Fast and Secure Handover Schemes Based on Proposed WiMAX over EPON Network Security Architecture

WEN GU, STAMATIOS V. KARTALOPOULOS, PRAMODE K. VERMA
School of Electrical and Computer Engineering
The University of Oklahoma
4502 E. 41st Street, Tulsa, OK 74135
UNITED STATES OF AMERICA
wen-gu@ou.edu, kartalopoulos@ou.edu, pverma@ou.edu http://tcom.ou.edu

Abstract: - In recent years, the integration of Worldwide Interoperability for Microwave Access (WiMAX) and Ethernet Passive Optical Network (EPON) has become one of the most promising broadband access solutions. The EPON network provides tremendous bandwidth while the WiMAX network can support mobility. Integration of PON and WiMAX combines the best of both technologies. However, the integration requires advanced secure mechanisms to overcome vulnerabilities of wireless mobile protocols. In this paper, we propose an end-to-end network architecture based on WiMAX over EPON networks, and we present a security framework that adopts the RSA protocol and the Extensible Authentication Protocol (EAP). We introduce three handover scenarios in the integrated network and propose the corresponding handover schemes. In the proposed handover schemes, we utilize a pre-authentication method for the authorization key (AK) pre-distribution, and we use the communication framework of the ranging step to implement mutual authentication between the subscriber and the mobile network. Through our analysis, we show that the proposed handover mechanisms can simplify and accelerate the handover process compared to the standard WiMAX handover scheme while keeping the handover procedure secure.

Key-Words: - WiMAX over EPON, Handover Security, Pre-authentication, Ranging

1 Introduction

Broadband access networks have experienced rapid development over the last decade. The Passive Optical Network (PON) is now deployed widely around the world providing substantial bandwidth and long transmission ranges. PONs using the time division multiplexing (TDM) technology are called TDM-PONs, such as EPON [1] and Gigabit PON (GPON) [2]. Wavelength division multiplexing PONs, (WDM)-PONs [3], utilizes the WDM technology to provide up to 1 Gbps bandwidth to the subscribers. Coarse WDM (CWDM)/TDM-PONs [4, 5] combine CWDM and TDM technologies to deliver elastic bandwidth on demand to end users. However, the fiber network lacks mobility and the installation is costly and also restricted by the geographic environment. Therefore, wireless access networks play an important role to realize the anytime and anywhere telecommunication and data services, including the Internet.

The WiMAX technology, based on IEEE 802.16 – 2004 standard [6], defines a fixed broadband wireless metropolitan area network. Mobile WiMAX, based on IEEE 802.16e – 2005 [7], adds functions and features to the original standard to support mobility. The most current IEEE 802.16 – 2009 standard [8] is a revision of IEEE 802.16 – 2004. It also consolidates material from IEEE 802.16e – 2005 and other previous 802.16 standards. Mobile WiMAX has a target transmission range of up to 31 miles and a target data rate exceeding 100 Mbps [9]. Compared to Mobile WiMAX, 3G data services provide a relatively low bandwidth and high price while Wi-Fi suffers from limited transmission ranges and from security issues.

The handover (HO) process in Mobile WiMAX networks is an essential element in supporting mobility and user roaming. The HO happens when the mobile station (MS) changes from one base station (BS) to another to obtain a higher signal quality or better quality of service (QoS) [8]. During the HO procedure, steps such as re-authentication, encryption key exchange and network registration need to be implemented, all of which add delay to the handover process. Therefore, it is very necessary to minimize the handover latency while keeping the whole procedure secure.

In recent years, hybrid fiber-wireless (Fi-Wi) access networks [10] have been explored to combine the strengths of optical and wireless technologies

and converge them seamlessly. It uses an optical backhaul to provide huge bandwidth and a wireless front-end to support mobility. We have recently proposed a WiMAX over EPON network [11], which can realize integrated and efficient system control and management. In this paper, we propose an end-to-end WiMAX over EPON network architecture and present its security framework utilizing both RSA [12] and EAP [13] authentication protocols. Based on the WiMAX over EPON network, we propose handover schemes using a pre-authentication method for AK pre-distribution. We use the communication framework of the ranging process to realize mutual authentication, which greatly simplifies the handover procedure compared to the standard Mobile WiMAX handover process defined in IEEE 802.16 – 2009.

The remainder of the paper is organized as follows. The WiMAX network architecture and its standard handover scheme are reviewed in section 2. The background information on the WiMAX over EPON network is introduced in section 3. Then in section 4, we propose the end-to-end WiMAX over EPON network architecture as well as its security framework. In section 5, we present the handover scenarios in the WiMAX over EPON network and propose the handover schemes. We analyze the proposed handover mechanisms in section 6. Section 7 concludes this paper.

2 WiMAX Network Architecture and Standard Handover Procedure

2.1 WiMAX Network Architecture

IEEE 802.16 standard focuses mainly on the specifications of the media access control (MAC) and physical (PHY) layers. To ensure the inter-vendor inter-networking interoperability for roaming, multi-vendor access networks and inter-company billing, the WiMAX Forum [14] formed the Networking Working Group (NWG) to create the end-to-end higher layer networking specifications for fixed, nomadic, portable and mobile WiMAX systems, beyond what is defined in the scope of IEEE 802.16.

The IP-based end-to-end WiMAX network architecture described by NWG is shown in Figure 1. The network architecture consists of user terminal, access service network (ASN) owned by the network access provider (NAP) and connectivity service network (CSN) owned by the network service provider (NSP) [15]. The user terminal could be fixed WiMAX terminals like houses installed with the WiMAX antennas, portable WiMAX terminals such as laptops and cell phones with WiMAX chipsets, or mobile WiMAX terminals such as moving vehicles equipped with WiMAX CPE devices. The ASN provides radio access connection to the WiMAX subscribers and it comprises BSs and ASN Gateways (ASN-GWs). The BS implements PHY and MAC functions defined in the 802.16 standard. Each ASN-GW controls and manages certain number of BSs and provides interfaces to the CSN. The ASN-GW also plays the role of the authenticator during EAP authorization process [16]. The CSN is responsible for providing IP connectivity services to the WiMAX subscribers. It includes functions such as authentication, authorization, and accounting (AAA) services, QoS management, DHCP/DNS services and WiMAX subscriber billing [17]. In roaming conditions, the subscriber might connect to the home NSP via visited NSPs with whom the home NSP has roaming agreements with.

