Overview of IEEE 802.21 Security Issues for MIH Networks

Ismail Saadat[1], Fábio Buiati[2], Delfín Rupérez Cañas[3] and Luis Javier García Villalba[4]

Grupo de Análisis, Seguridad y Sistemas (GASS)
Departamento de Ingeniería del Software e Inteligencia Artificial (DISIA)
Facultad de Informática, Despacho 431
Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n,
Ciudad Universitaria, 28040 Madrid, Spain

[1] saadat@fdi.ucm.es

[2] fabio@fdi.ucm.es

[3] delfinrc@fdi.ucm.es

[4] javiergv@fdi.ucm.es

***Abstract* - The convergence of different but complementary wireless networks brings the mobile user the opportunity to choose the network under an Always Best Connected scheme. In this heterogeneous environment the user can move between different administrative domains, aiming to make an inter-domain handover in a seamless manner. The IEEE 802.21 standard specifies a network information server entity providing network information within a geographical area by which the user can discover a service or a network. It is essential that the information comes from a reliable source. In this article, we describe the main technical requirements in order to establish a secure channel between the user and the information server. We also specify a scenario in which a proactive authentication mechanism is performed through an authentication server, focusing on optimization of the handover process.**

***Index Terms* — Mobility, MPA, IEEE 802.21, Heterogeneous Networks, Inter-Domain, Security.**

I. Introduction

The significant increase of usage wireless networks such as Wi-Fi, Wi-Max and 3G, brings the mobile user the ability to make handovers under an Always Best Connected [1] scheme. In general, the handover process is divided into three main phases [2]: system discovery, handover decision and handover execution.

In the system discovery phase, the most important requirement is to provide the Mobile Node (MN) with sufficient information about neighbor networks to make an accurate handover decision. In the second phase, the user should choose a network based on several parameters such as quality of service (QoS), receive signal strength, access point geographical location, security mechanisms and so on. Finally, in the handover execution phase the connection is routed to the new access point in a seamless way.

In the literature [3] [4], the neighbor information discovery is the most time-consuming phase in the handover process. In this way, the network information discovery phase is highly critical. To accomplish it, the MN can consult a network information server, which can store information from several networks and operators. The IEEE 802.21 standard [5] specifies a media independent information service (MIIS) providing network information within a geographical area by which the user can discover a service or a network. However, it is essential that the information comes from a reliable source. This requirement is even more imperative when handovers are done across different administrative domains. Accessing critical information from other operator through non-secure links, and 3rd party servers, raises important security risk as well.

The MIIS needs both to protect itself from attack and provide MN provable trust, in order that they can exchange the information securely and make their handovers decisions without fear of malicious inaccuracies or mischief.

One solution in secure inter-domain handover is presented in [6]. The authors propose a Media-Independent Pre-Authentication (MPA) which is a mobile-assisted higher-layer authentication, authorization and handover scheme that is performed prior to establishing L2 connectivity to a network where mobile may move in near future. Using such a technique, the MN can establish a secure channel with the information server, performing a security communication.

The rest of this article is organized as follows. Initially, we briefly present the main entities and services of the emerging IEEE 802.21 standard are showed focusing on the information server domain as well as the related work on the security subject. Then we introduce the MPA protocol structure, including its elements and the communication process.

Subsequently, we present a realistic scenario in which the MN performs an inter-domain handover obtaining the network information from a secure information server using the MPA protocol. As a final point, we conclude this work with some final considerations and open topics for future works.

II. IEEE 802.21 Background and Related Work

A. IEEE 802.21 Background

The IEEE 802.21 standard [5] specifies a Media Independent Handover (MIH) framework that facilitates handover in heterogeneous access networks by exchanging information and defining commands and event triggers to assist in the handover decision making process. Specifically the standard consists of a framework that enables service continuity while a MN transitions between heterogeneous link-layer technologies. Also, it defines a new logical entity created therein called the media independent handover function (MIHF).

The MIHF is the central entity of the emerging IEEE 802.21 standard, as illustrated in Fig.1. Its primary roles are to facilitate handovers and provide intelligence to the network selector entity.

