INTERWORKING TECHNIQUES AND ARCHITECTURES FOR WLAN/3G INTEGRATION TOWARD 4G MOBILE DATA NETWORKS

APOSTOLIS K. SALKINTZIS, MOTOROLA

ABSTRACT

The intense wireless LAN standardization and R&D activities worldwide, combined with the recent successful deployment of WLANs, provide prime evidence that WLAN technology will play a key role in the fourth generation of mobile data networks. In this context, there is a strong need to integrate WLANs with 3G mobile data networks and develop hybrid mobile data networks capable of ubiquitous data services and very high data rates in strategic locations. This article addresses this need by proposing and discussing some novel architectures able to provide interworking between WLAN and 3G networks, and meet the requirements of the most common interworking scenarios. These architectures can enable 3G subscribers to benefit from high-throughput IP connectivity in hotspots and also to attain service roaming across several radio access technologies, such as IEEE 802.11, HiperLan/2, UTRAN, and GERAN.

INTRODUCTION

The recent evolution and successful deployment of wireless local area networks (WLANs) worldwide has yield a demand to integrate them with third-generation (3G) mobile networks, such as Global System for Mobile Communications/General Packet Radio Service (GSM/GPRS), Universal Mobile Telecommunications System (UMTS), and cdma2000. The key goal of this integration is to develop heterogeneous mobile data networks capable of supporting ubiquitous data services with very high data rates in hotspots. The effort to develop such heterogeneous networks, also referred to as fourth-generation (4G) mobile data networks, is linked with many technical challenges, including seamless vertical handovers across WLAN and 3G radio technologies, security, common authentication, unified accounting and billing, WLAN sharing (by several 3G networks), and consistent QoS and service provisioning.

In this article we deal with several of these challenges and propose technical solutions that can effectively address them. In particular, we propose and discuss specific WLAN/3G interworking techniques and architectures that can support common authentication, authorization, and accounting (AAA), WLAN sharing, consistent service provisioning, and so on. Our architecture is based on the requirements associated with some typical interworking scenarios, such as those specified in [1].

We establish a general WLAN/3G interworking model in which a WLAN can be shared by one or more 3G networks. In addition, we discuss how a WLAN can support several access control schemes in order to support the 3G WLAN clients as well as the legacy WLAN clients. We present the most common WLAN/3G interworking scenarios and briefly discuss their associated requirements. We focus on two interworking scenarios and propose detailed architectures for WLAN/3G interworking that satisfy their respective requirements. We illustrate the key operational aspects of these architectures by means of some message flow diagrams. Finally, we summarize with our concluding remarks.

INTERWORKING MODEL AND REQUIREMENTS

The general WLAN/3G interworking environment we assume is illustrated in Fig. 1. To avoid using abstract examples and enhance clarity, we further assume that each 3G public land mobile network (PLMN) is based on UMTS technology, and each WLAN is based on IEEE 802.11 [2] technology. However, most of the techniques and architectures described below are equally applicable to any other type of 3G and WLAN technology. Each WLAN broadcasts a single service set identifier (SSID), which basically serves as a WLAN identifier. Note that multiple SSIDs can be supported by an IEEE 802.11 WLAN, but only one is broadcast (see probe request/response in [2]).

This work has been partially supported by the European IST project EVOLUTE (IST-2001-32449).
The arrows in Fig. 1 indicate direct roaming agreements. For example, WLAN-1 has a direct roaming agreement with 3G PLMN-1 and 3G PLMN-2, while WLAN-3 has a direct roaming agreement only with 3G PLMN-2. In addition, 3G PLMN-1 and 3G PLMN-3 have a direct roaming agreement between each other. Note that 3G PLMN-4 has a direct roaming agreement only with 3G PLMN-1. In addition, however, it has an indirect roaming agreement with WLAN-1.

