Security and AAA Architecture for WiFi-WiMAX Mesh Network

Abed Ellatif Samhat[1], Miloud Abdi[2]

[1]*France Telecom R&D Division*
40 rue du Général Leclerc, 92794 Issy les Moulineaux, France
[1]abed.samhat@orange-ftgroup.com

[2]*T&T Consulting*
10 Rue du Troyon, 92310 Sèvre Cedex, France
[2]miloud.abdi@t&tconsulting.com

Abstract— **This paper presents a flexible architecture for hybrid wireless network where WiFi and WiMAX in mesh mode are deployed in a complementary way. The end user can access to high bit rate Internet services directly by WiMAX technology through the 802.16 base stations or by WiFi technology through a CPE/AP connected to the 802.16 base station. We provide a brief description of the different functional entities and we investigate several technical issues including infrastructure and aspects related to the AAA (Authentication, Authorization, Accounting) procedures for users as well as the system security.**

I. Introduction

Wireless mesh networks (WMNs) have emerged as a key technology for next-generation wireless networking to provide high-bandwidth network coverage. WMNs are built by a set of spatially distributed nodes interconnected by wireless links. WMN is mesh networking that can be implemented over wireless networks such as WiFi, WiMAX, etc. In this context, the joint deployment and the complementarily between the IEEE 802.11 system and the IEEE 802.16 one in mesh configurations, are issues that are increasingly catching the interest of operators and manufacturers. In fact, the costs associated to these technologies are relatively smaller than the ones currently needed for 3G like technologies in a specific environment, such as the metropolitan areas.

WiFi (Wireless Fidelity) networks based on IEEE 802.11 standard [1] are being widely deployed in different environment due to standardisation and ease to use as well as low cost. However, this deployment is limited to hotspots, homes, offices, public zone including airports, etc. due to the limited coverage of Wi-Fi propagation and high cost of installing and maintaining a wired network backhaul connection. An extension of the IEEE 802.11 standard known as 802.11s to achieve mesh networking is under specification and not finalized yet.

As for WiMAX (Worldwide Interoperability for Microwave Access), it is a technology based on the IEEE 802.16 standard [2] and its amendments [3][4]. It provides tens of megabits of capacity per channel. The MAC protocol is designed in two modes PMP (Point-toMulti-Point) mode and mesh mode. The traffic in PMP mode occurs only between the base station (BS) and the subscriber stations (SS). But in mesh mode, the traffic can occur between SSs. There is no need to have direct link from SS to the BS of the mesh network. Mesh mode allows also the extension of the network coverage without wired connections for tens of kilometres.

One of the most likely scenarios that operators would be interested in, is the metropolitan deployment to implement public Internet access, which could simultaneously target the markets of residential, business and nomadic users. This statement can be explained considering the cost advantage that WiFi and WiMAX technologies seem to ensure and their complementarity in terms of performance and coverage. On the one hand the most spread version of 802.11 has coverage of about 100 meters of radius whereas the 802.16 coverage radius is almost several kilometres. On the other hand the wireless mesh networks are the ideal solution to provide both indoor and outdoor broadband wireless connectivity in urban, suburban, and rural environments without the need for extremely costly wired network infrastructure. In this context, we propose a flexible architecture for hybrid wireless mesh network where both 802.11 and 802.16 technologies are deployed in a complementary way. This architecture allows both public internet access and residential. End user can access to the network directly through the 802.16 BSs, or through a WiFi CPE/AP (customer premise equipment and WiFi Access Point) connected to the 802.16 BS by WiMAX. The PMP mode is supported at the WiMAX access links while the 802.16 base stations are interconnected in mesh mode until reaching the wired network. The WiMAX mesh network is then a backhaul network for WiFi and WiMAX users. A special attention should be given to the WiFi and WiMAX security due to the fact that such wireless networks are relatively less secure when compared to the wired networks. Indeed, allowing a device to route data coming from another user should involve robust mechanisms for confidentiality, data integrity and authentication. In this paper, we investigate several technical issues mainly the aspects related to the security and AAA procedures. The proposed architecture is compatible with the legacy technologies and can achieve a smooth migration to the future network generation.

