Bottom Up Survey of the WiMAX Technology

S.Frei[1,2], W.Fuhrmann[3], A.Rinkel[2] and B.Ghita[1]

[1]Centre for Security, Communications and Network Research,
University of Plymouth, Plymouth, United Kingdom
[2]University of Applied Sciences Rapperswil, Rapperswil, Switzerland
[3]University of Applied Sciences Darmstadt, Darmstadt, Germany
e-mail : {sandra.frei | bogdan.ghita}@plymouth.ac.uk, arinkel@hsr.ch and
w.fuhrmann@fbi.h-da.de

Abstract

Current subscribers except optimal QoS for their real-time services, both under fixed and mobile access scenarios. These expectations demand complex QoS mechanisms and flexible mobility management from the network to provide a smooth service to the user. This paper provides a bottom up survey of the QoS and mobility mechanisms from the WiMAX air interface over the network architecture up to the interworking with the 3GPP network. The analysis includes aspects on mobility, QoS and security as far as it is relevant for mobility and QoS.

Keywords

Mobile WiMAX, WiMAX Forum architecture, Quality of Service, Mobility, WiMAX 3GPP interworking

1. Introduction

Current subscribers want to use real-time services such as VoIP and video streaming even while they are moving around. To meet this demands high QoS and an appropriate mobility management has to be provided to the end user to enable a smooth service to them. Within the WiMAX technology the aspects of QoS and mobility are analysed in this paper.

A basic definition of the WiMAX physical and MAC layers are defined in (IEEE 802.16, 2004). The IEEE amendment (IEEE 802.16e, 2005) is defined to support mobility of up to 125 Km/h. But the two bottom layers are not enough to tackle the whole problem of QoS and mobility. This is where the WiMAX Forum comes into play. They formed a Network Working Group (NWG) which has the task to define an architecture to enable the WiMAX technology to provide QoS, mobility as well as the possibility to interwork with other networks such as 3GPP Service Architecture Evolution (SAE) network. Interworking definitions of 3GPP network with non-3GPP access technologies are given in (3GPP TS 23.402, 2009). An overview of the standardization roadmap and timelines of the IEEE 802.16 standard and the WiMAX Forum is given in (Etemad, 2008).

The paper provides an overview of the mobility and QoS mechanisms defined in both, the IEEE 802.16 standards and the releases from the WiMAX Forum, which implies also the interconnection with the 3GPP SAE network. It is structured as follows: In chapter 2 the mobility mechanisms in the IEEE 802.16e are analysed. Chapter 3 provides an overview about the QoS mechanisms defined in the IEEE 802.16 standard. The following chapter covers the definitions from the (WiMAX Forum Stage 2, 2009) and (WiMAX Forum Stage 3, 2009) and analyse the authentication and security architecture, the QoS architecture and the mobility management. In chapter 5 the architecture with which it is possible to interconnect with the 3GPP SAE network is presented. Finally chapter 6 concludes the paper.

2. Mobility in the IEEE 802.16e standard

The IEEE 802.16e standard (IEEE 802.16e, 2005) is an amendment to the IEEE 802.16 standard (IEEE 802.16, 2004). It provides support for Subscriber Stations (SSs) moving at vehicular speed. The SSs are called Mobile Stations (MSs) in this standard. Functions to support higher layer handover between Base Stations (BSs) or also sectors are specified, which operates in the licensed bands below 6GHz. Fixed subscriber capabilities are not compromised.

2.1. Providing network topology information

The more information of the surrounding BSs and its capabilities is available the merrier and smoother can a handover been processed. There are two ways of getting information about the neighbour BSs.

