Submitted to Computer Communications, Elsevier, in December 2004

Seamless Continuity of PS-Services in WLAN/3G Interworking

PAULO PINTO, LUIS BERNARDO
Universidade Nova de Lisboa, Lisboa, Portugal

PEDRO SOBRAL
Universidade Fernando Pessoa, Porto, Portugal

Abstract – The seamless continuity of services between 3G networks and WLANs will give users the feeling of a common environment towards the wireless technology. Three main aspects must be considered to obtain seamless continuity: an enabling interworking architecture, fast inter-system handovers (they must be fast enough in terms of human senses), and, in the case of real-time services, a similar quality of service (QoS) in both networks. This paper focuses on the two first issues. It presents an interworking architecture based on a 3G core-level integration of the WLANs. The GPRS network is available all the time forming a primary network, and WLANs are used as a complement when they are available. The switching times between networks are very low and the transitions are lossless. Our proposal does not disrupt with the current 3GPP standardization efforts making it viable in a medium time frame. This paper presents an overview of the architecture, describes the relevant events in the switching process (where the authentication and authorization procedures have an important role), and gives simulated values for the switching times.

Keywords: 4G networks; interconnection 3G/WLAN; seamless continuity of services

1. Introduction

The integration of wireless LANs (WLANs) and third-generation (3G) mobile networks, such as Global System for Mobile Communication/General Packet Radio Service (GSM/GPRS) and Universal Mobile Telecommunications Systems (UMTS) is opening up a broad range of possibilities due to the successful deployment of both technologies. This range begins with low-level issues of radio access integration until fulfilling one of the characteristics identified by the Wireless World Research Fund, namely the definition of a component-based architecture that will enable users, application developers, service and content providers, and manufacturers to efficiently and flexibly create new services [1]. The main subject of this paper is dedicated to the first issue but having the second in mind.

The interconnection of 3G systems with WLAN in general is being defined by 3GPP in a series of 6 scenarios [2]. The various scenarios describe an increasing level of integration between the two systems: (1) common billing; (2) 3G based access control, (3) access to 3G packet-switched (PS) services, (4) access to 3G PS services with service continuity, (5) the same as (4) with seamless continuity, and (6) access to 3G circuit-switched (CS) services with mobility.

Currently, [3] describes the architecture for scenarios 2 and 3. Its approach to scenario 3 is to interconnect both systems at IP-level following an interconnection architecture known as *loosely coupled* approach [4]. Although [3] provides an answer to scenario 3 there is the feeling that higher scenarios raise low-layer considerations [5].

In this paper we present an architecture that can handle scenarios 4 and 5 based on a *core-level coupling* of the systems. Extensions of this architecture might handle scenario 6 as well but this is out of the scope of the paper.

The paper begins with a description of the *core-level approach* introducing the innovative aspects of the architecture. Section 4 presents the authentication, authorization and accounting (AAA) procedures. They are critical to the handover times. Our AAA procedures follow very closely the 3GPP standard (which is already at an advanced state). However, they show a different perspective, not so 3G centric, for the inter-relation between the networks. The application of our architecture to scenarios 3, 4, and 5 precede the presentation of the simulations results and the conclusions.

2. Initial Assumptions

Throughout the paper we assume that mobile stations (MS) will have two (or more) wireless interfaces that can work simultaneously. We also assume that the security control provided by the smart card called UMTS Subscriber Identity Module (USIM) and the global roaming agreements amongst 3GPP

operators form the largest operational AAA system in the world to date. This system could be used by organizations not interested on setting up and manage a system of their own. Finally, we assume that WLANs are owned by any business organizations that rely on the 3G operators for just authentication (therefore excluding authorization). The organizations must trust each other up to the point of user identification and validation but remain independent in other aspects (for instance, user data directed to one network must not be understood by the other). A good example of such an organization is a University. It has already a WLAN installed and has a community that can use the local facilities for free at the sole discretion of the University services; and visitors that can use the WLAN to access 3G systems but not local services. For each access to the 3G system the University should be paid a fee.

3. Overview of the architecture

In our architecture the user is always connected to the GPRS network. Any use of a WLAN is complementary. There are two major consequences: all the control features (paging, compulsory registration update, user location, etc.) remain as they are today and are only needed in the GPRS network; and there is no need for inter-system vertical handovers such as they are defined in [6]. A similar approach of a primary network was taken by MIRAI [7]. In their case there is a controlling network (not for data) that has mainly the controlling functionality of the GPRS (with some add-ons such as choosing a data RAN – Radio Access Network). Our approach of having the GPRS as the primary network makes sense for two main reasons: if users want to use WLANs to interconnect to the 3G systems they are obviously 3G users and have access to GPRS; and GPRS is already ubiquitous. This section provides an overview of the architecture. A thorough description with state-of-the-art comparison and some discussion can be found in [8].

