



# A cross-layering based autonomic approach for QoS support in heterogeneous wireless networks

Tara Ali Yahiya, Kaouthar Sethom, Guy Pujolle, André-Luc Beylot

## ► To cite this version:

Tara Ali Yahiya, Kaouthar Sethom, Guy Pujolle, André-Luc Beylot. A cross-layering based autonomic approach for QoS support in heterogeneous wireless networks. International journal of communication networks and distributed systems, 2008, 1 (3), pp.312-329. 10.1504/IJCND.2008.020713 . hal-01167561

**HAL Id: hal-01167561**

**<https://hal.science/hal-01167561>**

Submitted on 26 Nov 2020

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution| 4.0 International License

# A cross-layering based autonomic approach for QoS support in heterogeneous wireless networks

**Tara Ali Yahiya, Kaouthar Sethom and Guy Pujolle**

Computer Science Laboratory, University of Pierre et Marie Curie, 104 Avenue du  
President Kennedy, 75016 Paris, France

**André-Luc Beylot**

ENSEEIH, IRIT Laboratory, 2, rue C. Camichel, BP 7122, F-31071 Toulouse Cedex 7, France

**Abstract:** Future network environments will be heterogeneous and mobile terminals will have the opportunity to dynamically select among many different access technologies. Therefore, it is important to provide service continuity in case of vertical handoffs when terminals change the access technology. Two important wireless access technologies are WLAN (wireless local access networks) and WMAN (wireless metropolitan access networks) networks. In this article, we address several challenges related to a seamless integration of those technologies. We highlight important aspects for designing WLAN/WMAN interworking architecture on the basis of IEEE 802.21 framework. Then, we address important quality of service (QoS) issues for such interworked systems like degree of QoS support provided by the technologies, QoS mapping and signalling for vertical handoff. We combine concepts of autonomic computing in the design of the framework in order to use intelligence to provide flexibility, accessibility and transparency to the mobile users.

## 1 Introduction

The main challenge in the development of future wireless communication system is to provide users with a wide range of services across different radio access technologies through a single mobile terminal, while maintaining the quality of service requirements (Fodo et al., 2003). These features require connectivity across multiple networks with different radio technologies, over different geographic areas, and access to different types of services. Such connectivity can be provided by 4G architecture which envisions highly flexible and adaptive integration of diverse radio technologies to support built-in capability for seamless interaction in these environments. Nevertheless, integration of heterogeneous networks poses many challenges such as interface selection, seamless handoff mechanisms, coordinated configuration of QoS mechanisms and content adaptation strategies (McNair and Zhu, 2004). Any mobile system in such integrated networks have to be able to adapt to changing access networks and changing environments automatically without bothering humans to intervene in order to make mobile computing feasible. To adapt to such changes, the system needs information about the environment, including various information about the access network itself, information about services supported by this access network, as well as more general information about the current context in which the mobile entity resides. To achieve these goals, some kind of infrastructure is needed.

The evolving IEEE 802.21 (2006) standard defines a framework intended to improve mobile devices' handoff decisions based mainly on lower-layer information from both mobile devices and the access network. Such information is provided by defining an abstraction layer providing media independent handoff (MIH). The MIH is used for the special case of handoff optimisation, particularly between heterogeneous networks. The

increase requirement of the intelligence in such environment is behind our motivation to introduce autonomic networking. This is because future network is expected to embrace the heterogeneity arising from the different network control technologies such that it appears homogenous to the potential users of network services. Therefore, next generation network is expected to be self-managed as it treats network composition and re-configuration in a self-managed way (IBM, 2003).

In this paper, we propose to use some of the autonomic networking concepts to assure the dynamic integration of the user's device to the management environment. This is done by introducing additional entities to the basic design of IEEE 802.21 framework to achieve this purpose. Therefore, the article is organised as follows. Section 2 describes an autonomic architecture for providing seamless handoff. Section 3 gives a brief description of IEEE 802.21 and then Section 4 explains in detail the proposed supplementary functions added to it. Sections 5 and 6 introduce the mobility and the QoS management based on our framework. Finally, Section 7 ends the paper with our conclusion and future work.

## **2 Autonomic architecture and mechanisms**

Seamless handoff enables the user to perform a variety of tasks using one device over different media in an 'always connected' presence, without worrying how to interact with a device or a changing environment. This requires increased system intelligence, which is the motivation for using autonomic mechanisms. Autonomic communication is the vision of next-generation networking which will be a self-behaving system with properties such as self-healing, self-protection, self-configuration and self-optimisation (IBM, 2003). These properties can be explained as follows:

- Self-healing: discover and repair potential problems to ensure that the system runs smoothly.
- Self-protection: identify threats quickly and take protective actions.
- Self-configuration: install and set-up application/patches/updates automatically, verify compliance with the specified service levels, optimise configuration of applications using adaptive algorithm.
- Self-optimisation: constantly monitor predefined system goal and perform levels to ensure that all systems are running at optimum levels.

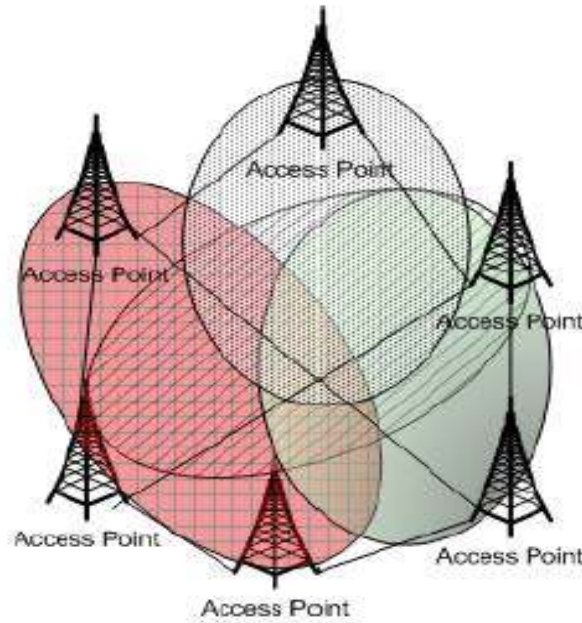
Therefore, seamless handoff depends on acquiring and understanding the current context of the user. The tasks performed by the user determine the type of information needed. Furthermore, if the context changes, then the system can determine what new data is needed. This enables the user to stay connected to critical data regardless of where he/she is, using any device. This vision can be achieved by gathering information about the environment as well as determining the best policy that can be adapted with the changing environment (Pujolle, 2006). Therefore, we propose two additional planes to the conceptual planes of telecommunication networks (control, data and management planes), which are described as the following:

- The governance plane. In order to achieve network autonomicity, standard control algorithms have to be configured to the state of the environment. This configuration

has to be performed in a coherent way over the network elements (e.g. access point, mobile device, home agent, etc.). It should be done considering the current state of the environment, and eventually the past and future states of this environment. Since cooperation between network elements is required, we assert that this plane must be strongly engineered using modern techniques from distributed algorithmic and artificial intelligence. We call this new distributed intelligence plane the ‘governance plane’.