The rest of this paper is organized as follows: Section II presents the proposed architecture and the main functional entities. In section III, we investigate the AAA and security issues and we describe the solution adopted in our architecture to achieve a secure service and protection against attacks. Finally, section IV concludes the paper.

1-4244-0979-9/07/$25.00 © 2007 IEEE

II. PROPOSED ARCHITECTURE

In the proposed architecture, 802.16 BSs act as Mesh routers to form an infrastructure providing a backhaul for conventional clients. Users are able to connect via different radio technologies. Indeed, the 802.11 and 802.16 technologies are considered in our studies. The network is a set of clusters where each one is composed of a number of cells as depicted in Figure 1. A cell is composed of one 802.16 BS and a number of CPE/APs connected to the BS using WiMAX link. Each cell is then limited by the coverage of a BS in addition to the coverage of the associated CPE/AP. Dashed and solid lines indicate wireless and wired links, respectively. Not all Mesh routers have gateway functionalities and consequently, not all the BSs are connected directly to the core network. The BS that is directly connected to the core network is called Core BS (CBS) while the Mesh BS (MBS) is connected to other BSs using a WiMAX mesh link before reaching the core network. Having a multi-mode terminal, a user can access to the network directly by WiMAX link through the BS (called in this paper user type A) or by WiFi link through a CPE/AP connected to the BS by WiMAX link (user type B). In our architecture, users type A and CPE/APs are considered as SSs in a cell and operate in PMP mode as defined in IEEE 802.16 standard [2]. The Mesh mode is supported between BSs to reach core network which performs better in relaying data traffic and increasing network coverage. Note that a new task group IEEE 802.16j was officially established, which attempts to support Mobile Multihop Relay (MMR) operation in WiMAX. These relays will functionally serve as an aggregating point on behalf of the BS for traffic collection from and distribution to the multiple users associated with them. In our architecture, BSs support more functionalities than relays and a full mesh configuration is used between them which provide a flexible and effective architecture against obstacles and breakdowns. In addition, a WiFi network in mesh configuration based on 802.11s can be supported by the access point. However, we consider the case where a WiFi user type B is directly connected to the CPE/AP in one hop. The overall architecture is mainly composed of the following components:

A. *AAA server*

AAA refers to a framework, based on IETF (Internet Engineering Task Force) activities that specify the procedures for authentication, authorization, and accounting associated with the user. Using AAA procedures, an operator or a network administrator can set up access control on network entry points. Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage time for billing purposes. AAA information is typically stored in an external database or remote server such as RADIUS (Remote Access Dial-In User Service) (See section III).

B. *QoS Manager*

The QoS manager encompasses the entities and functionalities required to offer and guarantee the QoS in end-to-end fashion. In our architecture end-to-end path includes different environments such as WiFi, WiMAX and IP backbone in the core network. The QoS parameters and classes of services defined in each environment require a mapping work to ensure end-to-end QoS which is out of scope of this paper. Briefly speaking a SLA (Service layer Agreement), i.e. the end-to-end QoS contract, will be negotiated between the user and the operator. The QoS Manager will be charged to setup the SLA.