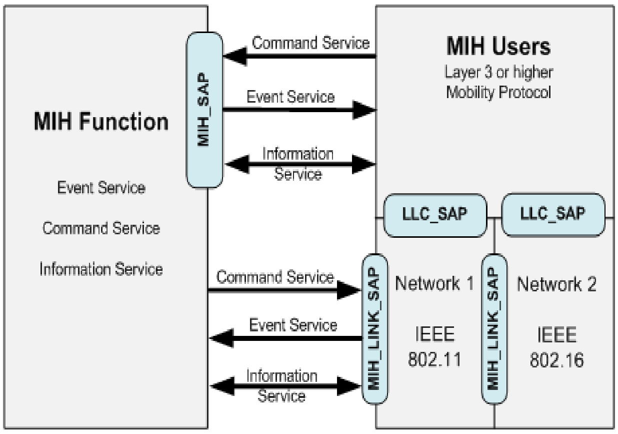

Fig. 1 MIH Architecture Overview

The MIHF also provides three primary services: event services, command services and information services. These services help the MIH users maintaining service continuity, quality of service monitoring, battery life conservation, and network discovery and link selection. A detailed explanation of each mobility service follows.

The *media independent event service (MIES)* is responsible for detecting events at lower layers and reporting them from both local and remote interfaces to the upper layers (the MIH users). A transport protocol is needed for supporting remote events. These events may indicate changes in state and transmission behavior of the physical, data link and logical link layers, or predict state changes of these layers.

The *media independent command service (MICS)* refers to the commands sent from MIH users to the lower (physical, data link, and logical link) layers in order to control it. The commands generally carry the upper layer decisions to the lower layers on the local device entity or at the remote entity. MIH users may utilize command services to determine the status of links and/or control the multi-mode device for optimal performance.

The *media independent information Service (MIIS)* provides a framework and corresponding mechanisms by means of which a MIHF entity may discover and obtain network information existing within a geographical area to facilitate the handovers. MIIS includes support for various information elements which provide information that is essential for a network selector to make intelligent handover decisions. The information may be present in some MIIS server where the MIHF in the MN may access it. Moreover, the MIIS provides capability for obtaining information about lower layers such as neighbor maps and other link layer parameters, as well as information about available higher layer services such as internet connectivity. For instance knowledge of whether security, supported channels, cost per use, networks categories (such as public, enterprise, home) and QoS supported may influence the decision to select such an access network during handover process.

The information supplied by the MIIS is provided in Information Elements (IE) which can relate to higher layer services such as availability of IP mobility schemes at a certain operator, or to lower layer such as link neighbor maps and link configuration parameters (as illustrated in Fig.2). More concretely, information available via the MIIS can be categorized as:

- General and Access Network Specific Information: general overview of different networks, providing coverage within a specific area such as network type, operator and service identifier. Information including QoS, security, technology revision and cost is also available.
- Link connection point information: information about points of attachment for each access network available, comprising aspects such as MAC address of the access point, geographical location, channel configuration, and so on.
- Other information: network, service or vendor specific information.