The mobile station (MS) illustrated in Fig. 1 is a WLAN device that has a subscription with a 3G PLMN, which is considered its home PLMN. Therefore, the MS is equipped with a smart card (commonly referred to as a user services identity module, USIM) that is primarily used for authentication and generation of security keys. In the case illustrated, the MS simultaneously receives signals from four WLANs, WLAN-1, WLAN-2, WLAN-3, and WLAN-4. The key requirement is that the MS use a WLAN to obtain wireless IP connectivity and still be authenticated by its 3G home PLMN using its USIM credentials and algorithms. To satisfy this requirement, several challenges need to be dealt with. For instance, the MS needs to select a WLAN that is capable of 3G interworking (i.e., it implements the enhancements required to interwork with 3G PLMNs) and also have a direct or indirect roaming agreement with its 3G home PLMN. Assume, for example, that the 3G home PLMN of the MS in Fig. 1 is 3G PLMN-1. It is clear that the MS must select WLAN-1 because it is the only one with a roaming agreement with 3G PLMN-1. On the other hand, if the home PLMN of the MS is 3G PLMN-3, WLAN-4 should be selected. Finally, if the home PLMN of MS is 3G PLMN-4, WLAN-1 should again be selected, since it provides indirect interworking with 3G PLMN-4 via 3G PLMN-1. Such network selection problems are crucial in the context of WLAN/3G interworking and are discussed in more detail in the next section.

The WLANs illustrated in Fig. 1 may be owned by either:

- A 3G PLMN operator
- A public network operator (e.g., a public WLAN operator) who is not a 3G PLMN operator
- An entity that provides WLAN access in a local area (i.e., building manager/owner or airport authority) but is otherwise not a public network operator
- A business organization that provides a WLAN for its own use and wishes to allow interconnection and possibly visitor use

A WLAN may support several types of access control, such as open access, universal access mechanism (UAM) [3], and IEEE 802.1X [4]. Open access is useful for providing free access to some types of services, as such as advertisements and local information. Open access uses IEEE 802.11 open authentication, which is merely a null authentication scheme. Most IEEE 802.11 WLANs today support open authentication at the 802.11 medium access control (MAC) layer for allowing access to free services. The access to chargeable services is controlled by an access control scheme implemented “on top” of IEEE 802.11, such as UAM [3]. With UAM the MS is associated with an AP and then assigned an IP address, usually with Dynamic Host Configuration Protocol (DHCP). Access to chargeable services is blocked by a gateway, referred to as a public access control (PAC) gateway. To get authorization from the PAC gateway, the WLAN subscriber uses a Web browser to access a welcome page, which prompts for the user’s credentials (usually a username and password). The privacy of these credentials is ensured by running HTTP over a secure layer, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). With 802.1X access control the MS uses an Extensible Authentication Protocol (EAP) method (as opposed to the HTTP method in UAM) to get authenticated. A particular characteristic of 802.1X access control is that it is enforced right after the MS associates with an AP. Therefore, with 802.1X a user must always be authenticated before being able to access the WLAN network. In this case, access to free services can be realized using a well-known guest username and password. Further details on 802.1X are provided later.

As mentioned above, one primary requirement of WLAN/3G interworking is to provide 3G-based authentication (i.e., authentication of USIM by the 3G home PLMN). This mandates that a WLAN able to interwork with 3G systems must support 802.1X access control. However, a WLAN may also be required to support the legacy UAM and open access control schemes, since these schemes are in wide use today and supported by all legacy WLAN clients. This calls for several access control schemes to be supported by a single WLAN. One proposed way to make that feasible is to employ at least two different SSIDs and select the access control scheme implemented “on top” of IEEE 802.11.
A user starting a WAP session from the 3G radio access technology should be able to continue this session after moving to a WLAN and vice versa. Although service continuity is required, the service continuity requirements are not very strict.

**Interworking Scenarios**

Bearing in mind the general interworking model illustrated in Fig. 1, several WLAN/3G interworking scenarios can be envisioned, with a vast range of interworking requirements. In order to provide the proper background for the interworking architectures discussed later in this article, it is instructive at this point to review some of these scenarios and identify their associated requirements. We discuss below six common interworking scenarios [1].

**Scenario 1 — Common Billing and Customer Care:** This is the simplest form of integration, which provides only a common bill and customer care to the subscriber but otherwise features no real interworking between the WLAN and 3G PLMN.

**Scenario 2 — 3G-Based Access Control and Charging:** This scenario requires AAA for 3G subscribers in a WLAN to be done by their 3G home PLMN. For example, a subscriber in a WLAN can use his/her USIM for authentication, as is normally done in a 3G environment. Also, authorization is provided by the 3G home PLMN based on 3G subscription data. This scenario basically enables IP connectivity via WLAN for 3G subscribers. In other words, the user is merely provided an IP connection to the Internet or an intranet through a WLAN. Apart from IP connectivity, no specific set of services are required.

