An IMS-based network architecture for WiMAX-UMTS and WiMAX-WLAN interworking

Nikolaos Psimogiannos a, Aggeliki Sgora a, Dimitrios D. Vergados a,b

aDepartment of Information and Communication Systems Engineering, University of the Aegean, GR-832 00 Karlovassi, Samos, Greece
bDepartment of Informatics, University of Piraeus, 80, Karaoli and Dimitriou Str, GR-185 34 Piraeus, Greece

A R T I C L E   I N F O

Article history:
Received 21 October 2009
Received in revised form 10 February 2010
Accepted 16 February 2010
Available online xxxx

Keywords:
NGN
IMS
Interworking
WiMAX
UMTS

A B S T R A C T

The IP Multimedia Subsystem (IMS) seems to be the technology that will prevail in Next Generation Networks (NGNs), since the interworking environment and the service flexibility that this technology offers to the currently deployed wireless broadband technologies makes it appealing to users, service developers and network operators. In this paper we propose a heterogeneous network model based on the IMS that integrates the Worldwide Interoperability for Microwave Access (WiMAX), Universal Mobile Telecommunications System (UMTS) and Wireless Local Area Network (WLAN) technologies and provides guaranteed QoS. We present the complete signalling flow concerning the authorization, registration, session set up and vertical handoff processes, as well as, an analytic model for cost analysis of the proposed architecture.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

Nowadays, several different wireless and wired network technologies exist that try to satisfy the different user needs and requirements. In the near future, network operators will try to combine various technologies in order to build large heterogeneous networks in order to provide the users with better services. However, the design and the development of such networks requires the consideration of different issues, such as the session control, the authorization, the authentication, the Quality of Service (QoS), the charging, the users’ mobility, etc.

The IP Multimedia Subsystem (IMS) [1] comes as a promising solution to the above issues, since it offers the needed interworking environment for the integration of, in principle, any broadband wireless access technology, whilst complemented with the necessary gateways it provides access to legacy telecommunications switching systems. Also, since the IMS uses the Session Initiation Protocol (SIP) [2] for session establishment, management, and transformation, its offerings include functions, such as authentication, addressing, routing capability negotiation, service invocation, provisioning, charging, session establishment, etc. However, since the IMS networks are still in an ongoing activity the industry and the research community constantly try to face open issues and extend IMS beyond 3G, by proposing interworking architectures that aim on seamless service provisioning.

In this paper, we propose an interworking model that integrates a Worldwide Interoperability for Microwave Access (WiMAX) network, a Universal Mobile Telecommunications System (UMTS) network and a Wireless Local Area Network (WLAN) in an IMS compatible architecture. More specifically, the proposed architecture incorporates a UMTS Core network (CNet), a WiMAX network and a WLAN network interconnected with the UMTS Core through specific functional entities and an IMS in charge of sessions’ control. Thus, users can access the UMTS Circuit-Switched (CS) based services through the WiMAX and WLAN networks, since they are authenticated in the Authentication, Authorization, and Accounting (AAA) Server and registered in the IMS core.

The rest of the paper is organised as follows. Section 2 presents an overview of the IMS including key features, architecture particularities and supported signalling protocols, while Section 3 overviews related work concerning the IMS deployment. Our proposed network architecture is presented and analysed in Section 4. An analytical model for cost analysis of the proposed architecture, as well as, numerical results that are used to evaluate the performance of our proposed architecture are presented in Section 5. Finally, Section 6 concludes the work and discusses some future research directions.

2. The IP Multimedia Subsystem – overview and key features

The IMS is a framework that was first designed and standardized by the 3GPP (3rd Generation Partnership Project) [1,3] with...
main goal the provision of the Internet Protocol (IP) [4] based telephony and multimedia services over 3G networks. It has been also extended by the 3GPP, 3GPP2 and TISPAN towards integrating different broadband wireless technologies, such as WLAN, CDMA2000, UMTS, WiMAX and also fixed line networks. The IMS provides horizontally integrated services and access independence supported by functions such as authentication, addressing, routing capability negotiation, service invocation, provisioning, charging, session establishment, etc.

As depicted in Fig. 1, the IMS is a 3-layer architecture that consists of the Transport Layer, which includes all the entities for the supported access networks; the Control Layer where the core IMS network resides; whereas at the top exists the Service Layer which includes the application servers hosting the IMS services. It should be noted that the 3GPP standardises functions and not physical components; thus, IMS deployments can combine or split these functions, referred to also as functional entities, into different physical network components.

The 3GPP IMS Reference Architecture defines various functional entities and the interfaces among them. The key entities of the IMS core include the user database(s) namely the Home Subscriber Servers HSSs and the Subscriber Location Functions (SLFs); the SIP servers known as Call-Session Control Functions (CSCFs); the Applications Servers (ASs); the Media Resource Functions (MRFs), the Breakout Gateway Control Functions (BGCFs) and the Public Switched Telephone Network (PSTN) gateways.

The HSS is the master database for a domain, where the profile of a given user is stored. A Home Network may contain one or several HSSs, depending on the number of mobile subscribers, on the capacity of the physical component where the HSS resides and on the overall structure and design of the network. The presence of the Subscription Location Function (SLF) is dictated by the existence of more than one HSS in a network and its main role is to respond to nodes’ queries on the HSS handling a particular user.

The CSCF is an essential node in the IMS that processes the SIP signalling. There are three types of CSCFs, referred to also as SIP Servers: the Proxy-CSCF (P-CSCF), the Interrogating-CSCF (I-SCSF) and the Serving-CSCF (S-CSCF) servers.

The P-CSCF server is the first point of contact for a User Equipment (UE) entering the IMS subsystem. Its address is discovered by the UE and its goals are to perform the registration of the UE, to compress/decompress SIP messages, to generate charging records and to enforce policies through the Policy Decision Function (PDF), whilst it can be located either in the Home Network or in the Visited one.

The I-CSCF server is the SIP proxy that resides at the administrative functional domain of the IMS. It queries the HSS in order to determine the location of a UE and routes UE’s messages to its assigned S-CSCF. The I-CSCF is usually located at the Home Network whilst towards enhancing the network’s redundancy and scalability a number of I-CSCFs can be deployed in the same network.

The S-CSCF server is the entity that controls the sessions and maintains the correlation between the UE’s SIP addresses. An S-CSCF is assigned to each UE during its registration to the IMS, however each S-CSCF may serve more than one UEs, depending on the capacity of the physical component the S-CSCF resides. The S-CSCF is responsible to forward the SIP messages to the appropriate AS and to enforce the service policies of the network operator.

In addition to the above IMS core entities, additional ones have been standardized towards completing the IMS interworking environment. The Breakout Gateway Control Function (BGCF) provides routing functionality based on telephone numbers; thus it serves sessions addressed to circuit-switched network users. Alongside with the Media Gateway Controller Function (MGCF) and the IMS-Media Gateway (IMS-MG) they provide connectivity between the IMS and circuit-switched networks.

As clearly presented above, the communication between the various IMS entities is achieved through standardized interfaces and protocols; thus making the IMS easily expandable. With reference to the 3GPP IMS Reference Architecture (Fig. 2), Table 1 summarises the IMS interfaces and protocols.
2.1. IMS signalling

The necessity of the IMS to be compatible with the majority of the existing network technologies imposed the support and usage of signalling protocols already standardized by the Internet Engineering Task Force (IETF) and the International Telecommunication Union-Telecommunications (ITU-T).

The crucial technology for supporting multimedia session establishment and controlling information negotiation in the IMS is the SIP. Specified by the IETF, SIP supports a wide variety of applications, such as video conferencing, streaming multimedia distribution, instant messaging and presence information. The protocol supports communication between two users (unicast) or between a number of users (multicast), as well as, communication with more than one media streams. A session can be modified in terms of changing addresses or port numbers, adding or deleting media streams or inviting more users to the session. The latest version of the protocol is specified in RFC 3261 [2].

Another protocol widely used in the IMS is DIAMETER, specified in RFC 3588 [6] that is used for the AAA procedure and for the exchange of some information between IMS entities. DIAMETER is an extension of RADIUS specified in RFC 2865 [7]. The main methods of security provisioning in DIAMETER are IPSec as specified in RFC 2401 [8] and Transport Layer Security (TLS) specified in RFC 2246 [9].

There are also several protocols that are currently used or could possibly be used in the IMS, mainly in the application-layer, protocols used in the IMS. These include:

- The Common Open Policy Service (COPS) protocol specified in RFC 2748 [10] that incorporates a model for supporting policy control over QoS signalling protocols e.g. Resource ReSerVation Protocol (RSVP) and the transfer of policies between the Policy Decision Points and the Policy Enforcement Points.
- The H.248 protocol (ITU-T Recommendation H.248 [11]), also referred to as Media Gateway Control (MEGACO) protocol, that is used for controlling media gateways on IP and PSTN networks.
- The Real-time Transport Protocol (RTP) specified in RFC 3550 [12] that provides support for real-time media transportation.
- The RTP Control Protocol (RTCP) which is always being used along with the RTP, provides QoS information and statistics whilst supports the inter-media synchronization, and
- The Secure RTP (SRTP), specified in RFC 3711 [13], which provides message authentication and confidentiality to RTP/RTCP traffic.

In support of IMS’ end-to-end QoS offerings, various link-layer resource reservation protocols could be used including the PDP Context Activation, the DiffServ and the RSVP protocols.

