End-to-End QoS and Mobility in Wireless Access Networks Interworking with the 3GPP EPC

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

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

Abstract

This paper gives an overview about the QoS and mobility mechanisms in several network environments: Wireless Local Area Network (WLAN) radio access, Evolved Packet Core (EPC), and 802.16 WiMAX radio access. A number of solutions aiming to provide QoS at the network layer are also covered, together with a comparative analysis of the mobility mechanisms within each technology, analysis that highlights the similarities and differences between these environments, as well as their drawbacks. The paper shows, that further research is required in the end-to-end QoS and mobility area, both in the wireless access networks as well as the core network.

Keywords

End-to-End Quality of Service, Mobility, Wireless Access Networks, Evolved Packet System

1. Introduction

The moving towards packet oriented networks, where IP plays an important role, leads to new possibilities and also requirements of the users regarding the network. Especially the increasing use of multimedia services, like voice and video streaming or live streaming, creates new requirements to the network. An end-to-end QoS has to be granted to enable smooth real time services, because these services consist of time critical data and therefore they are prone to jitter, delay and packet loss. On the other hand the users are getting more mobile and want to be able to use services anywhere and anytime. The mobility mechanisms have to be able to provide quick handover and roaming so that the session still remains. This is important for real time services. Otherwise the real time services will become useless for the users. QoS and mobility have a crucial impact on each other. With a walkthrough from the WLAN IEEE 802.11 access network with the amendment (IEEE 802.11e, 2005) over the EPC core network to the WiMAX (IEEE 802.16, 2004) access network the mechanisms of QoS and mobility are analysed in this paper.

2. Analysis of the networks focusing on QoS

2.1. QoS in WLAN

The IEEE 802.11e standard introduces the access mechanism Hybrid Coordination Function (HCF). The HCF contains two independent access mechanisms, the HCF Controlled Channel Access (HCCA) and the Enhanced Distributed Channel Access (EDCA). In (Ni, 2005) the QoS limitations of the IEEE 802.11 Standards are described as well as performance evaluation of the IEEE 802.11e standard.

The standard introduced two concepts: the Transmission Opportunities (TXOPs), which defines the exclusive use of the medium for a specific station from a certain time and a certain duration and the classification of data in four Access Categories (AC).

The idea behind the HCCA is to reduce the contention of the stations to a minimum. To realise this, the hybrid coordinator (HC), which is usually the access point, manages the access to the medium for the stations. The access point is called QoS access point (QAP) and the stations are called QoS stations in the IEEE 802.11e standard.

The QoS mechanism follows a two-step sequence:

- The QoS station signs on at the QAP. Through this the QoS station sends the Traffic Specifications (TSPEC). The TSPEC contains information about the quality of the connection the QoS station wants, including delay, jitter, packet loss and required bandwidth.
- If the QAP can support the requested TSPECS, it returns a confirmation message. Otherwise, the TSPECs are rejected. Only the QAP is responsible for granting TXOP’s.

The HCCA is an integrated service (IntServ) that uses TSPECs, which is a set of parameters that define the characteristics and QoS expectations of a traffic flow. The following parameters can be used to specify the QoS: the nominal MSDU size, the maximum MSDU size, the minimum/maximum service interval, the inactivity interval, the suspension interval, the service start time, the minimum/mean/peak data rate, the burst size, the delay bound, the minimum PHY rate, the surplus bandwidth and the medium time. In the IEEE 802.11e standard the following parameters forming the TSPECs are admissible:

S for specified, X for unspecified, and DC for “do not care.”

TSPEC Parameter	Continuous time QoS traffic (HCCA)	Controlled access CBR traffic (HCCA)	Bursty traffic (HCCA)	Unspecified non-QoS traffic (HCCA)	Contentionbased CBR traffic (EDCA)
Nominal MSDU Size	S	S	X	DC	S
Minimum Service Interval	S	Nominal MSDU size/mean data rate, if specified (VoIP typically uses this)	Mean data rate/ nominal MSDU size, if mean data rate specified	DC	DC
Maximum Service Interval	S	Delay bound/ number of retries (AV typically uses this)		DC	DC
Inactivity Interval	Always specified				DC
Suspension Interval	DC				
Minimum Data Rate	Must be specified if peak data rate is specified	Equal to mean data rate	X	DC	DC
Mean Data Rate	S	S	DC	DC	S
Burst Size	X	X	S	DC	DC
Minimum PHY Rate	Always specified				
Peak Data Rate	Must be specified if Minimum Data Rate Specified DC	Equal to Mean Data Rate	DC		
Delay Bound	S	S	DC	X	X
Surplus Bandwidth Allowance	Must be specified if the delay bound is present			DC	S
Medium Time	X (not specified by non-AP QSTA; only an output from the HC)				