A WLAN RAN is a set of islands. Each island is formed by a set of cells and is controlled by an Island Manager (IM). Islands do not cover the entire space (i.e. there will be dark areas). All islands of a certain technology are seen by the primary network as a **Hotspot Network** (HN) – a secondary network. The IM has the functionality of an access gateway to the 3G system, AAA server for the WLAN, and AAA proxy towards the 3G system.

A user is connected to the GPRS network and can be connected to other HN networks simultaneously. Each HN supports the notion of a session (i.e. IEEE 802.11 has one, HiperLan has another, etc.). A session is a high level concept to allow the maintenance of context during disconnection periods when the user is moving in a dark area of a certain HN. As the GPRS is always active this concept of session is useful, and is not seen in other systems. For instance, the user began a 802.11 session at the airport, took a taxi to a hotel, and when he is in the hotel, the same session is still on using the WLAN infrastructure of the hotel (it is assumed that both have agreements with the users' 3GPP operator). On the way from the airport to the hotel, if the user needs to be contacted in the context of that session the primary network can be used.

Figure 1 shows the architecture for the data traffic (no access control, billing, etc.). The new components are the HNAC (*Hotspot Network Area Controller*) which controls one (or more) island, and the GHSN (*Gateway Hotspot network Support Node*) which is responsible for context management and Internet access (here "context" has a similar meaning as used for the

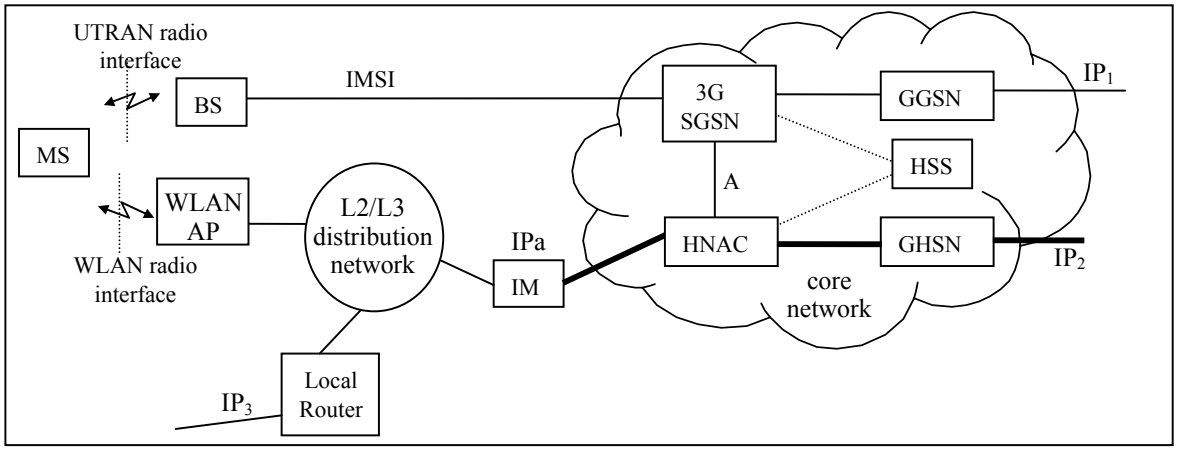

Figure 1. Data traffic paths in the hybrid network

PDP context in GPRS). The thicker lines belong to the core but they are not present in the current 3G core. All the high speed traffic goes through them not overloading the current 3G infrastructure.

Our *core-level approach* to wireless systems integration has subtle but important differences when compared to the *tightly approach* referred in the literature [4] – for instance, the HNAC allows the introduction of the user in the core as a first class member (similar to the UTRAN access); or the 3G interfaces do not need to be disclosed to the WLAN. See [8] for further details.

The solution in [3] is not directly comparable to our work because they connect both networks at IP level. In their system a component is also installed in the core – PDG (*Packet Data Gateway*). The PDG allows for the introduction of the user into the system at the IP level providing IP access to 3G services. It is more comparable to our GHSN than to our HNAC. Furthermore, the WLAN traffic goes directly into the core in our solution whereas in [3] it goes via an external IP network to the PDG.

As shown in figure 1, applications can use one out of three IP addresses: IP_1 address uses the standard GPRS; IP_2 address uses the HN network; and IP_3 address uses the local internet access of the LAN. Applications just choose the address related to the network they want to use. In the sequel it will become clear how the data and control paths are established, and the different communication possibilities between the core and the MS.

The GPRS part of the system is conform to the standard: the MS has its identification at core level in the form of the IMSI (*International Mobile Subscriber Identity*) and the attachment procedure for GPRS is the standard one (with temporary identifiers). In the GPRS part an IP session can be established via the GGSN (PDP context), having the routable address IP_1.