---

Table 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>IMS entities</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cr</td>
<td>MRFC ↔ AS</td>
<td>HTTP over dedicated TCP/SCTP channels</td>
</tr>
<tr>
<td>Dx</td>
<td>AS ↔ SLF</td>
<td>Diameter</td>
</tr>
<tr>
<td>Gm</td>
<td>UE ↔ P-SCSF</td>
<td>SIP</td>
</tr>
<tr>
<td>I SC</td>
<td>S-SCSF, I-SCSF ↔ AS, S-SCSF ↔ MRB</td>
<td>Diameter</td>
</tr>
<tr>
<td>Mg</td>
<td>S-SCSF, I-SCSF ↔ MGCF</td>
<td>SIP</td>
</tr>
<tr>
<td>Mj</td>
<td>BGCF ↔ MGCF</td>
<td>SIP</td>
</tr>
<tr>
<td>Mm</td>
<td>I-SCSF, S-SCSF ↔ external IP networks</td>
<td>SIP</td>
</tr>
<tr>
<td>Mn</td>
<td>MGCF ↔ IM-MGW</td>
<td>H.248</td>
</tr>
<tr>
<td>Mp</td>
<td>MRFC ↔ MRFP</td>
<td>H.248</td>
</tr>
<tr>
<td>Mr</td>
<td>S-SCSF ↔ MRFC</td>
<td>SIP</td>
</tr>
<tr>
<td>Mw</td>
<td>P-SCSF, I-SCSF, S-SCSF</td>
<td>SIP</td>
</tr>
<tr>
<td>C, D, Gc,</td>
<td>HSS ↔ Legacy Mobile Signalling</td>
<td>MAP</td>
</tr>
<tr>
<td>Gr</td>
<td>Networks</td>
<td></td>
</tr>
<tr>
<td>Sr</td>
<td>MRFC ↔ AS</td>
<td>HTTP</td>
</tr>
<tr>
<td>Ut</td>
<td>UE ↔ AS</td>
<td>HTTP(s), XCAP</td>
</tr>
<tr>
<td>Ma</td>
<td>I-SCSF ↔ AS</td>
<td>SIP</td>
</tr>
</tbody>
</table>
3. IMS deployment–related work

Since the IMS networks are still in an ongoing activity, researchers and operators are trying to solve open issues and extend the IMS beyond 3G towards a seamless universal wireless Next Generation Network (NGN). The use of the IMS to connect different wireless Access Networks (ANs) including legacy networks would offer several advantages to the users and the operators. Standardisation bodies and researchers have been trying to find ways to achieve this and several interworking architectures have been proposed focusing on seamless service provisioning and service continuity during handoffs.

In principle, there are two main interworking methods between wireless ANs: loose coupling and tight coupling. In a loose coupling configuration, the changes to the existing access technologies remain at the bare minimum; thus it guarantees the independence in terms of deployment. The ANs utilise the 3GPP AAA server and the data streams do not go through the 3GPP core network, resulting in high handoff latency. Alternatively, the tight coupling configuration imposes significant modifications to the protocols, interfaces and the services of the access networks. Since in this configuration the data streams pass through the 3GPP core network; the handoff latency is reduced and furthermore seamless mobility is supported. Additional interconnection levels can be found in the current research literature representing different operational capabilities. Taking into account the six interconnection levels presented focusing on seamless service provisioning and service continuity bodies and researchers have been trying to find ways to offer several advantages to the users and the operators. Standardisation bodies and researchers have been trying to find ways to achieve this and several interworking architectures have been proposed focusing on seamless service provisioning and service continuity during handoffs.

Following these requirements several IMS-based interworking proposals may be found in the current literature [15–20].

Hasswa et al. [15] present a model that uses the IMS to achieve 3G–WLAN interworking. The proposed model takes advantage of the IMS’s application layer in order to avoid modifying the core components of the IMS and the WLAN. To achieve the interworking of the two networks specific new components are introduced: a WLAN application server deployed in the IMS’s application layer and a SIP server residing in the WLAN. The proposed architecture achieves to support all the interworking scenarios of the Table 2 except from the 6th scenario.

| Table 2 Interworking architectures’ coupling levels vs. 3GPP interworking levels. |
|-----------------|-----------------|-----------------|-----------------|
| 3GPP interworking levels (Sc.) | Coupling levela | Loose | Tight | Very-tight/integration |
| Sc. 1: Common billing and customer care | • | • | • |
| Sc. 2: Sc. 1 + 3G based access control and charging | • | • | • |
| Sc. 3: Sc. 2 + access to 3G PS services | • | • | • |
| Sc. 4: Sc. 3 + service continuity | • | • | • |
| Sc. 5: Sc. 4 + seamless service continuity | • | • | • |
| Sc. 6: Sc. 5 + access to 3G circuit-switched services with seamless mobility | • | • | • |

Lossy: Interconnected ANs share a common database; ANs do not establish any connections with the SGSN and GGSN nodes; single authentication procedure is imposed.

Tight: ANs connect directly to the UMTS core and support the applicable UMTS signalling.

Very-tight: ANs connect at the RNC level.

\*The proposed model takes advantage of the IMS’s application layer in order to avoid modifying the core components of the IMS and the WLAN. To achieve the interworking of the two networks specific new components are introduced: a WLAN application server deployed in the IMS’s application layer and a SIP server residing in the WLAN. The proposed architecture achieves to support all the interworking scenarios of the Table 2 except from the 6th scenario.

Munasinghe and Jamalipour [16] present another IMS-based interworking solution for UMTS and WLAN networks. More specifically, the authors propose a tight coupling architecture, where the WLAN is connected to the UMTS via an SGSN emulator. With this approach, mobility issues can be handled by the already developed procedures of the UMTS network. Simulation results showed that the proposed architecture achieves service continuity in the case of a UMTS to WLAN handoff but with a small time frame of data duplication, while in the case of a WLAN to UMTS handoff there was a small service disruption period due to the reactive nature of the handoff procedure. The same authors also in [17] propose another IMS-based interworking solution for UMTS and WLAN networks. The uniqueness of this architecture is that the IMS proposed by the 3GPP has been used as an arbitrator for network coupling and real-time session management.

Chiang and Huang [18] propose a 3GPP Voice over WLAN (VoWLAN) architecture model incorporating a network-initiated triggering mechanism to support user terminal mobility based on the SIP. The proposed solution covers most of the 3GPP/WLAN interworking requirements, supports the mobile host’s mobility and at the same time demonstrates acceptable handoff delay.

Munasinghe and Jamalipour [19] propose a novel architecture to connect different ANs, i.e. a UMTS, a WiMAX and a CDMA2000 networks, with an IMS core in order to handle the sessions. More specifically, in the proposed architecture the ANs are connected to an IP core and a P-CSCF deployed in each of them. The Mobile IP (MIP) is used to handle mobility. The foreign agents are deployed in the GSN, CSN and PDSN for each of the ANs. The home agents reside in the IMS core. Simulations results showed good performance indicating a 210 ms delay for the establishment of a session and a 335 ms delay for a vertical handoff.

Munir and Wong [20] investigate the deployment of a 4G network and propose the use of the 3GPP IMS to help the provision of session handling. The authors propose two different approaches, the Loosely Coupled Satellite-Cellular-WiMAX-WLAN (LCSCW2) architecture and the Tightly Coupled Satellite-Cellular-WiMAX-WLAN (TCSCW2) architecture based on loosely coupled and tightly coupled paradigms, respectively. The authors evaluate both the two architectures, by providing a cost analysis for the signalling and data traffic of the proposed architecture. This analysis includes transmission, processing and queueing costs at the various network entities. Numerical results show that in the LCSCW2 architecture the system signalling cost is reduced in comparison with the TCSCW2 architecture.

In addition since the main protocol used by the IMS to handle mobility is SIP. In SIP when a session is lost, for example during a handoff, the caller has to re-register to the core of the network and re-invite the corresponding node in order to continue the session. This is a long procedure and results in data loss. Many solutions have been proposed to overcome this problem [21–26]; some including other mobility protocols, such as MIP [21] that is also often used for current interworking UMTS-WLAN solutions [27].

In [21], Le et al. propose a new method to handle handoffs in IMS networks, based on a combination of the MIP and the SIP in order to make the handoff procedure faster and more transparent to the user. More specifically, in the proposed solution a cross layer module is placed between the S-CSCF and the home agent. This solution offers a faster handoff compared to the MIP based one, since the signalling flow between the Mobile Node (MN) and the home network is only needed once.

Ronan et al. propose the use of an IPv6 multi homing technique, called SHIM6 [22], in order to reduce the service disruption during handoff to the minimum in a Wi-Fi -UMTS network. The IMS core that connects them includes a P-CSCF for each domain, an I-CSCF to connect the proxies and a S-CSCF to handle the sessions. The SHIM6 basically allows a user to register two pairs of addresses...
and transfer a session from the first to the second pair in case of a handoff. The proposed technique is compared with the MIP technique in terms of traffic received, traffic dropped and end-to-end packet delay. SHIM6 performed better than the MIP in all three categories. The handoff procedure only lasted 30 ms with SHIM6 and the users experienced a faint “click” in the sound.

Udagama et al. [23] provide another solution called NETworking Context-Aware Policy Environment (NetCape) that is based on a policy engine policy which runs on the user terminal (mobile phone, Personal Digital Assistant (PDA), laptop). The engine gathers information from the user, the operator of the network, as well as, the environment (protocols in use). The protocol stack information consists of the application, session, transport, network and link layer information. The authors evaluate the proposed method by considering a hierarchical 3G-WLAN network and a user of the 3G networks that has started a video conference with one of his friends. During his conversation the NetCape module decides to perform a hard handoff and deliver the ongoing session to a WLAN. Simulation results showed that the MIP (IPv6) without the NetCape fails to detect the need for a handoff in time. As a result, a time frame of zero throughput is observed. The NetCape architecture detects the need for a handoff successfully, thus achieving the desired session continuity.

Bellavista et al. [24] study a pro-active vertical handoff mechanism, as part of a wider architecture called IIMAS (IMS-compliant Handoff Management application server) with goals the handoff prediction and the session adaptation. The proposed architecture offers some advantages. Firstly, it uses a pro-active approach, meaning that it predicts the need for a handoff in the terminal and the necessary operations are initiated before the initial connection is lost. Secondly, it has low session adaptation latency and finally yet importantly, it is the first proposal fully compatible with the IMS and therefore it is ready to be deployed. The results showed a significant reduction of the play-out interruptions, the successful continuous service delivery, and a notable reduction of the handoff time i.e. from 2.230 ms to 220 ms.

Dutta et al. [25] study mobility management in MultiMedia Domain (MMD) networks. The authors developed a testbed architecture based on one of the architecture alternatives of 3GPP2, where the outbound signalling servers are distributed around the edges of the network and examined three different types of handoff: The non-Optimized Handoff Mode; The reactive Handoff Mode; The proactive Handoff Mode. Testbed results showed that the proactive handoff is much faster than the other two cases. The reactive mode was three times slower and the non-optimized mode four times slower.

Renier et al. [26] also discuss the problem of session continuity during an IMS handoff. The authors try to bypass the re-registration procedure by introducing two new SIP messages. More specifically, the handoff procedure with one active session is completed in four messages instead of the initial fifteen. In the case of five active sessions the number of messages is reduced from 59 to 12. A solution for mobility management in the network layer using MIP is also discussed.