1. **Neighbour advertisement:** The BSs can provide information about the surrounding BSs by sending advertisement messages MOB_NBR-ADV to the MSs at a periodic interval. The BS gets the information about the neighbour BSs over the backbone. This information provided to the MS enables the MS to synchronize with neighbouring BSs without monitoring the neighbour BS broadcasts. The MOB_NBR-ADV message contains information about the physical profile used by the BS as well as the supported scheduling services: Unsolicited Grant Service (UGS), Real-time Polling Service (rtPS), Non-real-time Polling Service (nrtPS), Best Effort, Extended real-time Polling Service (ertPS). The types of scheduling services are used to classify different types of QoS traffic. A description of these scheduling services can be found in (Frei et al. 2008). Therefore this information is very important for MSs carrying e.g. real-time traffic to decide which BS is suitable and supports the needs for the traffic when seeking initial network entry or before a handover is made.

2. **Scanning and association with BSs**: The MS can request a group of scanning intervals. If the intervals are granted by the BS the MS can scan and as a result getting information about the neighbouring BSs. The association procedure is optional and an initial ranging procedure which is processed during scanning interval on one of the neighbour BSs. The

association enables the MS to acquire and record ranging parameters and service availability information to select a suitable target for handover.

2.2. The handover process

There are three handover types defined in the (IEEE 802.16e, 2005). The two optional handover modes are called Macro Diversity Handover (MDHO) and Fast BS Switching (FBSS). They are not considered in this paper since these two handover modes are not supported by the WiMAX Forum so far. Only the Hard Handover (HHO) is mandatory and also supported from the WiMAX Forum. The HHO process has the following stages:

Cell reselection: The MS use the neighbour BS information gathered from the MOB_NBR-ADV message or request a scanning interval to scan and possibly range with the BS. The serving BS can inform the target BS that the MS has interrest to potentially select this BS as a target BS for handover.

Handover decision and initiation: The handover begins with the decision of an MS to change from the serving BS to a target BS. The handover decision can be made either from the MS or the BS. The handover decision is performed with either the BS sending a MOB_BSHO-REQ notification or the MS sending a MOB_MSHO-REQ message.

Synchronisation to target BS downlink: The MS has to synchronize to the downlink of the targetBS and get downlink (DL) and uplink (UL) transmission parameters. If the MS received a MOB_NBR-ADV message previously, containing the needed information this process can be shortened. If the target BS had previously received a handover notification from the serving BS over the backbone, the target BS can allocate a non-contention-based Initial Ranging opportunity for the MS.

Ranging: It is needed to adjust power and timing and get a valid basic Connection ID (CID). The target BS requests information about the MS over the backbone from the serving BS and from the backbone network itself. Depending on the kind of information the target BS is getting from serving BS and/or from the backbone network, the target BS can decide if the re-entry process will be shortened by skipping one or several network entry steps:

- Negotiate basic capabilities.
- Privacy Key Management (PKM) Authentication phase.
- Traffic Encryption Key (TEK) establishment phase.
- Send registration request message REG-REQ.

BS can send unsolicited REG-RSP message with updated capabilities information or skip REG-RSP message when no Type Length Value (TLV) information have to be updated.

Termination of MS context: This is the last step in the handover process. The serving BS terminates all connections belonging to the MS as well as the context associated with them.

Handover cancellation: An MS can precede a handover cancellation at any time during handover process.

In the sequence diagram Figure 1 the whole hard handover process, initiated by the MS, is depicted.