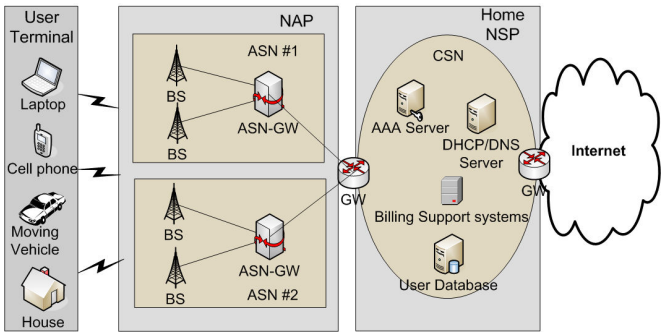

Fig.1 End-to-end WiMAX network architecture

2.2 Standard Mobile WiMAX Handover Procedure

IEEE 802.16e – 2005 defines three modes of handover: a standard hard handover and two types of soft handovers which are macro diversity handover (MDHO) and fast BS switching (FBSS). The hard handover is mandatory while the MDHO and FBSS are optional. In this paper, we consider only the standard hard handover process which is the basis for our proposed handover schemes. Descriptions of MDHO and FBSS are available in [7, 8].

The standard handover procedure consists of the following nine stages [8] as shown in Figure 2:

A. Network topology advertisement

In this stage, the serving BS broadcasts the network topology information to the MS using the

MOB_NBR-ADV (neighbor advertisement) message at a periodic interval. Channel information of neighboring BSs that are normally carried by each BS's own DCD (downlink channel descriptor) and UCD (uplink channel descriptor) are provided in MOB_NBR-ADV.

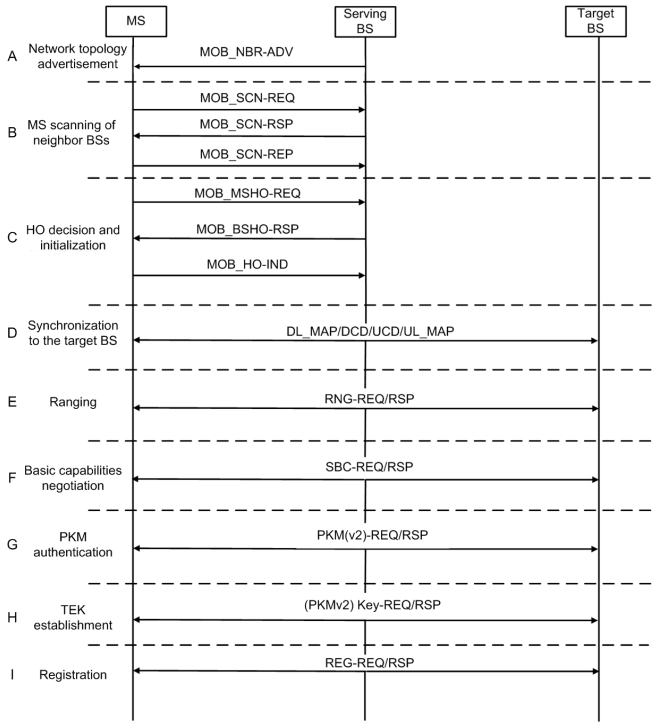

Fig.2 Standard WiMAX handover procedure

B. MS scanning of neighbor BSs

The MS sends a MOB_SCN-REQ (scanning interval allocation request) message to request scanning intervals thus seeking available BSs and determining the target BS. The serving BS replies with a MOB_SCN-RSP (scanning interval allocation response) message to allocate the scanning intervals for the MS. The MS then scans all recommended BSs and reports the scanning result in the MOB_SCN-REP (scanning result report) message which is sent to the serving BS.

C. HO decision and initialization

The HO decision can originate either at the MS by sending a MOB_MSHO-REQ (MS HO request) message or at the serving BS through a MOB_BSHO-REQ (BS HO request) message. In the handover process shown in Figure 2, we assume the HO is trigged by the MS. Within the MOB_MSHO-REQ message, the MS indicates one or more possible target BSs based on the evaluation from previous scanning results. Then the serving BS returns a MOB_BSHO-RSP (BS HO response) message as an acknowledgement. Finally, the MS sends a MOB_HO-IND (HO indication) message to indicate the release of the serving BS and that it is about to perform a handover.

D. Synchronization to the target BS

In this phrase, the MS synchronizes itself to the downlink (DL) transmission of the target BS and obtain the DL and uplink (UL) transmission parameters. The MS could already have received the target BS identity (BSID), physical frequency, DCD and UCD from the MOB_NBR-ADV which would shorten this process.

E. Ranging

The MS sends a RNG-REQ (ranging request) message to the target BS to acquire the correct timing offset and power adjustments. The MS's MAC address is also included in RNG-REQ to identify itself. A RNG-RSP (ranging response) message is transmitted by the BS in response to a received RNG-REQ. There is a HO Process Optimization type/length/value (TLV) field included in RNG-RSP which is used to identify the network reentry steps that could be skipped during the current HO process, because the target BS may obtain the MS information from the serving BS over the backbone network. This type of handover is named optimized HO. The possible omitted handover steps include basic capabilities negotiation, privacy key management (PKM) authentication, traffic encryption key (TEK) establishment and registration.

F. Basic capabilities negotiation

After the completion of ranging, the MS and the BS use the SBC-REQ (SS basic capability request) and SBC-RSP (SS basic capability response) messages to associate their basic capabilities, such as supported physical parameters and properties of the MS which are related to bandwidth allocation.

G. PKM authentication

This stage uses PKM-REQ (PKM request) and PKM-RSP (PKM response) messages to realize the MS's re-authentication to the WiMAX network. If PKM version 2 (PKMv2) defined in IEEE 802.16e – 2005 is enabled, then PKMv2-REQ and PKMv2-RSP messages are used. Depending on different modes, RSA-based authentication, or EAP-based authentication, or both need to be implemented in this step.

H. TEK establishment

During this phase, the MS sends a Key-REQ (key request) message to the BS to request new TEK and TEK-related parameters. TEK is created by the BS and sent using the Key-RSP (key response) message encrypted by the MS's public key. In PKMv2 mode, PKMv2 Key-REQ and PKMv2 Key-RSP messages are used.