The WLAN part has two authentication phases (fig. 2). The WLAN authentication gives access to local services (including direct Internet access). The MS is given a local IP address (IPa), and a routable IP address IP_3. Traffic using IP_3 uses the Local Router (fig. 1). The 3G authentication gives access to the 3G core via WLAN. The MS is identified at the core by IPa, instead of the IMSI. When it creates a context with the GHSN it is given the address IP_2 for external Internet access. When the user moves from one island to another the IPa changes but the IP_2 remains the same.

An important feature in our architecture is the connection between the HNAC and the SGSN (interface A in figure 1). It allows each of these components to communicate with the MS via the other one. It can be used, for instance, to maintain IP sessions in HN dark areas; to access SMS (*Short Message Service*) via WLAN, etc. – the MS identified by the IMSI can be contacted via UTRAN (*Universal Terrestrial Radio Access Network*) using the IMSI, or via WLAN using the IPa.

In terms of data path GTP-U (*GPRS Tunneling Protocol – for User Plan*) tunnels are used. Currently in GPRS a tunnel is established between the GGSN and the SRNC (*Serving Radio Network Controller*). In our architecture this tunnel is replaced by two half tunnels: one from GGSN to SGSN and another from SGSN to SRNC (and similarly for the WLAN – one from GHSN to HNAC and another from HNAC to IM). This half tunnel definition is pretty much a return to the first standardization phase of GPRS. The reason for the partition is to allow the SGSN (or HNAC) to use other radio networks through interface A.

4. Associations and Context Creation

Before a new secondary radio access becomes ready to be used there are two operations that take some time: security associations and QoS guarantees (for real-time services). The latter one is out of the scope of this paper. The former is probably longer and [3] contains a very clear definition of the process that we will follow very closely here. The major change here is a greater autonomy of the WLAN owner to authorize its users. [3] is, naturally, very 3G centric.

Figure 2 shows the four main phases. We assume that we are using an IEEE 802.11 WLAN.

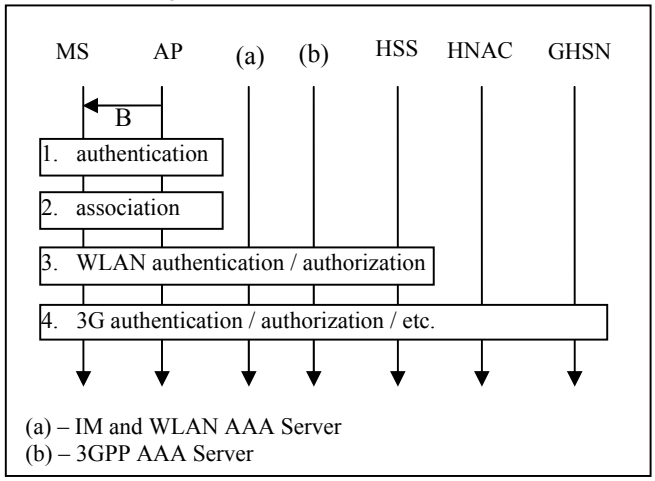

Figure 2. Four phases for AAA procedures

After a Beacon frame is received, the MS authenticates using the standard open-system authentication. This is a very weak procedure just to give free access to some trivial local services

(announcements, etc.). The second phase is an association to the SSID in order to exchange data packets. These are standard procedures and the packets involved are shown in figure 3.

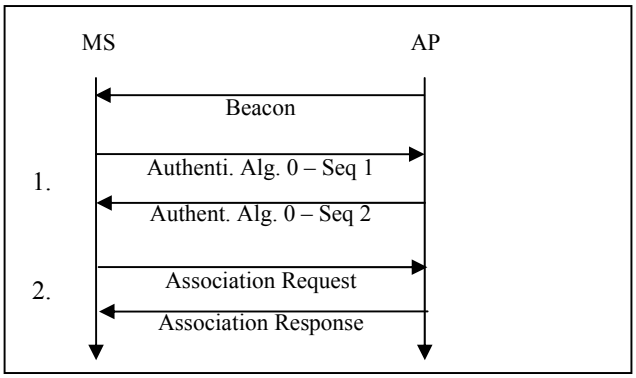

Figure 3. Open-system Authentication and Association

The third phase is initiated by the MS and the purpose is to identify itself and get authorization to use the local facilities. This phase is the one that deviate the most from [3]. We use the AKA method [9] supported by the EAP (*Extensible Authentication Protocol*) mechanism [10]. Figure 4 shows the various packets. The MS initiates an authentication procedure selecting a 3G PLMN (*Public Land Mobile Network*). The way to identify the PLMN is by using a network address identifier (NAI) in the form of *username@realm* (the *username* is the user identification and *realm* is a domain name [11] identifying the PLMN). We assume that the WLAN has an agreement with the user's PLMN. If it has not, an advertisement and a selection phases have to exist (see [3]). Another aspect we do not treat here is the differences between Home and Visiting PLMNs (again, see [3]). The IM behaves as an AAA proxy relaying the information to the 3GPP AAA Server (the HNAC, for instance). The outcome of the operation is an indication via the secure channel between the IM and the 3GPP AAA Server that the MS is what it claims to be. A possible piece of information can be the MSISDN (*Mobile Subscriber ISDN Number*) because it is not compromising to the 3G system. This is conveyed in the EAP-Success packet just before point 1. At point 1 the IM consults its data base and two things can happen: the user is a member of the community (student, teacher, etc.), or he is not.