- The knowledge plane. This plane provides a general view of the network in order to enrich the representation of the network by each element. Thus, network elements should share knowledge in a way that exchanging information will not lead to an increasing load on the whole network. However, exchanging knowledge between network elements is the most critical issue of the knowledge plane. In fact, to build a strong representation of the environment, a network element might exchange a large amount of information with its peers. Finding which type of data to share with which peer is not easy. Indeed, sharing too much information with too many peers can quickly deplete the resources. Therefore, several policies for knowledge sharing can be engineered for each type of information and each policy has to be tuned in real time depending on the state of the environment. Thus, we introduce the concept of situatedness. Situatedness means that each element in the network possesses its own vision of the environment that is not necessarily the same as its neighbours’ (Jennings et al., 1998). Elements then communicate to share parts of their knowledge. Each element knows everything about its own state and has a partial knowledge about its neighbours’ state. The width of the situated view will depend on the dynamicity of the shared information. This is because the more information is dynamic, the more exchanges occur. Figure 1 shows an example of situatedness view with a width of one hop. The knowledge sharing policy can be fulfilled by two modes: the request/response and the inform mode. Since request/response is not as robust as needed, then the policy of sharing relies mainly on the inform mode. An element sends a message to its neighbours when a change of its state has occurred, without waiting for them to request information.

**Figure 1** Situatedness view representation



### 3 IEEE 802.21 framework

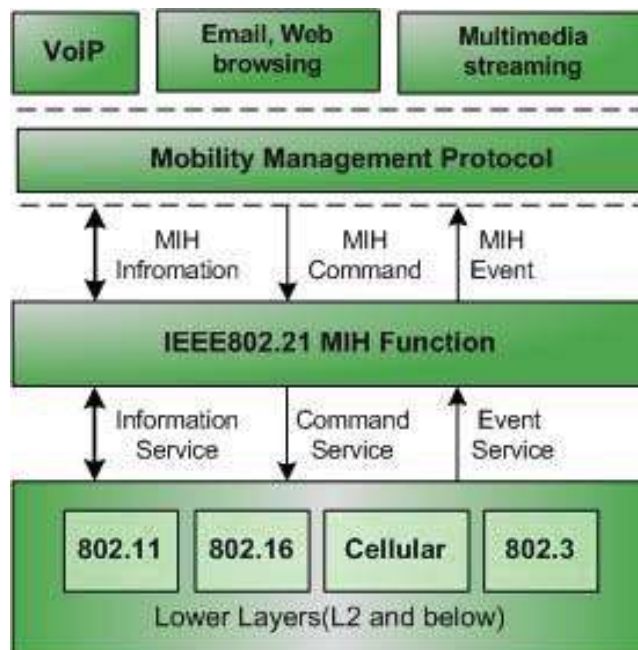
The design of IEEE 802.21 (2006) is intended to enable seamless handoff and interoperability between heterogeneous network types including both 802 and non-802 networks. This is done by introducing the layer 2.5 specified by media independent handoff function (MIHF) which provides three principal functionalities: media independent events service (MIES), media independent command service (MICS) and media independent information service (MIIS) (IEEE 802.21, 2006). These services provide methods and procedures that facilitate handover between these heterogeneous access networks. These handover procedures can make use of information gathered from both the mobile terminal and network infrastructure to satisfy user requirements. There are several factors that may determine the handover decision. Typically, these include service continuity, application call, quality of service, network discovery and selection, security, power management and handover policy. The IEEE 802.21 (2006) framework facilitates the network discovery and selection process by exchanging network information that helps mobile devices determine which networks are in their current neighbourhoods. This network information could include information about link type, the link identifier, link availability and link quality etc. of nearby network links. This process of network discovery and selection allows a mobile to connect to the most appropriate networks based on certain policies.

#### 3.1 IEEE 802.21 core architecture

The heart of the IEEE 802.21 (2006) framework is the MIHF which provides abstracted services to higher layers by means of unified interface. This unified interface exposes service primitives that are independent of the access technology. This interface is called Service Access Point (SAP). Figure 2 illustrates examples showing how the MIHF can

communicate with access specific lower layer MAC and PHY components, including IEEE 802.16, IEEE 802.11n and cellular, using lower layer interfaces, as well as with upper layer entities.