**Scenario 3 — Access to 3G Packet-Switched Services:** The goal of this scenario is to extend the access to 3G packet-switched (PS) services to subscribers in a WLAN environment. For example, if an operator maintains a Wireless Application Protocol (WAP) gateway for providing WAP and MMS services to his subscribers, under this interworking scenario these WAP and MMS services should also be accessible to subscribers in a WLAN environment. As explained later, to gain access to 3G PS-based services the user data traffic is tunneled between the WLAN and the 3G PLMN. In addition, an IP service selection scheme is used for selecting the PS-based service to which to connect. In general, with scenario 3 the user can have access to services such as IP multimedia, location-based services, instant messaging, presence-based services, and MMS. However, although the user is offered access to the same PS-based services over several access technologies (e.g., 3G and WLAN radio access), no service continuity across these access networks is required.

**Scenario 4 — Access to 3G Packet-Switched-Based Services with Service Continuity:** The goal of this scenario is to allow access to PS-based services as required in scenario 3 and also to maintain service continuity across 3G and WLAN radio access technologies. For example, a user starting a WAP session from 3G radio access technology should be able to continue this session after moving to a WLAN and vice versa. Although service continuity is required, the service continuity requirements are not very strict. This means that some services may not survive a vertical handover to/from the WLAN (e.g., due to varying capabilities and characteristics of access technologies). A typical example could be a PS-based service that requires tight delay performance, which cannot be met in a WLAN system. In this case, the service would most likely be terminated after the user moves to a WLAN. Also, under scenario 4, change in service quality is possible as a consequence of vertical handover.
Scenario 5 — Access to 3G Packet-Switched-Based Services with Seamless Service Continuity: This scenario is one step further from scenario 4. Its goal is to provide seamless service continuity between the 3G and WLAN radio access technologies. That is, PS-based services should be utilized across the 3G and WLAN radio access technologies in a seamless manner, without the user noticing any significant differences.

Scenario 6 — Access to 3G Circuit-Switched-Based Services with Seamless Mobility: The goal of this scenario is to allow access to 3G circuit-switched services (CS, e.g., normal voice calls) from the WLAN system. Seamless mobility for these services should be provided.

Table 1 summarizes the different interworking scenarios and their characteristics [1].

Table 1. Some WLAN/3G interworking scenarios and their characteristics [1].

<table>
<thead>
<tr>
<th>Scenario 1</th>
<th>Scenario 2</th>
<th>Scenario 3</th>
<th>Scenario 4</th>
<th>Scenario 5</th>
<th>Scenario 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common billing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Common customer care</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3G-based access control</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3G-based access charging</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to 3G PS-based services</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to 3G PS-based services with service continuity</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to 3G PS-based services with seamless service continuity</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to 3G CS-based services with seamless mobility</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

An Interworking Architecture for Scenario 2

Figure 2 illustrates the proposed WLAN/3G interworking architecture that meets the requirements of scenario 2, for the general case when the WLAN is not directly connected to the MS's 3G home PLMN (roaming case). The architecture for the non-roaming case can be straightforwardly derived: the 3G AAA server is directly connected to the WLAN over the Wr/Wb interface, and the Ws/Wc interface is not used. Note that we use the same notation as in [7].

The 3G home PLMN illustrated in Fig. 2 supports UMTS terrestrial radio access network (UTRAN) MSs that access the 3G home PLMN over the typical UTRAN access network and, in addition, supports WLAN MSs. Note that the user data traffic of UTRAN MSs and WLAN MSs is routed completely differently. In particular, the user data traffic of WLAN MSs is routed by the WLAN itself toward the Internet or an intranet, whereas the user data traffic of UTRAN MSs is routed through the 3G packet-switched core network, encompassing the serving GPRS support node (SGSN) and the gateway GPRS support node (GGSN). UTRAN MSs can typically have access to the Internet, a corporate intranet, or the 3G operator’s packet-switched services (WAP, MMS, etc.).

In scenario 2 only AAA signaling need be exchanged between the WLAN and the 3G home PLMN (via the 3G visited PLMN) for AAA purposes.