The QoS provisioning system of the IMS is policy based. This means that the operators of domains establish policies to control whether a certain user has the right to access a service or not. Such a system needs three elements to function properly: a policy repository, where the various policies are stored, a policy decision function that checks the user’s right to use a service and finally and a policy enforcement point where the decision that has been made is applied.

In the IMS, the policy repository and the policy decision function are implemented in the P-CSCF, whilst the policy enforcement point is implemented in the access network. The IMS is going to be used in NGN environments and in such an environment lots of different policies and QoS technologies are bound to exist. Researchers are having trying to find ways to coordinate the various technologies in order provide reliable QoS mechanisms.

In addition to the problem of session continuity during an IMS handoff, Renier et al. [26] discuss the Quality of service provisioning. The proposed architecture consists of an Access Serving Network Gateway (ASNG) which controls one or several APs and its main functionalities are to filter and route data packets from/to the MNs, but also to perform tasks related to the QoS establishment. ASNGs are connected via an IP network to the PDG which provides filtering functionalities equivalent to the GGSN in UMTS.

To avoid the re-negotiation of the quality of service parameters during a handoff, this task is assigned to an entity called Bandwidth Broker (BB). The bandwidth broker has the complete picture of the allocated and available resources of the network at all times. For ease of the configuration, the existence of a BB can be made transparent to the IMS. In such a case all communications between P-CSCF and BB is achieved through the Go interface to the PDG.

Lee et al. [28] discuss the problem of QoS provisioning for a user accessing the IMS through the conventional internet and propose a solution to deal with this problem. The solution is applied on an experimental network consisting of a UMTS domain, an internet domain, a DiffServ core and an IMS core. Users that access the IMS core through the UMTS domain have two ways of reserving resources of the network to ensure the appropriate QoS levels for their sessions: the PDP and the RSVP. The problem for internet users arises from the fact that their packets are marked as best effort. The solution proposed is called IPFIX and it uses the option field of the IP header for the necessary QoS parameter exchange. The IPFIX method has a minimum packet overhead compared to the PDP and RSVP methods, since it does not use new additional packets. The only disadvantage of the method is that it requires modifications to the IP option header.

Vallejo et al. [29] propose a signalling architecture for end-to-end QoS management in IMS/NGN networks. The main element of the architecture is the QoS broker which is responsible of monitoring the network bandwidth, as well as, of handling the policy exchanges between domains. The QoS broker implements the policy decision function and the transport resource control function. The protocols used in the architecture are the COPS-SLS and DIAMETER for communication between the QoS broker and the Service Control Functions.

Mani and Crespi [30] address the problem of end-to-end QoS provisioning between different domains and technologies. The authors propose a method that each access network has its own policy decision function or local policy depository that communicates with the central PDF residing in the IMS network. For the SLA exchange, the authors propose an entity called SLA broker that also resides in the IMS core and stores all the SLAs of the operators participating in the network.

De Gouveia and Magedanz [31] propose a framework that manages mobility and QoS in an IMS network. The architecture consists of the Dmain Policy Manager (DPM) and the policy enforcement point. The DPM is a policy decision function that also acts as policy decision point. The architecture includes a DPM management tool that offers a way for the operators to add, remove, or edit policies. A resource negotiation function communicates with other DPMs in order to exchange SLAs. The resource monitoring function makes sure that the already agreed services are being delivered. The authors provide a scenario of an inter-domain vertical handoff to highlight the functionality of the architecture.

4. A WiMAX-UMTS and WiMAX-WLAN IMS architecture

4.1. Network architecture

The proposed interworking model, as Fig. 3 depicts, integrates a WiMAX network, a UMTS network and a WLAN in an IMS compatible architecture. More specifically, the proposed architecture
incorporates a UMTS Core Network where the SGSN, the GGSN and the AAA Server reside, a WiMAX and a WLAN network interconnected with the UMTS Core through specific functional entities and an IMS in charge of sessions’ control.

Our primary focus for the proposed architecture was to replace the RAN part of the UMTS network with a WiMAX network and to place an IMS core on top of both technologies to manage sessions. This novel approach was driven by the fact that WiMAX offers a number of advantages compared to the UMTS’ RAN. Firstly, it is a very cost efficient solution, in terms of deployment and maintenance. Secondly, it has better performance in terms of data rates in comparison with the UMTS RAN for bandwidth greedy applications (e.g. video calls). In addition, a UMTS Node-B has very limited area coverage compared to a WiMAX Base Station (BS). A single WiMAX BS can cover many square kilometres, making the technology ideal for areas with crude geographical formation where the deployment of equipment is difficult. The biggest advantage that UMTS held against WiMAX was the mobility mechanism it offered. This disadvantage of the WiMAX has disappeared since in a latest release of the WiMAX mobility is supported.

Also a WLAN access network was ‘attached’ to our primary architecture following the architectural concept of [3,32] in order to enhance our network’s characteristics and technologies’ coverage, and thus building a converged network with IMS technology.

The proposed architecture is able to cover all the interworking scenarios described in [14] and depicted in Table 2. Users can access the UMTS CS based services through the WiMAX and WLAN networks, since they are authenticated in the AAA Server and registered in the IMS core. As far as scenario 5 (seamless services) is concerned, a handoff prediction method must be used in order to eliminate the service disruption time. In the handoff procedures described below, the old P-CSCF serving the user sends information concerning the active calls to the new P-CSCF thus reducing the amount of time needed for the handoff. However, as stated in [26] this technique does not completely eliminate the service disruption time. This problem can be solved by means of handoff prediction, similarly to [23,24].

The ANs can belong to the same different network operator(s). Each AN is connected to a distinct PDG and in principle to a distinct WAG. The same P-CSCF serves the ANs’ PDGs and WAGs, whilst different S-CSCF and I-CSCF servers could be allocated for each AN.

The MSs are identified by multiple IP addresses and have the ability to choose the Access Network that suits better the user requirements in terms of the type of the application to be activated, the connection costs, the AN’s area coverage, the QoS, etc.

Necessary functionalities for the Mobile Station (MS) include:

a. Support of the IEEE 802.16e and MIP.
b. Existence of the necessary credentials (i.e. IMSI (International Mobile Subscriber Identity) number, user subscription keys provided by the network operator, etc.) for its authentication at the UMTS Core.
c. Active IMS subscription for the registration to the HSS. For the successful registration to the IMS the public/private user identity is needed.
d. SIP support.
e. DiffServ support.

A user or MS that wants to register to the IMS core through the UMTS network must first activate a PDP context. A PDP context is a record that is saved in the SGSN and the GGSN, and contains information about the user, as well as, about the active session. The record includes the users’ IMSI number and IP address, the quality of service parameters of the given session, etc. The PDP context activation procedure takes place after the attach procedure.

Fig. 3. The WiMAX-UMTS and WiMAX-WLAN interworking architecture.
The procedure starts with the activate PDP context message sent by the user to the SGSN. The SGSN then queries the Domain Name Server (DNS) of the core network to find the GGSN to which the particular access point corresponds. The DNS replies with the GGSN’s IP address and the SGSN forwards the PDP context activation request to the received IP. The GGSN authenticates the subscriber and gets a dynamic IP address from the Dynamic Host Configuration Protocol (DHCP) [33] server to assign it afterwards to the MS. After that, the GGSN sends a create PDP context response to the SGSN. Finally the SGSN ends the procedure by sending an activate PDP context accept message to the user. At the end of this procedure, the user is ready to register to the IMS core with the SIP registration.

As regards the WiMAX network is concerned, each user that accesses the IMS or UMTS services must be registered in the HSS. An AAA Proxy Server must be deployed in the CSN of the WiMAX network to perform the authentication of the users. The AAA Proxy is responsible for various functions including:

a. Relaying the AAA information between WiMAX and the 3GPP AAA Server;
b. Enforcing policies derived from roaming agreements between the 3GPP operators and between the WLAN operator and the 3GPP operator;
c. Providing access scope limitation information to the WiMAX based on authorization information from the Home network;
d. Providing the means for protocols’ interworking in the case where the Wa and Wd interfaces use different protocols. These two interfaces are used for the communications between ASN and AAA Relay and between AAA Relay and AAA Server.

The AAA Server that resides in the home UMTS network of each user communicates via the Wd interface. An EAP AKA authentication procedure is used to authenticate the user in the AAA Server. The AAA Server implements functions such as:

a. Retrieving authentication information and information concerning the subscriber’s profile (including subscriber’s authorization information) from the HLR/HSS of the subscriber’s home 3GPP network;
b. Authenticating the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies/relays;
c. Updating the WiMAX access authorization information when user’s service subscription is modified and when it is requested by HSS/HLR;
d. Preserving the state of each user’s connection i.e. connected, disconnected, idle;
e. Producing billing information and sends the details to the offline billing system of each user’s home network;
f. Providing information concerning the network’s policy enforcement to the AAA Relays;
g. Transporting users’ profile to different AAA Servers if so requested by the HSS.

The WiMAX gateway is a gateway via which all the data to/from WiMAX mobile devices are routed. Among its core functionalities are:

a. Routing of packets to the appropriate PDG that serves each user;
b. Retrieving information concerning each ongoing session including duration, bandwidth allocated, volume of data exchanged, etc. Based on this information, WAG produce billing information which in turn are being sent to the per user specific serving AAA Relay.
c. Filtering packets based on their headers’ unencrypted information and rejects the non-authorised ones.
d. Ensuring the data packets’ routing through its user’s home network.

e. Incorporating authentication controls towards minimising security threats.

The element that completes the architecture is the PDG. The UMTS and IMS services are accessed through the PDG. Each mobile device connected through the WiMAX network is associated with one PDG. Some of the functions performed by the PDG are:

a. Stores the routing information for the WiMAX-3G connected users.
b. Routes packet data received from/sent to the PDN to/from the WiMAX-3G connected user.
c. Performs address translation and mapping.
d. Performs de-encapsulation and encapsulation.
e. Accepts or reject users’ access based on the decision made by the AAA Server.
f. Registers MS’ local addresses and attach them to the corresponding remote ones.
g. Provides the ability to reject data packets based on the policy enforced by the network operator.
h. Incorporates authentication controls towards minimising security threats.
i. Enforces billing policies to IP flows that incorporate UMTS services; while it supports the production of offline and online billing data.