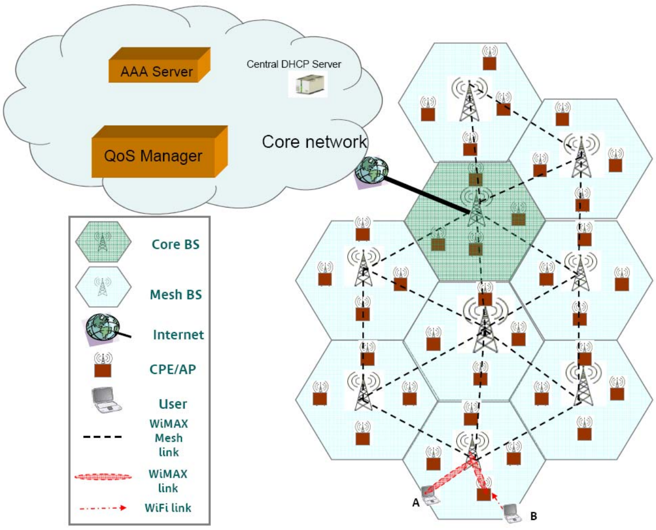

Figure 1: Overall architecture

C. *IP addressing scheme*

An efficient and flexible IP addressing scheme is adopted to allow nodes to obtain IP addresses to communicate. The IP address acquisition scheme consists of: i) A central DHCP (Dynamic Host Configuration Protocol) server at the core network to attribute an IP address for each Core Base station (CBS). ii) A Cluster Backhaul DHCP server uses the CBS addresses in order to attribute a backhaul IP addresses for each 802.16 bases station with hierarchical based approach. iii) A local DHCP server uses the backhaul 802.16 base station IP address in order to attribute an access IP address for each entity in the 802.16 cell (for the users type A and B, CPE/APs, and for 802.16 BS).

D. *CPE/AP*

This equipment is connected to the BS using 802.16 technology in PMP mode; it is considered as a user type A from BS side. It acts as a normal WiFi access point to provide transparent access of user type B to WiMAX network. To communicate with the MBS or CBS by the 802.16 interface, the CPE/AP achieves the PMP Network Entry Protocol as specified in the standard [2]. The authentication procedure is similar to the user type A authentication (see section III. D. 1) . After successful completion of authentication, the registration process is initiated. The CPE/AP sends a registration request message to the BS, and the BS sends a registration response to the CPE/AP. To establish the IP connectivity, the CPE/AP gets an IP address from the local DHCP server on 802.16 BS.

E. MBS

The MBS is a 802.16 BS connected to the network in mesh mode. IEEE802.16 standard [2] specifies the auto-discovery and topology update of the mesh network by using the mesh network entry procedure; The MBS will use the MSH-NCFG (Mesh Network Configuration) messages to acquire coarse synchronization with the network and to build a physical neighbour list. The MBS will select a potential sponsor MBS from the established list. Then it synchronizes its time with the potential sponsor MBS and sends a MSH-NetEntry (Mesh Network Entry) message including the Node ID (IDentity) of the potential sponsor MBS. After the basic capabilities negotiation, the MBS performs the authentication procedure (see section III C) and the registration process is initiated. The MBS starts DHCP procedure with the cluster DHCP server on the CBS in order to get the backhaul IP address. After registration and transfer of operational parameter, the MBS closes the entry procedure, and the sponsoring MBS acknowledges sponsor channel closure. After entering the network, the MBS can establish links with other MBS.

F. Core BS

In addition to the MBS functionalities, the CBS ensures the connection to the IP backbone core network. It is responsible of the mesh scheduling and mesh network management.

G. Routing

Topology-aware routing protocols can significantly improve the performance of the network while ensuring reliable connectivity. Optimized Link State Routing (OLSR) protocol [5] is used in our architecture to achieve routing in the mesh part of the network. OLSR is a proactive protocol proposed for routing in wireless mesh networks. Using OLSR, each BS (CBS or MBS) exchanges control and information messages with other BSs, collects data about available route in wireless mesh network and then calculates an optimized routing table. The advantage of this protocol is that it ensures reliable mesh connectivity with self-configuration and the connection is quickly established. The exchanged messages may also support information related to QoS.

III. Security and AAA

In this section, we present a brief overview of the security in WiFi and WiMAX networks. Then, we propose an efficient solution to offer a secure service for users.

