv4 based-application protocols (e.g. FTP). LSI has shorter lengths than HIT and the probability of their collisions is higher. Therefore, it should only be used for a local scope.

In HIP, a new protocol layer is added into the TCP/IP stack: Host Identity Layer. It is located between the networking layer and the transport layer. As shown in Fig. 2. The new layer hides IP addresses from the layer above. Applications need not rely on IP addresses but, instead, depend on HIT or LSI. The new layer transfers the HIT/LSI into IP address and vice versa. With this new approach, the application procedures create a socket that consists of the HIT and port pair. In addition, the socket is mapped to destination IP address. The application process will not deal with destination IP addresses but HIT. If the IP address is changed, the transport layer can still be connected to the HIT because the mapping between IP addresses and HIT can be retrieved such as the DNS. The HIP Base Exchange establishes a security association between two hosts. It utilizes the four-way handshake and creates a security association with IPSec. The Base Exchange is illustrated in Fig. 3. The initiator sends the trigger packet (I1) to the responder and starts the Base Exchange. This packet contains the HIT of the initiator and, if known, the HIT of the responder. Upon receiving the I1 packet, the responder immediately replies a prepared R1 packet. It contains a puzzle (a cryptographic challenge) that the initiator must solve before continuing the exchange. In addition, the R1 contains the initial Diffie-Hellman parameters and a signature; it is used to create a session key and to establish the IPsec Encapsulated Security Payload security association between the nodes. And then the initiator sends the I2 packet containing the solution of the received puzzle. Without a correct solution, the I2 message is discarded. Finally, the R2 packet completes the Base Exchange.

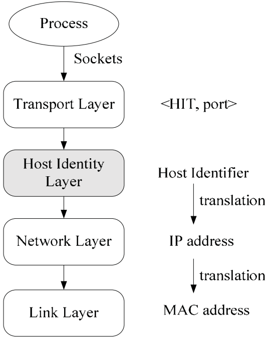


Figure 2. The Protocol Stack of HIP

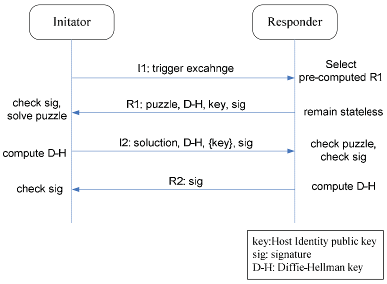


Figure 3. HIP Base Exchange

To be able to reach the mobile host, a HIP mobile host can change its IP address. The initial IP address has to be stored somewhere. The rendezvous server (RVS) [4] is designed to solve this problem. In order to be reachable mobility, each host has to register to its own RVS server. This server has to be updated with the latest IP addresses of the mobile host. Fig. 4 shows a HIP base exchange involving a RVS.

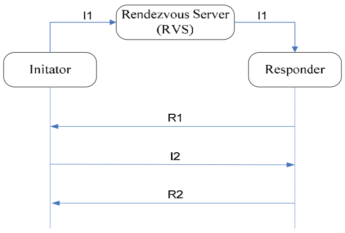


Figure 4. HIP Base Exchange using a RVS

As Fig. 5 indicates, the initiator sends I1 packet to the RVS for notifying the change of the IP address, and then RVS forwards this packet to responder. Later, responder answers with R1 packet. Finally, initiator and responder interchange I2 and R2 packet. The diagram notation and its meanings are listed in Table I.

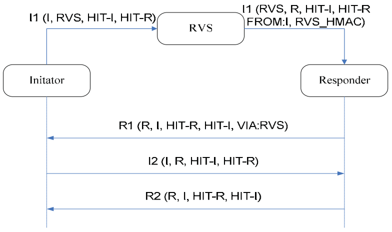

I1 (I, RVS, HIT-I, HIT-R)
RVS
I1 (RVS, R, HIT-I, HIT-R FROM:I, RVS_HMAC)
Initator
Responder
R1 (R, I, HIT-R, HIT-I, VIA:RVS)
I2 (I, R, HIT-I, HIT-R)
R2 (R, I, HIT-R, HIT-I)

Figure 5. RVS rewriting IP addresses

TABLE I. DIAGRAM NOTATION

I, R	I and R are the respective source and destination IP addresses in the IP header.
HIT-I, HIT-R	HIT-I and HIT-R are the Initiator's and the Responder's HITs in the packet, respectively.
FROM:I	A FROM parameter containing the IP address I is present in the HIP header.
RVS_HMAC	An RVS_HMAC parameter containing a Hash Message Authentication Code (HMAC) keyed with the appropriate registration key is present in the HIP header.
VIA:RVS	A VIA_RVS parameter containing the IP address RVS of a rendezvous server is present in the HIP header.