The PDG functionality can be implemented in the GGSN in a way similar to the one described in [32]. If a user wants to access IMS services he has to perform the SIP registration, as well as, the UMTS AKA procedure. The SIP registration is performed between the user and the IMS Core.

The main entities taking part to the WLAN integration are the WAG (WLAN access gateway) and the PDG.

The AAA traffic is routed to the AAA Server whilst the data traffic is routed to the PDG, through a WAG. The WAG ensures that user data traffic is routed to the appropriate PDG through the Wp interface. A proposed protocol across Wp is the GPRS Tunneling Protocol (GTP), that is used also on the Gn interface between the SGSN and GGSN. The WAG collects billing information and interfaces WLAN through the Wn for the transportation of tunnelled user data. The Wg interface is mainly used by the AAA Server to deliver routing policy enforcement information to the WAG. This information is used by the WAG to securely identify the user data traffic of a particular MS and apply the required routing policy.

The PDG performs address translations, enforce policy, generate charging records, etc. The PDG’s role can be seen as equivalent to the GGSN’s for the other integrated ANs; thus the IMS and the 3GPP PS services are accessed through the PDG in the home or visited network. The PDG allocates a remote IP address to the MS and builds the end-to-end tunnel between the MS and itself. In addition, the PDG being the start/end point for all MS ↔ PDG interconnection flows (tunnel establishments) and performs de-encapsulation and encapsulation. Through the Wm interface and using DIAMETER, the AAA Server retrieves tunnelled attributes and MS’s IP configuration parameters from the PDG.

As mentioned above, the MS needs to establish an end-to-end tunnel with the PDG before using the 3GPP Packet Switched (PS) services [18]. At the starting point of the tunnel establishment, the WLAN access authentication and authorization takes place through EAP request/response messages exchanged between the MS and the AAA Server. Upon successful completion of the EAP authentication and authorization, the WLAN allocates a local IP address to the MS, which is being used to identify itself in the WLAN.
Next, the MS performs DNS query in order to retrieve the addresses of the PDGs and selects the one to which afterwards it sends the initial end-to-end tunnel establishment request. The PDG retrieves from the AAA Server the needed information towards validating the authentication of the MS and upon successful validation allocates the MS with a remote IP address and a P-CSCF.

The main advantage of the WLAN being connected to the UMTS core network in the same manner as other UMTS RANs, is that the mechanisms for mobility, QoS and security in the UMTS core network can be directly reused.

4.2. Network entry process

4.2.1. UMTS entry process

The user who communicates through the UMTS follow the specified 3GPP procedure. More specifically upon the MS’ authentication, a PDP Context is activated and an IP address is obtained. The last step of the procedure involves its registration to the IMS core which is realized by the REGISTER method of SIP. In the following paragraphs, we present the signalling flows of the UMTS entry process and more specifically the ones of the Attach, the PDP Activation and the Registration processes.

Attach procedure: The complete message flow for the attach procedure is presented in Fig. 4. The MS initiates the attach process (“GMM Attach Request”) right after the terminal is switched on. The “GMM Attach Request”, received by the network’s SGSN, incorporates the previous TMSI (Temporary Mobile Subscriber Id) number, the Mobile Network Identity, the location area, as well as, information concerning the routing area. The SGSN, upon receipt of this information, query for the specified TMSI in its database. If no registration is retrieved concerning the received TMSI, the SGSN uses the information specified as regards the old Location Area of the MS towards the identification (“Identity Request TMSI”) of the old SGSN to which the MS was registered. The old SGSN responds back (“Identity Response IMSI”) with the IMSI (International Mobile Subscriber Identity) of the MS. There is a number of messages exchanged between

![Fig. 4. The signalling of the attach procedure.](image-url)
the SGSN and the MS towards the authentication of the latest. The SGSN sends an “Identity Request” to the MS requesting from the MS to identify itself. Upon reception of the MS’ response, the SGSN sends an “Authentication Request”. The SIM card of the MS applies specify algorithms to the RAND value and the secret key (Kc) and the Secret Response (SRES). The produced SRES value is sent to the SGSN (“Authentication Response”). After the “Identity Check” is completed; thus the MS identity has been acquired, the SGSN informs the AAA Server (“Update Location”) of the new location of the MS. Similar procedure is followed old SGSN which is informed by the AAA Server. Next the AAA server updates the SGSN with the all user’s information and upon completion of this process (“Update Location Ack”), the SGSN responds back to the initial message of the MS with a “GMM Attach Accept”. The attach procedure closes with the “GMM Attach Complete” sent by the MS to the SGSN.

**PDP activation:** The MS initiates the process towards the reservation of an IP address. The “Activate PDP Context” message incorporates the APN (Access Point Name) which is defined by the service provider. Then a “DNS Query” and a “DNS Response” are exchanged between the SGSN and the DNS server in order for the first to acquire the IP address of the GGSN. After that, the SGSN ‘forwards’ the initial “Activate PDP Context” to the GGSN, which is indicated by the APN, via the “Create PDP Context Request” message. The GGSN authenticates (“Radius Authentication Request”) the registration of the user and upon completion, requests from the DHCP server (DHCP Address Request) a dynamic IP to be allocated to the MS. With the requested IP address reserved, the GGSN responds to the SGSN that the PDP Context Activation has been completed and the same does the SGSN to the MS finalizing the overall procedure. The complete signalling flow of the procedure PDP Context Activation is presented in Fig. 5.

**Registration procedure:** This procedure includes 36 messages [5]. It is the standard 3GPP SIP REGISTER method, the flow of which is depicted in Fig. 6. The process is initiated by the MS, which sends a SIP “REGISTER” to the P-CSCF. The P-CSCF might not reside to MS’ home network, thus it is required to find an entry point to the MS’ home network. Towards this end, DNS actions are implemented so as for the P-CSCF to retrieve the SIP URI of an I-CSCF of the home network. Then, the P-CSCF attaches to the S-CSCF “REGISTER” the information needed by the MS’s home network, enabling it to transfer the traffic through itself, and then forward the message to the I-CSCF. The I-CSCF, in order to identify whether a S-CSCF is already allocated to the particular MS, sends a “UAR” to the HSS. The “UAR” incorporates MS’s information including the MS’s PuUI and PrUI, but also the identifier of the new network. The HSS then responds with a “UAA” containing either the SIP URI of the previous S-CSCF or a list of the qualifications of the available S-CSCFs. The I-CSCF chooses the most appropriate S-CSCF for the specific MS and forwards the SIP “REGISTER”.

The S-CSCF authenticates the MS and contacts HSS to store the MS’s SIP URI (“MAR”). Upon receipt of the MS’s authentication credentials from the HSS (“MAA”), the I-CSCF sends through I-CSCF to the P-CSCF a user invitation (“401 UNAUTHORIZED”), to which the MS responds with a SIP “REGISTER”. The P-CSCF repeats the above presented messages’ exchange, with exception of the new “UAA” which this time contains routing information i.e. the SIP URI to S-CSCF allocated to the MS. The S-CSCF receives the new SIP “REGISTER” containing the MS credentials and validates them with the ones retrieved earlier from the HSS. Upon validation’s successful completion, the S-CSCF informs the HSS of the MS’s successful registration and retrieves its profile. Finally, the S-CSCF informs the MS for the successful completion of the registration procedure.

**4.2.2. WiMAX entry process**

The entry process for users entering the network from the WiMAX AN is not so straightforward as the UMTS entry one. The user authentication method has to be defined and the procedure by which the MSs will be informed for the required IP addresses (PDC, P-CSCF) has to be determined.

In the following paragraphs, we analyse the proposed signalling diagram for our network entry process from the WiMAX perspective.

The main network entities participating in the entry process are the supplicant (MS) requesting its registration to the network, the ASN gateway also referred to as the authenticator as it controls the user authentications based on the retrieved information from the AAA Relay and the DHCP server located at the WiMAX CSN and responsible for the ‘addressing’ requirements.

As shown in Fig. 7, a complete network entry procedure for a MS registering from WiMAX includes 48 messages. These messages are not only exchanged between the MS and the BS but travel through various entities of the network.

The first stage of the procedure is the negotiation of the basic capabilities of the MS. The MS sends an “SBC-Request” to the BS

![Fig. 5. The signalling of the PDP context activation procedure.](image-url)
which replies with an “SBC-Response”. In the mean time the BS informs the authenticator for the received entry application which in turn responds with an “ms-preattachment_resp” message. The “SBC-Response” mentioned above imposes the authentication protocol to be applied based on the MS capabilities. It should to be noted that based on the network’s configuration, the “SBC-Response” could precede the message exchanges between the BS and the authenticator.

The next stage is the authorization of the MS. After that, the MS is authenticated in the UMTS domain and can use UMTS services. The authorization stage includes an EAP procedure between the MS and the AAA proxy and an SA-TEK procedure between the MS and the BS. The authenticator initiates the authentication process by sending the EAP identity request. The BS takes over the message forwarding between the entities taking part in the EAP process. The MS responds to the EAP identity request which it arrives to the authenticator through the BS. This response incorporates information identifying the MS’s home network. Based on this information, the authenticator identifies the MS’s AAA Server and retrieves the user’s profile. The message exchange between the authenticator and the AAA Server are done via the RADIUS protocol. During the main part of the EAP process, the authenticator challenges the MS with specific authentication credentials and the MS responds back based on specific keys pre-defined by the user’s service subscription. The MS response is validated by the authenticator. If the process completes successfully, the authenticator informs both the MS and the BS. Upon receipt of the successful completion of the EAP process, the BS initiates the production of new keys for the session establishment with the MS.

Next, the three-way-handshake process is initiated for the establishment of a secure connection between the MS and the BS. Upon completion, the MS requests from the BS the keys, which will be used for the encryption of data during the session. The BS responds with the key response message.

The entry procedure continuous with the 802.16 registration process. It takes place between the MS and the BS. The MS sends a Reg-request and the BS responds with a Reg-response. The Reg-request (“REG-REQ”) is the registration application message of the 802.16e. It incorporates MS’s capabilities concerning mobility and handoff support. The BS exchanges the “MS-attachment-req” and the “MS-attachment-resp” with the ASN gateway which compose the network attach request for the MS. With the “MS_Attachment_Ack”, the BS informs the ASN Gateway for the successful completion of the user registration via 802.16e. After this step, the MS is registered to the WiMAX domain, which means that the user authentication to the UMTS is completed via the EAP pro-
Protocol, the MS has been granted access to the WiMAX via the 802.16e registration and a secure connection with the BS has been established through the three-way-handshake process.