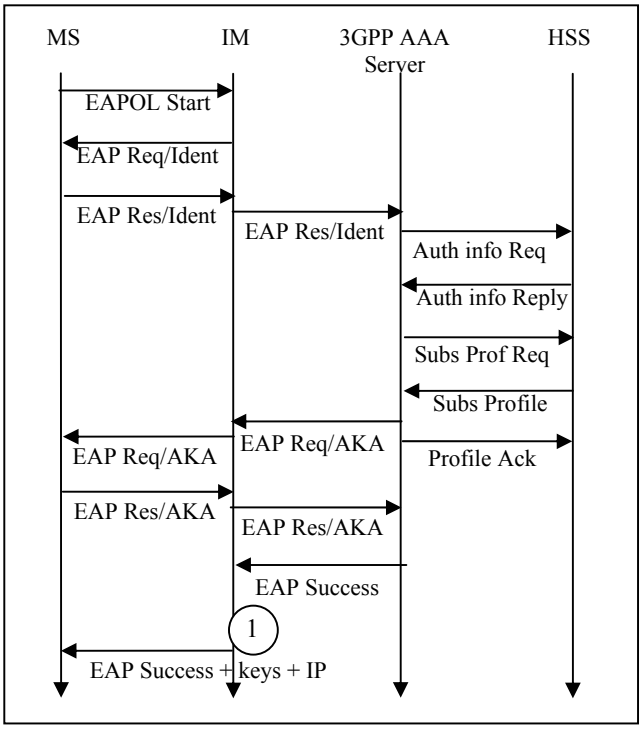

Figure 4. WLAN user authentication and authorization

If he is a member, the IM provides the MS with IP addresses IPa, IP address IP_3, the IP address of the HNAC to pursue authentication if the user wants to use the so called "WLAN 3GPP Access", and session keys for the purpose of radio interface integrity protection and encryption in the WLAN session. As it was stated before, IP_3 is a routable address that enables the MS to use all the services of the local network.

If he is not a member (e.g., he is a visitor at the University) the IM simply indicates the IPa and the IP address of the HNAC. This MS can use the WLAN to reach the 3G system but cannot use local services.

Note that the authorization decision to use local facilities is performed by the University and the 3G system is only used to authenticate users, making the overall WLAN AAA management in the University simpler.

Every user, recognized or not by the University, can use the WLAN to access the 3G system – it is now up to the 3G operator to allow it or not. This is the purpose of the last phase showed in figure 5. The MS initiates the procedure requesting an attach procedure to the HN. If the user was previously attached and went through a dark area, a re-attach procedure should have been done instead. The packet starts a similar procedure as before.

We assumed here that the HNAC behaves as AAA server getting information from the HSS (*Home Subscriber Service*). The HNAC issues the AKA challenge and if the response is valid it creates a context with GHSN the same way a context is created in GPRS with the GGSN. The final packet has the indication of success, session keys to be used by the MS without the knowledge of the IM or WLAN, temporary identification, and the IP_2 address to be used by the MS.

Phase 3 and phase 4 are very similar but they must both exist to keep the two systems as independent as

possible (for instance, a user might not want to have "WLAN 3GPP Access", not performing phase 4).