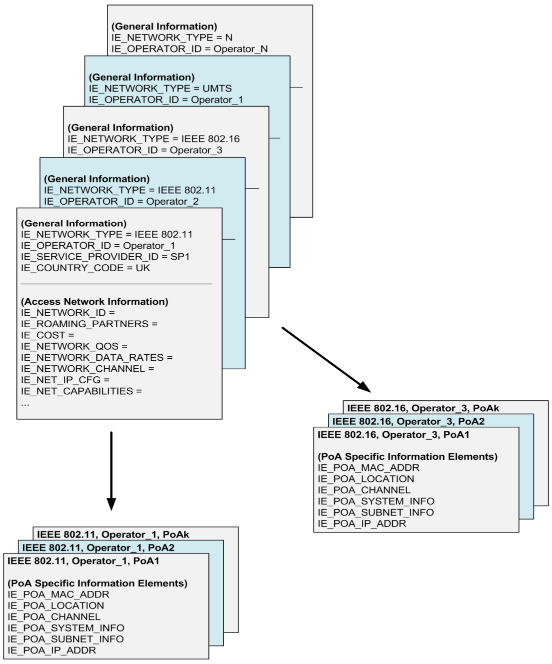
(General Information)
IE_NETWORK_TYPE = N
IE_OPERATOR_ID = Operator_N
(General Information)
IE_NETWORK_TYPE = UMTS
IE_OPERATOR_ID = Operator_1
(General Information)
IE_NETWORK_TYPE = IEEE 802.16
IE_OPERATOR_ID = Operator_3
(General Information)
IE_NETWORK_TYPE = IEEE 802.11
IE_OPERATOR_ID = Operator_2
(General Information)
IE_NETWORK_TYPE = IEEE 802.11
IE_OPERATOR_ID = Operator_1
IE_SERVICE_PROVIDER_ID = SP1
IE_COUNTRY_CODE = UK
(Access Network Information)
IE_NETWORK_ID =
IE_ROAMING_PARTNERS =
IE_COST =
IE_NETWORK_QOS =
IE_NETWORK_DATA_RATES =
IE_NETWORK_CHANNEL =
IE_NET_IP_CFG =
IE_NET_CAPABILITIES =
...
IEEE 802.16, Operator_3, PoAk
IEEE 802.16, Operator_3, PoA2
IEEE 802.16, Operator_3, PoA1
(PoA Specific Information Elements)
IE_POA_MAC_ADDR
IE_POA_LOCATION
IE_POA_CHANNEL
IE_POA_SYSTEM_INFO
IE_POA_SUBNET_INFO
IE_POA_IP_ADDR
IEEE 802.11, Operator_1, PoAk
IEEE 802.11, Operator_1, PoA2
IEEE 802.11, Operator_1, PoA1
(PoA Specific Information Elements)
IE_POA_MAC_ADDR
IE_POA_LOCATION
IE_POA_CHANNEL
IE_POA_SYSTEM_INFO
IE_POA_SUBNET_INFO
IE_POA_IP_ADDR

Fig. 2 MIIS Information Elements

Detailed information about the IEEE 802.21 standard, its services and characteristics can be found in [7] and [8].

B. Related Work

The research community has been very active in recent years in reducing the disruptive effects of network handovers by proposing optimizations to existing mechanisms that add to existing mechanisms and external services and protocols that the help the transition from one network to another. However, there are few security mechanisms for MIH services in the literature.

To ensure the validity of data communication between a MN and MIIS server or any MIH entity, the IETF MOBOPTS WG[1] is specifying a new secure handover optimization mechanism denoted media-independent pre-authentication (MPA) framework [6][7] that works over any link-layer and with any mobility management protocol including Mobile IPv4, Mobile IPv6, MOBIKE, HIP and SIP mobility. The same authors are working in the IEEE 802.21a task group, the security extension to the existing IEEE 802.21 standard.

In [10], the authors present a flexible architecture which can efficiently handle the secure and seamless mobility issue in Wi-Fi / Wi-Max integrated networks deployed for enterprise system, completing most parts of authentication and key exchange process at the stage of initialization and handover procedure.

A new security scheme is presented by authors in [11]. They propose an efficient handover mechanism among Wi-Fi and Wi-Max networks which allows a seamless roaming process by reducing the authentication processes. This scheme also involves security mechanisms that guarantee the handover messages to be secure and maintain the authenticity. The authors still need to simulate the proposed scheme. The simulation will focus on time spent during authentication phase.

The authors in [12] propose a novel scheme to transport 802.21 messages over a secure network layer protocol denoted PLA that has built in hop-by-hop security mechanism. This scheme has the advantage that ensures very strong security of the signaling framework without much overhead. PLA-MIH reduces the latency during the MIH signaling. On the other hand, this work is only theoretical and the authors intend to do a detailed simulation scenario in future.

In [13], proactive authentication techniques and MIH protocol level security mechanisms are elaborated. Proactive authentication is a process by which an entity can perform a-priori network access authentication with a media independent authenticator and key holder (MIA-KH) that is serving a candidate network. The entity performs such authentication in anticipation of handover to the neighboring networks.