**Figure 2** IEEE 802.21 architecture

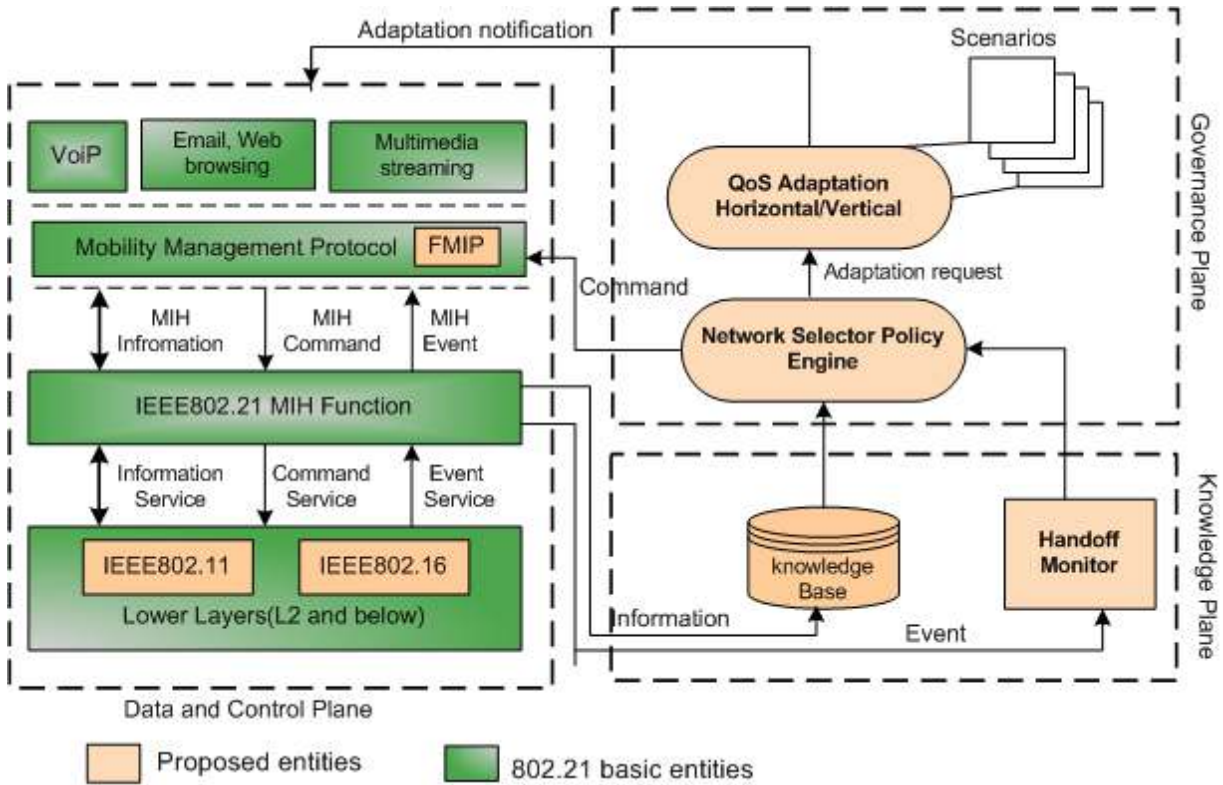


- MIES: The event service is used to facilitate handover detection. Events inform the condition of the present network and transmission behaviour of the L2 data links, such as MAC, radio resource management, etc. The defined events include pre-trigger (L2 handoff imminent), link available, link up, link parameter change, link going up, link down, link going down, etc.
- MICS: The higher layers use the MICS primitive to control the functions of the lower layers. MICS commands are used to gather information about the status of connected links, as well as to execute higher layer mobility and connectivity decisions to the lower layers. MIH command can both be local and remote. These include commands from the upper layers to the MIH and from the MIH to the lower layers.
- MIIS: As a mobile is about to move out of the current network, it needs to discover the available neighbouring networks and communicate with the elements within these networks so as to optimise the handover. MIIS provides a framework and corresponding mechanisms by which an MIHF entity can discover and obtain network information within a geographic area. MIIS primarily provides a set of information elements, the information structure and its representation by query/response type mechanism. The information service provides access to both static information as well as dynamic information.

## 4 Proposed interworking framework

The proposed framework of the interworking between WLAN and WMAN is based on IEEE 802.21 (2006) standard, IEEE 802.16e (2006) and IEEE 802.11e (2003). However, the IEEE 802.21 does not specify how to achieve these services, for example, it does not specify rules or policies for link selection nor determine whether the handoff has to be mobile node (MN) or network initiated. Moreover, the mechanism by which it maintains service continuity as well as QoS adaptation is not specified either (Caccace and Vollero, 2006). Despite IEEE 802.21 (2006) being designed to provide generic link intelligence independent of radio technologies, we choose rather to integrate both WLAN and WMAN as a case study in the current work, and then we will extend our work to the different radio technologies such as 3GPP and the other 802 network family. To achieve the functionalities described earlier, we added further functional elements to the initial IEEE 802.21 (2006) framework depicted in Figure 3, and described as follows:

**Figure 3** IEEE 802.21 proposed framework



### 4.1 Network selector policy engine (NSPE)

The core functionality of the whole architecture resides in NSPE where the decision of handoff is made. We assume that the handoff is terminal-controlled, therefore the MN should be provided with all the necessary information for making the decision. Such information is provided by the MIIS and stored in a knowledge base. Note that the knowledge base contains two types of information: local and global. The local information concerns locally available information from different layers in the local node's network stack such as: battery status, load, signal to noise ratio transmit power, bit error rate, velocity, etc. While global information includes a general overview of the different networks providing coverage within an area such as list of available networks



and their associated operators, roaming agreements between different operators, cost of connecting to the network and network security and quality of service capabilities, etc. In addition, NSPE receives information related to the current link status sent by the handoff monitor. Upon receiving the above information and according to some policies predefined in NSPE, the decision of hand is made. Consequently, NSPE will send an adaptation request to the QoS adaptation, by which applications can adjust their quality of service in order to cope with the QoS provisioned in the visited network. Afterwards, it will send a command to the mobility manager to execute mobility in layer 3. We choose to implement fast mobile IP as a mobility protocol. This is because FMIP aims to eliminate the factor of delay introduced by the address auto-configuration procedure. It achieves this by informing the MN of the new access router's advertised prefix, thus the MN is already configured with the new address at the time it attaches to the new link. This would reduce packet loss by providing fast IP connectivity as soon as the new link is established. It is considerable to note that the knowledge base and handoff monitor represent the knowledge plane. The knowledge plane can be a simple database with local and global view related information, or as a database with intelligence, which manipulate its information. We consider the database with intelligence; this would mean that we have a certain monitor that checks the values of thresholds of all information and then initiate triggers to the NSPE. While NSPE represents the governance plane because all the policies concerning a handoff decision reside on it, and it is up to this plane to decide and choose the best algorithm of decision as well as the algorithm of QoS adaptation according to the current situation of the system.

## 4.2 Handoff monitor

Handoff monitor (HM) detects the quality of current link and sends its status to NSPE. In order to receive triggers from the MIHF, HM should subscribe to receive certain event triggers. The communication by triggers in IEEE 802.21 (2006) is obtained through SAP. SAPs are used to enable communication between MIHF and other layers. In the present standard, there is one technology independent MIH\_SAP which allows the communication between the MIHF and the upper layers, namely, IP, transport and application. However, the communication between low layers (medium access control and physical layer) and the MIHF should be medium dependent. Therefore, we introduce two dependent technologies SAP: WLAN\_SAP and WMAN\_SAP. HM would rather subscribe to receive predictive triggers. This would help to make a decision to handoff in an IP layer before it occurs in link layer. These triggers are described as the following:

- WLAN\_LINK\_UP: is an indication that layer 3 can now send packets over the link. This means that a WLAN station not only has been associated with an AP, but also the four-way handshake has been completed.
- WLAN\_LINK\_DOWN: is an indication that layer 3 cannot send any more packets over the link.
- WLAN\_LINK\_GOING\_DOWN: is a predictive SAP which implies that a LINK\_DOWN is imminent within a certain time interval.
- WLAN\_INTERFACE\_ON: is an indication that WLAN interface power is on.
- WLAN\_INTERFACE\_OFF: is an indication that WLAN interface power is off.