A. WiFi security

WiFi Protected Access (and WPA2) has been created to improve WEP (Wired Equivalent privacy) mechanism which is the first WiFi security solution well known for its security limitations. WPA2 is a solution included in WiFi certification that allows an enterprise to deploy an AAA infrastructure to authenticate users and ensure data confidentiality and integrity over the WLAN. WPA2 provides a robust security mechanism that addresses the specific requirements for WiFi networks. WPA2 is based on RADUIS and a protocol called EAP (Extensible Authentication Protocol) [6] for authentication. EAP supports multiple authentication methods, certificates, and public key authentication and used to both the wired and wireless LANs. For confidentiality, data integrity control and cryptographic key management, WPA2 suggests the use of TKIP (Temporal Key Integrity Protocol), and an optional CCMP (Counter with Cipher Blok Chaining message Authentication Code Protocol) scheme. TKIP provides a solution to WEP limitations by using per-packet key mixing, a message integrity check and a re-keying mechanism. TKIP ensures that every data packet is sent with its own unique encryption key. TKIP does not require the update of the hardware of the devices to run it. Simple software upgrade is enough. The CCMP uses AES (Advanced Encryption Standard) for encryption and will require a hardware upgrade to support it.

B. WiMAX security

To provide authentication and confidentiality to users and to protect unauthorised users, IEEE 802.16 security is implemented as a privacy sub-layer at the bottom of the MAC protocol. The Privacy Key Management (PKM) protocol defined in [2] and named version 1 (PKMv1) supports both PMP and Mesh modes. The protocol employs X.509 digital certificate [8] and Authorization Key (AK) as well as Traffic Encryption Key (TEK). Due to lack of a BS certificate, PKMv1 is vulnerable and not well protected against attacks [7]. The amendment [3] defines PKMv2 which introduces a solution to mutual authentication and promotes a key hierarchy structure to reduce the cost of key exchanges in PKM. PKMv2 protocol does not support operations in mesh mode, only PMP mode is operational with PKMv2. PKMv2 specifies two authentication schemes, one based on RSA (Rivest, Shamir, Adelman) and another based on EAP.

The PKMv2-RSA is an optional scheme of PKMv2 protocol to mutually authenticate user type A and BS in order to transport the preliminary Primary Authorization Key (Pre-PAK) securely to the user type A. To create a secure tunnel between the user type A and the server, PKM-EAP based authentication is better because PKM-EAP is executed between the user type A and the AAA server in the user's home network, while PKMv2-RSA is executed between the user and the BS in the access network.

C. Proposed solution

A robust security framework is adopted to protect user personal data and network from malicious attacks. The proposed architecture is illustrated in Figure 2. WPA2 is used in WiFi, i.e. TKIP/EAP/RADIUS; TKIP for confidentiality, data integrity and key management; EAP/RADIUS for authentication and authorization. In WiMAX PMP mode for user type A and CPE/AP, PKMv2, i.e. PKM/EAP/RADUIS is adopted. As for Mesh mode between BSs, PKMv2-RSA based authentication can be used to achieve mutual authentication between a new MBS and a sponsoring MBS or CBS. This solution will protect the network against malicious sponsor MBS. When a new MBS builds the physical neighbours

MBSs and selects one MBS sponsoring node, it sends a start message with its manufacturer certificate. Then it sends an authorization request including the new MBS's X509 digital certificate [3].

The BS's certificate includes the following information:

ContryName =<Country of Operation>
OrganizationName =<Name of Infrastructure Operator>
OrganizationalUniteName =<WirelessMAN>
Commonname =<SerialNumber>
CommonName =<BS ID>

Each 802.16 BS has a BS's IDentity (BS's ID). The BS ID is an operator defined value; consequently the BS ID is typically issued by the operator, who must ensure that the BS ID is unique within the operator's network.