A key element in the architecture of Fig. 2 is the 3G AAA server, which is a new functional component incorporated in a 3G PLMN in order to support interworking with WLANs. The 3G AAA server in the 3G home PLMN terminates all AAA signaling with the WLAN and interfaces with other 3G components, such as the home subscriber server (HSS), home location register (HLR), charging gateway/charging collection function (CGw/CCF), and online charging system (OCS). Both the HLR and HSS are basically subscription databases, used by the 3G AAA server for acquiring subscription information for particular WLAN MSs. Typically, if an HSS is available, the HLR need not be used. The CGw/CCF and the OCS are 3G functional elements used to provide offline and online charging services, respectively.

The 3G AAA server can also route AAA signaling to/from another 3G PLMN, in which case it serves as a proxy and is referred to as a 3G AAA proxy. In Fig. 2 the 3G AAA server in the 3G visited PLMN takes the role of a proxy that routes AAA signaling to/from the 3G AAA serv-
The user data traffic of WLAN MSs is routed through the WLAN to an external intranet/Internet. Although this traffic is routed by the WLAN, the 3G PLMN (both home and visited) can apply a specific policy to this traffic.

As noted before, the user data traffic of WLAN MSs is routed through the WLAN to an external intranet/Internet. Although this traffic is routed by the WLAN, the 3G PLMN (both home and visited) can apply a specific policy to this traffic. For example, during the authorization phase the 3G AAA server may define a set of restrictions to police user data traffic, such as “do not allow FTP traffic” or “allow HTTP traffic only to/from a specific IP address.”

**REFERENCE POINTS**

The reference points (also referred to as interfaces) illustrated in the architecture diagram of Fig. 2 are briefly discussed below. A more thorough discussion can be found in [7]. Note that we only discuss the interfaces relevant to WLAN/3G interworking; a brief description of 3G internal interfaces, such as Gr, Iu-ps, Gi, and Gn, can be found in [8].

**Wr/Wb:** This interface carries AAA signaling between the WLAN and the 3G visited or home PLMN in a secure manner. The proposed protocol across this interface is Diameter [9, 10], which is used for providing AAA functions and carrying the EAP messages exchanged between the MS and the 3G AAA server. However, since legacy WLANs need to be supported, the Radius [11] protocol must also be supported across Wr/Wb; this calls for Radius-Diameter inter-working functions across the legacy WLAN and 3G AAA proxy/server. Diameter is the preferred AAA protocol since it can provide enhanced functionality compared to Radius. Note that the term Wr is used to specifically refer to the interface that carries authentication and authorization information, while Wb is used to refer to the interface that carries accounting information. Wr and Wb corresponds to the Ls and Lp interfaces specified by WIG [12].

**Ws/Wc:** This interface provides the same functionality as Wr/Wb but runs between a 3G AAA proxy and a 3G AAA server. Since Ws/Wc is across two 3G networks, it does not have to support Radius (i.e., it supports only Diameter). Again, the term Ws is used to refer to the interface that carries authentication and authorization information, and Wc is used to refer to the interface that carries accounting information.

**Wf:** It is located between the 3G AAA server/proxy and the 3G CGw/CCF. The primary purpose of the protocols on this interface is to transport charging information toward the 3G operator’s CGw/CCF located in the visited or home PLMN. The application protocol on this interface is Diameter-based. The Wf interface corresponds to the Ls interface specified by WIG [12].

**Wo:** This interface is used by the 3G AAA server to communicate with the 3G OCS and exchange online charging information so as to perform credit control for online charged sub-
scribers. The application protocol across this interface is again Diameter-based.

Wx: This interface is located between the 3G AAA server and the HSS, and is used primarily for accessing the WLAN subscription profiles of the users, retrieving authentication vectors, and like tasks. As noted before, if Wx is implemented, the interface to the HLR is not required. The protocol across Wx is either Mobile Application Part (MAP) or Diameter-based.

D’/Gr’: This optional interface is used for exchanging subscription information between the 3G AAA server and the HLR by means of the MAP protocol. It is typically used when the enhanced functionality provided by the HSS is not available. Note that this interface is based on either the D interface, which runs between the 3G mobile switching center (MSC) and the HLR, or the Gr interface, which runs between the SGSN and the HLR (Fig. 2). In other words, it normally implements a subset of either the D (denoted D’) or Gr functionality (denoted Gr’).