I. Registration

Finally, the MS registers itself to the network using a REG-REQ (registration request) message. A REG-RSP (registration response) message is sent back by the BS in response to the received REG-REQ.

After registration, a few more steps, including establishment of IP connectivity and time of day, and operational parameters transfer [8], need to be implemented for the MS to establish connection to the mobile network. In this paper, we consider registration as the last step of the handover.

3 Background Knowledge on WiMAX over EPON Networks

The reference model for the WiMAX over EPON network proposed in [11] is shown in part (c) of Figure 3. Part (a) shows the reference model of EPON defined in IEEE 802.3ah [1] at the bottom and the reference model of WiMAX defined in IEEE 802.16 – 2004 [6] at the top. From left to right in Figure 3, the WiMAX physical layer is removed and the WiMAX MAC layer is placed on top of the EPON MAC layer, named WiMAX over EPON. Higher layer protocol data units (PDUs) are classified and mapped into the WiMAX MAC frames, which are then encapsulated into the EPON Ethernet frames. Each WiMAX MAC PDU is encapsulated into the payload of one EPON Ethernet frame. The Ethernet frame payload with a 1500-byte maximum length is sufficient to accommodate the WiMAX MAC PDU, the length of which is variable [17].

The layer-2 architecture of the WiMAX over EPON network is shown in Figure 4. The WiMAX BS and ONU are integrated into a single system called ONU-BS [18]. The OLT is renamed OLT-BS because the WiMAX MAC layer functions are moved from the BS to the OLT-BS while the ONU-BS does the WiMAX physical layer processing. In the downstream direction at the OLT-BS, each WiMAX MAC PDU is encapsulated into an Ethernet frame which is sent to the EPON network. The logical link ID (LLID) [19] in the Ethernet frame preamble is used to identify the ONU-BS that the WiMAX MAC PDU is intended for. At the ONU-BS, the Ethernet header and trailer are stripped away, which turns the Ethernet frame back to the WiMAX MAC PDU. Then the WiMAX MAC frame is processed at the physical layer to generate the WiMAX wireless signal. Similarly, in the upstream direction, the WiMAX MAC PDU from the MS is encapsulated into the Ethernet frame at the ONU-BS and recovered at the OLT-BS. Therefore, ONU-BS is used to relay the WiMAX MAC PDU within the EPON network while the OLT-BS is actually the management center for WiMAX subscribers.

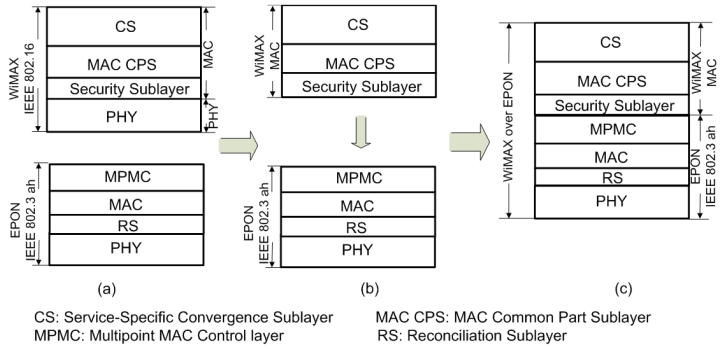

Fig.3 WiMAX over EPON reference model

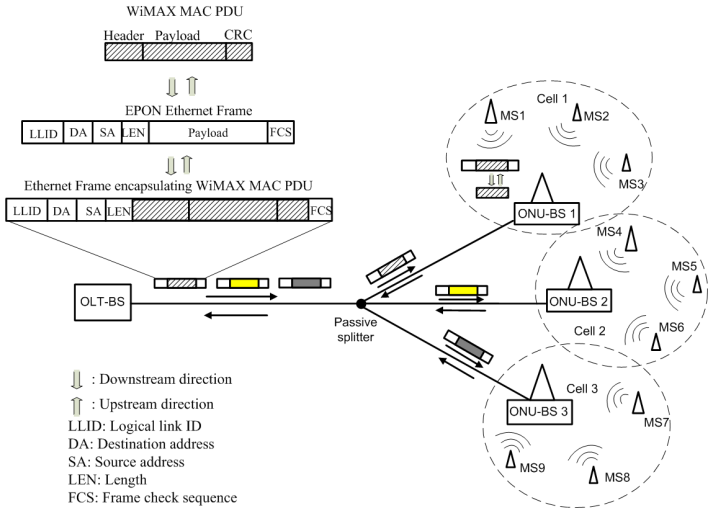

Fig.4 WiMAX over EPON architecture

Compared to other integration solutions proposed in [18, 20], the WiMAX over EPON network has the following advantages. (1) It integrates ONU-BSs' MAC control functions into the OLT-BS which greatly simplifies the overall system management thus saving the maintenance

cost. (2) It eliminates double encryption, which reduces the processing delay and hardware cost. (3) The OLT-BS is the key management center for both EPON and WiMAX networks which makes the whole security system easy and simple to manage and control.

4 Proposed End-to-End WiMAX over EPON Network Architecture and Its Security Framework

4.1 End-to-end WiMAX over EPON network architecture

As shown in Figure 5, our proposed architecture is based on the end-to-end WiMAX network architecture. Instead of connecting directly to the BS, the ASN-GW is connected with certain number of OLT-BSs. Depending on the splitting ratio, each OLT-BS connects to 16 or 32 or more ONU-BSs through a passive optical splitter. The user terminal connects to the OLT-BS via the ONU-BS. Each OLT-BS has a BSID for operator identification just as does the BS in WiMAX network. The BSID is also used as one of the attributes to derive the primary authorization key (PAK) and AK shared between the MS and the OLT-BS during the RSA mutual authentication. Each ONU-BS has a BSID as well which we name sub-BSID. The sub-BSID is only used to identify different ONU-BSs during the handover process and has no contributes to key management and generation.