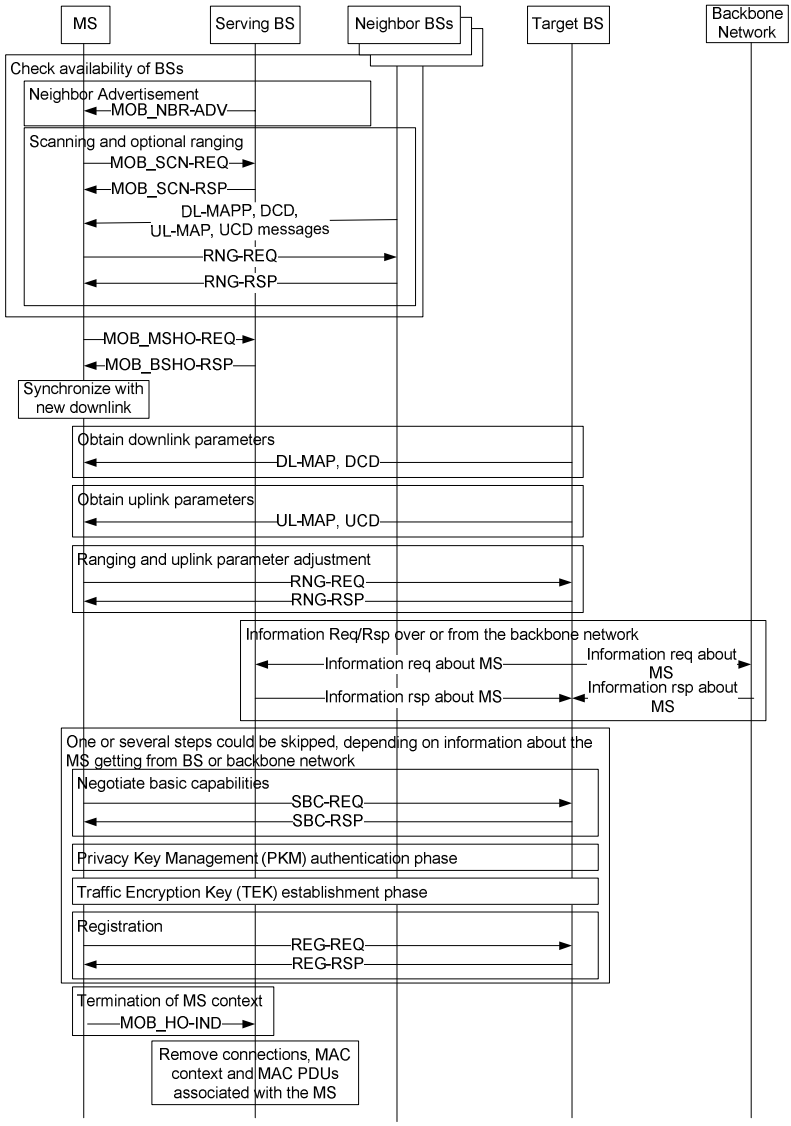

Figure 1: Handover process initiated by the MS

3. QoS support in the IEEE 802.16 standard

The IEEE 802.16 standard provides QoS support on the level of Service Flows (SFs). A service flow is a MAC transport service provided to transport either uplink or downlink traffic. Service flows can be created either statically (provisioned) or dynamically. Each service flow is associated with a QoS parameter set which could consist of e.g. throughput, latency, jitter, packet error rate. Three types of states are defined in which a service flow could be. To change the state of a service flow the appropriate QoS parameter sets have to be set by the MS and also authorized by the BS. In Figure the activation model of the three different service flow types are shown. The DSA and DSD are not supported if static/provisioned QoS is used. These are only supported if dynamic QoS is used.

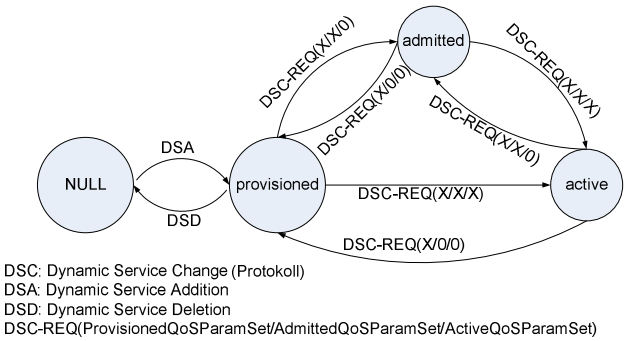

Figure 2: Service Flow types and its activation model

The two step activation via the state admitted is important for e.g. voice communication. The resources for the call are reserved while in the admitted state, but the resources are not activated for data traffic until the end-to-end signalisation is completed.

If only static QoS is supported the provisioned QoS parameter set cannot be modified. This is checked by the authorization module in the BS. Whereas a modification of the ProvisionedQoSParamSet is allowed if dynamic QoS is supported. The fact that both static and dynamic QoS mechanisms are defined in the IEEE 802.16 leads to the need of two separate authorization models namely the static or provisioned and the dynamic authorization model.