AAA SIGNALING FOR SCENARIO 2

Figure 3 illustrates a typical message sequence diagram and some associated comments applicable to scenario 2 interworking. The figure corresponds to the roaming case shown in Fig. 2. Our assumption is that the general principles of 802.1X access control are known; thus, we refrain from discussing them again. The novice reader is referred to the 802.1X specification [4] for more details.

Initially, the MS sends its identity to the WLAN within an EAP-Response/Identity message. Note that the WLAN is considered to encompass an access point (AP) and the WLAN AAA proxy shown in Fig. 2. The MS’s identity, NAI-1, is formatted as an NAI and has the structure username@realm, where the realm is in the form of an Internet domain name as specified in RFC 1035. In this case, a possible realm value could be homeMNC.homeMCC.WLAN.3Gnetwork.org. The WLAN discovers if it can route AAA messages to the 3G PLMN corresponding to this realm, for example, by trying a DNS query to resolve this realm into an IP address. If the resolution is successful (i.e., the WLAN has a direct roaming agreement with this 3G PLMN), an AAA access request is sent to the identified 3G PLMN over the Wr interface. Otherwise, the WLAN sends network advertisement data to the MS, which includes the 3G PLMNs with which it can interwork. A proposed way to send this advertisement data is to use a new EAP method, called 3G-Info [6], which carries...
After the EAP-Success message, which effectively terminates the authentication and authorization phase, the MS typically uses DHCP to get an IP address from within the address space of the WLAN. This may be either a public or a private IP address. 

A simplified AAA protocol architecture that applies to interworking scenario 2 (and scenario 3, as explained in the next section) is illustrated in Fig. 4. Note that the method used to authenticate the MS and possibly the 3G home PLMN needs to be implemented only by the MS and the 3G AAA server in the MS’s home PLMN. The WLAN need only support generic EAP and EAP-over-LAN (EAPOL) as specified in IEEE 802.1X.

### The Interworking Architecture for Scenario 3

For satisfying the key requirement of scenario 3, access to 3G PS-based services, user data traffic needs to be routed to the 3G home or visited PLMN. A network architecture that fulfills this requirement is illustrated in Fig. 5. Note that Fig. 5 also corresponds to a roaming case. Compared to Fig. 2, we note that although AAA traffic follows the same route, user data traffic is routed to the MS’s 3G home PLMN, to a new component called a packet data gateway (PDG). User data traffic is also routed through a data gateway, referred to as a wireless access gateway (WAG), which in the case of roaming is located in the preferred 3G visited PLMN. As discussed below, this routing is enforced by establishing appropriate tunnels. The PDG functions much like a GGSN in a 3G PS network. It routes user data traffic between the MS and an external packet data network (PDN), which is selected based on the 3G PS-based service requested by the MS (e.g., WAP, MMS, IP Multimedia). The requested 3G PS-based service is identified by the MS through a WLAN-Access Point Name (W-APN) that is included in the AAA signaling messages (see below for details). The PDG may also perform address translation, enforce policy, generate charging records, and so on. The WAG functions mainly as a route policy element, ensuring that user data traffic from authorized MSs is routed to the appropriate PDGs, located in either the same or another PLMN (as shown in Fig. 5).

It is easy to note from Fig. 5 that WLAN MSs can have access to the same services (or an XML structure populated with a list of PLMN identities. Work is currently underway in the Internet Engineering Task Force (IETF) to specify a suitable set of EAP extensions to support the network advertisement (see [15]). Based on the network advertisement data as well as on its roaming preferences, the MS selects a preferred 3G visited PLMN and forms a second NAI (NAI-2) corresponding to this PLMN. NAI-2 is used by both the WLAN and the 3G AAA proxy to make routing decisions and finally reach the 3G AAA server in the MS’s home PLMN. Therefore, NAI-2 needs to encode both the preferred 3G visited PLMN and the MS’s 3G home PLMN. For this purpose, it could be encoded as homeMNC.homeMCC//username@visitedMNC.visitedMCC.WLAN. 3Gnework.org. Note that this encoding includes both the identity of the 3G home PLMN (homeMNC, homeMCC) and the identity of the preferred 3G visited PLMN (visitedMNC, visitedMCC). Note also that the username needs to point to a 3G subscription in the home PLMN, and therefore could include either the permanent 3G International Mobile Subscriber Identity (IMSI) of the MS, or a temporary identity previously assigned to the MS.