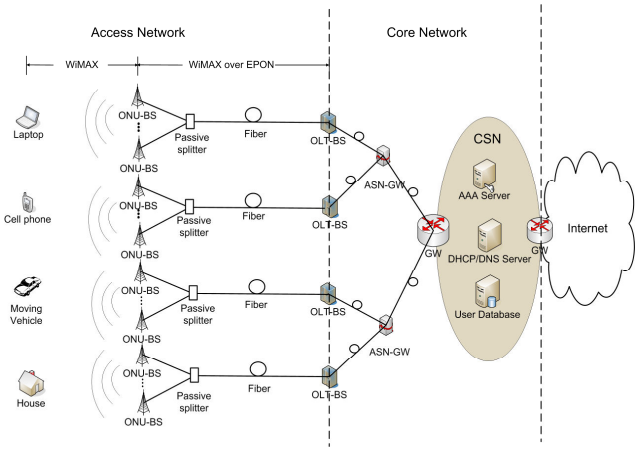

Fig.5 End-to-end WiMAX over EPON network architecture

The OLT-BS keeps the OLT functions and manages the WiMAX MAC layer of the original WiMAX BS. The ONU-BS maintains the ONU functions and performs the WiMAX physical layer processing. For example, in the downstream direction, higher layer data from the Internet is sent to the OLT-BS via the ASN-GW. At the OLT-BS, the upper layer data is mapped to the WiMAX MAC PDU, which is then encapsulated into the Ethernet frame sent down to the EPON network. At the ONU-BS, the payload part of the Ethernet frame is turned back to the WiMAX MAC PDU, which is transformed to the wireless signal. In the upstream direction, the WiMAX signal from the user is received by the ONU-BS, encapsulated into the EPON frame, and sent to the EPON network. At the OLT-BS, the WiMAX MAC PDU is recovered from the Ethernet frame and sent to the upper layer.

4.2 Security framework for the WiMAX over EPON network

In [11], we presented a layer-2 security framework based on X.509 certificate [12] and RSA public-key algorithm. It consists of the following steps. First, the ONU-BS registers itself to the OLT-BS and establishes a shared encryption key (EK) with the OLT-BS. During this process, the ONU-BS and OLT-BS exchange their X.509 certificates, which are encrypted by a pre-distributed secret keyword, to realize mutual authentication. The EK used within the optical network is generated by the OLT-BS and sent to the ONU-BS encrypted using the ONU-BS's public key. Second, the WiMAX MS synchronizes itself to the network and performs initial ranging and basic capabilities negotiation. Third, the MS and OLT-BS exchange their X.509 certificates to authenticate each other's identity. The OLT-BS generates the pre-PAK encrypted by the MS's public key and sends it to the MS. The pre-PAK is used to derive the PAK which generates the AK. Fourth, the MS and OLT-BS performs the 3-way security association (SA) - TEK handshake and the TEK exchange to distribute the TEK generated by the OLT-BS to the MS.

Except the RSA protocol, IEEE 802.16e also defines an EAP-based authentication [7], which is implemented above the 802.16 layer, and the EAP credentials are encapsulated in the PKM management messages. The particular EAP methods to be used are not described in the 802.16e standard. A variety of EAP types such as EAP-Transport Layer Security (EAP-TLS) [21], EAP for GSM Subscriber Identity (EAP-SIM) [22], and EAP for UMTS Authentication and Key Agreement (EAP-AKA) [23] are available to choose. The

implementation of each EAP method is detailed in the specific EAP standard, and we will not present them here. When it is applied to the WiMAX network, the EAP authentication process yields a shared master session key (MSK) between the MS and a backend AAA server in the CSN. The AAA server then transfers the MSK to the authenticator (ASN-GW), and a pairwise master key (PMK) is derived from the MSK. After the EAP authentication, the MS and the authenticator will both possess the PMK which is used to generate the AK. Although the implementation is optional as defined in the 802.16e standard, EAP authentication mechanism is very necessary for global roaming across WiMAX operator networks where credential reuse, consistent use of AAA for accounting and billing are supported [15]. In this paper, we choose the mode in which the RSA-based authentication is implemented first and followed by the EAP-based authentication. In this case, the AK is derived from both the PAK and PMK [7].

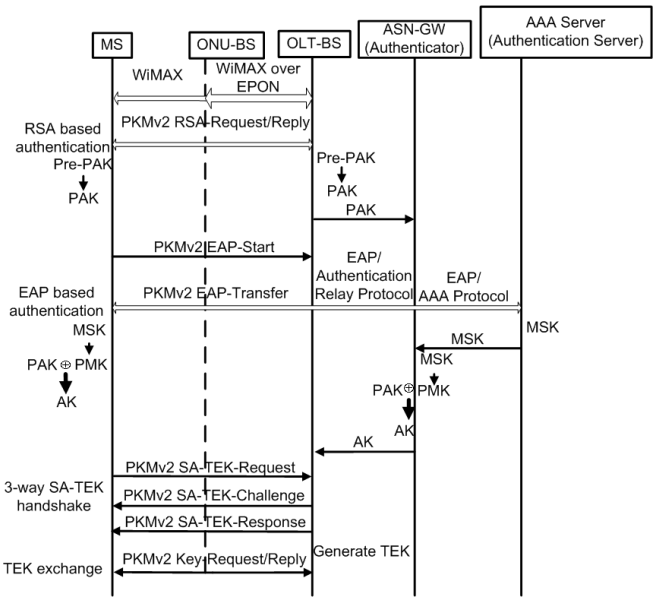

Fig.6 A Layer-3 security framework for the WiMAX over EPON network

The proposed layer-3 security framework for the WiMAX over EPON network is shown in Figure 6. The ASN-GW is used as the authenticator and the AAA server acts as the authentication server. The WiMAX over EPON architecture is applied between the ONU-BS and OLT-BS, and the ONU-BS relays the WiMAX MAC PDUs between the MS and the OLT-BS. We assume that the ONU-BS has already established connection with the OLT-BS and that the MS has completed synchronization, ranging and basic capability association. The security framework is described as follows. First, the RSA-based authentication process is implemented using PKMv2 RSA-Request and PKMv2 RSA-Reply message, which derives the pre-PAK to generate the PAK shared between the MS and OLT-BS. The PAK is then transferred from the OLT-BS to the ASN-GW for future use. Second, the EAP-based authentication is initiated by the PKMv2 EAP-Start message. The PKMv2 EAP-Transfer message is then used to encapsulate the EAP payload between the MS and OLT-BS. An authentication relay protocol is utilized to relay the EAP messages from the OLT-BS to the ASN-GW, which then forwards the EAP credentials to the AAA server over the AAA protocol such as Remote Authentication Dial In User Service (RADIUS) [24] or Diameter [25]. After the EAP authentication procedure, a MSK is generated in both the MS and AAA server. The MSK is then sent from the AAA server to the ASN-GW where the PMK is derived from the MSK. So far, both the MS and ASN-GW hold the PAK and PMK, which are subsequently used to derive the AK. Next, the ASN-GW transfers the AK to the OLT-BS. In the third step, the PKMv2 3-way SA-TEK handshake is performed between the MS and OLT-BS to verify the security association based on the AK. Finally, TEK exchange is implemented to transmit the generated TEK from the OLT-BS to the MS which completes the framework.