In [14] the authors propose an access authentication scheme with user anonymity denoted Secure Access of MIIS (SAM). The scheme provides an anonymous access authentication of MIIS considering that the access control for information is applied through an access authentication controller. The protocol can be used to establish a secure channel between the mobile node and the information server. The solution has the advantages of lightweight computation, low communication cost, and easy implementation, but it could have the disadvantage in a MIIS hierarchical framework.

In [15], Won et al propose a secure message transport (MIHSec) using the Master Shared Key (MSK) in order to overcome the handover overhead and hence minimizes authentication time. The MIHSec operates at the application layer and utilizes Extensible Authentication Protocol (EAP) to provide security to MIH messages.

In [16] the authors use the information capabilities provided by IEEE 802.21 and propose an extension to current network selection algorithms that takes into account security parameters and policies to optimize the handover performance and reduce the negotiation delay. The authors present two modular extensions to network selection algorithms that prevent the problems resulting from incompatible security policies, and provide more accurate security signaling delay estimations, which, in turn, result in more accurate handover delay

[1] IP Mobility Optimizations (Mob Opts) Research Group. The research group addresses questions of an evolutionary nature, starting with the current Mobile IP architecture, including handover optimizations such as Fast Handover and Hierarchical Mobile IP.

estimations.

III. MEDIA PRE-AUTHENTICATION PROTOCOL (MPA)

The MPA [9] is a mobile-assisted higher-layer authentication, authorization and handover scheme that is performed prior to establishing link-layer connectivity to a network in which a MN may move in near future. As mentioned before, the MPA mobility optimization works with any mobility management protocol. With MPA, a MN can set parameters for Candidate Target Network (CTN) and also able to send and receive IP packets using the IP address obtained before it actually attaches to the CTN. Fig. 3 shows the main MPA functional components.

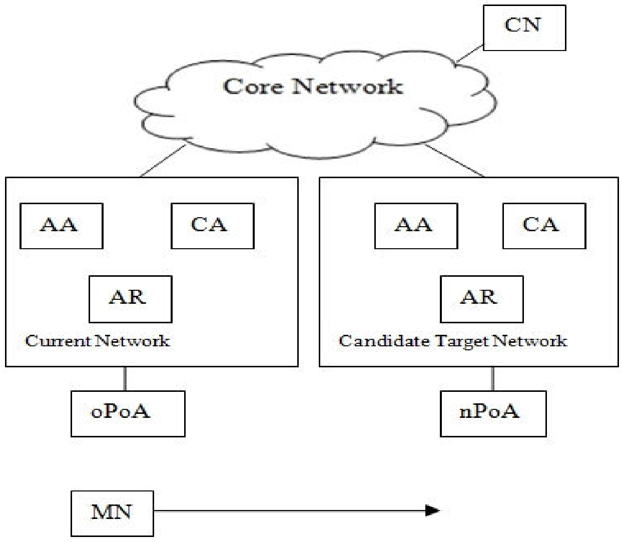

Fig. 3 MPA Functional Components

In the MPA framework, the following functional elements are expected to reside in each CTN to communicate with a MN:

Authentication Agent (AA): it is responsible for the pre-authentication phase. An authentication protocol is executed between the MN and the authentication agent to establish an MPA-SA (MPA Secure Association). The authentication protocol should can to interact with an AAA entity such as Radius and Diameter to carry authentication credentials to an appropriate authentication server in the AAA infrastructure. The EAP (Extensible Authentication Protocol) [17] or ERP (EAP Reauthentication Protocol) [18] can be used as the authentication protocol for MPA.

Configuration Agent (CA): it is responsible for one part of the pre-configuration phase, namely securely executing a configuration protocol to deliver an IP address and other configuration parameters to the MN. DHCP is an example of a configuration protocol that can be used to the configuration process.

Access Router (AR): it is a router that is responsible for the other part of pre-configuration process.