At point 3 in Fig. 3 the 3G AAA server interacts with either the HLR or the HSS to retrieve the WLAN subscription profile of the MS and authentication information. Subsequently, the authentication and key agreement phase is initiated, which is based on either EAP-AKA or EAP-SIM methods. More details on these methods, including message flow diagrams, can be found in the EAP-AKA and EAP-SIM [13, 14] Internet drafts.

After successful authentication and key agreement, the 3G AAA server transmits an AAA access accept message, which contains the cipher key to be used for data encryption on the radio interface and possibly some filter rules for policing user data traffic. These filter rules might be modified (e.g., more rules could be added) by the 3G AAA proxy based on the policy of the 3G visited PLMN. Note that after the EAP-Success message, which effectively terminates the authentication and authorization phase, the MS typically uses DHCP to get an IP address from within the address space of the WLAN. This may be either a public or private IP address.
PDNs used by UTRAN MSs. In other words, 3G subscribers can maintain access to the same set of services as they roam across WLAN- and 3G-specific radio networks.

It is pointed out that user data traffic need not always be routed to the MS’s home PLMN as shown in Fig. 5. Alternatively, user data could be routed to the PDG in the 3G visited PLMN in order to have access to the 3G PS-based services offered by the visited PLMN.

**REFERENCE POINTS**

As shown in Fig. 5, several additional interfaces, WN, WM, WI, Wg, and WP, are introduced to satisfy the requirements of scenario 3. For these interfaces we adopt the notation and functionality specified in [7].

**WN:** This interface is used for transporting tunneled user data between the WLAN and the WAG. WLANs that need to provide scenario 3 interworking with 3G networks shall have to deploy a WN-compliant interface.

**WM:** It is located between the 3G AAA server and PDG, and used to enable the 3G AAA server to retrieve tunneling attributes and an MS’s IP configuration parameters from/via the PDG. The AAA protocol across this interface is Diameter-based.

**WI:** It is similar to the Gi reference point provided by the PS domain (Fig. 5). Interworking with packet data networks (PDN-1, PDN-2, etc.) is provided via the WI interface based on IP. A PDN may be an external public or private packet data network, or an intra-operator packet data network.

**WG:** This interface is mainly used by the 3G AAA proxy 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.

**WP:** This interface transports tunneled user data traffic between the WAG and the PDG. The WP is not only used in the roaming case shown in Fig. 5. Even in the non-roaming case, user data traffic goes through the WAG in the home PLMN to the PDG, also in the home PLMN. A proposed protocol across WP is the GPRS Tunneling Protocol (GTP) used on the Gn interface between the SGSN and GGSN.

In addition to the above interfaces, an interface from the PDG to a policy server could be implemented to support service-based local policy. An interface with similar functionality has already been defined for the GGSN (the so-called Go interface) and is specified in 3GPP TS 29.208.

**AAA SIGNALING FOR SCENARIO 3**

The key requirement of scenario 3 is the routing enforcement of user data traffic between the MS and the PDG. This routing enforcement is applied through establishment of the appropriate tunnel(s). As discussed below, this tunnel may be either MS-initiated or MS-transparent. Note that although there are many tunneling options that could be considered, for the sake of brevity we restrict our discussion to only a few.

Another particular characteristic of scenario 3 is that the MS conveys a W-APN to the 3G AAA server in order to explicitly indicate that access to
a 3G PS-based service is requested. The W-APN is an identifier formatted as an Internet domain name that designates the PS-based service requested by the MS and possibly the operator through which this service is requested. In effect, the W-APN identifies the PDN that provides the requested PS-based service.

**MS-Initiated Tunneling** — The MS-initiated tunneling corresponds to the case when tunnel establishment is initiated by the MS itself, and hence originates at the MS and terminates at the PDG. Figure 6 illustrates a typical signaling flow for this case. Note that up to point 6 the signaling flow is the same as that shown in Fig. 4. The only difference is that the W-APN is also carried from the MS to the 3G AAA server in order to explicitly indicate that access to a 3G PS-based service is requested. This W-APN is used by the 3G AAA server for authorization purposes and initiating tunnel establishment procedures if necessary.