Having successfully validated the new MBS's certificate, the sponsoring MBS activates a PAK, encrypts it using the new MBS's Public Key and sends, in an authorization replay to the new MBS, the encrypted key together with the sponsoring MBS's X509 digital certificate and other parameters. The new MBS verifies the sponsoring MBS certificate and the TEK exchanges' messages start after validation.

This solution satisfies the main requirements for an efficient user authentication and security. Those requirements include:

- *The mutual authentication:* each two communicating nodes should exchange and validate credentials presented to each other. Whereas a manufacturer's certificate identifies the manufacturer of an IEEE802.16 device, a CPE/AP or user type A certificate (identified by MAC address) is typically created and signed by a manufacturer, and used for identification.
- *Encryption and data authenticity:* robust and scalable solutions are adopted for over-the-air encryption to ensure data origin authenticity and to protect against attacks.

D. User Authentication

User authentication can be based on a variety of authentication mechanisms such as Username/password, Universal SIM (USIM) and Removable User Identity Module (RUIM), etc. We will describe the authentication procedures for both user type A and user type B.

1) User type A

After completing the PMP Network Entry process and capabilities negotiation, user type A starts the authentication process, based on PKM-EAP recommendations as follows:

- In order to initiate the EAP conversation, a user type A may send PKMv2-EAP-start message (see Figure 3).
- The MBS sends an EAP-Identity request to the user. The EAP request may be encapsulated into a MAC management PDU (Packet data Unit) in the BS and may be transmitted in format of [PKM-Request (PKMv2-EAP-transfer)]. User receives EAP-Request, forwards it to the local EAP method for processing, and transmits EAP-Response (PKM-Response/PKMv2 EAP-transfer). From now, the BSs (MBS and CBS) forward all users' messages to the AAA server.
- After one or more EAP-Request/Response exchanges, the AAA server connected remotely via Radius protocol, determines whether or not the authentication is successful. The shared session keys are established at user type A and at the AAA server. The AAA server then transfers the generated keys to the MBS. As specified in 802.16e [3], both user type A and MBS generate a PMK. Then, the AAA Server and user type A generate AK from shared session keys. The key distribution entity in MBS delivers AK and its context to key receiver entity (in MBS) which is responsible of generating subsequent subordinate keys from AK and its context.

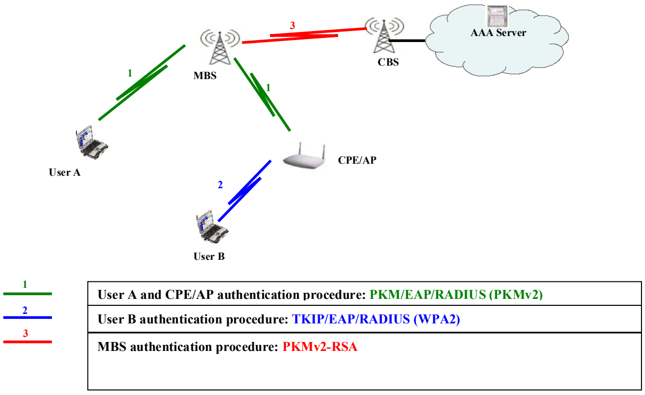
3
AAA Server
CBS
MBS
1
1
User A
CPE/AP
2
User B
1
2
3
User A and CPE/AP authentication procedure: PKM/EAP/RADIUS (PKMv2)
User B authentication procedure: TKIP/EAP/RADIUS (WPA2)
MBS authentication procedure: PKMv2-RSA

Figure 2: Proposed architecture of security

- To mutually prove possession of valid security association based on AK, the MBS sends the Security Association Traffic Encryption Key (SA-TEK) challenges message, the user type A responds by sending the SA-TEK request, and the MBS perform the procedure by sending the SA-TEK response. The SA-TEK proves liveliness of the security association in the user type A and its possession of the valid AK.
- For each SA, the user requests from BS two TEKs which are randomly created by the MBS and transferred to the user.
- Service flow Addition MAC management messages are used to create a new service flow.