Static or provisioned authorization model: All service flows are preconfigured. A dynamically adding of service flows as well as modifications on ProvisionedQoSParamSet are prohibited and such request will be declined. The ProvisionedQoSParamSet is in this case also the AuthorizationQoSParamSet which is the highest QoS which can be granted. Admission and activation requests are accepted if the following conditions both are fulfilled:

- requested AdmittedQoSParamSet <= ProvisionedQoSParamSet (AuthorizationQoSParamSet).

- requested ActiveQoSParamSet <= AdmittedQoSParamSet

Dynamic authorization model: Service flows are created dynamically at run time through DSA (Dynamic Service Addition) Requests. Additional to the authorization module in the BS a policy server is needed. The policy server is out of scope of the IEEE 802.16 standard but the Network Working Group (NWG) of the WiMAX Forum defined it, see chapter 4.2. The policy server provides rules and actions to define the processing of requests. The dynamic authorization model provides more flexibility and therefore more complex authorization mechanisms can be performed. In this case the ProvisionedQoSParamSet could be different than the AuthorizationQoSParamSet which is the highest QoS which can be granted. An admission or activation request is accepted if:

- requested AdmittedQoSParamSet <= AuthorizationQoSParamSet.
- requested ActiveQoSParamSet <= AdmittedQoSParamSet.

4. The WiMAX Forum architecture

The IEEE 802.16 standard provides standardisation only for the air interface between the Subscriber Station (SS) or Mobile Station (MS) and the BS at the PHY and MAC layer. The network specification is beyond the scope of the IEEE 802.16 standard and therefore the WiMAX Forum defined the architecture to connect the BS to the IP network. The WiMAX Forum is a non-profit industry group devoted to the global adaption and interoperability of WiMAX systems. The Network Working Group (NWG) specified in (WiMAX Forum Stage 2, 2009) the end-to-end network architecture which is depicted in Figure 3. The network architecture contains two parts. One is the Access Service Network (ASN) which is owned, maintained and operated by the Network Access Provider (NAP) and the other one is the Connectivity Service Network (CSN) relating to the Network Service Provider (NSP) which ownes the subscriber and provides the broadband access service. The MS/SS is connected over the reference point R1 to the ASN. The R1 is the air-interface implementation of e.g. the IEEE 802.16 standard. As seen in Figure 3 the ASN consists of one or more BS and ASN Gateways, which are connected over the reference point R6. To connect ASN GWs with each other the reference point R4 is used which supports control and data bearer plane protocols.

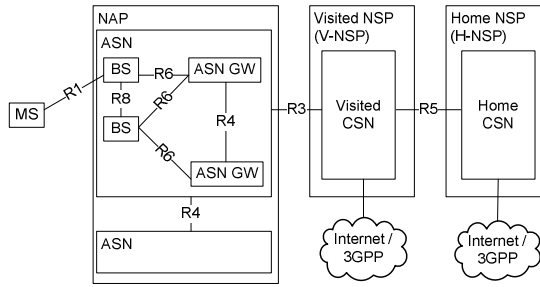

Figure 3: Fine WiMAX network architecture Profile C

To ensure a fast handover the BSs can communicate on the data and control plane with one and another over the virtual R8 reference point. On the control plane the inter-BS communication protocol defined in the IEEE 802.16e standard as well as other protocols are used. The Reference point R6 between the BS and ASN GW contains a set of control and data bearer plane protocols. The control plane consists of protocols to support the mobility tunnel management like establishing, modifying and releasing mobility tunnels. The data bearer plane includes the intra-ASN data path or inter-ASN tunnels between the BS and the ASN GW. The reference point R3 between the ASN and the CSN supports policy enforcement, mobility management, tunneling and Authentication, Authorization and Accounting (AAA). To enable the interworking between the visited CSN and the home CSN the reference point R5, settled between them, is used. The deployment of the components are defined by the NWG within three profiles A, B and C. Profile A was removed in the WiMAX Forum release 1.5 and therefore this profile is ignored. The profile B distributes the ASN GW and the BS in one device. The Radio Resource Management (RRM) which consists of the Radio Resource Agent (RRA) and the Radio Resource Controller (RRC) are both located in the BS. Profile C is nearly the same as Profile B except that the ASN GW and the BS do not reside in the same device, they are separated. Profile C leads to a hierarchical network architecture whereas profile B results in a flat architecture. A discussion about flat and hierarchical network architecture and the mobility impacts and possible solutions is given in (Sim et al. 2009).