5 Proposed Handover Schemes for WiMAX over EPON networks

The proposed handover scheme is based on the standard WiMAX hard handover procedure described in section 2. In this paper, we assume the handover happens within the home NSP, referred as the intra-CSN handover. Figure 7 shows the handover scenarios in the WiMAX over EPON network. The NAP has two ASNs managed by the home NSP: ASN #1 and ASN #2. The ASN-GW1 contained in the ASN #1 connects to the OLT-BS1 and OLT-BS2. The ASN #2 owns the ASN-GW2 which is connected with the OLT-BS3. For simplicity while not losing generosity, each OLT-BS connects to only two ONU-BSs instead of to 16 or 32. For example, the OLT-BS1 controls ONU-BS11 and ONU-BS12, the OLT-BS2 controls ONU-BS11 and ONU-BS12, and the OLT-BS3 controls ONU-BS31 and ONU-BS32. Cell 11 is the area covered by ONU-BS11, and cell 12 is controlled by ONU-BS12. Both cell 11 and 12 are covered by cell 1 which refers to the area managed by OLT-BS1.

The name of cells covered by OLT-BS2 and OLT-BS3 follow the same rules as shown in Figure 7.

Three types of handover scenarios are defined: intra-OLT-BS handover, inter-OLT-BS handover and inter-ASN handover. Intra-OLT-BS handover happens within the area covered by a single OLT-BS, when the MS moves from cell 11 to cell 12 (within cell 1). Inter-OLT-BS handover takes place when the serving ONU-BS and the target ONU-BS belong to different OLT-BSs while still inside the same ASN, for example, when the MS moves from cell 12 (cell 1) to cell 21 (cell 2). Inter-ASN handover refers to the handoff between different ASNs but managed by the same CSN, for instance, when the MS moves from cell 22 (cell 2) to cell 31 (cell 3).

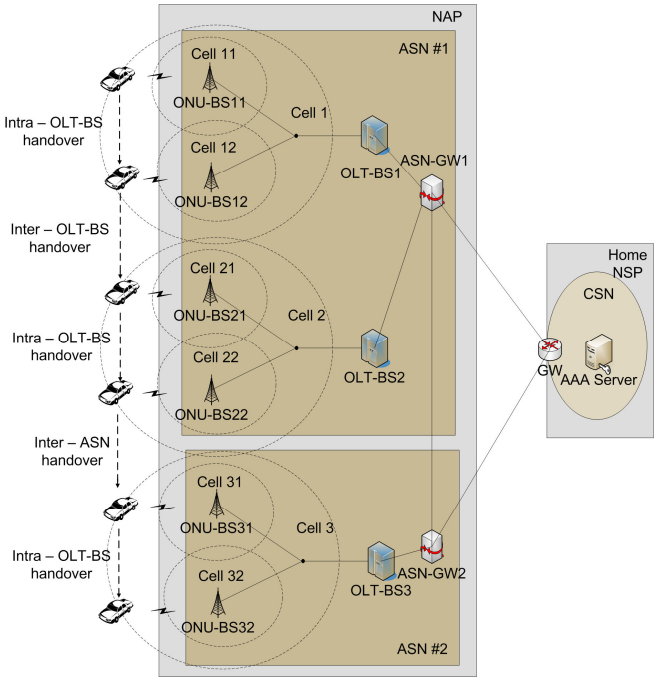

Fig.7 Handover scenarios in WiMAX over EPON network

Table 1. Terms used in the handover procedure

Terms	Descriptions
PU_{MS}	Public key of the MS
PR_{MS}	Private key of the MS
MS-Random	Random number generated by the MS
MS_{MAC}	MAC address of the MS
PU_{OLT-BS}	Public key of the OLT-BS
PR_{OLT-BS}	Private key of the OLT-BS
OLT-BS-Random	Random number generated by the OLT-BS
(pre-)PAK#	(Pre-) primary authorization key shared between the MS and OLT-BS#
AK#	authorization key shared between the MS and OLT-BS#

The ranging management messages including RNG-REQ and RNG-RSP are used to carry authentication related information to realize mutual authentication between the MS and the mobile network. Pre-authentication is used in our scheme to pre-distribute the AK thus accelerating the handover process in the inter-OLT-BS handover and inter-ASN handover. Details of the three handover procedures are described in sections 5.1 - 5.3, and the terms used in the handover are shown in Table 1.

5.1 Intra-OLT-BS handover

We use the scenario where ONU-BS11 is the serving ONU-BS and ONU-BS12 is the target ONU-BS. Because the MS is communicating with the same OLT-BS during the handover, the OLT-BS holds all the MS-related information including the MS_{MAC} and keying materials. The handover procedure is shown in Figure 8. The first four steps are network topology advertisement, MS scanning of neighbor ONU-BSs, HO decision and initialization, and synchronization to the target ONU-BS. During this process, the MS compares the scanning results of the neighbor ONU-BSs, makes the HO decision, and synchronizes to the chosen ONU-BS which is ONU-BS22. Because the neighbor of ONU-BS11 is ONU-BS12, which is managed by the same OLT-BS, it is very convenient for OLT-BS1 to collect channel information of ONU-BS12 and send it to the MS through ONU-BS11. The sub-BSIDs are used to identify different ONU-BSs.