A. MPA Protocol Flow

In the MPA protocol flow, illustrated in Fig. 4, we assume that the MN is already connected to a point of attachment referred to as the old point of attachment (oPoA) and assigned an old CoA (oCoA). Next we explain each phase of the MPA process:

1) Stage 1: Pre-Authentication: The MN finds a CTN through a discovery process, and obtains the address and capabilities of the AA, CA, and AR in the CTN. The MN pre-authenticates with the authentication agent. If the pre-authentication is successful, an MPA-SA is created between the MN and the authentication agent. Two keys are derived from the MPA-SA, a MN-CA and MN-AR keys, which are used to protect subsequent signaling messages of a configuration protocol and a tunnel management protocol, respectively. The MN-CA and MN-AR keys are then securely delivered to the configuration agent and access router. Layer 2 pre-authentication is initiated at this stage.

2) Stage 2: Pre-configuration: The MN realizes that its point of attachment is likely to change from oPoA to a new one, denoted new point of attachment (nPoA). Then it performs pre-configuration with the configuration agent to obtain several configuration parameters and default router from the CTN. The MN then communicates with the access router using the tunnel management protocol. A configuration protocol and a tunnel management protocol may be combined in a single protocol or executed in different orders depending on the actual protocol(s) used for configuration and tunnel management.

After completion of the tunnel establishment, the MN can communicate using both old *care-of address* (oCoA) and new *care-of address* (nCoA) by the end of step 3.

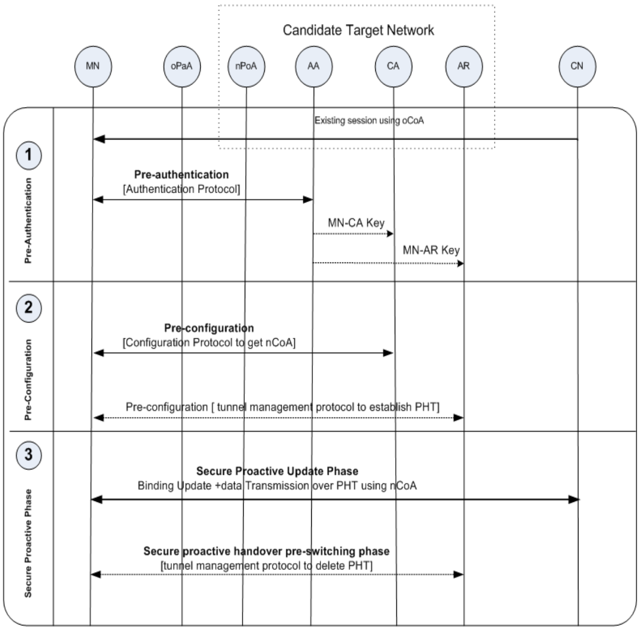
Candidate Target Network
MN
oPaA
nPoA
AA
CA
AR
CN
Existing session using oCoA
1
Pre-Authentication
Pre-authentication
[Authentication Protocol]
MN-CA Key
MN-AR Key
2
Pre-Configuration
Pre-configuration
[Configuration Protocol to get nCoA]
Pre-configuration [tunnel management protocol to establish PHT]
3
Secure Proactive Phase
Secure Proactive Update Phase
Binding Update +data Transmission over PHT using nCoA
Secure proactive handover pre-switching phase
[tunnel management protocol to delete PHT]

Fig 4 MPA Phases

3) Stage 3: Secure proactive handover: The MN decides to switch to the nPoA. Before it switches to the nPoA, it starts a secure proactive handover by executing the binding update operation using a mobility management protocol and transmitting subsequent data traffic over the tunnel. This stage is divided into two minor phases:

- *Secure proactive handover pre-switching (sub-phase)*: The MN completes the binding update and becomes ready to switch to the new point of attachment. The MN might execute the tunnel management protocol to delete or disable the proactive handover tunnel and cache nCoA after deletion or disabling of the tunnel. This transient tunnel can be deleted prior to or after the handover. In this step, link-layer handover occurs.
- *Secure proactive handover post-switching (sub-phase)*: The MN executes the switching procedure. Upon successful completion of the switching procedure, the mobile node immediately restores the cached nCoA and assigns it to the physical interface attached to nPoA. If the proactive handover tunnel was not deleted or disabled, the tunnel is deleted or disabled as well. After this, direct transmission of data packets using nCoA is possible without using the tunnel.