Table 1: admissible TSPECS

Within the EDCA access control, the medium is not managed by a single device. The mechanism used resembles the Distributed Coordination Function (DCF) from the IEEE 802.11 standard, including a backoff time used to control the access to the medium. In contrast of the DCF, where the maximum backoff time for each station is the same, the EDCA uses different backoff times for different QoS classes. Therefore the stations with higher QoS classes can send more often than stations with lower

QoS classes. The EDCA cannot give any guarantees about bandwidth and delay. The EDCA is a differentiated service (DiffServ) that is contention based. Four Access Categories (ACs) are used to differentiate the quality of the services. The AC Background (BK), Best Effort (BE), Video (VI) and Voice (VO). The four ACs are mapped to the QoS categories from the IEEE 802.1d standard as follows, like in the standard (IEEE 802.11e, 2005) described:

Priority	802.1D tags	AC	Designation (informative)
Lowest	1	AC_BK	Background Priority
	2	AC_BK	Background Priority
	0	AC_BE	Best Effort Priority
	3	AC_BE	Best Effort Priority
	4	AC_VI	Video Priority
	5	AC_VI	Video Priority
	6	AC_VO	Voice Priority
Highest	7	AC_VO	Voice Priority

Table 2: AC to 802.1D tags mapping

The HCCA can give QoS guarantees to stations, as soon as the QAP will acknowledge the parameters in the TSPEC across the stations. Another advantage of the HCCA is that there is no contention and because of that, there is no waste of time.

2.2. EPS QoS

The 3GPP is currently developing a new core network, the Evolved Packet Core (EPC), which is planned for the release 8. It supports 3GPP access technology as well as non-3GPP access technology as described in (3GPP TS 23.402, 2007). The Evolved Packet System (EPS) contains the EPC and several access systems including eUTRAN, UTRAN and LTE. The new architecture is less hierarchical than the traditional one, fact that leads to the reduction of signalling delay and, implicitly, to better efficiency and network performance.

Mobility and QoS provisioning are both goals in the development of the EPS. Within the EPS, a logical concept of a bearer is defined, called EPS bearer. Each bearer is associated with one corresponding QoS profile. As a result each elementary data flow, called Service Data Flow (SDF), is associated with one EPS bearer. On the other hand an EPS bearer is aggregated to one or more SDFs. The default EPS bearer consists of non Guaranteed Bit Rate (GBR) with no admission control and with no guaranteed resources whereas the dedicated bearers have a GBR and a Maximum Bit Rate (MBR) defined.

2.3. QoS in WiMAX

Very often the support of QoS is an add-on for an already existing access technology. But this is not the case with the IEEE 802.16 standard. From the beginning of the standardization QoS was a point that had to be supported. An overview of mobility and QoS of WiMAX is given in (Iyer *et al*. 2007).

Five scheduling services exist in the IEEE 802.16 and IEEE 802.16e standard:

- **Unsolicited Grant Service** (UGS) is designed to support real-time traffic. It offers a constant bit rate (CBR), using a fixed-sized grant on a periodic interval. Therefore no bandwidth requests are needed. An example of an application which may employ UGS is Voice over IP (VoIP) without silent suppression.

- **Real-time polling service** (rtPS) is also designed for real-time traffic. The supported data packets have a variable size and are on a periodical basis. Unicast bandwidth requests were used to regulate the bandwidth requirements. Audio and video streaming may typically use rtPS.

- **Non-real-time polling service** (nrtPS) is very similar to the rtPS. The bandwidth requirements can be signalized with unicast bandwidth requests and additionally with multicast/broadcast requests through a contention based polling opportunity.

- **Best effort service** (BE) only provides little QoS. It is suitable for traffic that has no or very low QoS requirements. The BE traffic is only sent when the media is available, and no higher service class request the media to send traffic. Only the contention based polling opportunity is used.