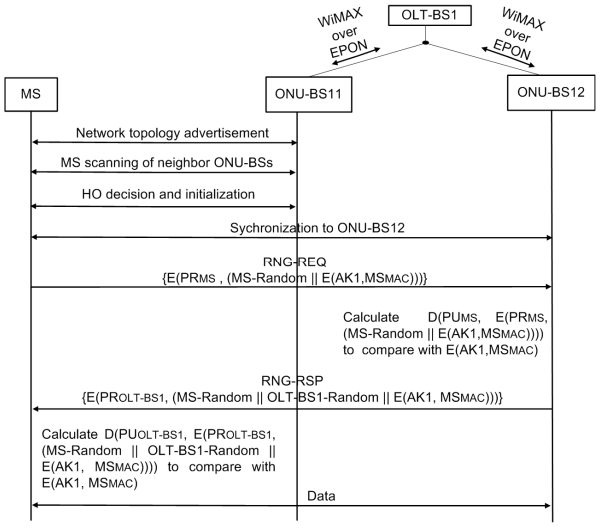

Fig.8 Intra-OLT-BS handover in the WiMAX over EPON network

During the subsequent ranging process, the MS encrypts the MS_{MAC} using AK1, referred to as E

(AK1, MS_{MAC}); and the MS-Random is concatenated with E (AK1, MS_{MAC}) to ensure the freshness of the message. (MS-Random || E (AK1, MS_{MAC})) is then encrypted by PR_{MS} to form E (PR_{MS}, (MS-Random || E (AK1, MS_{MAC}))) which is incorporated in the RNG-REQ message. The RNG-REQ message is sent to ONU-BS12, which relays the message to OLT-BS1. Upon the receipt of RNG-REQ, OLT-BS1 decrypts E (PR_{MS}, (MS-Random || E (AK1, MS_{MAC}))) using PU_{MS} to get E (AK1, MS_{MAC}) and compares it with its own calculation to verify the MS's identity. After that, OLT-BS1 concatenates ONU-BS-Random to (MS-Random || E (AK1, MS_{MAC})) and encrypts (OLT-BS1-Random || MS-Random || E (AK1, MS_{MAC})) by PR_{OLT-BS} to form E ($PR_{OLT-BS1}$, (OLT-BS1-Random || MS-Random || E (AK1, MS_{MAC}))), which is contained in the RNG-RSP message. OLT-BS1 then sends the RNG-RSP message to the MS. The MS decrypts it with $PU_{OLT-BS1}$ and compares the E (AK1, MS_{MAC}) with the one it already has to verify the identity of OLT-BS1.

So far, since the MS and OLT-BS1 are authenticated by each other within the ranging process and the new ONU-BS connects the MS to the same OLT-BS, the following standard handover steps, including basic capabilities negotiation, PKM authentication, TEK establishment, and registration could all be skipped by indicating in the HO Process Optimization TLV field contained in the RNG-RSP message.

5.2 Inter-OLT-BS handover

We use the scenario in which the MS moves from ONU-BS12 to ONU-BS21. Now the MS switches to a different OLT-BS while still within the area covered by the same ASN. Therefore, the PAK derived by RSA-based authentication needs to be updated while the PMK derived by the EAP-based authentication, which is cached in the same ASN-GW, is still valid. A pre-authentication method is used to derive the PAK2, thus generating the AK2. The procedure is described in Figure 9.

During the pre-authentication phase, OLT-BS2's certificate is sent to OLT-BS1 via ASN-GW1, and RSA-based pre-authentication is implemented to derive a shared pre-PAK2, which is sent to OLT-BS2 via ASN-GW1. The pre-PAK2 is used to generate the PAK2, which is then transferred back to ASN-GW1. Combing the PAK2 and PMK, an AK2 is derived. At the MS, an AK2 is generated as well. So far, the pre-authentication procedure completes.

During the handover phase, the first four steps are the same as the intra-OLT-BS handover. ONU-BS21's channel information controlled by OLT-BS2 is collected by OLT-BS1 via ASN-GW1 and then sent to the MS through ONU-BS12 for evaluation. In the HO decision and initialization step, MS_{MAC} is transferred from the OLT-BS1 to OLT-BS2 via ASN-GW1, and the AK2 is sent from the ASN-GW1 to the OLT-BS2. After this point, both the MS and OLT-BS2 holds the MS_{MAC} and AK2. The following ranging step is the same as the ranging process in the intra-OLT-BS handover except that AK2 and OLT-BS2's keying materials are used. This step realizes mutual authentication between the MS and OLT-BS2 and confirms the authentication of MS to the AAA server. After ranging, basic capabilities negotiations takes place to negotiate channel capabilities. Then the TEK establishment step is implemented to transmit the newly generated TEK from the OLT-BS2 to the MS.

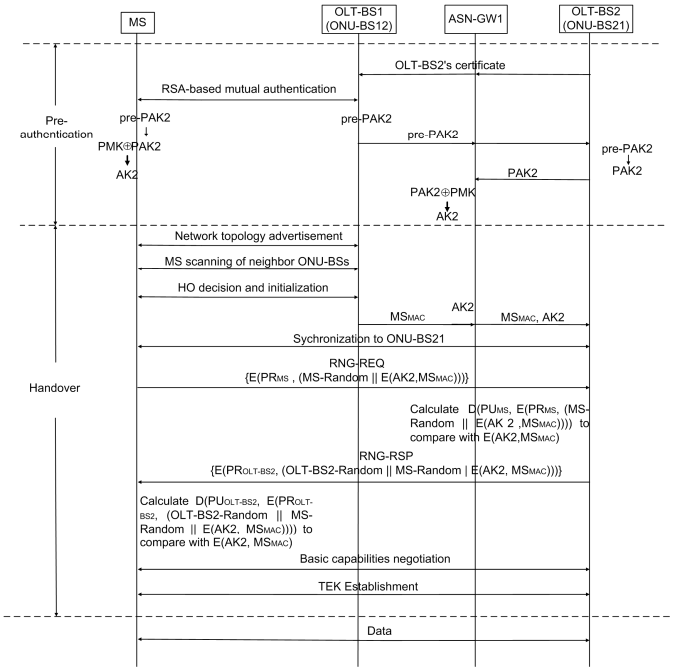

Fig.9 Inter-OLT-BS handover in the WiMAX over EPON network

5.3 Inter-ASN handover

In this scenario, we assume the MS moves from ONU-BS22 to ONU-BS31. During this process, the MS changes both its attached OLT-BS and ASN-GW while still within the same CSN. Therefore, the PAK needs to be updated, and the PMK needs to be sent from ASN-GW1 to ASN-GW2 during pre-authentication. The handover procedure is shown in Figure 10.