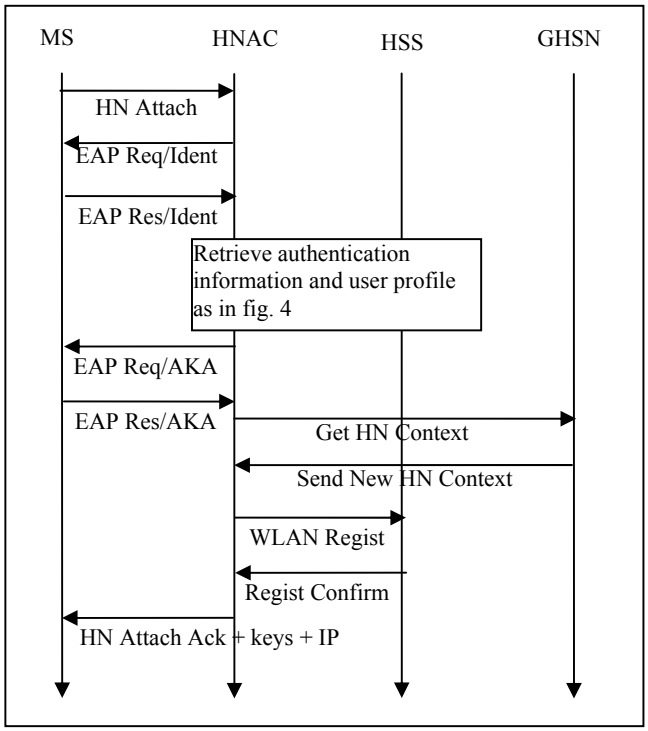

Figure 5. 3G user authentication and authorization

5. Interconnection of the Different Systems

If the user gets authorization to use the three networks the three possible data flows together with the main components involved are depicted in figure 6(a). The interface A between the SGSN and the HNAC allows other interesting scenarios. When the user is in an HN dark area communication using IP_2 can still be done using the GPRS, as showed in part (b). Part (c) shows the case when the user is under HN coverage and decides (or the network decides) that an SMS, for instance, can be delivered via WLAN. Note that the control part (paging, etc.) uses always the GPRS network.

Figure 7 shows the protocol stack used to manage the communication and these various possibilities. The full stack exists in the MS and HNAC and the three lower layers (up to IP) exist in the SGSN. The session control and application layers are part of the component-based architecture referred in the introduction and allow, among other things, to maintain user sessions between WLAN contacts. The focus in this paper is on the lower layers. The IP layer can be working with one of three IP addresses: IP_1 and the communication is with SGSN, IP_2 and the peer is the

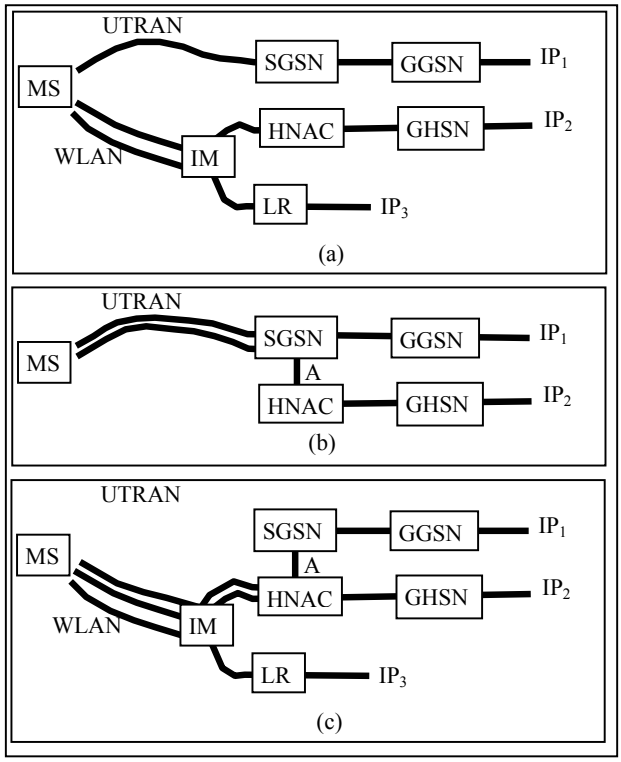

Figure 6. Different possibilities for the data flows

HNAC, or IP_3 and the peer is the IM. The Delivery Service (DS) is used in the first two cases. The DSs in the various core components cooperate to offer alternative paths for data packets – e.g., the DS in

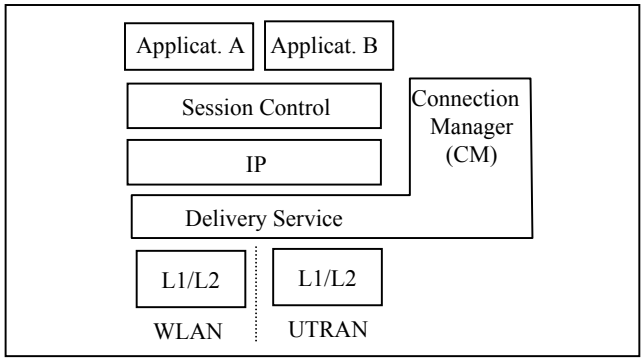

Figure 7. Protocol Stack at the MS/HNAC/SGSN

HNAC can give a packet to the DS in the SGSN to be delivered to the MS. Between the MS and HNAC it offers a confirmed service of packet delivery because the WLAN path can fail in dark areas (it is assumed that the UTRAN is ubiquitous). When the WLAN path fails there is an indication upwards to the service or application (similar to a control plane indication) to inform it. The application is free to keep sending data or pause until an indication of availability is received, meaning that the user reappeared at another HN island.

Each time data is sent for delivery by the service or application it can carry a control indication stating the radio path to be used. The DS will use this information to deliver the packets. If no control indication exists (legacy applications, for instance) then the default radio path is chosen (UTRAN for IP_1 and WLAN for IP_2). In the case of the WLAN, if the path is not available the UTRAN is used automatically. In summary, applications can stop sending data if they know the MS is out of coverage, but any data sent will be delivered.