- **Extended real-time polling service** (ertPS) was defined in the 802.16e standard. It is designed to support real-time traffic with variable datarate. For example VoIP with silent suppression.

Another basic concept of the IEEE 802.16 standard, which is very important for the QoS, is the use of service flows (SF). A service flow is a transport service on the MAC layer for simplex up- and downlinks. Each Service Flow (SF) is associated with a QoS parameter set, which describes the QoS that the system wants to reach and it is also associated with a scheduling service. The parameters of the QoS parameter set, are not defined in the 802.16 standard. It is left to the vendors. Just to name a few popular parameters: jitter, delay, packet loss, throughput, packet error rate etc.

There are three types of QoS parameter sets: The Provisioned QoS parameter set, the Admitted QoS parameter set and the Active QoS parameter set. As mentioned above, each SF is described with at least one QoS parameter set. That is the reason why also three types of SF exist: the provisioned, the admitted and the active SF. A SF has a 32 bit SFID and also a 16 bit Connection ID (CID) which identifies the logical connection. The standard does not define which parameters build a QoS parameter set. This definition is left to the network operators.

2.4. QoS signalling

The Resource Reservation Protocol (RSVP) (IETF RFC 2205, 1997) is a transport protocol to reserve resources from a sender along a path through the network to the receiver. It is an Integrated Service (IntServ). IntServ (IETF RFC 1633, 1994) is a fine based mechanism that is applied per flow using end-to-end signalling. The required resources are reported to all involved devices and all devices have to agree. If one device refuses to support the demanded resource, the resource can not be reserved and there will not be any QoS guarantees. The same principle applies if a device does not support the RSVP, this, the huge signalling overhead required, is one of the reasons why IntServ is not used very often. But if it is employed, it is mainly used in access networks, where the numbers of hops are relatively small.

Another approach is the differentiated service (DiffServ) that uses a classification of the packets. DiffServ is a coarse grained mechanism which uses classes to differentiate the services, also called Class of Service (CoS). To divide the packets into different classes, the Type of Service (ToS) byte in the IPv4 and IPv6 header are used. Each network device applies a specific forwarding treatment to the packets, which is called Per Hop Behaviour (PHB).

The Next Step in Signalling (NSIS) IETF working group deals with signalling protocols in the internet. The working group is defining also a framework for signalling QoS. The protocol to establish QoS reservations in the internet is the QoS NSIS Signalling Layer Protocol (NSLP). It is independent from the QoS specifications used in lower layers. The NSLP is relying on the NSIS Transport Layer Protocol (NTLP) which is an abstract protocol and is defined in the concrete protocol General Internet Signalling Transport (GIST). In (Angori *et al.* 2007) NSIS is used to signalling End-to-End QoS over an End-to-End QoS enabled architecture where WiMAX is used as the access network.

2.5. Interworking between EPS and other wireless access technologies

The wireless technologies like 802.11b, 802.11g as well as the 802.11n and also the 802.16 WiMAX developed rapidly and the possible data rate also increased constantly. This indicates that these technologies are potential alternative access technologies to access the EPC packet network. Therefore the 3GPP defined the interworking between 3GPP and WLAN in (3GPP TS 23.234). The TS mainly focuses on the IEEE 802.11 standard but other wireless access technologies are not excluded. To enable QoS mechanisms the DiffServ is used between the WLAN UE and the Packet Data Gateway (PDG) using the IPv4 Type of Service field (TOS) or the IPv6 Traffic Class field. The architecture to integrate non-3GPP access technologies is independent from the access technology. Therefore it works for WLAN as well as for 802.16 WiMAX. In the following figures the WLAN is used as the access network technology. Figure 1 presents the architecture of a trusted WLAN access. This is the case when the WLAN is controlled by the operator itself, or by another provider which can be trusted through mutual agreements.