During the pre-authentication process,

OLT-BS3's certificate is transferred via the ASN-GW1 and ASW-GW2 to OLT-BS2 for RSA-based mutual authentication to derive a shared pre-PAK3 between the MS and OLT-BS2. The pre-PAK3 is then transmitted over the two ASN-GWs to OLT-BS3 where a PAK3 is derived. The PMK cached in the ASN-GW1 is sent to ASN-GW2, and is combined with the PAK3 transmitted from OLT-BS3 to derive an AK3. The AK3 is cached at the ASN-GW2 for future use. At the same time, the MS generates the AK3 since it holds both the PMK and PAK3.

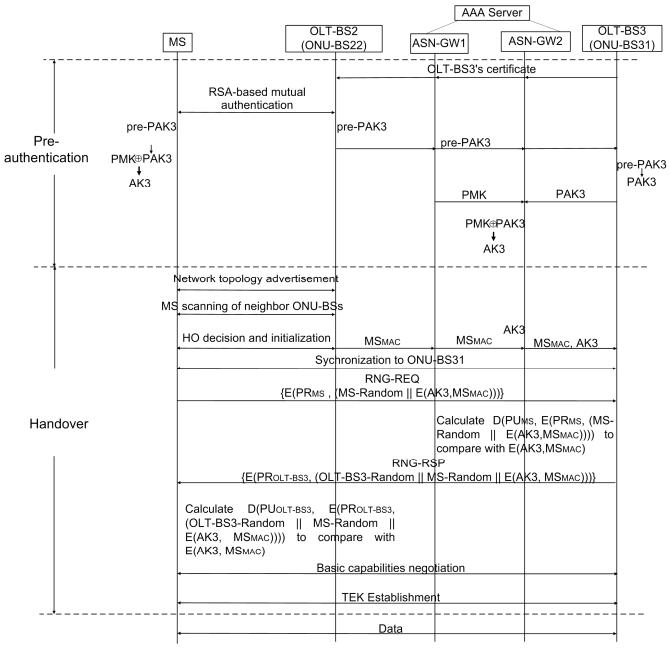

Fig.10 Inter-ASN handover in the WiMAX over EPON network

The first four steps of the handover are the same as the intra-OLT-BS handover procedure. The channel information of ONU-BS31 is transferred from OLT-BS3 to OLT-BS2 via ASN-GW1 and ASN-GW2 for the MS to scan and evaluate. During the HO decision and initialization step, the MS_{MAC} is transferred from the OLT-BS2 to OLT-BS3 via the two ASN-GWs, and AK3 is transferred from the ASN-GW2 to OLT-BS3. The next ranging step is the same as the intra-OLT-BS handover ranging process except that AK3 and OLT-BS3's keying materials are used. Mutual authentication between the MS and OLT-BS3 is realized during this step, and the MS is verified that it has already been authenticated by the AAA server. After the ranging step, the basic capabilities negotiation takes place to negotiate channel capabilities. The TEK establishment step is needed to exchange the TEK generated by OLT-BS3.

6 Analysis of the Proposed Handover Schemes

In our proposed three handover scenarios, the communication framework of the ranging step is used to realize both the RSA-based and EAP-based authentication. During the ranging process, as described in section 5, we incorporate E (PR_{MS}, (MS-Random || E (AK, MS_{MAC}))) in the RNG-REQ message sent from the MS to the OLT-BS. Since the OLT-BS holds the MS's public key, it can decrypt the message and obtain E (AK, MS_{MAC}). If the E (AK, MS_{MAC}) is the same as the OLT-BS's own calculation result, the MS's identity is verified because only the MS that holds the correct private key can encrypt (MS-Random || E (AK, MS_{MAC})). The match also proves that the MS holds the same AK as the OLT-BS because only the MS that has the correct AK is able to calculate the right E (AK, MS_{MAC}). In the RNG-RSP message replied by the OLT-BS, (PR_{OLT-BS}, (OLT-BS-Random || MS-Random || E (AK, MS_{MAC}))) is contained. The MS decrypts the message using the OLT-BS's public key and compares the obtained E (AK, MS_{MAC}) to the one it holds. The match verifies that the OLT-BS has the correct private key thus confirming its identity. Therefore, the ranging step realizes mutual authentication between the MS and the mobile network which means the PKM authentication step could be skipped.

Although the security context in the RNG-REQ message is encrypted by the MS's private key, which means any malicious OLT-BS or MS that holds the MS's public key can decrypt the message, the MS's MAC address is encrypted by the AK, which is hard for an attacker to compromise. To implement the masquerade attack, the malicious entity needs to obtain the private key from either the legal OLT-BS or the MS to encrypt E (AK, MS_{MAC}), which makes the attack difficult. For the same reason, the RNG-RSP message is also not easy to compromise. The random numbers generated by the MS and the OLT-BS are used as nonce to ensure the freshness of the message, thus preventing the reply attack.

Given that the AK is derived from the PAK and PMK while the PMK is generated through the EAP authentication process, it is verified that the MS holds the correct PMK. It also proves that before the handover process, the MS has already been authenticated by the AAA server via EAP protocol and registered to the CSN. Therefore, the

registration step could also be skipped.

For the intra-OLT-BS handover, because the MS and the OLT-BS holds the same keying material and the original TEK is still valid, the basic capabilities negotiation and TEK establishment steps could also be skipped. For the inter-OLT-BS and inter-ASN handover, because the MS is switched to a different OLT-BS, the basic capabilities negotiation step is needed to negotiate channel capabilities. The TEK establishment step also needs to be implemented for the MS and the target OLT-BS to exchange the new TEK.

To shorten the handover procedure in inter-OLT-BS and inter-ASN handover, a pre-authentication method is utilized. During the inter-OLT-BS handover, the MS changes the attached OLT-BS while still managed by the same ASN. So the MS only shares the PMK with the target OLT-BS and the PMK is cached in the ASN-GW. During the pre-authentication process, the target OLT-BS's certificate is sent via the ASN-GW to the serving OLT-BS to implement RSA-based mutual authentication. The derived pre-PAK is transferred to the ASN-GW to generate the AK shared between the MS and the target OLT-BS. Thus, during the handover process, the MS and the target OLT-BS will hold the shared AK and each other's public/private key pair. In the HO decision and initialization, the MS's MAC address is sent from the serving OLT-BS to the target OLT-BS for authentication use.