B. Diameter Protocol

AAA (Authentication, Authorization, and Accounting) protocol, the integration of authentication, authorization and accounting technologies, has been widely used in Internet services and provided those services safety and reliability. Diameter protocol will be the next generation AAA protocol. It includes base protocol and various application protocols, such as NAS (Network Access Server) Application, Mobile IP, CMS (Cryptographic Message Syntax security) and so on. Fig. 6 shows the relationship between the Diameter base protocol and various Diameter applications.

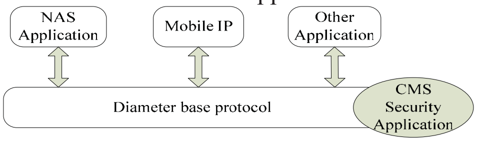


Figure 6. Diameter Application

Diameter Base Protocol [5, 9] defines the same functions used in the various applications, and provides basic mechanisms for credible transport message delivery and error handling services. It supports IPSec (Internet Protocol Security) or TLS (Transport Layer Security), in order to protect the message. On the other hand, Diameter NAS application describes the details of authentication procedures in the Diameter servers and network access servers (NAS) [6]. NAS specification defines an AA-request and an AA-answer command that deal with the first two "A"s of AAA: authentication and authorization. AA-request (AAR): this command is sent by a NAS to request authentication and/or authorization for a given NAS user. All requests must contain information to uniquely identify the source of the call, such as user-name, NAS port identifier, and so on. If authentication is requested, the user-name and related authentication Attribution Value Pair (AVPs) should be present. AA-answer (AAA): this command is sent in response to AA-request message. If authorization is requested and processed successfully, it will include related authorization AVPs for service being provided. An example of Diameter server-NAS message exchange is shown in Fig. 7.