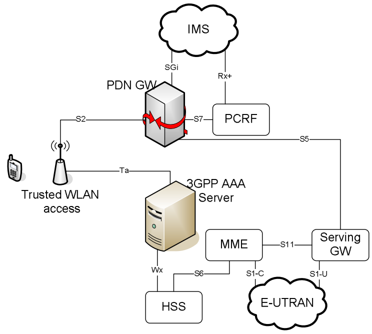

Figure 1: Trusted WLAN access

The 3GPP AAA server facilitates end-to-end authentication for WLAN terminals using 3GPP credentials. To get 3GPP authentication vectors and also user related subscription information, the 3GPP AAA server has a connection to the HSS through the Wx interface. Data traffic is sent to the PDN GW over the S2 interface. The Ta interface was defined to transport authentication, authorization and charging related information in a secure manner. In this architecture, the MME and the Serving GW is not needed anymore, but are depicted for completeness, to provide an overview. The location management and the packet session signalling are in the responsibility area of the WLAN access.

The architecture, depicted in Figure 2, serves the non-trusted WLAN access.

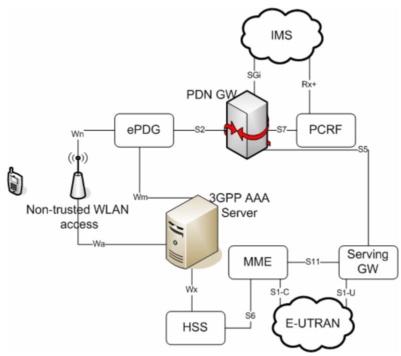

Figure 2: Non-trusted WLAN access

In this architecture the evolved Packet Data Gateway (ePDG) is introduced. All the data traffic from the WLAN is sent through the ePDG. The function of the ePDG is to filter unauthorized traffic and establish a secure tunnel with the terminal through IPSec. The new interface Wm between the ePDG and the 3GPP AAA server is defined to get user related information from the 3GPP AAA server. This enables the ePDG to provide user data tunnelling and encryption to the terminal. The Wa interface, which supports authentication for non-trusted access is equivalent to the Ta interface which supports trusted access. In (Krishnan *et al.* 2008) a possible mobility architecture is introduced which is based on the Proxy Mobile IP (PMIP).

3. Analysis of the networks focusing on Mobility

3.1. Mobility in WLAN

There are three types of handover in WLANs. The first is the movement inside a Basic Service Set (BSS), which means that the Mobile Node (MN) does not change the access point (AP). The second type is the handover between APs. The APs are located in an Extended Service Set (ESS) and usually have the same subnet. This kind of handover is addressed by the IEEE 802.11r draft. The third handover type is the one between APs which are located in different ESS and where the IP address of the MN will change.

In case of real-time applications like voice over IP (VoIP) the delay should not exceed 50 ms. Currently a BSS transition requires hundreds of ms, which is too much for real-time applications.

This is why the draft standard IEEE 802.11r introduced Fast BSS transition in order to reduce the delay as much as possible. In addition, the 802.11r standard tackles security issue of traditional handover by allowing the MN to establish the security state before or during re-association on the new AP and thereby reduce the delay.

Another problem occurs within the field of QoS while a handover is taking place: the MN cannot determine what level of QoS the new AP can offer until the MN attaches to the new AP. This could lead to a situation where the new AP can not offer the required QoS from the application, but the problem would be noted only after the whole transition. To avoid this situation, the MN in the 802.11r draft is allowed to establish the QoS state before or during re-association on the new AP.

A handover sequence contains the following stages:

- Scanning to detect a new AP (responsibility: lower layers 1 and 2)
- Association with the new AP (responsibility: lower layers 1 and 2)
- QoS renegotiation (responsibility: lower layers 1 and 2)

If the subnet changes the following steps are necessary:

- Acquire a new IP address (responsibility: higher layer 3)
- Notify the corresponding node (CN) about the new IP address (responsibility: higher layer 3)

The draft standard 802.11r is considering only the lower layers 1 and 2. To manage the mobility on the IP layer, other layer 3 protocols are used. A few of them are described later on in this paper.

3.2. EPS mobility

The Mobility Management Entity (MME) is used for inter core network signalling for mobility between 3GPP access networks. It manages and stores the User Entity UE context, it generates temporary identities and it allocates them to UEs. The MME is also responsible for session and subscriber management functions such as QoS radio negotiation and authentication, while the Serving Gateway (S-GW) is responsible for inter 3GPP mobility. This is also called the 3GPP anchor function. In case of an active handover, if the target access node is already chosen, the S-GW establishes the tunnel and the MME is responsible to coordinate the tunnel switching after the handover on the access nodes is completed. The idle mobility is managed almost the same way like in the GSM system. There are Tracking Areas (TAs) containing a few access nodes, like eNodeBs. The UEs have stored their actual TA and compare this information with the frequently received TA information from the access node. If they do not match anymore, the UE will update the MME with the new TA. The MME pages the UE in the current TA, if data for the UE are available.