4.1. Authentication and Security Architecture

The authentication and security architecture is only taken into account as long as it is relevant for QoS or mobility.The WiMAX authentication and security architecture supports all of the IEEE 802.16e security services with an IETF EAP based AAA framework (WiMAX Forum Stage 2, 2009). The AAA framework is not only used for security issues but also for service flow authorization and QoS and policy control. The QoS profiles and policy rules are stored in the AAA server. In Figure 4 there is the AAA architecture framework depicted with the MS connected to a visited CSN requesting for a service. If the MS is directly connected to the home CSN the AAA proxy server in the visited CSN would not be needed and therefore it is not present. The AAA proxy server can priviously load the required data from the AAA server located in the home CSN. This way the AAA Proxy Server is able to evaluate the request and send an appropriate response itself.

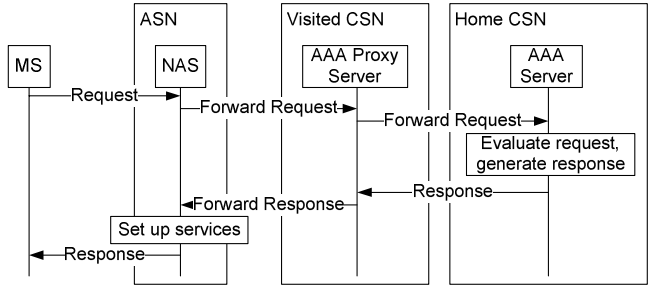

Figure 4: Service Request from MS via a visited CSN to the home CSN

4.2. QoS Architecture

The WiMAX QoS framework supports both static and dynamic provisioning of service flows like it is defined in the IEEE 802.16e standard. The (WiMAX Forum Stage 2, 2009) only supports static/provisioned QoS which means there is no modification of the service flows allowed and the deletion is only done when exiting network. In the WiMAX Forum release 1.5 dynamic QoS is supported. The WiMAX QoS framework provides mechanisms for provisioning and managing the service flows and their policies as well as admission control, bandwidth management and differentiated levels of QoS applied to a user or service flows. The QoS functional architecture defined by the (WiMAX Forum Stage 2, 2009) is shown in Figure 5 where the Profile C, defined by the NWG, is used.

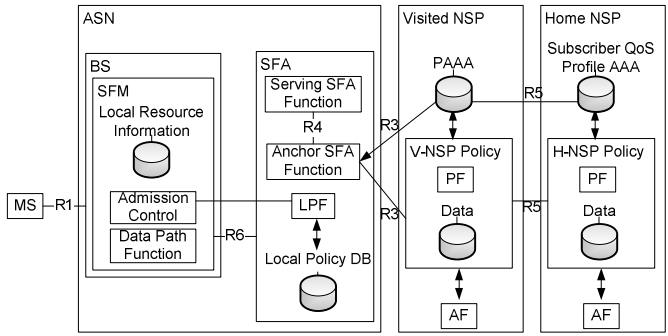

Figure 5: QoS functional architecture within profile C

This QoS functional architecture supports the dynamic creation, admission, activation, modification and deletion of service flows. The entities are described in the following:

Service Flow Management (SFM): The SFM is a logical entity located in the BS and manages the local resource information to provide information needed for the admission control decision. It is responsible for the creation, admission, activation, modification and deletion of IEEE 802.16 service flows.