- WMAN\_LINK\_UP: is an indication that layer 3 can now send packets over the link. This means that a WMAN station has completed network initialisation with the BS.
- WMAN\_LINK\_DOWN: is an indication that layer 3 cannot send any more packets over the link.
- WMAN\_LINK\_GOING\_DOWN: is a predictive SAP which implies that a LINK\_DOWN is imminent within a certain time interval.
- WMAN\_INTERFACE\_ON: is an indication that WMAN interface power is on
- WMAN\_INTERFACE\_OFF: is an indication that WMAN interface power is off.

### 4.3 *QoS adaptation (horizontal/vertical)*

This entity performs an adaptation mechanism as soon as it receives an adaptation request from NSPE. Therefore, it first verifies if the handoff is horizontal i.e. WMAN to WMAN and WLAN to WLAN or vertical (WLAN to WMAN and vice versa) (Ali Yahya et al., 2007). Thus, if it is horizontal, then the same negotiated context in the home network will be transferred to the visited network as both networks have the same characteristics. However, if the handoff is vertical, mapping between different QoS classes should occur. More details will be discussed in Section 6.

### 4.4 *Knowledge base and policies*

In the knowledge base reside all the information elements (IEs) supported by MIIS. These IEs can be obtained either by doing request/response from other MIIS resident in the same network or in the exterior or from the broadcast messages sent by the neighbour networks. The aim of IE is primarily to be used by NSPE in order to make an effective handoff decision. Since the MIIS has the capability to obtain information about lower and higher layer; we therefore choose to include the following IEs and policies related to WLAN and WMAN networks:

- 1 Signal strength. The most trivial criterion to decide handoff is the strength of the signal, i.e., if the signal strength falls below a predetermined threshold, then handoff will occur (McNair and Zhu, 2004). However, this is not true when handing off from WLAN to WMAN and vice versa as each system has different value of thresholds, thus this parameter cannot be the only parameter to determine the handoff between these two systems. The deterioration of signal strength will trigger an event service to the HM in order that the latter take this change into account.
- 2 Type of physical layer. It is expected that a MN hands off to the network that supports higher data rate. However, in scenarios related to horizontal handoff especially in WLAN, the MN should handoff to the WLAN network that supports 54 Mbps rather than 11 Mbps. This signifies that in scenarios that contain a WMAN cell and several WLAN hotspots, a MN should handoff to higher data rate WLAN rather than WMAN.
- 3 Available bandwidth. Determining the physical layer when handing off to WLAN hotspot is not sufficient if it is not preceded by detecting the value of NAV in the

visited hotspot. By means of NAV, the available bandwidth can be calculated in each type of WLAN (Nie et al., 2005).

- 4 Economical cost. In the service provider billing policies, it is expected that the cost of connecting to WLAN hotspot be less expensive than its WMAN counterpart, because WLAN is operating in unlicensed frequency band while WMAN operates in licensed frequency band. This rate of using frequency spectrum would be included in the total rate for connecting to WMAN. Thus, in the scenario where a MN in a WLAN hotspot intends to handoff, and there is another hotspot as well as WMAN cell, MN should handoff to WLAN rather than WMAN.
- 5 MAC parameters. Medium access method employed by each network influences the type of application intending to handoff. For example, it is well known that WLAN does not support well VoIP because carrier sense multiple access collision avoidance (CSMA/CA) performs poorly especially under increased load as it is based on probabilistic method for accessing the medium (Paschos et al., 2006). Consequently, it would be better to handoff to WMAN as it provides periodic grant size for such application. In this way, the QoS of the application is guaranteed even when the load of the network is increased.
- 6 QoS application. Handoff should occur as a reaction to QoS violation of an ongoing application. This is because either the load of the current network is increased or the bit error rate (BER) is increased as a result of bad channel quality. Thus, the need to investigate new robust QoS provisioning and adaptation mechanism to satisfy the QoS requirements within both networks emerges (Chen and Shu, 2005).