3.3. Mobility in WiMAX

A location management entity is required to provide mobility for the Mobile Station (MS); the entity provides information about the location of all MSs no matter if they are in the idle or active mode. Therefore the MSs have to update their location information, which is sent to the Base Station (BS) and from there it is stored in a database located remotely in the network. If the MS has to make a location update every time the MS is attached through another BS, the signalling overhead from the location update would increase drastically as the cell range gets smaller and the number of subscribers increases. In order to address this problem, multiple BSs were linked to the same location area. As a result, the MS has to do only a location update if the MS changes the location area, which is less often than doing a location update each time the MS is reaching a covered area from another BS. This means less signalling overhead.

On the other hand, large location areas also introduce drawbacks. If data packets come along the network for a specific MS, the location area is looked up in the location database. If the location area contains several BSs then the paging signal is sent to all of them. The BS then has to forward the paging signal to the Subscriber Stations (SS) until the specific MS is finally found. A big location area will, implicitly, cause also a substantial amount of paging traffic in the core and access networks.

In (Li *et al.* 2007) an overview of the IEEE 802.16e standard with focus on QoS provisioning and mobile WiMAX specification is provided. The IEEE 802.16e standard states that mobility has to be provided up to a speed of 125 km/h that the handover must last no longer than 50ms. To achieve these requirements, the handover management has to be very fast. The standard provides three types of handovers.

- The hard handoff (HHO) is mandatory. It is also known under the term "Break before make". It implies that the connection to the serving BS is first disconnected and afterwards the connection to the target BS is established.

- The macro diversity handover (MDHO) is optional. The MS is receiving the same packets from two or more BS. In the uplink the sent packets from the MS would be processed by two or more BSs. A diversity set is used, where all the active BSs to the MS are listed.

- The fast base station switching (FBSS) is also optional. The MS has only a connection to one active BS (anchor BS), receiving and sending frames. The anchor BS can change any frame. The diversity set is used as well.

The handover can be initiated either by the network or by the MS itself. The decision whether a handover should be made is based on the measurements and estimates of different parameters of the channel. These parameters are directly dependent on the QoS of the application which is using the connection. As an example, one of the parameters is the Minimum Signal Level (MSL). If the QoS is defined on a high level, then the MSL is also much higher than a MSL from a low level [of] QoS. QoS has a direct influence on the handover decisions.

3.4. Mobility on the network layer

All the described mobility mechanisms described before are dealing with the handover on layer 1 and 2 and especially with the keep alive of the physical connection. If the connection on layer three breaks, the physical connection still remains connected, but the session breaks down and the application is also losing the connection. No communication is possible anymore until the session is re-built again. Obviously, it is not sufficient only to manage the physical connection. Also the connection on layer three has to be managed. To address this problem there exist several variants of Mobile IP (MIP). In this paper a few of them where introduced, for a handoff latency analysis of other variants like Fast MIP and Hierarchical MIP (Haseeb and Ismail, 2007) is recommended. The problem on layer three is that the IP address could change. In such a case the layer three connection will be disconnected. One possible answer to this problem is the Mobile IP (MIP) which is defined by the IETF. In the case of using mobile IP there are two IP addresses. One is the home address (HoA). It is provided by the home network of the mobile station, in this case called mobile node (MN). The other address is the care of address (CoA), which is a temporarily provided address of the visited network. To manage the mapping of the HoA and the CoA, a Home Agent (HA) and a Foreign Agent (FA) is used. If the MN moves to a foreign network it informs the HA about the new CoA. The CoA is the address of the FA. If a correspondent node (CN) sends packets to the MN, the packets will be first sent to the HA. Then a tunnel from the HA to the CoA (FA) will be established. From the FA, the packets are normally distributed to the MN. The packets sent from a CN to a MN take a triangular route (CN – HA- FA- MN). Triangular routing causes several drawbacks. An example of such a problem caused by triangular routing occurs if the CN and the FA are located in the same geographical area and the HA is far away. Then the packets have to travel a long distance and that leads to a massive delay. The packets sent from the MN to the CN can be routed directly, so there is no triangular routing in the opposite direction. Another drawback of MIP is the fact that through the IP in IP tunnel between the HA and the FA the QoS information provided in the IP header is hidden. The router between the tunnel can not use the originally QoS information.