B. MPA Applicability

The MPA can be used to optimize the mobility protocols that work in the network and application layers. The authors recommend that the MPA has more accuracy when the prediction of movement can be easily done. In other words, MPA is more viable as a solution for inter-domain predictive handover without the simultaneous use of multiple interfaces. Since MPA is not tied to a specific mobility protocol, it is also applicable to support optimization for inter-domain handover where each domain may be equipped with a different mobility protocol.

IV. PRACTICAL HANDOVER SCENARIO

This section presents a practical handover scenario that takes advantage of Wi-Fi and Wi-Max networks in which the MN get information from a secure IEEE 802.21 MIIS, as illustrated in the Fig. 5. We consider the MN as a multimodal device (equipped with two interfaces: Wi-Fi and Wi-Max). We assume that the MN is already connected to a point of attachment as the old point of attachment (oPoA) Wi-Max BS. The MIIS server is located in anywhere in the Internet. There is an AS (Authentication Server) that provides MIH level protection independent to media and access network.

Initially, the MN resides in Network1 and moves from its domain to another domain and in the process changes its subnet. Network 2 is the (nPoA) Wi-Fi AP, Network 3 is where the CN resides, and finally, Network 4 is where the MIIS server resides. Next we explain the signaling flow and how the MN obtains information from the MIIS in a secure manner.

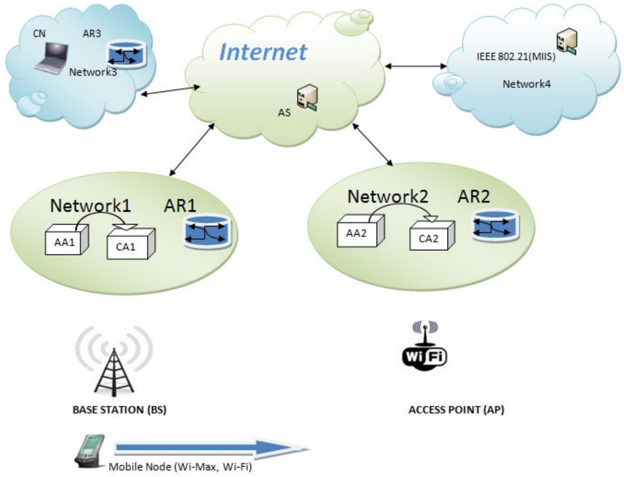

Fig. 5 Integrated Wi-Fi and Wi-Max scenario

Fig. 6 depicts the handover signaling and mechanisms in an MPA scenario in which the MN is initially connected to the Wi-Max BS belonging to the Network1. We have divided the signaling into six minor phases, as follows:

At point 1, upon receiving a beacon from the Wi-Fi AP followed by a "*MIH_Link_Detected"* event from MAC layer toward the MIHF, the MN becomes aware of new connectivity opportunity. Discovery of neighboring networking elements such as access points, access routers, authentication servers helps expedite the handover process during a mobile's movement between networks.

At point 2, the MN first performs an authentication process with the AS server. Upon a successful authentication, a key is generated to the MIIS server (MN-MIIS). Then, the MN is authorized to ask the MIIS server for more information about the detected PoA. First, is sends a "*MIH_Get_Information request*" to the MIIS that answers with a "*MIH_Get_Information response*" message. In this phase, the MN also checks the resources availability at the candidate PoA (AP) and decides to make a handover. At the final, the MN obtains the IP addresses of AA2, CA2 AR2 from Network2.

At point 3, after the handover decision making, the MPA signaling starts (pre-authentication phase). The MN performs a pre-authentication with the authentication agent. If pre-authentication is successful, an MPA-SA is created between AA2 and MN. Two keys are derived from the MPA-SA, namely an MN-CA2 key and MN-AR2 key, which are used to protect subsequent signaling messages. The keys are then securely delivered to the CA2 and the AR2, respectively.