After the EAP-Success message is transmitted, the MS uses DHCP to receive an IP address and then initiates tunnel establishment with the PDG. To find the IP address of the PDG that provides access to the requested PS-based service (or PDN) the MS may perform a DNS query to resolve the W-APN into an IP address. For example, an W-APN encoded as MMS.homeMNC.homeMCC.WLAN.3Goperator.org would be resolved to the IP address of the PDG that provides access to the MMS service in the PLMN with identity <homeMCC, homeMNC>. Alternatively, the IP address of the PDG could be sent to the MS by the 3G AAA server embedded into an EAP message. As noted in Fig. 6 (right after point 6), the W-APN value may also be one of the parameters exchanged during MS-initiated tunnel establishment. It is used by the PDG for service authorization, policy enforcement, and routing the traffic on the MS-Initiated tunnel to/from the designated PDN. Before the tunnel is accepted by the PDG, tunnel authorization information is retrieved from the 3G AAA server through the Wm interface.

The MS-Initiated tunnel establishment may or may not request user intervention. The WLAN is expected to filter user data traffic and allow only traffic to/from the PDG to pass through.

**MS-Transparent Tunneling** — MS-transparent tunneling corresponds to the case when the tunnel is established without any MS intervention. An example of such a configuration is depicted in Fig. 7. In this case, the MS is roaming and uses PS-based services in the home PLMN. Two MS-transparent tunnels are established: one from a
WLAN access gateway (WLAN AG) to the WAG and another from the WAG to the PDG in the home PLMN. In this case, all MS outbound traffic is routed to the WLAN AG with normal IP routing, then enters the first tunnel to the WAG, and finally reaches the PDG over the second tunnel. Note that the WLAN AG, WAG, and PDG need to make forwarding decisions based on previously installed information, which is communicated during the AAA phase. The PDG would also perform address translation if the MS’s IP address is not assigned from the address space of the 3G home PLMN.

Several other alternative configurations can be realized for MS-transparent tunneling. For example, the tunnel from the WLAN AG to the WAG could be an aggregate tunnel (or site-to-site tunnel) that aggregates all user data traffic to/from the 3G visited PLMN. Also, the first tunnel could originate directly from an AP instead of the WLAN AG.

A simplified signaling flow that corresponds to MS-transparent tunneling is depicted in Fig. 8. After the MS is correctly authenticated, the 3G AAA server determines (e.g., from the MS’s subscription) that MS-transparent tunneling should be used. Hence, it negotiates with the PDG the tunnel attributes to be used across the Wp interface, and informs the PDG about the W-APN requested by the MS. After the 3G AAA proxy receives the Access Accept, it communicates to the WAG the tunnel attributes (e.g., the IP address of PDG, tunnel type). In addition, the 3G AAA proxy decides what type of tunnel should be used across the Wn interface and forwards the corresponding tunnel attributes to the WLAN AAA proxy. After the two MS-transparent tunnels are successfully established, the MS receives the EAP-Success message and subsequently uses DHCP to receive an IP address. The DHCP packets could be either tunneled to the PDG, in which case the MS is assigned an IP address from the address space of the 3G home PLMN, or processed by the WLAN, in which case the MS is assigned an IP address from the address space of the WLAN.

Table 2 provides a brief list of characteristics of MS-transparent and MS-initiated tunneling. It is evident that both approaches feature advantages and disadvantages, and real implementations could support both. Hybrid approaches are also feasible (e.g., MS-initiated tunneling from the MS to the WAG and MS-transparent tunneling, with the GTP protocol, from the WAG to the PDG). This particular approach resembles the way tunnels are established in a 3G PLMN (MS-initiated tunneling from the MS to the SGSN and MS-transparent tunneling from the SGSN to the GGSN); thus, it is expected to be preferred by many network operators.
CONCLUSIONS

In this article we propose and discuss some techniques and architectures capable of providing interworking between WLAN and 3G networks and meeting the requirements of two typical scenarios that currently feature the highest market interest. The discussed architectures can enable 3G subscribers to benefit from high-throughput IP connectivity in strategic hot spot locations (e.g., airports, hotels) and also maintain access to the same 3G packet-switched services across several radio access technologies, such as IEEE 802.11, HiperLan/2, UTRAN, and GERAN. This service availability across hybrid radio technologies (or service roaming) is considered important for establishing a common user experience. However, session mobility (i.e., the continuation of IP sessions when changing radio technology) is also very important as the user becomes more mobile and frequently moves between different radio access technologies. Session mobility is an additional requirement that needs further consideration and presents considerable technical challenges. It will be an evolutionary step beyond the service roaming of scenario 3, discussed in this article. After the technical challenges of session mobility are efficiently addressed, 3G data subscribers will be able to maintain the same multimedia sessions with the same quality of service as they move across different radio access technologies. This is the technical subject and vision of many R&D projects currently carried out worldwide.