2) User type B

To obtain Internet access, a user first completes the network discovery process and sends an associate request to an AP. After the reception of an associate response, user type B starts the authentication process, based on WPA2 recommendations, by sending user authentication information (ex: user name and password), in order to be allowed to use network resources. To get a better idea of how the authentication will operate, the interactions between elements are illustrated in the diagram of Figure 4:

- The user type B sends an EAP-start message.
- The AP replies with an EAP-request identity message.
- The user type B sends an EAP-response packet containing the identity to be sent to the authentication server. In a secure environment, the AP, MBS and CBS forward this information to the authentication server.
- The authentication server using a specific authentication algorithm verifies the user's identity. This could be through the use of digital certificates or other EAP authentication type.
- The authentication server will either send an acceptation (or reject) message to the AP. Then the AP sends an EAP-success packet (or fail) message to the user type B.

- If the authentication server accepts the user type B, the AP will transit the user type B's port to an authorized state and forward additional traffic. This is similar to the AP automatically opening the gate to let in only people belonging to the group cleared for entry.

In this procedure for user type B, all BS’s are merely a secure conduit for the AAA messages and does not play a significant role in the AAA process.

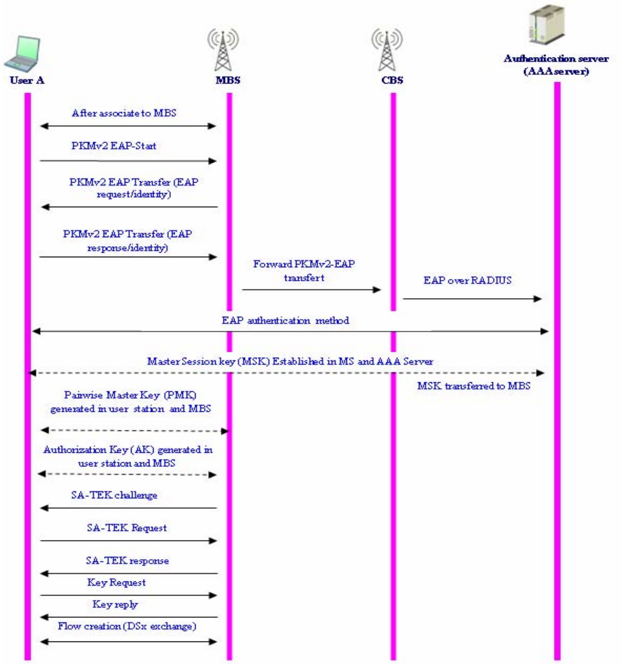
User A
MBS
CBS
Authentication server (AAA server)
After associate to MBS
PKMv2 EAP-Start
PKMv2 EAP Transfer (EAP request/identity)
PKMv2 EAP Transfer (EAP response/identity)
Forward PKMv2-EAP transfert
EAP over RADIUS
EAP authentication method
Master Session key (MSK) Established in MS and AAA Server
MSK transferred to MBS
Pairwise Master Key (PMK) generated in user station and MBS
Authorization Key (AK) generated in user station and MBS
SA-TEK challenge
SA-TEK Request
SA-TEK response
Key Request
Key reply
Flow creation (DSx exchange)

Figure 3: User type A Authentication procedure

E. *Accounting*

Accounting consists traditionally of the operations of the metering resource consumption, collection information and billing. The challenge is to collect accurate usage data and match this data to the appropriate account so that payment can be derived. The accounting architecture is based on an access sever using RADIUS infrastructure [9]. Two modes of accounting procedures can be envisaged:

- *Postpaid (offline accounting) mechanism:* is implemented via contract between the user and the operator. Subscriptions may be typically a monthly fee for device or user and may include additional charges for accumulated usage.