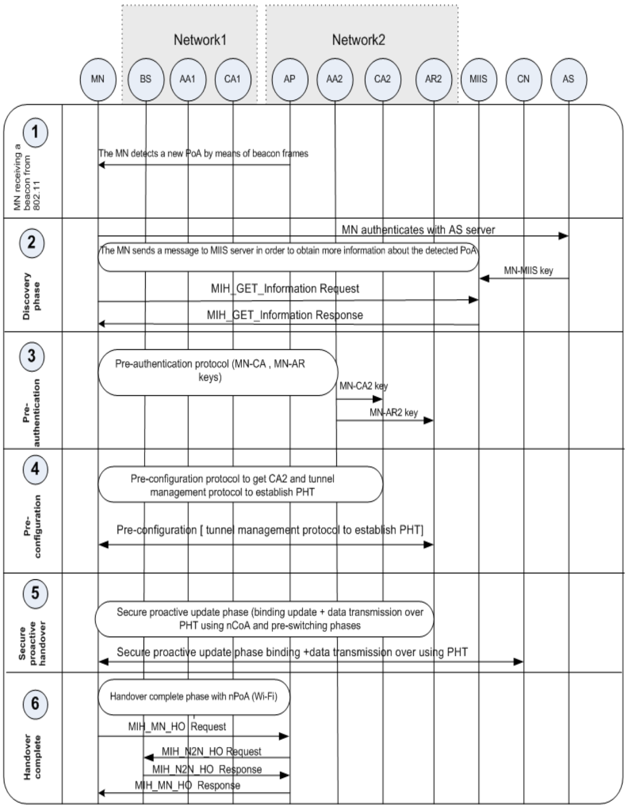
Network1
Network2
MN
BS
AA1
CA1
AP
AA2
CA2
AR2
MIIS
CN
AS
1
MN receiving a beacon from 802.11
The MN detects a new PoA by means of beacon frames
2
Discovery phase
MN authenticates with AS server
The MN sends a message to MIIS server in order to obtain more information about the detected PoA
MN-MIIS key
MIH_GET_Information Request
MIH_GET_Information Response
3
Pre-authentication
Pre-authentication protocol (MN-CA , MN-AR keys)
MN-CA2 key
MN-AR2 key
4
Pre-configuration
Pre-configuration protocol to get CA2 and tunnel management protocol to establish PHT
Pre-configuration [tunnel management protocol to establish PHT]
5
Secure proactive handover
Secure proactive update phase (binding update + data transmission over PHT using nCoA and pre-switching phases
Secure proactive update phase binding +data transmission over using PHT
6
Handover complete
Handover complete phase with nPoA (Wi-Fi)
MIH_MN_HO Request
MIH_N2N_HO Request
MIH_N2N_HO Response
MIH_MN_HO Response

Fig. 6 Handover signaling flow with a secure MIIS server.

At point 4, (pre-configuration phase), the MN realizes that its attachment is likely to change from Wi-Max (oPoA) to Wi-Fi (nPoA). It then performs a pre-configuration with CA2 using the configuration protocol to obtain several configuration parameters such as a new IP address and default router from Network2. The MN then starts a communication with the access router in Network2 using the tunnel management protocol to establish a proactive handover tunnel. The MN is able to communicate using both IP address from Network1 and IP address from Network2 by the end point 4. The signaling messages of the pre-configuration protocol are protected using the MN-CA2 key and the MN-AR2 key.

At point 5, (secure proactive handover), before the MN completes the binding update and becomes ready to switch to Wi-Fi, it starts secure proactive handover by executing the binding update operation of a mobility management protocol and transmitting data traffic over the tunnel. The MN may choose new addresses as the binding update address and send it to the CN. The MN completes the binding update and ready to switch to the Wi-Fi network. After that, the MN deletes or disables the proactive handover tunnel. The decision as to when the mobile node is ready to switch to the new point of attachment depends on the handover policy.

At Point 6, the MN finalizes the inter-domain handover by sending a "*MIH_MN _Handover_complete request*" message to the new PoA which confirms with the old PoA. Upon receiving the confirmation, the new PoA sends a "*MIH_MN _Handover_complete response*" message back to the MN. Finally, the MN releases the allocated Wi-Max resources and deactivates the it´s corresponding interface.