The next step is to assign an IP address to the MS. This is done by the CSN of the WiMAX following the DHCP procedure. The DHCP server of our network resides in the CSN of the WiMAX domain. The “DHCP Discover” message sent from the MS to the DHCP server initiates the procedure. The server responds with the “DHCP offer” and the MS responds back with a “DHCP request”. The final message of the procedure is the “DHCP ack” which includes the parameters requested by the MS. The addressing can be done based on either IPv4 or IPv6 protocol. Two IPs (home and foreign) should be allocated to the MSs. MIP will be used for the mobility support.

The DHCP protocol provides the network with the ability to send configuration information to the MSs. DHCP reserves IP addresses from a list dedicated to a specific network domain. Upon an MS network disconnection, its IP address is released and can be allocated to a different MS. Further information on the DHCP messages is presented in [18].

| MS | ADB Gateway | Authenticator | CSN AAA | DHCP Server | WiMAX Gateway | PDG | AAA/EAP Server (3GPP Home) | I-CSCF | HSS | S-CSCF | P-CSCF | SBC | SBC_req | MS_Preattachment_req | MS_Preattachment_resp | SBC_resp | MS_Preattachment_Ack | Starting EAP AKA | EAP_Identity_req | EAP_Transfer | EAP_Transfer | EAP_Identity_resp | EAP_over_RADIUS | EAP_request / AKA challenge | EAP_response / AKA challenge | EAP success | EAP success | Key_change_Directive | PMK, AK generated in MS and ASN Gateway | Key_change_Ack | SA TEK challenge | SA TEK_req | SA TEK_resp | Key_req | Key_resp | Registration Begins | REG-REG | MS_Attachement_Req | MS_Attachement Resp | MS_Attachement_Ack | REG-RESP | REG | MS_Attachement_Ack | Cx-Query | Cx-Select pull | Cx-Select pull Resp | Cx-put | Cx-put Resp | Cx-pull | Cx-pull Resp | 200 OK | 200 OK | 200 OK | 200 OK | Registration Completed

Fig. 7. The WiMAX → IMS entry procedure signalling.
With the “Time of Day Request/Response” messages, the MS is informed by the BS on the time. Following, the service flow is created. The service flow is required for WiMAX quality of service provisioning. The MS sends a “DSA req” by which it requests for a specific QoS class for the service flow. The BS validates the correctness of this request, and responds back with a “DSA resp” which incorporates the QoS class allocated to the service flow. The MS informs back the BS with a “DSA Ack” for the successful receipt of the “DSA resp”. After all these steps the MS is able to use the 3G and WiMAX services.

In WiMAX, each connection between a MS and a BS has a distinct identifier, the CID (Connection Identifier), each bidirectional packet flow is identified by a specific SFID (Service Flow Identifier) and each service flow has specific QoS characteristics. WiMAX supports five different QoS classes, which are presented in the 2nd column of Table 3.

To complete the entry in our network the MS has to perform the SIP Registration to the IMS core. To do so, it has to be aware of the IP addresses of the PDG and the P-CSCF that serve it. There are two ways for this to be accomplished. The first option would be to perform a second DHCP procedure towards retrieving these IP addresses. However, this would increase the number of network’s control messages for the MS’s registration; thus extending and slowing down the overall entry procedure. The second and proposed one is to use the “OPTIONS” field of the DHCP message [27]. More specifically, our proposal is to use an unused code of the DHCP options and pass these addresses to the MS during the initial DHCP message exchanges. During the SIP registration the MS’s registered state is stored in the HSS and an S-CSCF is assigned to it.

### Table 3

<table>
<thead>
<tr>
<th>UMTS-WiMAX-WLAN QoS classes mapping.</th>
<th>WiMAX</th>
<th>WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conversational</td>
<td>Unsolicited Grant Service (UGS)</td>
<td>Continuous time QoS Traffic</td>
</tr>
<tr>
<td>Streaming</td>
<td>Extended Real Time Polling Service (erTPS) – added in 802.16e</td>
<td>Controlled access CBR traffic</td>
</tr>
<tr>
<td>Interactive</td>
<td>Non-real-time polling service (nrtPS)</td>
<td>EffortBursty Traffic</td>
</tr>
<tr>
<td>Background</td>
<td>Best Effort Service (BE)</td>
<td>Unspecified non-QoS traffic</td>
</tr>
</tbody>
</table>

4.2.3. WLAN entry process

The WLAN Authorization includes 17 messages (Fig. 8). At first, the MS sends an “EAPOW start” to the AP initiating the 802.1x authentication process. The MS is authenticated by the “EAP-Request/Response” method, and it sends a RADIUS message containing its identity to the WAG. The WAG retrieves from the RADIUS message the address of the AAA Server serving the MS. The WAG contacts the respective AAA Server and gets back the authentication credentials. The following message exchanges includes a RADIUS access challenge which is forwarded to the AP and then the MS and the MS’s EAP response based on the authentication algorithm stored in its (U)SIM card. MS’s EAP response is forwarded to the WAG, where the latest validates it in conjunction with the authentication credentials received from the AAA Server. If the validation is successful, the WAG sends a RADIUS Access Accept to the AP. It is then when the AP authorises the MS by sending an EAP-Success and the EAPOW-Key.

As regards the IMS registration for an MS entering the network from WLAN, the overall process includes 32 messages (Fig. 9).

The process is initiated by the MS, which sends a SIP “REGISTRATION” to the P-CSCF. The P-CSCF might not reside to MS’ home network, thus it is required to find an entry point to the MS’ home network. Towards this end, DNS actions are implemented so as for the P-CSCF to retrieve the SIP URI of an I-CSCF of the home net-
work. Then, the P-CSCF attaches to the SIP “REGISTER” the information needed by the MS’s home network to be able to transfer the traffic through itself, and then forward the message to the previously identified I-CSCF. The I-CSCF, in order to identify whether a S-CSCF is already allocated to the particular MS, sends a “UAR” to the HSS. The “UAR” incorporates MS’s information including the MS’s PuUI and PrUI, but also the identifier of the new network to which the MS is entering. The HSS then responds with a “UAA” containing either the SIP URI of the previous S-CSCF or a list of the qualifications of the available S-CSCFs. The I-CSCF chooses the most appropriate S-CSCF for the specific MS and forwards the SIP “REGISTER”.

The S-CSCF authenticates the MS and contacts HSS to store the MS’s SIP URI (“MAR”). Upon receipt of the MS’s authentication credentials from the HSS (“MAA”), the I-CSCF sends through I-CSCF to the P-CSCF a user invitation (“401 UNAUTHORIZED”), to which the MS responds with a SIP “REGISTER”. The P-CSCF repeats the above presented messages’ exchange, with exception of the new “UAA” which this time contains routing information i.e. the SIP URI of the S-CSCF allocated to the MS. The S-CSCF receives the new SIP “REGISTER” containing the MS credentials and validates them with the ones retrieved earlier from the HSS. Upon validation’s successful completion, the S-CSCF informs the HSS of the MS’s successful registration and retrieves its profile. Finally, the S-CSCF informs the MS for the successful completion of the registration procedure.

4.3. Session set-up

The proposed architecture is capable of supporting all the 3GPP interworking scenarios. Users that access services from WiMAX are capable of communicating with users residing in the UMTS and vice versa. The same applies also for users accessing services from WLAN.

During the session setup procedure, each MS has to reserve resources of his access network in order to support the session. The P-CSCF that serves each MS must authorize the QoS parameters that have been negotiated by the MSs. As different service classes are supported by each network technology involved, a specific correlation between these classes should be identified.

WiMAX supports five classes while UMTS only four. The top two classes of WiMAX have to be merged and every session belonging to them is categorized in the UMTS’ top class. In addition, the IEEE 802.11e standard, released in 2005, defined a set of QoS enhancements for WLAN applications. Specifically four QoS classes are defined. The top class, the one that requires more resources is intended for applications such as video calls. The second class sup-

<table>
<thead>
<tr>
<th></th>
<th>AP</th>
<th>ARG</th>
<th>WAG</th>
<th>P-CSCF</th>
<th>I-CSCF</th>
<th>HSS</th>
<th>S-CSCF</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>2</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>3</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>4</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>5</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>6</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>7</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>8</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>9</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>10</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>11</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>12</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>13</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>14</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>15</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>16</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>17</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>18</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>19</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>20</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>21</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>22</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>23</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>24</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>25</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>26</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>27</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>28</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>29</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>30</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>31</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
<tr>
<td>32</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
<td>REGISTER</td>
</tr>
</tbody>
</table>

Fig. 9. The WLAN → IMS registration process signalling.

Please cite this article in press as: N. Psimogiannos et al., An IMS-based network architecture for WiMAX-UMTS and WiMAX-WLAN interworking, Comput. Commun. (2010), doi:10.1016/j.comcom.2010.02.017
ports less demanding applications such as voice calls but still it has to provide low delay. The last two classes are the effort bursty traffic and the unspecified non-QoS traffic. The WLAN classes can be mapped directly to the four UMTS classes.

Table 3 presents a possible correlation between the service classes supported by UMTS, WiMAX and WLAN [34].

The following sections give an overview of the signalling flow involved in the session setup [5] between the ANs.

4.3.1. WiMAX-UMTS session setup

When the INVITE message arrives at the P-CSCF 1 (messages 1-5), it is verified for the correctness of its Route header field and is inspected if the Session Description Protocol (SDP) [35] offer is valid with QoS values that are applied to the Home Network. If it passes the previous check, then it is forwarded to the S-CSCF 1 which has become known during the registration procedure presented in previous section.

The S-CSCF 1, when it receives the INVITE message, (message 6) identifies the caller's identity from the relevant header field and tries to route the SIP request based on the originating user in the Request-URI. Following, with the DNS procedures, it tries to locate a SIP Server, which is actually an I-CSCF, in the terminating network to forward the INVITE message. The I-CSCF receives the INVITE message and has to forward it to the S-CSCF 2 which is allocated to the callee (message 7). In order to discover the address of the S-CSCF 2, which is the next node that the message has to pass, the I-CSCF has to query the HSS with a Diameter LIR request (message 8). The HSS receives the Diameter request, and searches for data associated with the user of the Public-Identity AVP header field, one of which is the S-CSCF 2 address which inserts into a Server-Name AVP in a Diameter Location-Information-Answer (LIA) message.