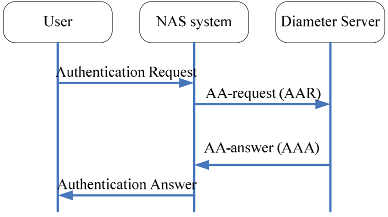


Figure 7. The message exchange for Diameter NAS Application

III. Heterogeneous Mobile Integrated Architecture

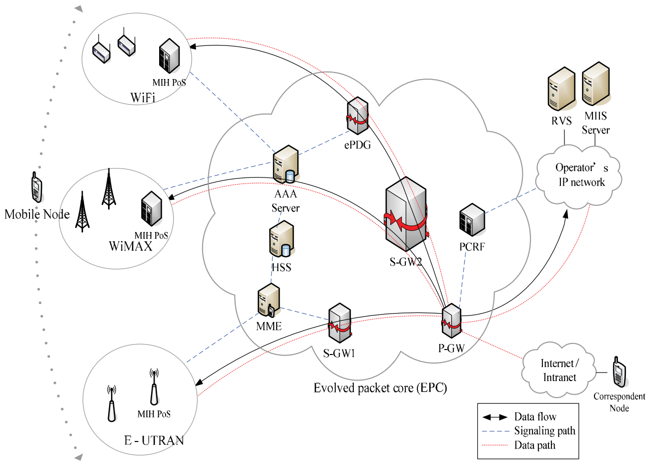


Figure 8. Heterogeneous Mobile Integrated Architecture

In order to satisfy seamless mobility in heterogeneous wireless network, we propose a new heterogeneous mobile integrated architecture in Fig. 8 which utilizes MIH in HIP mobility management protocol [7, 8, 12]. In the following further details on this architecture are provided. The Mobile Node (MN) has WiFi, WiMAX and E-UTRAN network interfaces, which support MIHF and mobility. The Correspondent Node (CN) has IEEE 802.3 network interfaces without MIHF and mobility. Moreover, a number of various access networks, such as WiFi, WiMAX and E-UTRAN, are connected to a common core network (the EPC) based on IP technology through different interfaces. All 3GPP networks are connected through the serving gateway 1 (S-GW1), and all non-3GPP networks are connected through the S-GW2. Different paths also are used in the case of WiFi and WiMAX. A WiMAX network is considered trusted non-3GPP accesses and directly connected to the S-GW2. On the other hand, a WiFi network is considered as distrusted access connects to the evolved packet data gateway (ePDG) and then to the S-GW2. For E-UTRAN, the S-GW1 is directly connected to it. The Mobility Management Entity (MME) is incorporated in the architecture for handling control functions such as authentication, security, and mobility. For distrusted non-3GPP accesses, the ePDG secures the access of the MN to the EPC by means of an IPSec tunnel between itself and the MN. All data paths from the access networks are combined at the P-GW, which incorporates functionality such as packet filtering, QoS policing, interception, charging, and IP address allocation, and routes traffic control. Besides, EPC also contains network control entities for keeping user subscription information (home subscriber server [HSS]), determining the identity and privileges of a user and tracking his/her activities (authentication, authorization, and accounting [AAA] server), and enforcing charging and QoS policies through a policy and charging rules function (PCRF).

In order to achieve seamless handover of the architecture, extra functionality is needed in the network elements, based on the IEEE 802.21 protocol. The MIH functionality placed at the mobile node (MN), the wireless accesses networks (MIH PoSs), and the operator's IP network (MIIS server). Moreover, due to mobility management based on the HIP, the rendezvous server (RVS) placed at the operator's IP network for handle IP address of MN.

IV. Handover Execution Scheme

In handover procedure for heterogeneous wireless network, we offer a handover execution scheme which is a HIP-based vertical handover scheme which utilizes MIH. In addition, the Diameter Protocol is used for authentication of registered users. The following sub-sections describe each handover procedure between WiMAX and WiFi.

Fig. 9. shows the handover procedure from WiMAX to WiFi for heterogeneous wireless network. The detail schemes are in Table II.

TABLE II. WiMAX to WiFi handover

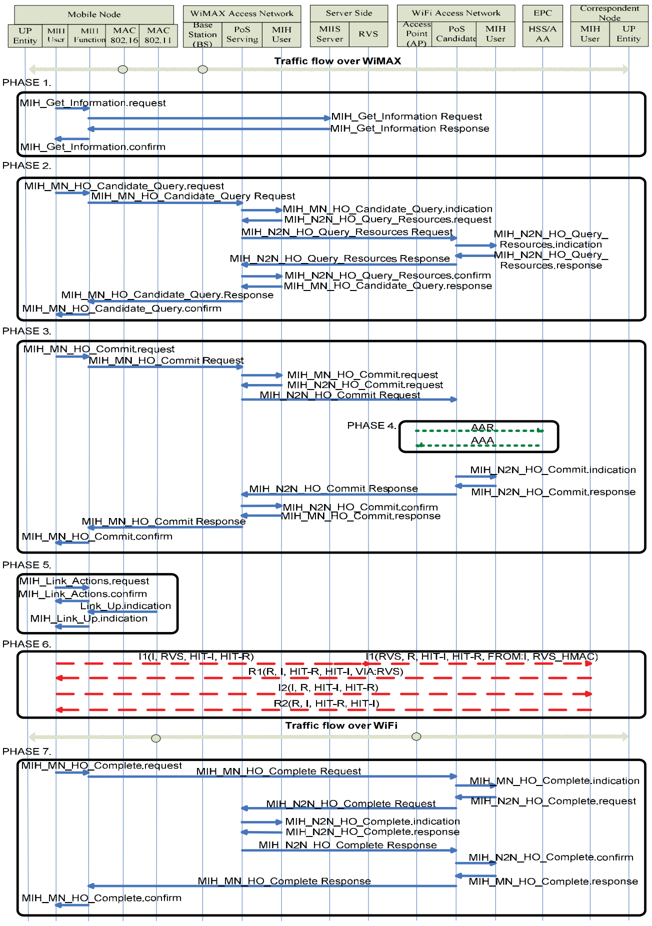
Phase 1.	The handover procedure starts from querying the information of neighboring networks by the MIH user of the MN. The following is the detailed procedure: 1) The MIH user of MN sends the MIH_Get_Information.request to MIHF. 2) The MIHF transmits the MIH_Get_Information Request message to MIIS server which locates at the operator network. 3) The basic neighbor information in the MIH_Get_Information Response message returned from the MIIS server to the MIHF. 4) The MIH_Get_Information.confirm is delivered from the MIHF to the MIH User.
Phase 2.	After information of neighboring networks received, the serving PoS starts querying the available candidate network asking for the list of resources available. This is performed