For services that do not use the IP stack the choice of the radio path is performed by the core identification of the MS – either the IMSI or the IPa.

As stated above the WLAN part of the DS is confirmed to detect when users leave WLAN coverage. If an acknowledgement of a packet is not received at the DS in the HNAC it forces a kind of handover. The packet that failed is sent via SGSN and the originator is signaled that the user is no longer reached by WLAN (legacy applications are not able to catch these signals, obviously).

When a user attaches to an island its profile at the HSS is updated. Entities delivering 3G services, such as SMS, can query the HSS for information and decide to use the WLAN instead of the UTRAN. The HNAC can also run an event service to notify any other core entity that a particular MS entered in an island.

Note that no information is ever lost in handovers because the core components will transmit the packet again through another interface.

A final point refers to the communication at DS level between the HNAC and the MS. There are several possibilities: one is to establish an IP tunnel (not shown in the protocol stack in figure 7). The DS in HNAC establishes an IP-tunnel directly to the MS using the IPa address; another possibility is to establish an IP-tunnel to the IM and use VLANs after that (in this case IPa is just an identifier); still another possibility is to use layer 2 switching all over.

6. Use of the Architecture for scenario 3

The option in [3] was to "*provide WLAN MSs with IP bearer capability to access PS based services which are provided by PLMN*". Our approach is completely different – the WLAN MSs have the capability to join the 3G core and access any PS service at core level, and not at IP level. However, it is interesting to see how PS services can be accessed using our architecture. We will see that some procedures defined in [3] are not needed and the whole process becomes much simpler. Figure 8, taken from [3] shows the necessary components for the case of SMS (*Short Message Service*). The IP-SM-Gateway:

- must maintain an association between the users' MSISDN and its IP address;
- must interface the GMSC behaving as an SGSN or MSC;
- must support registration and authentication of the MS for SMS services;
- must support security associations between the MS and itself; and
- communicates with the MS using IP based protocols.

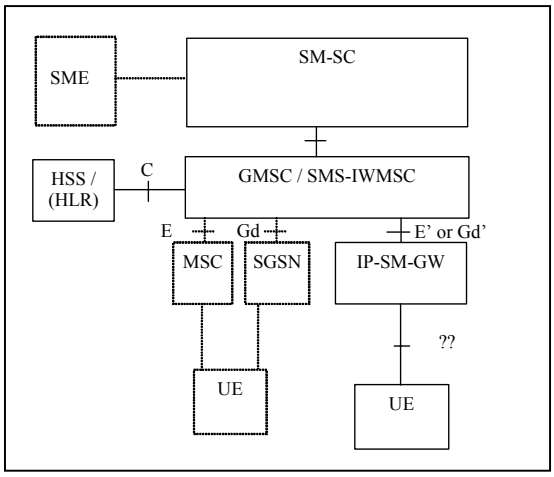

Figure 8. Architecture for SMS support with an IP terminal

In our architecture the SGSN is contacted by the MS (via WLAN) and the SMS is just delivered. There are, of course, changes in the current logic of the components (SGSN and MS) to make them aware of different radio possibilities of delivery but there are no extra authentications or registrations. These changes are also needed in the architecture of figure 8 (they were left for further study).

7. Interworking Architecture for scenarios 4 and 5

With our architecture, scenarios 4 and 5 of [2] are indistinguishable because new RANs take some time to get ready but the activation is instantaneous (strictly speaking in scenario 5 there is also some bandwidth and delay guarantees that must be satisfied, but this is out of the scope of this paper).

There are two situations to analyze: (a) Find Coverage – a user is connected to the UTRAN and a WLAN becomes active, and (b) Lose Coverage – a user using a WLAN walks out of coverage and the UTRAN has to be used.

In the first situation the user is running a service/application (using either the IP_1 or IP_2 addresses) and the terminal receives a Beacon frame. The situation is depicted in figure 9. Since the moment the user enters the WLAN cell until it receives the Beacon it lasts Δt1 seconds. The procedures described in section 4 are then performed and will last Δt2 seconds. Alternatively, a re-attach procedure would have been performed if the user had already done an attach procedure previously (the elapsed times are similar). In either case, once the procedures are done there is an indication from the DS in the HNAC upwards to the applications and to the DS in the SGSN signaling that the connection is ON. Services/applications using either the SGSN or the HNAC can deliver their packets through the WLAN. So, the continuity of the services is seamless. It is just the time from the reception of the indication and the delivery of the packet. Both Δt1 and Δt2 are not in the critical time path because the user is using the UTRAN. An interesting time interval is how long it takes since the Beacon frame is received until the first packet arrives to the MS via WLAN.