V. CONCLUSION

In this article we have discussed the main characteristics and security issues in an inter-domain handover in heterogeneous wireless networks. We first described the MPA and its functional components. Then, through a practical scenario, we show an inter-domain signaling flow in which the MN can obtain information from a MIIS server in a secure manner.

As future work, we are working in a specification of new security mechanism as well as new deployment real implementations modules.

ACKNOWLEDGMENTS

This work was supported by the Ministerio de Industria, Turismo y Comercio (MITyC, Spain) through the Project Avanza Competitividad I+D+I TSI-020100-2010-482 and the Ministerio de Ciencia e Innovación (MICINN, Spain) through the Project TEC2010-18894/TCM.

REFERENCES

[1] E. Gustafsson and A. Johnson, “Always Best Connected,” IEEE Wireless Communications, Vol. 10, No. 1, pp. 49-55, 2003.

[2] J. Manner and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[3] Sang-Jo Yoo, David Cypher and Nada Golmie, “Timely Effective Handover Mechanism in Heterogeneous Wireless Networks,” Proceedings of the Springer Wireless Personal Communications, 2008.

[4] J. Floroiu, M. Corici, Byoung-Joon Lee, S. Lee, S.Arbanowski, and T. Magedanz, “A Vertical Handover Architecture for End-to-End Service Optimization,” 16th IST Mobile and Wireless Communications Summit, 2007, July 2007.

[5] IEEE 802.21 Standard, “Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services”, January 2009.

[6] A. Dutta et al, “Media-Independent Pre-Authentication Supporting Secure Interdomain Handover Optimization”, IEEE Wireless Communications, Vol. 15, No. 2, pp. 55-64, April 2008.

[7] A. Oliva, A. Banchs, I. Soto, T. Melia and A.Vidal, “An Overview of IEEE 802.21: Media-Independent Handover Services”, IEEE Wireless Communications, Vol. 15 (4), pp. 96-103, August 2008.

[8] G. Lampropoulos, A. Salkintzis and N. Passas, "Media-Independent Handover for Seamless Service Provision in Heterogeneous Networks", IEEE Communications Magazine, Vol. 46 (1), pp. 64-71, January 2008.

[9] A. Dutta, (Ed.), Y. Yohba, V. Fajardo, K. Taniuchi & H. Schulzrinneh, “A Framework of Media Independent Pre-Authentication (MPA) for Inter-Domain Handover Optimization”, draft-irtf-mobopts-mpa-framework-08.txt, September 2010, (work in progress).

[10] J. Zhao, J. Pan and L. Hou, “Security and Seamless Mobility Based Architecture for Hybrid Network of Enterprise”, 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09, pp. 1, September 2009.

[11] H. Sun, S Chen, Y. Chen et al, “Secure and Efficient Handover Scheme for Heterogeneous Networks”, IEEE Asia-Pacific Services Computing Conference, 2008. APSCC '08, pp. 205, December 2008.

[12] S. Saha and D. Lagutin, “PLA-MIH: A Secure IEEE802.21 Signaling Scheme”, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009, pp. 252 – 257, November 2009.

[13] S. Das, A. Dutta, and T. Kodama, “Proactive authentication and MIH security,” 2009, https://mentor.ieee.org/802.21/documents.

[14] Guangsong Li, Qi Jiang, Xi Chen and Jianfeng Ma, “Secure Access Authentication for Media Independent Information Service”, EURASIP Journal on Wireless Communications and Networking, Volume 2010, Article ID 249169.

[15] J. Won, M. Vadapalli, C. Cho, and V. Leung, “Secure Media Independent Handover Message Transport in Heterogeneous Networks,” EURASIP Journal on Wireless Communications and Networking, Volume 2009, Article ID 716480.

[16] Antonio Izquierdo and Nada T. Golmie, “Improving Security Information Gathering with IEEE 802.21 to Optimize Handover Performance”, ACM. 2009.

[17] B. Aboba, D. Simon, and P. Eronen, “Extensible Authentication Protocol (EAP) Key Management Framework,” RFC 5247, 2008.

[18] V. Narayan and L. Dondeti, “EAP extensions for EAP re-authentication protocol (ERP),” RFC 5296, 2008.