	by a successive exchange of querying resources messages with one or several candidate PoSs (in this case, only one candidate network [WiFi access network]). Afterward the MN has enough information about the surrounding networks for making the handover decision. The following is the detailed procedure: 1) The MIH user of the MN sends the MIH_MN_HO_Candidate_Query.request to MIHF. 2) The MIHF makes a query (MIH_MN_HO_Candidate_Query Request message) to the serving PoS which is located on the WiMAX access network. 3) The serving PoS transmits the MIH_MN_HO_Candidate_Query.indication to the MIH user. 4) The MIH user sends the MIH_M2N_HO_Query_Resources.request to the serving PoS to check for resource availability at the candidate PoSs. 5) The serving PoS transmits MIH_N2N_HO_Query_Resources Request message to the candidate PoS which is located on the WiFi access network. 6) The MIH_N2N_HO_Query_Resources.indication is forwarded by the candidate PoS to MIH user. 7) The result of the queries is sent to the candidate PoS through the MIH_N2N_HO_Query_Resources.response. 8) The candidate PoS sends the MIH_N2N_HO_Query_Resources Response message to the serving PoS which is located on WiMAX access network. 9) The serving PoS forwards the MIH_N2N_HO_Query_Resources.confirm to the MIH user. 10) The MIH user sends MIH_MN_HO_Candidate_Query.response to the serving PoS. 11) The serving PoS transmits the MIH_MN_HO_Candidate_Query Response message to the MIHF of the MN. 12) The MIHF forwards the MIH_MN_HO_Candidate_Query.confirm to the MIH user.
Phase 3.	Once the MIH user of the MN decides the target network to handover, it confirms that the handover will be executed. The resource of the target network will be reserved. The following are the detailed procedure: 1) The MIH user of the MN sends the MIH_MN_HO_Commit.request to MIHF. 2) The MIHF transmits the MIH_MN_HO_Commit Request message to the serving PoS which is located on the WiMAX access network. 3) The serving PoS transmits the MIH_MN_HO_Commit.indication to MIH user. 4) The MIH user sends the MIH_M2N_HO_Commit.request to the serving PoS to reserve for resource availability at the target PoSs. 5) The serving PoS transmits MIH_N2N_HO_Commit Request message to the target PoS which is located on the WiFi access network. 6) The MIH_N2N_HO_Commit.indication is forwarded by the target PoS to MIH user. 7) The result of the resource reservation is sent to the target PoS through the MIH_N2N_HO_Commit.response. 8) The target PoS sends the MIH_N2N_HO_Commit Response message to the serving PoS which is located on WiMAX access network. 9) The serving PoS forwards the MIH_N2N_HO_Commit.confirm to the MIH user. 10) The MIH user sends MIH_MN_HO_Commit.response to the serving PoS. 11) The serving PoS transmits the MIH_MN_HO_Commit Response message to the MIHF of the MN. 12) The MIHF forwards the MIH_MN_HO_Commit.confirm to the MIH user.
Phase 4.	Upon receiving the MIH_N2N_HO_Commit Request message, the Access Point (AP) queries the incoming MN's profile to HSS/AAA server which is located on the EPC. Furthermore, the authentication procedure is performed. The following are the detailed procedure: 1) The AP sends the AAR message to the HSS/AAA server. 2) The HSS/AAA server answers with the AAA message.
Phase 5.	After receiving the MIH_MN_Commit.confirm, the MIH user will trigger a WiFi layer 2 (L2) connections. The following are the detailed procedure: 1) The MIH user of the MN sends the MIH_Link_Actions.request to MIHF. 2) The MIHF sends the MIH_Link_Actions.confirm to the MIH user when the radio link bearer is confirmed. 3) The MAC 802.11 sends the Link_Up.indication to the MIHF when the connection is established. 4) The MIHF forwards the MIH_Link_Up.indication to the MIH user.
Phase 6.	Once the MN establishes the layer 2 connection to the target PoS. The MN updates its IP address to the RVS which locates at the operation network to keep its contact information accurate, and then RVS notifies CN that IP address of the MN changes. The following are the detailed procedure: 1) The MIH user of the MN sends the I1 message to the RVS. In turn, the RVS forwards the I1 message to the CN. 2) The CN sends the R1 message to the MIH user. 3) The MIH user sends the I2 message to the CN. 4) The CN sends the R2 message to the MIH user.
Phase 7.	When the handover completed, the MIH user of the MN informs all the implied Network Elements (NEs) of the handover finalization. Moreover, resources over WiMAX are released. After this, data can be transfer via the WiFi. The following are the detailed procedure: 1) The MIH user of the MN sends the MIH_MN_HO_Complete.reuqest to MIHF. 2) The MIHF transmits the MIH_MN_HO_Complete Request message to target PoS on the WiFi access network, which becomes the new serving PoS. 3) The target PoS sends the MIH_MN_HO_Complete.indication to the MIH user. 4) The MIH user sends the MIH_N2N_HO_Complete.request to the target PoS. 5) The target PoS sends an MIH_N2N_HO_Complete Request message to the previous serving PoS which is located on the WiMAX access network to release resource, which was allocated to the MN. 6) The serving PoS sends MIH_N2N_HO_Complete.indication to the MIHF. 7) After resource is successfully released, the MIHF sends the MIH_N2N_HO_Complete.response to the serving PoS. 8) The serving PoS forwards the MIH_N2N_HO_Complete Response message to the target PoS which is located on the WiFi access network. 9) The target PoS transmits the MIH_N2N_HO_Complete.confirm to the MIH user. 10) The MIH user informs the target PoS that the procedure has finished through the