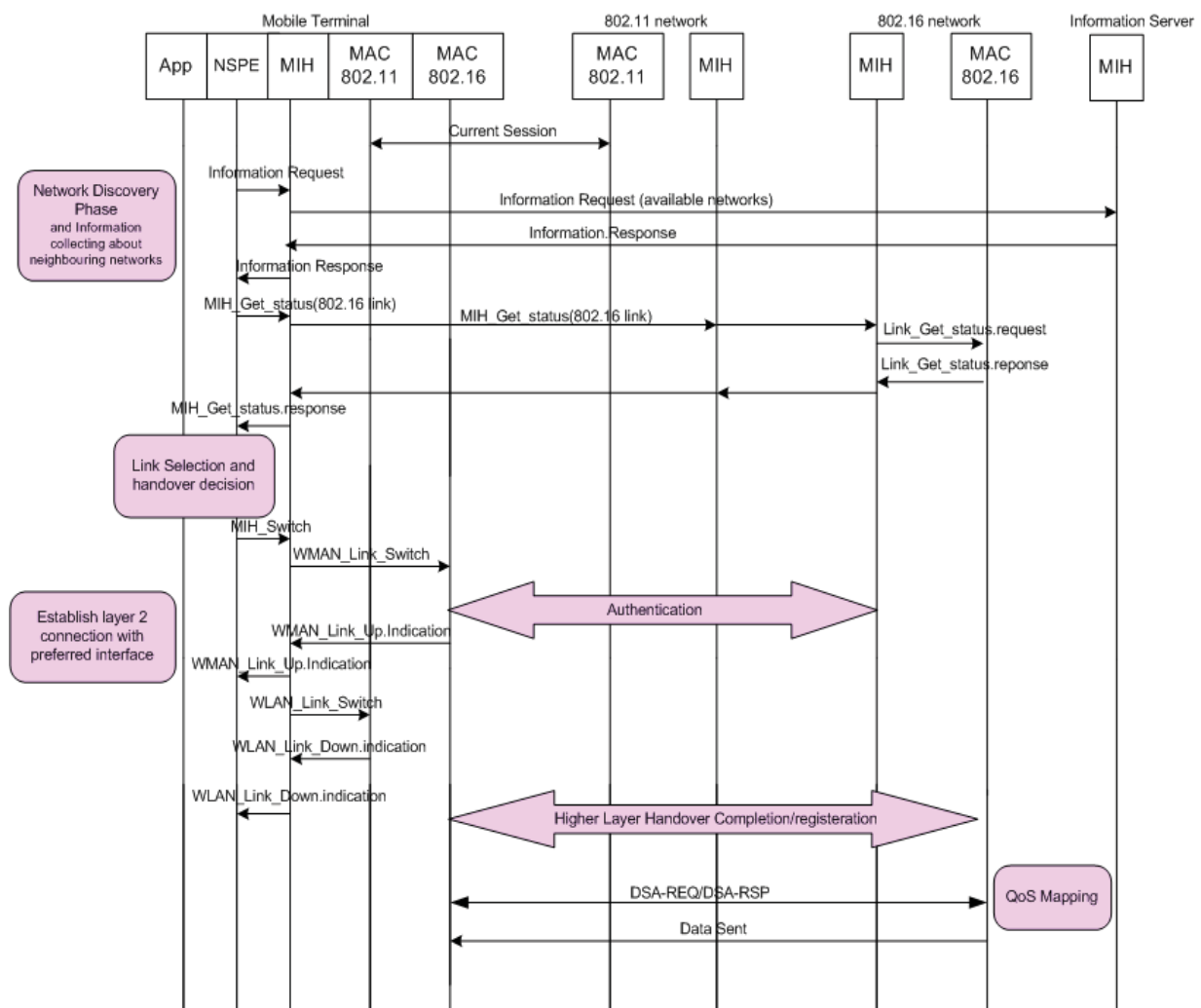
## 5 Mobility management

The proposed framework assists the mobility management in order to make handoff process as optimised as possible. Thus, an example of handoff scenario between WLAN and WMAN is depicted in Figure 4. A MN has two types of interfaces (WiFi and WiMax). Initially, the MN is using WLAN network as its primary interface to communicate a multimedia session with a correspondent host. Within the mobile's neighbourhood, there are many WMAN networks. The NSPE queries information from MIH which in turn queries an information server residing in the network to learn the types of networks that are nearby. This is done by sending a MIH queries about link information which specifies the status of WiMax network. Upon receiving a response, the NSPE initiates the handoff to the detected WiMax using an appropriate policy. Another possibility would be that the NSPE will decide to handoff because the current received signal strength is below a predefined threshold. The MN begins scanning its frequency list to identify an operating channel for WMAN by receiving broadcast messages DL-MAP and UL-MAP from nearby WMAN base stations. We assume that this can happen concurrently with the ongoing sessions because although the MN has one transceiver available for sending and receiving data in WLAN, it uses the other transceiver for periodically decoding signals on other frequency channels for intersystem handoff purposes.

After deciding on which channel to attempt communication, the MN tries to synchronise to the downlink transmission by detecting the periodic frame preambles.

Afterward, it looks for both downlink channel descriptor (DCD) and uplink channel descriptor (UCD) messages which are periodically broadcasted. These messages contain burst profile which determines physical layer characteristics. Once the WMAN link is up, the MN performs a series of authentication requests. At this time MICS helps switch the interface to the active interface of WMAN network. After the MN has decided the new interface to be its primary interface, it goes ahead with other configuration process such as obtaining the IP address from the new network. During this time the MN is still communicating through WiFi interface. After this point, the MN will establish a connection by setting up a service flow with BS. Then the MN will send DSA-REQ which contains service flow traffic characteristic or QoS requirements to the BS. The latter will map QoS classes of MN to the service flows of WMAN. For seamless interworking, it is evident that the WMAN service flow traffic characteristics need to be set appropriate to the WLAN TSPEC. The BS will send DSA-RSP which will be acknowledged by the MN with DSA-ACK message which completes the handoff process. This mobile sends a binding update to the corresponding host after the new interface is configured with the new IP address. At this time, traffic to the mobile flows through the new interface and the handover is completed.

**Figure 4** WLAN-WMAN handoff sequence diagram (see online version for colours)



## 6 Quality of service management

In this section, we address several issues in relation to QoS when handing over between WLAN and WMAN technologies. We will investigate the difference in QoS support provided by those technologies and the difference in QoS classes and propose QoS mapping mechanisms.

### 6.1 Channel access method

QoS consistency is one of the most important issues for a seamless integration of both systems. We assume that a mobile station has several ongoing sessions with each session having different QoS requirements. An important aspect to consider is that the basic support for QoS differs significantly between WLAN and WMAN due to their different physical and MAC layer design. Therefore, it is likely that different sessions in both systems will experience different QoS levels. Normally, WLAN is using CSMA/CA, which performs poorly under increased load as it is based on probabilistic method for accessing the channel (McNair and Zhu, 2004). In contrast, the IEEE 802.16 MAC uses a scheduling algorithm for which the MS need compete once (for initial entry into the network). After that it is allocated an access slot by the base station. The time slot can enlarge and contract, but remains assigned to the subscriber station which means that other subscribers cannot use it. In addition to being stable under overload and over-subscription (unlike IEEE 802.11), the IEEE 802.16 scheduling algorithm can also be more bandwidth efficient. The scheduling algorithm also allows the base station to control QoS parameters by balancing the time-slot assignments among the application needs of the subscriber stations (IEEE 802.16e, 2006).

### 6.2 QoS support and classes

While IEEE 802.11 standard supports only best effort service, IEEE 802.11e (2003) introduced basic QoS support by defining four different access categories (ACs), namely AC\_VO (voice) with highest priority, AC\_VI (video), AC\_BE (best effort), and AC\_BK (background) with lowest priority. EDCF (enhanced distribution coordination function) is the enhancement of the standard IEEE 802.11 DCF (distributed coordination function), and it provides eight different user priorities. Additionally, it defines four access categories for traffic that can be mapped to user priorities as shown below.

**Table 1** IEEE 802.11e access category and user priority mapping

<i>User priority</i>	<i>AC</i>	<i>Informative</i>
1	AC_BK	Background
2	AC_BK	Background
0	AC_BE	Best effort
3	AC_BE	Best effort
4	AC_VI	Video
5	AC_VI	Video
6	AC_VO	Voice
7	AC_VO	Voice

Stations supporting EDCF maintain four queues and packets with several user priorities can be mapped to one queue. Each access category can be considered as a separated virtual station as it has its own values for backoff timer, arbitration interframe space time (AIFS) and contention windows (CW). EDCF maintains service differentiation by assigning each AC with different values for AIFS and CW. ACs with higher priority will have smaller AIFS as well as smaller values of CW; this will give higher priority ACs the possibility to access the channel without additional delay.