IPv6 was designed to support mobility from the beginning of the specification. MIPv6 is based on IPv6 and could therefore eliminate some drawbacks of the MIP. The triangular routing is not necessary anylonger because the IPv6 has a built-in routing optimization. Due to the huge improvement of IPv6 there is also no need for an FA. The IPv6 header can carry the CoA of the MN. As a result no tunnel is needed anymore and the problem of the lost QoS information is eliminated. The development of the IPv6 protocol solves many of the primary disadvantages of MIP.

With the MIPv6 most of the problems would be solved, but unfortunately IPv6 is not established very frequently. Therefore other ways have to be found to accomplish the goal of seamless mobility. Another drawback is that the mobile node needs to support MIP but with the Proxy MIP (PMIP) this problem is addressed. The most striking point in the use of PMIP is the elimination of the need to support MIP in the mobile node. The Foreign Agent that is placed in the foreign network, is not necessary anymore. It is replaced by the Proxy Mobile Agent. The Proxy Mobile Agent handles the registering procedure of the mobile node with the Home Agent. And therefore the mobile node need not to know or even record any mobility mechanisms. The latency during authentication and re-authentication could be reduced (Gondi *et al*. 2008).

3.5. Media independent handover

In future, there will be more and more multimode enabled devices. Such devices support more than one access technology, no matter if it is wireless or wirelined technology. The intersystem handover, a handover between different access technologies, is also called vertical handover. The standard (IEEE 802.21, 2008), which is still a draft, defines mechanisms to provide such medium independent handovers (MIH). The scope of the standard is the initiation and preparation of handovers. In (Lampropoulos *et al.* 2008) the IEEE 802.21 standard is analysed concerning seamless mobility in inter technology handover. The standard defines Service Access Points (SAP) and primitives that provide generic link layer intelligence. The dependent SAPs of the specific media have to be amended to support MIH. The standard defines three types of services: the Media Independent Event Service (MIES) providing notification in changed link characteristics and management actions, the Media Independent Command Service (MICS) providing mobility relevant management and control functions of the link layer, and the Media Independent Information Service (MIIS) providing Information about the surrounding networks. In this paper the focus is on the MIIS which provides a framework to make it possible for the Mobile Node (MN) and the network to gather information about the heterogeneous networks in the surroundings of a geographical area. The information is provided for lower and higher layers and also for secure and non-secure ports. It is an advantage that the standard also supports non- secure ports to provide the information at layer 2 because security issues are causing delays. Therefore the information request on a non-secure port is faster but the information is less sensitive. It is used for a quick handover decision and it depends on the access technology, whether the use of the insecure port is allowed or not. The information about the surrounding networks is provided in form of Information Elements (IE) and is used to make intelligent handover decisions.

4. Conclusion

This paper provides a detailed comparative QoS and mobility analysis of the two access networks IEEE 802.11 WLAN (including the improvements brought by IEEE 802.11e) and the IEEE 802.16 WiMAX (with the EPS network). Furthermore, the paper also presents the QoS and mobility aspects during handover between the 802.11 WLAN and the 802.16 WiMAX network via EPS.

Each technology has it own, independent QoS concept. The different networks allow mapping between the QoS concepts in QoS classes. This enables the use of DiffServ over the different networks. But a guaranteed end-to-end QoS could only be established if the various network domains which are traversed, and are maintained by different operators, have common QoS agreements. Therefore agreements have to be defined between all the operators which data will traverse from the source to the destination. From a global point of view it will be very hard to realize such agreements between all or most of the operators in the world. Another approach is the use of IntServ technologies like RSVP. But the signalling overhead and the delay is not acceptable. Especially in case of a handover, the delay would not be small enough to keep up a VoIP connection. In case of the analysed access networks the QoS service parameters are left up to the network operators to be defined. This leads to different parameter definitions and this will cause problems in mapping them with each other.