MIH_MN_HO_Complete.response.

11) The target PoS transmits the MIH_MN_HO_Complete Response message to the MIHF of the MN.

12) The MIHF forwards the MIH_MN_HO_Complete.confim to the MIH user.



Mobile Node
UP Entity
MIH User
MIH Function
MAC 802.16
MAC 802.11
WiMAX Access Network
Base Station (BS)
PoS Serving
MIH User
Server Side
MIIS Server
RVS
WiFi Access Network
Access Point (AP)
PoS Candidate
MIH User
EPC
HSS/AAA
Correspondent Node
MIH User
UP Entity
Traffic flow over WiMAX
PHASE 1.
MIH_Get_Information.request
MIH_Get_Information Request
MIH_Get_Information Response
MIH_Get_Information.confirm
PHASE 2.
MIH_MN_HO_Candidate_Query.request
MIH_MN_HO_Candidate_Query Request
MIH_MN_HO_Candidate_Query.indication
MIH_N2N_HO_Query_Resources.request
MIH_N2N_HO_Query_Resources Request
MIH_N2N_HO_Query_ Resources.indication
MIH_N2N_HO_Query_ Resources.response
MIH_N2N_HO_Query_Resources Response
MIH_N2N_HO_Query_Resources.confirm
MIH_MN_HO_Candidate_Query.response
MIH_MN_HO_Candidate_Query.Response
MIH_MN_HO_Candidate_Query.confirm
PHASE 3.
MIH_MN_HO_Commit.request
MIH_MN_HO_Commit Request
MIH_MN_HO_Commit.request
MIH_N2N_HO_Commit.request
MIH_N2N_HO_Commit Request
PHASE 4.
AAR
AAA
MIH_N2N_HO_Commit.indication
MIH_N2N_HO_Commit Response
MIH_N2N_HO_Commit.response
MIH_N2N_HO_Commit.confirm
MIH_MN_HO_Commit.response
MIH_MN_HO_Commit Response
MIH_MN_HO_Commit.confirm
PHASE 5.
MIH_Link_Actions.request
MIH_Link_Actions.confirm
Link_Up.indication
MIH_Link_Up.indication
PHASE 6.
I1(I, RVS, HIT-I, HIT-R)
I1(RVS, R, HIT-I, HIT-R, FROM:I, RVS_HMAC)
R1(R, I, HIT-R, HIT-I, VIA:RVS)
I2(I, R, HIT-I, HIT-R)
R2(R, I, HIT-R, HIT-I)
Traffic flow over WiFi
PHASE 7.
MIH_MN_HO_Complete.request
MIH_MN_HO_Complete Request
MIH_MN_HO_Complete.indication
MIH_N2N_HO_Complete.request
MIH_N2N_HO_Complete Request
MIH_N2N_HO_Complete.indication
MIH_N2N_HO_Complete.response
MIH_N2N_HO_Complete Response
MIH_N2N_HO_Complete.confirm
MIH_MN_HO_Complete Response
MIH_MN_HO_Complete.response
MIH_MN_HO_Complete.confirm