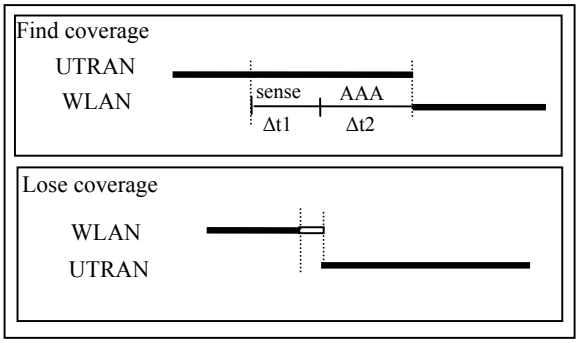

Figure 9. Handovers between RANs

In the second situation the user walks out of coverage without making a disassociation (the worst and probably the most common case). The DS in the HNAC transmits a packet and does not receive an acknowledgment. At that moment it declares the interface as OFF, signals upwards, and also to the DS in the SGSN. If the packet belongs to an application using the HNAC, and the application persists on delivering it, the packet goes to the DS of the SGSN for delivery. If the packet belongs to a service using the SGSN it is transmitted back to the DS in the SGSN and delivered. Our simulations measured the duration between the first delivery of a packet that was going to fail and the moment the MS receives that same packet via UTRAN.

The retransmission timeout for the WLAN is the critical time to consider if we want the change of networks to be seamless. It should be noted, however, that its value can be short because it is a low-level timer. A failure of a single packet turns the link to OFF and triggers the recovery described in the previous paragraph.

After a failure and a declaration of the link to OFF, a WLAN disconnection procedure for the MS must be initiated. But the failure could be due to transient disturbances and the MS might still be contacted after a while initiating a re-attachment procedure. To avoid this kind of instability, after the link is declared OFF the DS in the HNAC tries to send k echo packets to the DS in the MS. If they fail the user has moved away and the disconnection procedure is initiated. If there are replies the link comes back to ON again and indications are sent to the DS in the SGSN and upwards in the HNAC.

The disconnection procedures in our architecture are much lighter than in the approach followed in [3]. The tunnel from the GHSN to the HNAC, for instance, is not disconnected because the application can still use the UTRAN. The main operation is the update of the WLAN user status at the HSS (applications are already aware because of the signaling), and the disconnection of the tunnel between the DS in the HNAC and the DS in the MS/IM (if it exists).

8. Simulation Results

We simulated the exchange of packets using the ns-2 with add-ons for PCF (Point Coordination Function) in 802.11 [12], and for UMTS [13]. Our choice of PCF was to consider a longer delay due to having to wait for the time slot, and to use a mode that can provide certain resource guarantees. PCF was never popular but an equivalent mode is appearing in 801.11e.

Due to incompatibilities in the address types of both add-ons, simulations had to run separately but the correspondent times for switching between simulators were registered for a complete story. The radio interface was DSSS (*Direct Sequence Spread-Spectrum*) with a bandwidth of 10Mbps in the band of 914 MHz. This band is a ISM (Industrial, Scientific, Medical) window in USA and the ns-2 uses it. Taking into account the size of our packets, the difference between using this window or the 2,49 GHz window, or between using 10 Mbps or 11 Mbps is irrelevant. The radio propagation model was a Free-space attenuation at near distances and two ray ground approximation at far distances. For the cell dimension configuration the default values were used.

In the PCF setting agents were created in the ns-2 to represent the real components as shown in figure10. The link between the IM and the HNAC was the longer one (around 30 Km) with a delay of 10 ms. All the

other wired links had a delay of 0.1 ms. The bandwidth on all wired links was 10 Mbps (again, this is not so relevant because the traffic is low). To simulate data

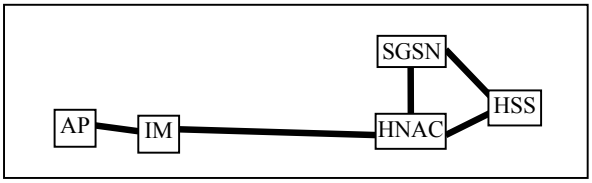

Figure 10. Components in the ns-2 setting

base accesses a value of 20 ms was used. There are four of these periods in the situation of find coverage (these periods could be reduced if the AAA server and the HNAC were the same component). The timeout value to recover from a failed packet from HNAC to MS via WLAN was 40 ms.

Table 1 shows the values obtained. Cases labeled as 1 are services running over SGSN (e.g. SMS). Cases labeled as 2 are new applications running over HNAC. There are some minor differences because for instance in the situation of lose coverage for case 1 the packet has to be sent back to SGSN. In all other situations and cases only signaling packets travel from HNAC to SGSN. Basically the simulations proved that these differences can be reduced to packet dimensions and are very small (in one case the PCF slots compensate them entirely).