In contrast, in IEEE 802.16 based WMAN networks, packets traversing the MAC interface are associated to a service flow as identified by a connection identifier (CID), where a connection is a unidirectional mapping between the BS and the MS with the purpose of transporting service flow (IEEE 802.16e, 2006). A service flow is defined as a MAC transport service that provides unidirectional transport of packets either to uplink packets transmitted by the MS or to downlink packets transmitted by the BS. Each service flow is identified by a service flow identifier (SFID) and is defined by a particular set of QoS parameters (latency, jitter, data rate). The association between CID and SFID is provided by a classifier both in the MSs and in the BS. Moreover, each service flow will be assigned resources between MS and BS that will last for the duration of the connection. These mechanisms will allow the basic support of QoS in IEEE 802.16. The scheduling service is associated to each connection at connection setup time and as a consequence, associated to a service flow. The scheduling services defined by IEEE 802.16 are the following:

- UGS (unsolicited grant service) is designed to support real-time service flows that generate fixed size data packets on a periodic basis, such as VoIP. This service offers fixed size unsolicited data grants on a periodic basis. This eliminates the latency and overhead of requiring the MS to send requests for transmission opportunities, and assures that grants are available to meet the flow's real-time needs.
- rtPS (real time polling service) is designed to support real-time service flows that generate variable size data packets on a periodic basis, such as video. The service offers real-time, periodic, unicast request opportunities, which meet the flows real-time needs and allow the MS to specify the size of the desired grant.
- ertPS (extended rtPS) combines the efficiency of both UGS and rtPS. The BS shall provide unicast grants in an unsolicited manner like in UGS, thus saving the latency of a bandwidth request. However, whereas UGS allocations are fixed in size, ertPS allocations are dynamic.
- nrtPS (non-real time polling service) is designed to support non real-time service flows that require variable size data grants on a regular basis, such as high bandwidth FTP. The service offers unicast polls on a periodic basis, but using more space intervals than rtPS. This ensures that the flow receives request opportunities even during network congestion.
- BE (best effort) is designed to provide efficient service to best effort traffic. In this case, neither throughput nor delay guarantees are provided. The MS sends requests for bandwidth in either random access slots using contention mechanism or dedicated transmission opportunities. As the availability of dedicated opportunities depends on the network load, the MS cannot rely on their presence.

### 6.3 Mapping

From the difference in the access methods and the QoS classes supported, it becomes clear that a vertical handoff from WLAN to WMAN needs to involve a QoS mapping procedure in both the MSs and BS. Therefore, we have to define for each WLAN QoS class or AC, which WMAN service flow type we assign and additionally we have to provide a mapping from TSPEC (traffic specification) negotiated in WLAN in Action.ADDT request to DSA-REQ negotiated in WMAN. As an example, we can obtain the following statistic mapping between different classes of service for both systems as shown in Table 2. We adopt this mapping table after some results of simulations. Classes are mapped according to the key QoS requirement for each service type. For example, for voice or video conferencing, packets based on e.g. G.729 coder for IP telephony of H.263 or H.264 for video, the end-to-end delay is the most important QoS criterion as the service becomes not really useful if the delay exceeds e.g. 150 ms due to interactivity constraints. Therefore, we choose to map AC\_VO to UGS service flow. As for video, the delay is not that critical as for voice and clever video coder can cope with variable delay to some extent (e.g. using adaptive play out technology), we chose for the real-time video conferencing the mapping between AC\_VI to rtPS. For data intensive applications like FTP with high volume traffic, we chose throughput parameter as the most important metric. Thus, we mapped AC\_BE to nrtPS if the throughput requirement is high. Finally, we map medium and low load elastic traffic such as FTP, web browsing and e-mail from AC\_BE and AC\_BK to IEEE 802.16 type BE service flow.

**Table 2** QoS mapping between IEEE 802.11e and IEEE 802.16e service flows

<i>Application</i>	<i>IEEE 802.11e</i>	<i>IEEE 802.16e</i>
Voice	AC_VO	UGS, ertPS
Video	AC_VI	rtPS
FTP (high load)	AC_BE ( high load)	nrtPS
FTP (medium load), web browsing	AC_BE (medium load)	BE
FTP (low load), e-mail	AC_BK (low load)	BE

## 7 Simulation

In this section, we are interested in QoS provisioning for different type of sessions that have been established in the WLAN and are being handed over to WMAN. We investigate the capability of WMAN to guarantee the QoS requirements for these applications (voice, video, FTP). We based on three scenarios for simulation. In each scenario, we have 31 Mbps in the downlink, while we chose 640 kbps for the voice in uplink, 10.4 Mbps for video and FTP, respectively. This is due to the little amount of bandwidth demanded for the voice in comparison with video and FTP that are greedy bandwidth consuming. The WLAN stations that handoff to WMAN network are considered to be statistically identical. All WLAN stations, including the AP, support IEEE 802.11e MAC layer and the physical layer is specified by IEEE 802.11g. For the interworking scenario discussed above, our main goal is to evaluate how many WLAN roamers the WMAN network can be supported given that the sessions of all WLAN

stations admitted to the WMAN must experience at least the same QoS level experienced in WLAN network before initiating handoff.

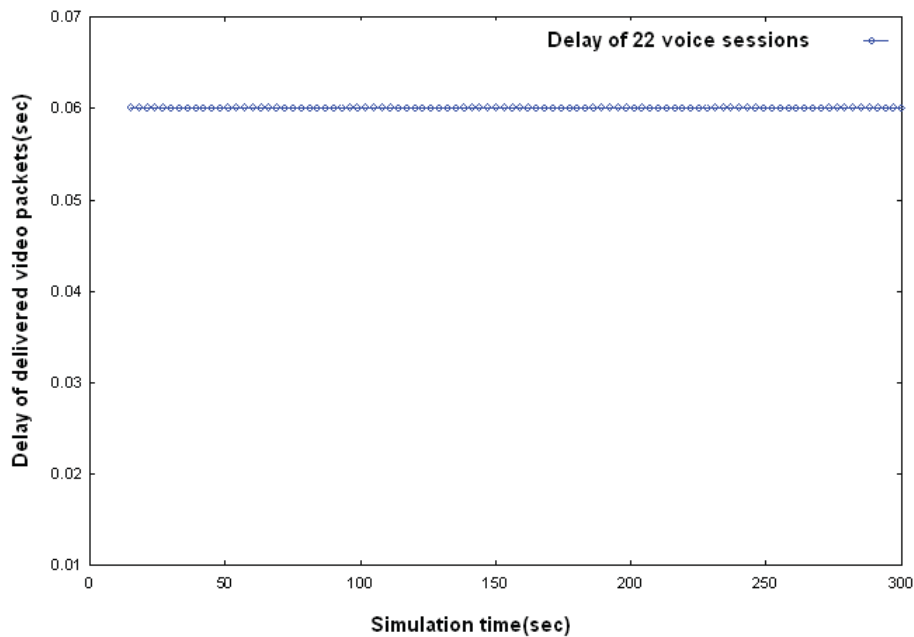
We used OPNET to simulate and calculate the QoS requirements for each application and we utilised Traffic Analyzer in order to extract the values of TSPEC each application in WLAN network before the WLAN station handoffs to WMAN network as follows:

**Table 3** IEEE 802.11e traffic parameters

<i>Traffic class</i>	<i>Data rate</i>	<i>Delay</i>
AC_VO	30.4 kbps	0.06 sec
AC_VI	1.38 Mbps	0.08 sec
AC_BE	480 kbps	—

We first investigate if the WMAN will guarantee the QoS requirements for voice traffic. As described above, UGS will be the most suitable class mapping for AC\_VO. Hence, in our simulation, each handoff of voice session from WLAN triggers the establishment of a new 802.16 service flow. Once the voice session was initiated after the handoff, it will not suffer an obvious degradation of its quality of service parameters in terms of delay although it is smaller in comparison with its correspondence in WLAN. Our aim is to analyse how many voice sessions can be supported by the WMAN and still satisfy the required maximum latency. During the simulation runs, we noted that the WMAN can support 24 voice sessions without any packet drop. Figure 5 shows the delay of all the voice station accepted in WMAN without the application suffering from the augmentation of the delay. This means here that the session continuity will be seamless. The reason behind this continuity is due to the UGS scheduling, because once the AC\_VO is mapped to UGS, this will give it a priority of granting it a fix grant size periodically, hence, the UGS has a low bounded constant delay as the scheduler issues grants every nominal grant interval of 0.005 sec which specifies how often grants will be issued to UGS and their size by grant size of 1,300 bytes.

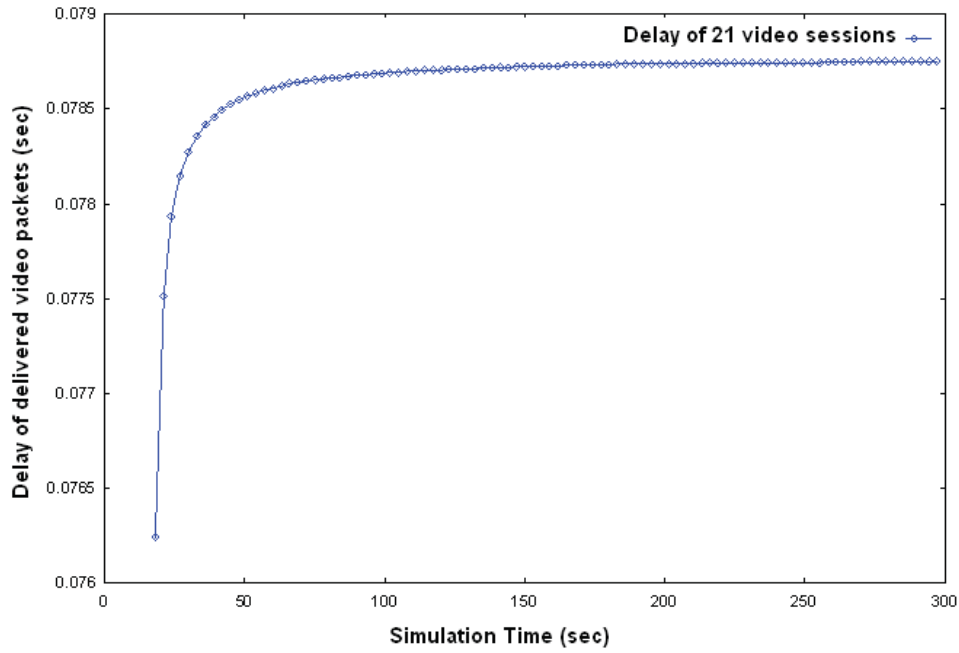
**Figure 5** Maximum delay of WMAN when entering 22-voice traffic





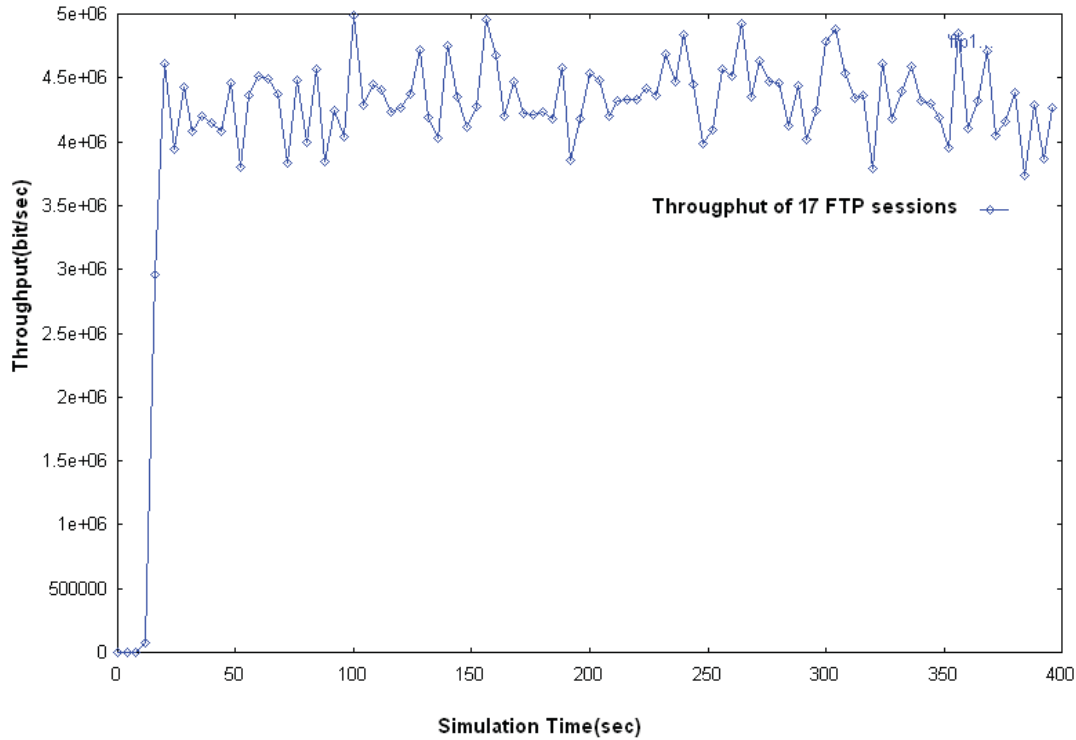
Now, we will study the video case which will experience a little increase of delay due to the packet scheduling algorithm. As the rtPS uses polling scheduling, this may be a normal behaviour in WMAN. Whenever an rtPS service flow intends to send traffic, it will first wait for the polling request message sent by the BS. Whenever it receives this message, then it will send a bandwidth request to the BS, upon receiving grant size from BS, it will start sending its traffic. This will lead to a delay overhead as the station should wait until receiving polling request message. Our scheduler grants rtPS service flow every nominal polling interval of 0.5 sec. Figure 6 shows that the WMAN can support only 21 video sessions as adding other session will lead to the increasing delay of the whole network and dropping video packet.