Figure 9. WiMAX to WiFi handover procedure

V. CONCLUSIONS AND FUTURE WORKS

In this paper, we presented an integrated architectural to accomplish seamless mobility between heterogeneous wireless networks. The idea is MIH-based HIP mobility management protocol. MIH offers the common interface and negotiation mechanism among heterogeneous wireless networks. We use HIP mobility management to solve problems of mobility and multi-homing. Moreover, the Diameter Protocol is used for authentication of registered users. We wish the architecture can accomplish seamless mobility between heterogeneous wireless networks and performance improving. We also design a complete handover execution mechanism among heterogeneous wireless networks. The handover procedures will utilize MIH framework and composite HIP protocol. Diameter protocol will solve the AAA operations. A complete handover mechanism for heterogeneous wireless network should include handover decision algorithm besides handover execution. A good handover decision algorithm is very important to avoid unnecessary handover execution when mobile users roam in heterogeneous wireless network. Therefore, handover decision algorithm will be the objective of our upcoming research. A complete handover mechanism enables mobile user roam in heterogeneous wireless network more smoothly.

REFERENCES

[1] IEEE P802.21/D14, "Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services," Sep. 2008.

[2] R. Moskowitz, et al., "Host Identity Protocol," RFC 5201, April 2008.

[3] R. Moskowitz, et al., "Host Identity Protocol (HIP) Architecture," RFC 4423, May 2006.

[4] J. Laganier, et al., "Host Identity Protocol (HIP) Rendezvous Extension," RFC 5204, April 2008.

[5] P. Calhoun, et al., "Diameter base protocol," RFC 3588, September 2003.

[6] P. Calhoun, et al., "Diameter Network Access Server Application," RFC 4005, August 2005.

[7] George Lampropoulos, "Media-Independent Handover for Seamless Service Provision in Heterogeneous Network," IEEE Commun. Mag., Vol. 46, Issue 1, pp.64-71, Jan. 2008.

[8] 3GPP TS 23.402 V1.0.0, "3gPP System Architecture Evolution: Architecture Enhancements for Non-3GPP Accesses (Rel. 8)," May 2007.

[9] Madjid Nakhjiri and Mahsa Nakhjiri, "AAA and network security for mobile access : radius, diameter, EAP, PKI, and IP mobility," John Wiley & Sons Ltd, 2005.

[10] Andrei Gurtov, "Host Identity Protocol (HIP) : Towards the Secure Mobile Internet," John Wiley & Sons Ltd, UK, 2008.

[11] Nitul Dutta, Iti Saha Misra, Abhishek Majumder, "Mathematical Analysis of Signaling Overhead in MIPv6 Based N-Layer Architecture", JCIT: Journal of Convergence Information Technology, Vol. 5, No. 8, pp. 252 ~ 261, 2010

[12] Hasina Attaullah , Muhammad Younus Javed , "QoS based Vertical handover between UMTS, WiFi and WiMAX Networks ", JCIT: Journal of Convergence Information Technology, Vol. 4, No. 3, pp. 59 ~ 64, 2009

[13] Pyung-Soo Kim, and Yong Jin Kim, "Hierarchical Mobile IPv6 Based Fast Vertical Handover using IEEE 802.21 Media Independent Handover Function", JCIT: Journal of Convergence Information Technology, Vol. 2, No. 4, pp.41 ~ pp.45, 2007