The I-CSCF receives the LIA (message 9) and routes the INVITE request (S-CSCF 2). Eventually, the INVITE message reaches the terminal of USER 2 (messages 10–16).

The USER 2 responds with a 183 Session Progress to the SDP offer and may start its resource reservation due to the knowledge of all the required parameters (messages 17–30). In messages 31–43, the USER 1 terminal examines the SDP answer which contains the IP address of the callee where the media streams are sent. Answers with a PRACK which includes a new SDP offer due to the changes that might be occurred at the SDP negotiation. Furthermore, the USER 1 terminal starts its resource reservation.

USER 2 responds to the PRACK with the 200 OK (messages 44–56), and starts its resource reservation. Within this 200 OK, there is a notification in the SDP field, which informs the caller’s terminal that the resource reservation has not been completed at the callee’s. The USER 1’s terminal sends an UPDATE request (messages 57–69), which contains another SDP offer, in which indicates that the resources has been reserved at his local segment. The callee’s IMS terminal sends as an answer a 200 OK message according to the SDP offer/answer model (messages 70–82). It is likely at this point, that the USER 2’s terminal has also finished its resource reservation according to the time the procedure takes to be completed. The IMS terminal rings and generates a 180 Ringing response which travels far to the caller’s terminal (messages 83–95). When the USER 1’s IMS terminal receives the 180 Ringing response, it will likely generate a ring-back tone to indicate at the other side that the terminal is ringing. It, also, sends a PRACK as a response to the previous 180 Ringing response (messages 96–108). The USER 2’s IMS terminal responds with a 200 OK, which completes the INVITE transaction (messages 109–121). Then, the USER 1’s IMS terminal sends an ACK request (messages 122–134), to confirm the receipt of the 200 OK response and starts generating a media-plane traffic across the USER 2’s terminal (message 135).

The flow sequence diagram of the WiMAX-UMTS session setup signalling process is depicted in Fig. 10.

4.3.2. WiMAX-WiMAX session setup

The signalling sequence for the WiMAX-WiMAX session setup is equivalent to the WiMAX-UMTS session setup presented in subsection 4.3.1. The difference rests with the different nodes at the terminating network. Fig. 11 shows the sequence flow i.e. messages 1–135, for a WiMAX-WiMAX session setup.

4.3.3. WiMAX-WLAN session setup

The signalling sequence for the WiMAX-WLAN session setup is equivalent to the WiMAX-UMTS session setup presented in subsection 4.3.1. The difference rests with the different nodes at the terminating network. Fig. 12 shows the sequence flow i.e. messages 1–123 for a WiMAX-WLAN session setup.
**Fig. 11.** The WiMAX-WiMAX session setup process signalling.

**Fig. 12.** The WiMAX-WLAN session setup process signalling.

**Fig. 13.** The UMTS-WLAN session setup process signalling.
4.3.4. UMTS-WLAN session setup

The signalling sequence for the UMTS-WLAN session setup is equivalent to the WiMAX-UMTS session setup presented in subsection 4.3.1. The only difference is the different nodes at the originating and terminating network. Fig. 13 shows the sequence flow i.e. messages 1–123, for a UMTS-WLAN session setup.

4.3.5. UMTS-UMTS session setup

The signalling sequence for the UMTS-UMTS session setup is equivalent to the WiMAX-UMTS session setup presented in subsection 4.3.1. The only difference is the different nodes at the originating and terminating network. Fig. 14 shows the sequence flow i.e. messages 1–135, for a UMTS-UMTS session setup.

4.3.6. WLAN-WLAN session setup

The signalling sequence for the WLAN-WLAN session setup is equivalent to the WiMAX-UMTS session setup presented in subsection 4.3.1. The difference rests with the different nodes at the originating and terminating network. Fig. 15 shows the sequence flow i.e. messages 1–114 for a WLAN-WLAN session setup.

4.4. Vertical handoff

The proposed architecture can support all the six levels of interworking (Table 2). In the following subsections, the call flows for the handoff procedures are presented and explained.

4.4.1. WiMAX → UMTS vertical handoff

In Fig. 16 the call flow for the WiMAX-UMTS handoff is presented. The MS (USER 1) is accessing through WiMAX and is engaged in a session with USER 2 accessing from UMTS. Between messages 13 and 14, the handoff prediction mechanism detects the need for a handoff. The process starts with the MS attaching to the UMTS core and activating a PDP context. Messages 15–20 describe the IMS re-registration phase including the context transfer mechanism. Following, the mobile terminal re-invites the corresponding node to the session. At this point the new P-CSCF has

Please cite this article in press as: N. Psimogiannos et al., An IMS-based network architecture for WiMAX-UMTS and WiMAX-WLAN interworking, Comput. Commun. (2010), doi:10.1016/j.comcom.2010.02.017
to authorize the QoS class of the session based on the service classes’ correlation presented in previous section. The re-invite request is forwarded to USER 1 before the data flow can be re-established.

4.4.2. UMTS → WiMAX vertical handoff

The UMTS-WiMAX handoff procedure is also proactive and the above described methods are used to ensure service continuity. The main difference between the current process and the one of the WiMAX-UMTS handoff is the entrance to the target network (Fig. 17). In this case instead of the attach and PDP context procedures, the network entry process presented in 5.2.1 is used. The MS includes the IP of the old P-CSCF in the register request in order to enable the context transfer between the two P-CSCFs.

4.4.3. Handoffs to WLAN

The difference with the previous presented handoff call flows is the network entry. The MS that needs to perform the handoff has to be authorized by the WLAN access point. A QoS class mapping should be provided in order to categorize sessions correctly.

5. Performance evaluation

5.1. Cost analysis

In this section, an analytic model for cost analysis in order to evaluate the performance of the proposed architecture is presented.

The total cost \( C_{\text{total}} \) for the intersystem communication of two users belonging into two different networks is computed as the aggregated cost for the transmission of the IMS signalling and data traffic, for the encapsulation, decapsulation and routing of packets, and for the queueing of packets of each entity. This cost can be given by:

\[
C_{\text{total}} = C_{\text{trans}} + C_{\text{proc}} + C_{\text{queue}}
\]

where \( C_{\text{trans}} \), \( C_{\text{proc}} \), and \( C_{\text{queue}} \) denote the transmission cost, the processing cost and the queueing cost respectively.
5.1.1. WiMAX–UMTS scenario

In the following of the analysis we consider the case of a user belonging to a WiMAX network is trying to communicate with a user belonging to a UMTS wireless network.

5.1.1.1. Transmission cost. The transmission cost is the aggregated cost for the transmission of the signalling and data traffic and is given by:

$$C_{\text{trans}} = C_{\text{sign}} + C_{\text{data}}$$

(2)

In our analysis, we assume that there are different unit packet transmission costs for the transmission of a packet in the wireless and wireless links, denoted as $u_{\text{wireless}}$ and $u_{\text{wired}}$ respectively.

If we denote the IMS signalling traffic arrival rate as $\lambda$ (requests per second) and the number of packets per request both for signalling and data from a source node as $l$, then the signalling transmission cost between the WiMAX and the UMTS network for the delivery of the IMS signalling traffic can be given by:

$$C_{sign}^{\text{trans}} = \lambda \left( 2 \times u_{\text{wireless}} \times u_{\text{wired}} \right) \left( d_{\text{sign}} + d_{\text{sign,-WiMAX-WiMAX}} + d_{\text{sign,-WiMAX-ASN-GW}} + d_{\text{sign,-ASN-GW-BS}} + d_{\text{sign,-BS-BS}} \right)$$

(3)

where $d_i$ denotes the number of hops between the two communicating entities and the coefficient of each $d_i$ denotes the number of messages that had to be passed through the two entities (for example 11 messages had to be passed through the BS and the ASN-GW).

Similarly, the transmission cost for the delivery of the IMS data traffic can be given by

$$C_{\text{data}}^{\text{trans}} = \lambda \left( 2 \times u_{\text{wireless}} \times u_{\text{wired}} \right) \left( d_{\text{data}} + d_{\text{data,-WiMAX-WiMAX}} + d_{\text{data,-WiMAX-ASN-GW}} + d_{\text{data,-ASN-GW-BS}} + d_{\text{data,-BS-BS}} \right)$$

(4)

It should be noted that in our analysis $l$ is equal to 1, since as in [20] we assume that one signalling packet can carry one particular signalling message, such as 200 OK from one node to its adjacent node.

By following the same methodology, the transmission cost for each communication path between WiMAX and WiMAX, WiMAX and WLAN (please see also the APPENDIX) can be computed.

5.1.1.2. Processing cost. For the processing cost analysis we follow the same methodology with the one proposed in [20]. More specifically, we denote as $N_{\text{NodeB}}$ the number of Node-Bs that are connected to each RNC, $N_{\text{RNC}}$ the number of RNCs that are connected to each SGSN, $N_{\text{GGSN}}$ the number of SGSNs that are connected to each GGSN, $N_{\text{PCSF}}$ the number of P-CSFs in the architecture. In addition, we assume that there are $N$ users in the network that are distributed in coverage area of each network. Therefore, the total number of users $N$ is equals to $N = N_{\text{WiMAX}} + N_{\text{UMTS}} + N_{\text{WLAN}}$

(5)

where $N_{\text{WiMAX}}$, $N_{\text{UMTS}}$, and $N_{\text{WLAN}}$ denote the numbers of users in the coverage area of the WiMAX network, the UMTS network and the WLAN.

Furthermore, we assume that each entity of the IMS has each own unit packet processing cost denoted as $\gamma_i$ (i.e. $\gamma_i$ denotes the unit packet processing cost at the BS). Since the WiMAX user requests communication with the UMTS user, the processing cost of each WiMAX entity (i.e. BS and ASN-GW) in order to encapsulate and decapsulate packets can be given by:

$$C_{\text{proc}}^{\text{trans}} = \lambda N_i$$

(6)

where $i$ can be a BS or a ASN-GW.