Service Flow Authorization (SFA): The SFA is a logical entity located in the ASN GW. As mentioned before, data can be preloaded from the AAA server in the Home NSP into the PAAA. It is also possible to load user QoS profiles during network entry from the PAAA into the SFA. In this case all incoming service requests are evaluated against this loaded QoS profile and the decision wether or not to allow the flow is made. Otherwise the service request is forwarded to the PF. The anchor SFA is responsible for the communication with the PF, whereas the serving SFA relays QoS related primitives, applies QoS policy for that MS and communicates directly with the SFM. The SFAs can perform policy enforcement on the ASN level using the Local Policy Function (LPF) and the corresponding database. Furthermore the LPF can be used for local admission control enforcement.

Policy Funcions (PF): The PF is located at the visited and the home network each with the corresponding database. The databases store general policy rules and application dependent policy rules of the NSP. The AAA server can provision the PF with subscriber related QoS information. Then the PF located in the home network determines how incoming service flows are handled. The PF evaluates incoming service requests against the provisioned.

Authentication, Authorization and Accounting (AAA) Server: In the AAA server the subscriber´s QoS profile and the associated policy rules are stored.

Application Function (AF): The AF can initiate service flows creation. This entity could be e.g. a SIP proxy.

4.3. Mobility Management

User wants to move around while they are connected to the network. In the access technology WiMAX a handover needs to be processed when a MS moves and there is a need to change the BS because e.g. the signal strength is getting lower towards the connected BS. The NWG (WiMAX Forum Stage 2, 2009) decided to use the two IETF protocols, the Mobile IPv4 (MIPv4) and the Mobile IPv6 (MIPv6), to tackle the mobility problem if the IP address of the MS has to change. Therefore a tunnel is established between the Home Agent (HA) located in the CSN and the Foreign Agent (FA) in the ASN GW. The mobility management defined by the NWG consists of two types of handover handling:

Intra ASN mobility also called ASN-anchored mobility or micro mobility: The old BS and the target BS are both located in the same ASN or different ASNs but in the same operator´s domain. In this case the IP address of the MS does not have to change, it remains the same. Since the FA is the tunnel end point and stays the same, there is no need for layer 3 mobility changes. In Figure 6 the handover of the MS is shown where the old BS and the target BS remain in the same ASN. The R6/R8 ASN Anchored Mobility Scenarios are defined in (WiMAX Forum Stage 3, 2009).

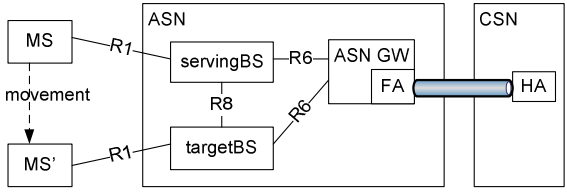

Figure 6: ASN anchored mobility where MS remains in the same ASN

There is a possibility to do an ASN anchored mobility even when the MS is changing the ASN it is attached to. In this case the ASNs have to be in the same operator´s domain. The tunnel between the HA and the FA remains unchanged, while the traffic from the old ASN GW is redirected to the new ASN GW. An overview about this handover is given in the Figure 7. The redirection is done through Data Path Function (DPF) which can reside in the ASN GW. This redirection reduces the

handover latency because the communication is kept locally in the ASN operator´s domain. But if the data path is too long it becomes less efficient because of the distance between the FA and the MS. In such a case it is better to do a CSN anchored mobility handover and change the FA to reduce the distance towards the MS.