ACKNOWLEDGMENTS

The author would like to thank Mr. Speros Velentzas and Dr. Tim Charity of Motorola, Applied Technology and Knowledge Engineering, for their important support in the course of this work.

REFERENCES

Table 2. MS-transparent vs. MS-initiated tunneling.

<table>
<thead>
<tr>
<th>Feature</th>
<th>MS-transparent tunneling</th>
<th>MS-initiated tunneling</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS intervention</td>
<td>Not required.</td>
<td>Required.</td>
</tr>
<tr>
<td>Simultaneous access to many PDNs</td>
<td>Since the tunnel is established as part of WLAN session setup, the MS can only have access to one PDN.</td>
<td>More than one tunnel can be established, each associated with a different PDN. Hence, access to more than one PDN is feasible, e.g., access to the Internet as well as to a corporate intranet.</td>
</tr>
<tr>
<td>Mobility impact</td>
<td>MS mobility may have a great impact on the tunnel. In particular, as the MS moves between APs, the MS-transparent tunnel might need to be re-established. Note that the MS-transparent tunnel might not originate at an AP but from some other device in the WLAN (e.g., a WLAN access gateway as shown in Fig. 7).</td>
<td>Tunnel re-establishment is not required as the MS hands over from one AP to another. So, MS mobility has minimal impact on the MS-initiated tunnel(s).</td>
</tr>
<tr>
<td>Air interface impact</td>
<td>No additional air interface overhead.</td>
<td>Overhead on the air interface is increased due to the encapsulation performed by the MS.</td>
</tr>
<tr>
<td>Security</td>
<td>More secure since the MS is not involved with tunnel establishment.</td>
<td>Less secure.</td>
</tr>
<tr>
<td>MS processing</td>
<td>Demands no additional MS processing capabilities.</td>
<td>Additional MS processing capabilities required for performing tunnel management.</td>
</tr>
</tbody>
</table>

### ADDITIONAL READING


### ADDITIONAL READING


### APOSTOLIS K. SALKINTZIS [SM] (a.k.salkintzis@ieee.org) received his Diploma in 1991 (honors) and his Ph.D. degree in 1997, both from the Department of Electrical and Computer Engineering, Democritus University of Thrace, Xanthi, Greece. From 1992 to 1997 he was a research engineer at Democritus University, studying mobile data networks and working on research projects dealing with the design and implementation of wireless data networks and protocols. In 1999 he was a sessional lecturer at the Department of Electrical and Computer Engineering, University of British Columbia, Canada, and from October 1998 to December 1999 he was also a post-doctoral fellow in the same department. During 1999 he was also a visiting fellow at the Advanced Systems Institute of British Columbia, Canada; during 2000, he was with the Institute of Space Applications and Remote Sensing (ISARS) of the National Observatory of Athens, Greece, where he conducted research on digital satellite communication systems. Since September 1999 he has been with Motorola Inc., working on the design and standardization of modern telecommunication networks, focusing in particular on GPRS, UMTS, and WLANs. He has served as lead guest editor for a number of special issues of Mobile Networks and Applications Journal, IEEE Personal Communications, IEEE Communications Magazine, and IEEE Wireless Communications. He has organized several technical sessions and symposia at various conferences and has chaired most of them. He has published over 40 papers in peer-reviewed journals and international conferences, and has also published three book chapters. His primary research activities lie in the areas of wireless communications and mobile networking. He is particularly interested in mobility management, IP multimedia over mobile networks, mobile network architectures and protocols, QoS for wireless networks, and radio modem design with DSPs. Currently, he is most active in WLAN3G interworking, and the evolution and standardization of GPRS and UMTS networks. Until 2002 he was an active participant and contributor in 3GPP, and was an editor of 13 3GPP specifications.