In addition, since the UMTS entities (WiMAX-GW, P-CSCF1, P-CSCF2) and the IMS entities (S-CSCF1, S-CSCF2, I-CSCF) only forward the packets by adding their information to the packets, their processing cost can be given with similar expressions as that of Eq. (6) by replacing the value of $\gamma_i$ with the corresponding unit packet processing cost value.

For the processing cost for the other entities (HSS, GGSN, RNC, Node-B), since an additional cost for searching in their information tables their processing cost can be given by:

$$C_i = \lambda \left( \ln N_j + \frac{1}{\lambda} \right)$$

(7)

where $\gamma_i$, the unit packet processing cost value of each entity, $k$ is a system- dependent constant, $\sigma$ is a weighting factor, $L$ is the IP address length in bits and $S$ the machine word size in bits. $N_i$ denotes the number of entities in each information table of the corresponding entity (HSS, GGSN, RNC, Node-B).

Therefore, the processing cost for IMS signalling traffic between the WiMAX and the UMTS network is given by:

$$C_{\text{proc}}^{\text{trans}} = \lambda N_i$$

(8)

By following the same methodology, the processing cost for communication paths between WiMAX and WiMAX, WiMAX and WLAN (please see also the APPENDIX) can be computed.

5.1.1.3. Queueing cost. We model the IMS network as a tandem M/M/1 queueing network, assuming that each entity of the network as a server [20,36]. Therefore, the queueing cost is proportional to the total number of packets in the tandem queueing network.

The queueing cost for IMS signalling traffic between the WiMAX and the UMTS network is given by:

$$C_{\text{queue}}^{\text{trans}} = 11 \ast E[n_{\text{PDC}}} + 11 \ast E[n_{\text{CSCF-CP}}] + 11 \ast E[n_{\text{S-GGSN}}] + 11 \ast E[n_{\text{S-CSCF-2}}] + 11 \ast E[n_{\text{BS-BS}}] + 11 \ast E[n_{\text{ASN-GW-BS}}]$$

(9)

Thus, the processing cost $C_{\text{proc}}$ which is the aggregated cost for the processing of the signalling and data traffic can be given by:

$$C_{\text{proc}} = C_{\text{sign}}^{\text{trans}} + C_{\text{data}}^{\text{trans}}$$

(10)

where $\lambda$ is the arrival rate and $\mu_i$ the service rate respectively at each entity of the network.
In addition, the queueing cost for IMS data traffic between the WiMAX and the UMTS network is given by:

\[
c_{\text{queue}}^{\text{data}} = E[n_{\text{BS}}] + E[n_{\text{ASN-GW}}] + E[n_{\text{NG-WiMAX-GW}}] + E[n_{\text{PGW}}] + E[n_{\text{PS-CSCF1}}] + E[n_{\text{PS-CSCF2}}] + E[n_{\text{PS-CGF}}] + E[n_{\text{SGSN}}] + E[n_{\text{GGSN}}] + E[n_{\text{RNC}}] + E[n_{\text{NodeB}}].
\]

(13)

Therefore, the queueing cost \(C_{\text{queue}}\) which is the aggregated cost for the queueing of the signalling and data traffic and can be given by:

\[
C_{\text{queue}} = C_{\text{queue}}^{\text{sig}} + C_{\text{queue}}^{\text{data}}
\]

(14)

By following the same methodology, the processing cost for communication paths between WiMAX and UMTS, WiMAX and WLAN (please see also the Appendix) can be computed.

5.2. Numerical results

In this section, we present the numerical results for our proposed architecture in several use cases.

In our architecture, we consider a network that consists of three WiMAX networks, five WLANs, and one UMTS network. The number of users in each type of network are:

\[N_{\text{WiMAX}} = 2000, \quad N_{\text{UMTS}} = 3000, \quad \text{and} \quad N_{\text{WLAN}} = 300.\]

We, also, assume that each GGSN supports three SGSNs, each SGSN supports four RNCs, and each RNC controls two NodeBs. The unit packet transmission cost for the wireless links \(u_{\text{wireless}}\) and the wired links \(u_{\text{wired}}\) are set to 3.84 \times 10^{-6} and 0.1 respectively. The hop distances for the \(d_{\text{H2G}}\), and the \(d_{\text{H2R}}\) are set to 4, while the rest hop distances are set to 2 in accordance with [6].

The IP address length \(L\), as well as, the machine word size \(S\) are set to 32 bits [20]. Also, the system value \(k\) is selected to be 5. The weighting factor \(w\) is set to \(1 \times 10^{-6}\) as the lookup delay is increased by 100 ns for each memory access [6]. The service rate \(\mu\) at all network entities is set to 250 packets/s. Furthermore, the unit processing cost for all the network entities are set to \(4 \times 10^{-3}\) except for the SGSN and the GGSN that the unit processing cost for all the network entities are set to \(8 \times 10^{-3}\).

5.2.1. WiMAX-UMTS

In this section, we present the numerical results for our proposed architecture in the case of a user belonging to a WiMAX trying to communicate with a UMTS wireless network.

Fig. 18 depicts the transmission cost and the processing cost for signalling and data traffic for different values of IMS arrival rates \(\lambda\). More specifically, the labels \(C_{\text{t sig}}\) and \(C_{\text{t data}}\) denote the values for the \(C_{\text{trans}}^{\text{sig}}\) and the \(C_{\text{trans}}^{\text{data}}\) respectively and the labels \(C_{\text{p sig}}\) and \(C_{\text{p data}}\) denote the values for the \(C_{\text{proc}}^{\text{sig}}\) and the \(C_{\text{proc}}^{\text{data}}\) respectively.

As it was expected the transmission cost for signalling IMS traffic is higher than the transmission cost for IMS data traffic. This difference is increased with the value of increasing arrival rate \(\lambda\). As it is shown from the figure the processing cost for signalling IMS traffic is more than 10 times higher than the processing cost for IMS data traffic. This difference is kept constant independently of the value of the arrival rate \(\lambda\).

Fig. 19 depicts the queueing cost for signalling and data traffic for different values of IMS arrival rates \(\lambda\). More specifically, the labels \(C_{\text{q sig}}\) and \(C_{\text{q data}}\) denote the values for the \(C_{\text{queue}}^{\text{sig}}\) and the \(C_{\text{queue}}^{\text{data}}\) respectively.

![Fig. 18. Transmission cost and processing cost versus different IMS arrival rates \(\lambda\).](image)

![Fig. 19. Queueing cost versus different IMS arrival rates \(\lambda\).](image)

![Fig. 20. Signalling cost versus different IMS arrival rates \(\lambda\).](image)
bels $C_{q\_sig}$ and $C_{q\_data}$ denote the values for the $C_{\text{queue}}$ and the $C_{\text{queue}}$ respectively. It can be observed that the queueing cost for

signalling IMS traffic is significantly higher than the queueing cost for IMS data traffic. As the value of the arrival rate $\lambda$ increases the difference between the signalling and the data IMS traffic decreases.

Fig. 20 depicts the effect of varying IMS arrival rate $\lambda$ on the signalling cost where both the transmission signalling cost and the transmission processing cost increase linearly with the increasing value of $\lambda$. In addition, the queueing signalling cost also increases with the increasing value of $\lambda$.

5.2.2. WiMAX-WiMAX

In this section, we present the numerical results for our proposed architecture in the case of a user belonging to a WiMAX is trying to communicate with a user belonging to another WiMAX.

Fig. 21 depicts the transmission cost and the processing cost for signalling and data traffic for different values of IMS arrival rates $\lambda$. More specifically, the labels $C_{t\_sig}$ and $C_{t\_data}$ denote the values for the $C_{\text{trans}}$ and the $C_{\text{trans}}$ respectively and the labels $C_{p\_sig}$ and $C_{p\_data}$ denote the values for the $C_{\text{proc}}$ and the $C_{\text{proc}}$ respectively. As it was expected the transmission cost for signalling IMS traffic is higher than the transmission cost for IMS data traffic. This difference is increased with the value of increasing arrival rate $\lambda$. As it was seen from the figure the processing cost for signalling IMS traffic is more than 11 times higher than the processing cost for IMS data traffic. This difference is kept constant independently of the value of the arrival rate $\lambda$.

Fig. 22 depicts the queueing cost for signalling and data traffic for different values of IMS arrival rates $\lambda$. More specifically, the labels $C_{q\_sig}$ and $C_{q\_data}$ denote the values for the $C_{\text{queue}}$ and the $C_{\text{queue}}$ respectively. It can be observed that the queueing cost for signalling IMS traffic is significantly higher than the queueing cost for IMS data traffic. As the value of the arrival rate $\lambda$ increases the difference between the signalling and the data IMS traffic decreases.

Fig. 23 depicts the queueing cost for signalling and data traffic for different values of IMS arrival rates $\lambda$. More specifically, the labels $C_{q\_sig}$ and $C_{q\_data}$ denote the values for the $C_{\text{queue}}$ and the $C_{\text{queue}}$ respectively. As it was expected the queueing cost for signalling IMS traffic is significantly higher than the queueing cost for IMS data traffic. As the value of the arrival rate $\lambda$ increases the difference between the signalling and the data IMS traffic decreases.
Fig. 23 depicts the effect of varying IMS arrival rate $k$ on the signalling cost. As it can been seen from the figure both the transmission signalling cost and the transmission processing cost increase linearly with the increasing value of $k$. In addition, the queueing signalling cost also increases with the increasing value of $k$.

5.2.3. WiMAX-WLAN

In this section, we present the numerical results for our proposed architecture in the case of a user belonging to a WiMAX is trying to communicate with a user belonging to WLAN.

Fig. 24 depicts the transmission cost and the processing cost for signalling and data traffic for different values of IMS arrival rates $k$. More specifically, the labels $C_{t_{\text{sig}}}$ and $C_{t_{\text{data}}}$ denote the values for the $C_{\text{sig}}^{\text{trans}}$ and the $C_{\text{data}}^{\text{trans}}$ respectively and the labels $C_{p_{\text{sig}}}$ and $C_{p_{\text{data}}}$ denote the values for the $C_{\text{sig}}^{\text{proc}}$ and the $C_{\text{data}}^{\text{proc}}$ respectively. As it was expected the transmission cost for signalling IMS traffic is higher than the transmission cost for IMS data traffic. This difference is increased with the value of increasing arrival rate $\lambda$.