In the situation of find coverage the first line shows the time between the moment the EAPOL Start packet was sent (start of the first phase), and finished when the attach reply is received by the MS. The second line shows the real switching time:

- for case 1 it starts when the SGSN receives a signal indicating that the WLAN via is ON and finishes when the MS receives a packet via HNAC (we assumed that a data packet was immediately available to be sent);
- for case 2 it starts when the HNAC receives the attach-reply (a packet is already there to be sent) and finishes when the MS receives the data packet.

Find Coverage		Lose Coverage	
Case 1	Case 2	Case 1	Case 2
216.5 ms	216.5 ms	40.5+56.0	40.2+56.0
16.7 ms	16.7 ms		

Table 1. Values for handovers

In the situation of lose coverage the time began when a packet that is going to fail was sent via WLAN and finished when the same packet was received by the MS via UTRAN. The table presents the partial values (WLAN + UTRAN).

As a first comment it is important to note that for the situation of find coverage the values of 216.5 ms are not in the critical path. The MS starts these procedures but is still communicating using the UTRAN (or other WLANs). The real switching time is 16.7 ms. Secondly, the overall times are very small and show that the architecture is viable. Thirdly, 37% of the preparation time in the situation of find coverage (216.5) is due to processing times (four times 20 ms). In some situations 20 ms can be too long and if the 3GPP AAA server is inside the HNAC half of the interactions with HSS could disappear. Lastly, 41% of the time in the situation of lose coverage is due to the timeout. This situation is the real critical one in this system but the overall time (less than 100 ms) is promising. Note however that this is the real critical situation in all systems [6], and our architecture behaves better due to the absence of a real vertical (fully inter-system) handover. In these type of handovers AAA procedures to the new RAN have to be done in the critical path.

9. Conclusions and further work

In this paper we have shown that seamless continuity of services and applications between 3G networks and WLANs can be achieved in a very easy way if a proper interworking architecture is considered. We consider a primary network and introduce HN management components in the 3G core. The system does not need inter-system vertical handovers because the user never leaves the primary network making the switching times very small.

The introduction of a new component in the core does not disrupt the standardization work done so far because it interacts with the existent components following the same behavior as the SGSN does today. The major modifications are a physical interface at the SGSN and an update of software to enable it to use the HNAC.

As issues for further work it is important to study which QoS parameters might be important to help in the decision of using a certain HN for a certain service; and which services/applications could be interesting to build on higher layers of the HNAC to manage the intermittent appearances of MS in WLAN islands.

Acknowledgments

The authors would like to thank João Reis and Bernardo Alves for their work in helping simulating the system.

References

[1] Lu, W., et al, “4G Mobile Communications: Toward Open Wireless Architecture”, IEEE Wireless Communication, v.11, pp 4-6, April 2004.

[2] 3GPP TR 22.934 v6.2.0, “Feasibility Study on 3GPP system to WLAN interworking (Release 6)”, Setp. 2003

[3] 3GPP TR 23.234 v6.1.0, “3GPP system to WLAN interworking; System description (Release 6)”, June 2004

[4] Salkintzis, A., et al., “WLAN-GPRS Integration for Next-Generation Mobile Data Networks”, IEEE Wireless Communication, v.9, pp 112-124, Oct. 2002.

[5] Salkintzis, A., “Interworking techniques and Architectures for WLAN/3G Integration toward 4G Mobile Data Networks”, IEEE Wireless Communication, v.11, pp 50-61, Jun. 2004.

[6] Steem, M., Katz, R., “Vertical Handoffs in wireless overlay networks”, Mobile Networks and Applications, v.3, pp 335-350, 1998

[7] Wu, G., “MIRAI Architecture for Heterogeneous Network”, IEEE Comm. Mag., pp 126-134, Feb 2002

[8] Pinto, P., Bernardo, L., Sobral, P., “UMTS-WLAN Service Integration at Core Network Level”, 3rd Europ. Conf. on Universal Multiservice Networks (ECUMN'04), LNCS, Springer-Verlag Heidelberg, Vol 3262/2004, Oct 04, DOI: 10.1007/b101785. A copy for the reviewers can be found in http://tele1.dee.fct.unl.pt/papers/ecumn04.pdf

[9] Arkko, J., Haverinen, H., “EAP AKA Authentication”, Internet Draft, draft-arkko-pppext-eap-aka-12.txt, April 2004

[10] Blunk, L., Vollbrecht, J., “PPP Extensible Authentication Protocol”, IETF RFC 2284, March 1998

[11] Mockapetris, P., “Domain Names – Implementation and Specification”, IETF RFC 1035, November 1987.

[12] Lindgren, A., Support for the PCF mode of IEEE 802.11 for ns-2.1b8, http://www.sm.luth.se/~dugdale/index/software.shtml/

[13] EURANE – Enhanced UMTS Radio Access Network Extensions for ns-2 home page, http://www.ti-wmv.nl/eurane/