The inter-ASN handover follows the same procedure as the inter-OLT-BS handover, except that in the pre-authentication process, the security context transfers between the serving OLT-BS and the target OLT-BS need to travel through two ASN-GWs instead of one. Also an extra step, the transfer of the PMK from the serving ASN-GW to the target ASN-GW, is needed. So a new AK is generated between the MS and the target OLT-BS through the pre-authentication process while the original PMK is still in use.

The comparison between the standard handover scheme defined in the IEEE 802.16e and our proposed three types of handover schemes is shown in Table 2. All the three proposed handover schemes *eliminate the PKM authentication step*, which contains the time-consuming RSA-based and EAP-based authentication, thus improving the efficiency of the handover. Compared to the standard nine-step WiMAX handover procedure, the intra-OLT-BS handover *consists of only five steps*, which greatly simplifies the handover process. The number of steps involved in both the inter-OLT-BS and inter-ASN handover is *reduced to seven*, which also shortens the handover process.

One disadvantage of the proposed handover schemes is that the use of pre-authentication brings extra cost and power consumption for the key transfer between different OLT-BSs and increases the amount of computations within the MS and the OLT-BS. However, because in practice, each OLT-BS can connect to 16 to 32 or even more ONU-BSs, the area covered by a single OLT-BS could be sufficiently large. As long as the topology of the WiMAX over EPON network is designed properly, the chance for the MS to apply the inter-OLT-BS and inter-ASN handover could be reduced while the intra-OLT-BS handover serves as the major handover scheme.

Table 2. Comparison between standard WiMAX handover and proposed handover schemes

Handover types		Standard	Intra-OLT-BS	Inter-OLT-BS	Inter-ASN
Pre-authentication		-	-	✓	✓
Handover procedures	Network topology advertisement	✓	✓	✓	✓
	MS scanning	✓	✓	✓	✓
	HO decision and initialization	✓	✓	✓	✓
	Synchronization	✓	✓	✓	✓
	Ranging	✓	✓	✓	✓
	Basic capabilities negotiation	✓	-	✓	✓
	PKM authentication	✓	-	-	-
	TEK establishment	✓	-	✓	✓
	Registration	✓	-	-	-

7 Conclusion

In this paper, we have proposed an end-to-end WiMAX over EPON network architecture and presented its layer-3 security framework. We have introduced three handover scenarios in the WiMAX over EPON network, which are intra-OLT-BS, inter-OLT-BS and inter-ASN handover, and proposed the corresponding handover schemes. In the proposed mechanisms, the ranging management messages including RNG-REQ and RNG-RSP are used to carry authentication related information to implement authentication and a pre-authentication method is utilized to pre-distribute the shared authentication key. Through our analysis, we showed that compared to the standard nine-step WiMAX handover process, the proposed intra-OLT-BS handover scheme consists of only five

steps and both the inter-OLT-BS and inter-ASN handover procedure is reduced to seven steps which shortens and accelerates the handover process. Further, the proposed schemes realize mutual authentication between the MS and the mobile network.

References:

[1] IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CMSA/CD) Access Method and Physical Layer Specifications, *IEEE Std 802.3ah* 2008.

[2] ITU-T Recommendation ITU-T G.984. Gigabit Capable Optical Access Network.

[3] K. Grobe and J. P. Elbers, PON in adolescence: from TDMA to WDM-PON, *Communications Magazine, IEEE*, vol.46, no.1, 2008, pp. 26-34.

[4] S. V. Kartalopoulos, Next Generation Hierarchical CWDM/TDM-PON network with Scalable Bandwidth Deliverability to the Premises, *Optical Systems and Networks*, vol.2, 2005, pp. 164-175.

[5] S. V. Kartalopoulos and A. Sierra, Engineering a Scalable and Bandwidth Elastic Next Generation PON, *Optical Fiber Communication and the National Fiber Optic Engineers Conference, 2007. OFC/NFOEC 2007. Conference on*, 2007, pp. 1-8.

[6] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001), 2004.

[7] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004), 2006.

[8] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems, IEEE Std 802.16-2009 (Revision of IEEE Std 802.16-2004), 2009.

[9] Z. Abichar, P. Yanlin and J. M. Chang, WiMax: The Emergence of Wireless Broadband, *IT Professional*, vol.8, no.4, 2006, pp. 44-48.

[10] N. Ghazisaidi, M. Maier and C. Assi, Fiber-wireless (FiWi) access networks: a survey, *Communications Magazine, IEEE*, vol.47, no.2, 2009, pp. 160-167.

[11] W. Gu, P. Verma and S. V. Kartalopoulos, A Unified Security Framework for WiMAX over EPON Access Networks, *Security and Communication Networks, Wiley*, to appear.

[12] W. Stallings, *Cryptography and network security: principles and practice*, Pearson / Prentice Hall, 2006.

[13] Extensible Authentication Protocol (EAP), RFC 3748, 2004.

[14] WiMAX Forum, http://www.wimaxforum.org/.

[15] Mobile WiMAX–Part I A Technical Overview and Performance Evaluation, WiMAX Forum white paper, 2006.

[16] K. Tsagkaris and P. Demestichas, WiMax network, *Vehicular Technology Magazine, IEEE*, vol.4, no.2, 2009, pp. 24-35.

[17] L. Nuaymi, *WiMAX: Technology for Broadband Wireless Access*, Wiley, 2007.

[18] S. Gangxiang, R. S. Tucker and C. Chang-Joon, Fixed Mobile Convergence Architectures for Broadband Access: Integration of EPON and WiMAX [Topics in Optical Communications], *Communications Magazine, IEEE*, vol.45, no.8, 2007, pp. 44-50.

[19] K. Glen, *Ethernet passive optical networks*, McGraw-Hill, 2005.

[20] Y. Kun, O. Shumao, K. Guild and C. Hsiao-Hwa, Convergence of ethernet PON and IEEE 802.16 broadband access networks and its QoS-aware dynamic bandwidth allocation scheme, *Selected Areas in Communications, IEEE Journal on*, vol.27, no.2, 2009, pp. 101-116.

[21] The EAP-TLS Authentication Protocol, *RFC 5216*, 2008.

[22] Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM), *RFC 4186*, 2006.

[23] Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), *RFC 4187*, 2006.

[24] Remote Authentication Dial In User Service (RADIUS), *RFC 2865*, 2000.

[25] Diameter Base Protocol, *RFC 3588*, 2003.