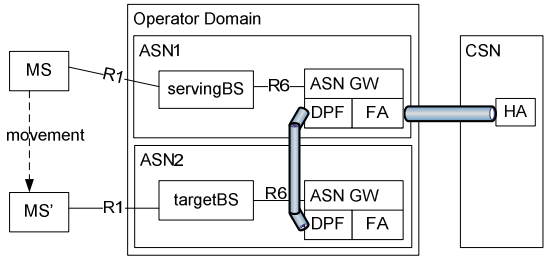

Figure 7: ASN anchored mobility where MS changes ASN but remains in the same operator domain

In Figure 8 the Data Path Functions before, during and after the handover with the changing of the ASN GW is shown. The DPF is responsible to set up bearer plane between components with tunnels. Bearer planes can be set up between ASN GW and BS, or between ASN GWs, or between BSs. Depending on the role of the DPF, they have separate names, as can be seen in Figure . Every DPF can buffer the packets to send them later on to the air link. Generic Routing Encapsulation (GRE) is taken as an example of an IP in IP tunnel protocol.

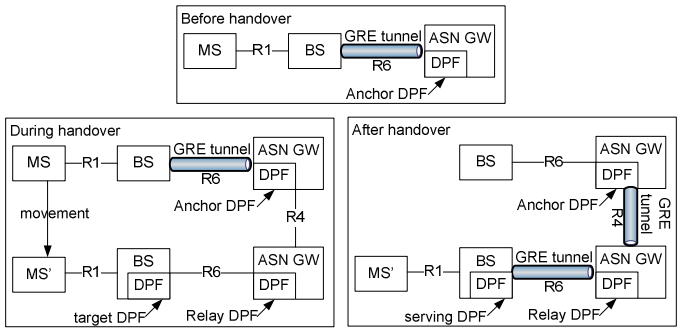

Figure 8: DPF before, during and after handover

To provide ASN anchored mobility there are three functions defined by the NWG. One of these was previously already described in this paper, it is the DPF. The other two are the handoff and the context function.

- **The handoff function** is responsible to decide about the Handover (HO) and do all the HO related signaling. Like the DPF the handoff function also has different entities namely the serving- relay- and the target HO Function. One task of the serving HO function is to communicate with the target BS to prepare for handover either directly over the virtual R8 reference point or

indirectly through the ASN GW Relay HO function. Another task of the serving HO function is to inform the MS about the results of the handover preparation.

- **The context function** is used to exchange and move the context information of a subscriber to an entity which is newly involved in the Data Path (DP). The context server located in the ASN GW can hold the mobile subscriber´s or BS´s context. The context includes e.g. security information, MAC context, like SFIDs, QoS information, idle mode behaviour of the MS etc.

Inter ASN mobility also called CSN-anchored mobility or macro mobility: The old BS and the target BS are located in different ASNs. As a consequence the IP address of the MS changes. To tackle the change of the MS´s IP address the Mobile IP Protocol, defined by the IETF in an RFC, is used. The tunnel between the HA and the old FA is removed and a new tunnel between the HA and the target FA is established. This way the data path between the FA and the MS is kept short as you can see in Figure 9. The CSN anchored mobility always comes along with the ASN anchored mobility because the Data Path (DP) has to be set up by the DPF from the target ASN GW to the target BS.

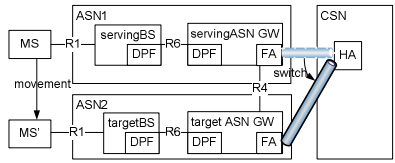

Figure 9: CSN anchored mobility handover

Even nowadays many end devices only support the IP stack and are not MIP capable. To handle both device types, with and without MIP support, the NWG also enables the possibility to deploy Proxy MIP (PMIP). With PMIP the proxy will do any MIP signalisation on behalf of the MS. As a consequence the MS has not to implement the MIP and is not aware of the mobility. To support both IP versions IPv4 and IPv6 the according MIPv4 and MIPv6 are defined to be enabled by the NWG.

5. WiMAX interworking with 3GPP

A step towards converged networks is the interworking between the WiMAX and the 3GPP SAE network. In the WiMAX Forum document WiMAX-3GPP interworking the interworking with the 3GPP Release 7 is described. Here the possible interworking of WiMAX and 3GPP Release 8 is presented. With this scenario dynamic QoS can be established over the 3GPP Policy and Charging Control (PCC) framework. A description of the 3GPP reference architecture is given in (Frei et al. 2009). An analysis of WiMAX and 3GPP PCC framework interworking is not considered in this paper. A survey of the WiMAX PCC interworking, which allows dynamic QoS is given in (Taaghol et al. 2008). There are two ways non-3GPP technologies can interwork with the 3GPP architecture as it is depicted in Figure 10.