**Figure 6** Maximum delay of WMAN when handing over 21 video flows



Now, let us consider the FTP application and we use the throughput as the most important factor for measuring the efficiency of a file transfer (downloading or uploading). Figure 7 shows the throughput over time for the FTP for the WLAN station who tries to download a file size of 50,000 bytes. We remark that the throughput after the handoff is higher than its correspondence in WLAN. This is due to polling scheduling for the nrtPS in WMAN in which the BS assigns it a periodic polling (0.5 sec). In our simulation, this will guarantee that the nrtPS request opportunity even during network congestions. While in WLAN, the FTP is considered as best effort, as it should contend for the medium with the largest CW and AFIS values compared with other ACs. Also, the throughput of FTP in WLAN will decrease because of the increased MAC layer contention while in WMAN it is contention free.

**Figure 7** Throughput of 17 FTP sessions (see online version for colours)



## 8 Conclusions

Even the QoS discrepancies between these two networks raise challenges as we remarked above, there are still other challenges that should be addressed to enable seamless interworking of WLAN and WMAN networks. We introduced in this paper the first experience to integrate WLAN IEEE 802.11e based and WMAN IEEE 802.16e. The continuity of service is examined for different number of ongoing sessions with different applications. The integration of both networks is based on a framework to enable an autonomic interworking of different technologies based on IEEE 802.21. We first analysed the basic services provided by IEEE 802.21, after that we enhanced them by adding supplementary functional entities, by which we provide some autonomic networking principles. By introducing these entities, we intend to give a generic solution for all types of networks, while focusing on WLAN and WMAN as a case study. The additional entities are aimed primarily to provide QoS adaptation for different applications when handing off forms one system to another. In addition, they provide the necessary information for MN to make an intelligent handoff decision based on predetermined policies in the system. Thus, the autonomic system will be enabled to adjust to changing needs and conditions while obeying some policies. In our study of various interworking scenarios, where WLAN stations with different ongoing sessions handed off to WMAN, we mainly quantified the maximum number of WLAN stations that can be admitted to WMAN, subject to maintaining the same level of QoS in WMAN and respecting the WMAN bandwidth reservation policies. We remarked that the scheduling in WMAN is playing a great role in the continuity of service in terms of guaranteeing the QoS for each application. In future work we will investigate the handoff from WMAN to WLAN and analyse whether WLAN can guarantee the QoS requirements for different application sessions initiated in WMAN. Also, we will study

the impact of different scheduling techniques on heterogeneous traffic, making our simulation more applicable to real-life scenarios.

## References

- Ali Yahiya, T., Sethom, K. and Pujolle, G. (2007) 'Seamless continuity of service across WLAN and WMAN networks: challenges and performance evaluation', *EEE/IFIP International Workshop on Broadband Convergence Networks*, pp.1–12.
- Caccace, F. and Vollero, L. (2006) 'Managing mobility and adaptation in upcoming 802.21-enabled device', *International Conference on Mobile Computing and Networking*, pp.1–10.
- Chen, W. and Shu, Y. (2005) 'Active application oriented vertical handoff in next-generation wireless networks', *IEEE Wireless Communications and Networking Conference*, Vol. 3, pp.1383–1388.
- Fodo, G., Eriksson, A. and Tuoriniemi, A. (2003) 'Providing quality of service in always best connected networks', *IEEE Communication Magazine*, Vol. 41, pp.154–163.
- IEEE P802.21/D02.00 (2006) 'IEEE draft standard for local and metropolitan area networks: media independent handover services', *IEEE Standard*.
- IEEE Std. 802.11e (2003) 'IEEE draft standard medium access control (MAC) quality of service (QoS) enhancements', *IEEE Standard*.
- IEEE Std. 802.16e (2006) 'IEEE standard for local and metropolitan area networks-part 16: air interface for fixed and mobile broadband wireless access systems', *IEEE Standard*.
- International Business Machines (2003) *An Architectural Blueprint for Autonomic Computing*, IBM Corporation.
- Jennings, N.R., Sycara, K. and Wooldridge, M. (1998) 'A roadmap of agent research and development, autonomous agents and multi-agent systems', *Journal on Autonomous Agents and Multi-Agent Systems*, Vol. 1, pp.7–38.
- McNair, J. and Zhu, F. (2004) 'Vertical handoffs in fourth-generation multinet network environments', *IEEE Wireless Communications Magazine*, Vol. 11, pp.8–15.
- Nie, J., Wen, J., Dong, Q. and Zheng, Z. (2005) 'A seamless handoff in IEEE 802.16a and IEEE 802.11n hybrid networks', *International Conference on Communications, Circuits and Systems*, Vol. 1, pp.383–387.
- Paschos, G.S., Papapanagiotou, I., Kotsopoulos, S.A. and Karagiannidis, G.K. (2006) 'A new MAC protocol with pseudo-TDMA behaviour for supporting quality of service in 802.11 wireless LANs', *EURASIP Journal on Wireless Communications and Networking*, Vol. 6, pp.76–84.
- Pujolle, G. (2006) 'An autonomic-oriented architecture for the internet of things', *IEEE John Vincent Atanasoff 2006 International Symposium on Modern Computing*, pp.163–168.