The mobility mechanisms on layer one and two are media dependent. The mobility mechanisms on the two bottom layers were described and also the mobility solutions on the third layer. The draft standard (IEEE 802.11r, 2008) has the goal to fasten the BSS transition by reducing security overhead and allowing to check QoS availability before completely connecting to the new AP. The QoS influences the mobility in this matter and has also impact on handover decisions. To get additional information about surrounding networks, the draft standard (IEEE 802.21, 2008) could be used to additionally improve the decision making of handover/roaming. And while the (IEEE 802.21, 2008) is media independent, it is applicable to all kind of access networks.

On the layer 3 several protocols have been analysed. The MIPv4 is not able to provide only short delays. The cause is the triangular routing from the CN to the MN. But for real time services handover latency may not exceed 50ms, otherwise the service becomes unusable. The MIPv6 is an incredible improvement due to the fact, that triangular routing is no longer needed and therefore the delays getting smaller than compared to MIPv4. But since IPv6 is not widely accepted and used yet, this solution to provide mobility on layer 3 is still insufficient nowadays. An advantage of the use of PMIP is the fact, that the mobile node need not be aware of any mobility mechanisms and therefore no MIP support is needed to be implemented in the mobile node. There are still open research points, especially in the combination of the QoS and the mobility area because of the impact that they have on each other.

5. References

3GPP TS 23.401 (2008), Technical Specification, *3rd Generation Partnership Project*, "Architecture enhancements for non-3GPP accesses (Release 8)", V 8.2.0, 3GPP

3GPP TS 23.402 (2007), Technical Specification, *3rd Generation Partnership Project*, "Architecture enhancements for non-3GPP accesses (Release 8)", V 8.0.0, 3GPP

Angori, E., Borcoci, E., Mignanti, S., Nardini, C., Landi, G., Ciulli, N., Sergio, G. and Neves, P. (2007), "Extending WiMAX technology to support End to End QoS guarantees", *WEIRD workshop proceedings*, May, 2007

Gondi, V.K., Quoc-Thinh, N.V. and Agoulmine, N.(2008), "A new Mobility solution based on PMIP using AAA mobility extensions in heterogeneous networks", *Network Operations and Management Symposium Workshops*, 2008. NOMS Workshops 2008, IEEE

Haseeb, S. and Ismail, A. F. (2007), Handoff latency analysis of mobile IPv6 protocol variations, *Computer Communications*, Volume 30, Issue 4, 26 February 2007, Pages: 849-855

IEEE 802.11e (2005), "Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements", *IEEE*

IEEE 802.11r (2008), "Draft Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Amendment 2: Fast BSS Transition", P802.11r/D9.0, *IEEE*

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*

IEEE 802.21 (2008), "Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services", P802.21/D9.1, *IEEE*

IETF RFC 1633 (1994), Request For Comments, "Integrated Services in the Internet Architecture: an Overview", *IETF*

IETF RFC 2474 (1998), Request For Comments, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", *IETF*

IETF RFC 2475 (1998), Request For Comments, "An Architecture for Differentiated Services", *IETF*

IETF RFC 3344 (2002), Request For Comment, "IP Mobility Support for IPv4", *IETF*

IETF RFC 3775 (2004), Request For Comments, "Mobility Support in IPv6", *IETF*

IETF (2007), "Mobility Management using Proxy Mobile IPv4", Internet Draft, *IETF*

Iyer, P., Natarajan, N., Venkatachalam, M., Bedekar, A., Gonen, E., Etemad, K. and Taaghol, P. (2007), "All-IP Network Architecture for Mobile WiMAX", *Mobile WiMAX Symposium*, 2007, IEEE

Krishnan, S., Marchand, L., Nilsson and Cassel, G. (2008), "An IETF-based Evolved Packet System beyond the 3GPP Release 8", *CTIA The Wireless Association*

Lampropoulos, G., Salkintzis, A.K. and Passas, N. (2008), "Media-independent handover for seamless service provision in heterogeneous networks", *IEEE Communications Magazine*, Volume 46, Issue 1, January 2008 Pages: 64 – 71

Li, B., Qin, Y., Low, C. P. and Gwee, C. L. (2007), "A Survey on Mobile WiMAX [Wireless Broadband Access]", *IEEE Communications Magazine*, Volume 45, Issue 12, December 2007 Pages: 70 - 75

Ni, Q (2005), "Performance analysis and enhancements for IEEE 802.11e wireless networks", *IEEE Network*, Volume 19, Issue 4, July-Aug. 2005 Pages: 21 – 27