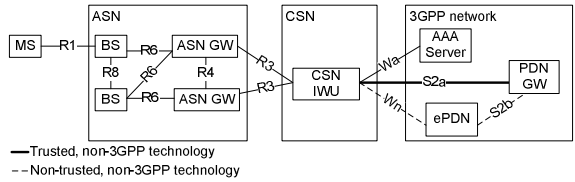

Figure 10: WiMAX and 3GPP interworking

The connection of the WiMAX radio access network which is a trusted network towards the 3GPP network is done through the reference point S2a. The Interworking Unit (IWU) located in the CSN is connected directly with the PDN GW. If the WiMAX radio access network is not a trusted partner of the 3GPP network operator the WiMAX network is connected to the PDN GW through the ePDN component over the Wn and the S2b reference points. Both approaches communicate over the Wa reference point with a 3GPP AAA server. From the PDN gateway the PCC framework from the 3GPP SAE network is accessible.

6. Conclusion

The paper provides a bottom up overview of the QoS, mobility and security mechanisms in WiMAX technology, whereas the security architecture is only considered as long it has an impact on QoS or mobility. Therefore the mobility and QoS mechanisms of the IEEE 802.16/e standard are analysed in detail, especially the mandatory hard handover process and its required functions as well as the static QoS. To provide a comprehensive overview which goes beyond the WiMAX air interface the defined network architecture from the WiMAX Forum, which is necessary to connect the WiMAX air interface towards IP networks and provide further QoS and mobility management, is described. Finally, to move a step closer towards converged networks the interworking architecture of WiMAX and 3GPP network is presented.

7. References

3GPP TS 23.402 (2009), Technical Specification, *3rd Generation Partnership Project*, "Architecture enhancements for non-3GPP accesses (Release 9)", V 9.1.0

Etemad, K., (2008), "Overview of mobile WiMAX technology and evolution", *IEEE Communications Magazine*, Volume 46, Issue 10, October 2008 pp. 31 - 40

Frei, S., Fuhrmann, W., Rinkel, A., Ghita, B. (2008), "End-to-End QoS and mobility in wireless access networks interworking with the 3GPP EPC", *Proceedings of the fourth collaborative research symposium on Security, E-learning, Internet and Networking SEIN 2008*, pp. 195-208, Glyndwr University, United Kingdom, ISBN: 987-1-84102-196-6

Frei, S., Fuhrmann, W., Rinkel, A., Ghita, B. (2009), "Reference architecture for end-to-end QoS in heterogeneous wireless network environments", *third international conference on Internet Technologies and Applications ITA 2009*, Wrexham, United Kingdom

IEEE 802.16 (2004), "Part 16: Air Interface for Fixed Broadband Wireless Access Systems", *IEEE*

IEEE 802.16e (2005), “Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems”, *IEEE*

Sim, S., Han, S., Park, J., Lee, S., (2009), “Seamless IP mobility support for flat architecture mobile WiMAX networks - [WiMAX update]”, *IEEE Communications Magazine*, Volume 47, Issue 6, June 2009 pp. 142 - 148

Taaghol, P.; Salkintzis, A.; Iyer, J. (2008), ”Seamless integration of mobile WiMAX in 3GPP networks”, *IEEE Communications Magazine*, Volume 46, Issue 10, October 2008 pp. 74 - 85

WiMAX Forum, (2009), “Architecture Tenets, Reference Model and Reference Points”, Release 1.0 Version 4 - Stage 2, http://www.wimaxforum.org/technology/documents, *WiMAX Forum*

WiMAX Forum, (2009), “Detailed Protocols and Procedures”, Release 1.0 Version 4 - Stage 3, http://www.wimaxforum.org/technology/documents, *WiMAX Forum*