- *Prepaid (online accounting) mechanism*: the prepaid packet data service allows a user to purchase packet data service in advance based on volume or duration. A prepaid server (PPS) function may be collocated with the RADIUS server to support the capability to provide tariff volume/duration based prepaid packet data service. This capability includes charge by volume with different tariff for different QoS, time of day, etc. and charge by duration for different time of day etc.

IV. CONCLUSIONS

In this paper, we proposed a flexible architecture for hybrid wireless mesh network where both 802.11 and 802.16 technologies are deployed in a complementary way. Users can access to the network directly by WiMAX through the 802.16 base stations, or by WiFi through a WiFi CPE/AP connected to the 802.16 BS by WiMAX. The functional entities as well as aspects related to security and AAA are investigated and efficient solutions are proposed to provide robust secure service for users. Future work will focus on the QoS support as well as mobility management in the proposed architecture.

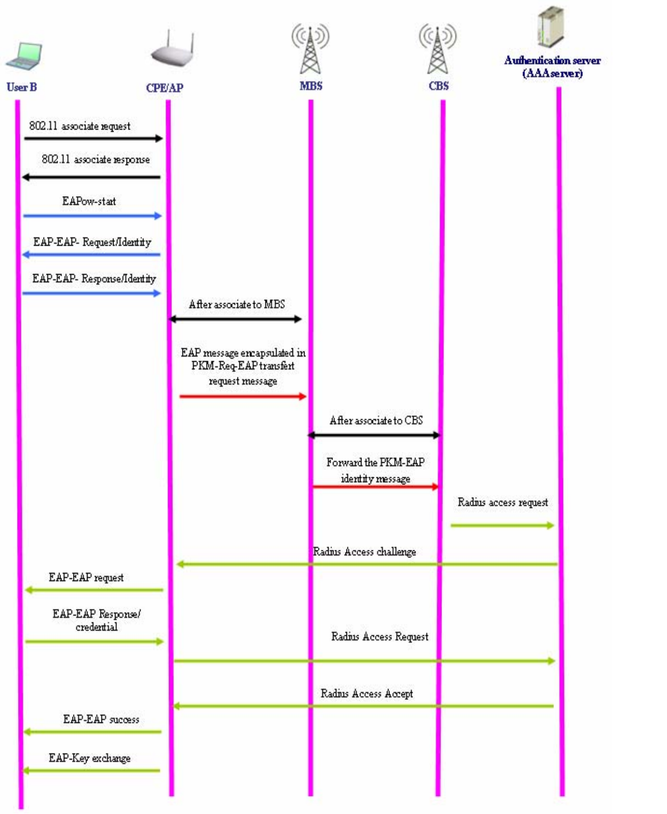
User B
CPE/AP
MBS
CBS
Authentication server (AAA server)
802.11 associate request
802.11 associate response
EAPow-start
EAP-EAP- Request/Identity
EAP-EAP- Response/Identity
After associate to MBS
EAP message encapsulated in PKM-Req-EAP transfert request message
After associate to CBS
Forward the PKM-EAP identity message
Radius access request
Radius Access challenge
EAP-EAP request
EAP-EAP Response/ credential
Radius Access Request
Radius Access Accept
EAP-EAP success
EAP-Key exchange

Figure 4: User type B Authentication procedure

REFERENCES

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

[2] IEEE Standard 802.16-2004 "Air Interface for Fixed Broadband Wireless Access Systems", October 2004.

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

[4] IEEE Standard 802.16f: Air Interface for Fixed Broadband Wireless Access Systems, Amendment 1: Management Information base, December 2005.

[5] T. Clausen, P. Jacquet, "OLSR Optimized Link State Routing", RFC 3626, October 2003.

[6] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[7] D. Johnston and J. Walker, "Overview of IEEE 802.16 security", IEEE Security & Privacy, 2004.

[8] R. Housley, W. Polk,W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[9] C. Rigney, "RADIUS Accounting", IETF RFC 2866, June 2000.