Fig. 25 depicts the queueing cost for signalling and data traffic for different values of IMS arrival rates $k$. More specifically, the labels $C_{q_{\text{sig}}}$ and $C_{q_{\text{data}}}$ denote the values for the $C_{\text{sig}}^{\text{queue}}$ and the $C_{\text{data}}^{\text{queue}}$ respectively. It can be observed that the queueing cost for

![Figure 25. Queueing cost versus different IMS arrival rates $\lambda$.](image)

![Figure 26. Signalling cost versus different IMS arrival rates $\lambda$.](image)

![Figure 27. Transmission and processing cost versus different IMS arrival rates $\lambda$.](image)

![Figure 28. Queueing cost versus different IMS arrival rates $\lambda$.](image)

![Figure 29. Signalling cost versus different IMS arrival rates $\lambda$.](image)
signalling IMS traffic is significantly higher than the queuing cost for IMS data traffic. As the value of the arrival rate \( \lambda \) increases the difference between the signalling and the data IMS traffic decreases.

Fig. 26 depicts the effect of varying IMS arrival rate \( \lambda \) on the signalling cost. As it can be seen from the figure both the transmission signalling cost and the transmission processing cost increase linearly with the increasing value of \( \lambda \). In addition, the queuing signalling cost also increases with the increasing value of \( \lambda \).

5.2.4. UMTS–WLAN

In this section, we present the numerical results for our proposed architecture in the case of a user belonging to a UMTS network. A UMTS-WLAN network is trying to communicate with a user belonging to WLAN.

Fig. 27 depicts the transmission cost and the processing cost for signalling and data traffic for different values of IMS arrival rates \( \lambda \). More specifically, the labels \( C_{\text{sig}} \) and \( C_{\text{data}} \) denote the values for the \( C_{\text{trans}} \) and the \( C_{\text{data}} \) respectively and the labels \( C_{\text{sig}} \) and \( C_{\text{data}} \) denote the values for the \( C_{\text{trans}} \) and the \( C_{\text{data}} \) respectively. As it was expected the transmission cost for signalling IMS traffic is higher than the transmission cost for IMS data traffic. This difference is increased with the value of increasing arrival rate \( \lambda \). As it was seen from the figure the processing cost for signalling IMS traffic is more than 11 times higher than the processing cost for IMS data traffic. A difference that is kept constant independently of the value of the arrival rate \( \lambda \).

Fig. 28 depicts the queueing cost for signalling and data traffic for different values of IMS arrival rates \( \lambda \). More specifically, the labels \( C_{\text{sig}} \) and \( C_{\text{data}} \) denote the values for the \( C_{\text{queue}} \) and the \( C_{\text{queue}} \) respectively. It can be observed that the queueing cost for IMS traffic is significantly higher than the queueing cost for IMS data traffic. As the value of the arrival rate \( \lambda \) increases the difference between the signalling and the data IMS traffic decreases.

Fig. 29 depicts the effect of varying IMS arrival rate \( \lambda \) on the signalling cost. As it can be seen from the figure both the transmission signalling cost and the transmission processing cost increase linearly with the increasing value of \( \lambda \). In addition, the queuing signalling cost also increases with the increasing value of \( \lambda \).

6. Conclusion

In this paper an interworking model that integrates a WiMAX network, a UMTS network and a WLAN is proposed in an IMS compatible architecture. Our primary focus for the proposed architecture was to replace the RAN part of the UMTS network with a WiMAX network and to place an IMS core on top of both technologies to manage sessions. This novel approach was driven by the fact that the WiMAX if it is interworked with the already established 3G cellular networks (e.g. UMTS), it is foreseen that it will form an important part of a future 4G network. Using a cost model we evaluated the performance of our proposed architecture and successfully validated its concept.

IMS networks are still in an ongoing activity with the industry and the research community to constantly trying to solve open issues concerning session control, authorization, authentication, Quality of Service (QoS), charging, personal mobility, etc. and extend IMS beyond 3G towards the evolution of a seamless universal next generation wireless network. Seamless mobility support is from the most critical research issues and its standardisation will be the basis to provide uninterrupted wireless services to mobile users in such a heterogeneous network environments.

Appendix A

A.1. WiMAX-WiMAX

The transmission cost for the delivery of the IMS signalling traffic can be given by

\[
C_{\text{trans}}^{\text{sig}}(\lambda) = \left( 2 \times \mu_{\text{service}} + \mu_{\text{result}} + 2 \times d_{\text{cscf}} + d_{\text{sig}} + d_{\text{data}} + d_{\text{trans}}/\text{trans} \right)
\]

And the transmission cost for the delivery of the IMS data traffic can be given by

\[
C_{\text{trans}}^{\text{data}}(\lambda) = \left( 2 \times \mu_{\text{service}} + \mu_{\text{result}} + 2 \times d_{\text{cscf}} + d_{\text{trans}}/\text{trans} \right)
\]

The processing cost for the delivery of the IMS signalling traffic can be given by

\[
C_{\text{proc}}^{\text{sig}}(\lambda) = 22 \times C_{\text{BSC}1} + C_{\text{ANS} + \text{GW}1} + C_{\text{UTRAN} + \text{GW1}} + C_{\text{WiMAX} + \text{GW1}} + C_{\text{PCSCF}1} + C_{\text{CSCF}1} + C_{\text{PCSCF}2} + C_{\text{CSCF}2} + C_{\text{HSS}}
\]

and the processing cost for IMS data traffic between two WiMAX networks is given by:

\[
C_{\text{proc}}^{\text{data}}(\lambda) = 2 \times C_{\text{BSC}1} + 2 \times C_{\text{ANS} + \text{GW}1} + 2 \times C_{\text{WiMAX} + \text{GW1}} + 2 \times C_{\text{PCSCF}} + 2 \times C_{\text{CSCF}} + 2 \times C_{\text{HSS}}
\]

The queueing cost for the delivery of the IMS signalling traffic can be given by

\[
C_{\text{queue}}^{\text{sig}}(\lambda) = 2 \times E[C_{\text{BSC}1}] + 2 \times E[C_{\text{HSS}}] + 2 \times E[C_{\text{WiMAX} + \text{GW1}}] + 2 \times E[C_{\text{PCSCF}1}] + 2 \times E[C_{\text{CSCF}1}] + 2 \times E[C_{\text{CSCF}2}] + 2 \times E[C_{\text{HSS}}]
\]

and the queueing cost for the delivery of the IMS data traffic can be given by

\[
C_{\text{queue}}^{\text{data}}(\lambda) = 2 \times E[C_{\text{BSC}1}] + 2 \times E[C_{\text{HSS}}] + 2 \times E[C_{\text{WiMAX} + \text{GW1}}] + 2 \times E[C_{\text{PCSCF}1}] + 2 \times E[C_{\text{CSCF}1}] + 2 \times E[C_{\text{CSCF}2}] + 2 \times E[C_{\text{HSS}}]
\]

A.2. WiMAX–WLAN

The transmission cost for the delivery of the IMS signalling traffic can be given by

\[
C_{\text{trans}}^{\text{sig}}(\lambda) = \left( 2 \times \mu_{\text{service}} + \mu_{\text{result}} + 11 \times d_{\text{trans}} + 11 \times d_{\text{data}} + 11 \times d_{\text{trans}} + d_{\text{trans}}/\text{trans} \right)
\]

And the transmission cost for the delivery of the IMS data traffic can be given by

\[
C_{\text{trans}}^{\text{data}}(\lambda) = \left( 2 \times \mu_{\text{service}} + \mu_{\text{result}} + 11 \times d_{\text{trans}} + 11 \times d_{\text{data}} + 11 \times d_{\text{trans}}/\text{trans} \right)
\]

The processing cost for the delivery of the IMS signalling traffic can be given by

\[
C_{\text{proc}}^{\text{sig}}(\lambda) = 11 \times C_{\text{BSC}} + 11 \times C_{\text{ANS} + \text{GW}} + 11 \times C_{\text{WiMAX} + \text{GW}} + 11 \times C_{\text{PCSCF}} + 22 \times C_{\text{PCSCF}1} + 22 \times C_{\text{CSCF}} + 2 \times C_{\text{HSS}} + 11 \times C_{\text{trans}}/\text{trans}
\]

and the processing cost for IMS data traffic between two WiMAX networks is given by:

\[
C_{\text{proc}}^{\text{data}}(\lambda) = 2 \times C_{\text{BSC}} + 11 \times C_{\text{ANS} + \text{GW}} + 11 \times C_{\text{WiMAX} + \text{GW}} + 11 \times C_{\text{PCSCF}} + 22 \times C_{\text{PCSCF}1} + 22 \times C_{\text{CSCF}} + 2 \times C_{\text{HSS}} + 11 \times C_{\text{trans}}/\text{trans}
\]
and the processing cost for IMS data traffic between the WiMAX and the WLAN network is given by:

\[
C_{\text{proc}} = C_{\text{BS}} + C_{\text{ASN-CGW}} + C_{\text{WMAX-CGW}} + C_{\text{PDG}} + 2 \times C_{F} + C_{\text{CSCP1.2}} + 2 \\
* C_{\text{S}} + C_{\text{WAC}} + C_{\text{ARC}} + C_{\text{AP}}
\]

The queueing cost for the delivery of the IMS signalling traffic can be given by

\[
C_{\text{queue}} = 11 \times E[n_{\text{BS}}] + 11 \times E[n_{\text{ASN-CGW}}] + 11 \times E[n_{\text{WMAX-CGW}}] \\
+ 11 \times E[n_{\text{PDG}}] + 22 \times E[n_{\text{F}-\text{CSCP1.2}}] + 22 \times E[n_{\text{F}-\text{CSCP1.2}}] \\
+ 4 \times E[n_{\text{CP}}] + E[n_{\text{BS}}] + 11 \times E[n_{\text{WAC}}] + 11 \times E[n_{\text{ARC}}] \\
+ 11 \times E[n_{\text{AP}}]
\]

and the queueing cost for the delivery of the IMS data traffic can be given by

\[
C_{\text{queue}} = E[n_{\text{BS}}] + E[n_{\text{ASN-CGW}}] + E[n_{\text{WMAX-CGW}}] + E[n_{\text{PDG}}] + 2 \times E[n_{\text{F}-\text{CSCP1.2}}] \\
+ 2 \times E[n_{\text{F}-\text{CSCP1.2}}] + E[n_{\text{WAC}}] + E[n_{\text{ARC}}] + E[n_{\text{AP}}]
\]

References