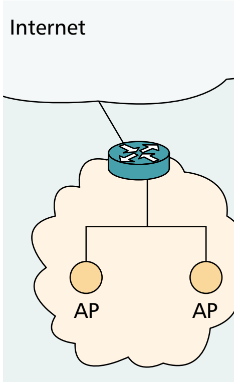
WLAN-GPRS INTEGRATION FOR NEXT-GENERATION MOBILE DATA NETWORKS

APOSTOLIS K. SALKINTZIS, CHAD FORS, AND RAJESH PAZHYANNUR, MOTOROLA



The Wireless LANs standardization and R&D activities worldwide, combined with the recent successful deployment of WLANs in numerous hotspots, justify the fact that WLAN technology will play a key role in the wireless data transmission.

ABSTRACT

The ongoing wireless LAN standardization and R&D activities worldwide, which target bit rates higher than 100 Mb/s, combined with the recent successful deployment of WLANs in numerous hotspots justify the fact that WLAN technology will play a key role in wireless data transmission. Cellular network operators have recognized this fact, and strive to exploit WLAN technology and integrate this technology into their cellular data networks. For this reason, there is currently a strong need for interworking mechanisms between WLANs and cellular data networks.

In this article we focus on these interworking mechanisms, which effectively combine WLANs and cellular data networks into integrated wireless data environments capable of ubiquitous data services and very high data rates in hotspot locations. We discuss the general aspects of integrated WLANs and cellular data networks, and we examine the generic interworking architectures that have been proposed in the technical literature. In addition, we review the current standardization activities in the area of WLAN-cellular data network integration. Moreover, we propose and explain two different interworking architectures, which feature different coupling mechanisms. Finally, we briefly compare the proposed interworking architectures, and discuss their advantages and drawbacks.

INTRODUCTION

In today's world economy, the ability to communicate on the move is becoming less of a luxury and more of a necessity. Second-generation (2G) cellular systems have enabled a high level of mobility, with wired-equivalent quality, for voice and low-speed data (< 9.6 kb/s) services. This is done via the implementation of global standards based on digital technology, such as Global System for Mobile Communications (GSM) and cdmaOne, with roaming agreements between operators acting as the glue that binds disparate networks together into one ubiquitous system from the end user's perspective.

Although 2G technology is adequate in meeting the voice communication needs of the typical cellular subscriber, its data communication capabilities are cumbersome and limited. The low bandwidth and complexity associated with these services have discouraged the average consumer from investing in wireless data. In contrast, wired data service, which can offer high bandwidth and always-on connectivity, has grown in popularity due to its availability and affordability. To compete with this technology, third-generation (3G) cellular systems promise competitive data rates, at speeds of up to 300 kb/s initially and increasing up to 2 Mb/s, with the same always-on connectivity of wired technology.

However, due to the delay of 3G cellular networks and the large investments made for new spectrum in which to offer 3G services, cellular operators are now looking for ways to augment their current offerings with "3G-like" services in efforts to generate new revenue stream in today's environment. 2.5G cellular data technology, and in particular General Packet Radio Service (GPRS) [1], which provides wireless data services at speeds of up to approximately 100 kb/s, is gaining support as a wide area data solution, but has limited potential because it cannot support the high data rates required in business and multimedia applications. Therefore, since 2.5G cellular data technology is insufficient to meet market needs and 3G cellular data technology is not yet available, mobile network operators are turning to wireless local area network (WLAN) technology. This interest in WLAN technology also arises from the recent evolution and successful deployment of WLAN systems worldwide, as well as the very high data rates (in excess of 100 Mb/s) future WLAN developments promise.

WLAN systems are expected to be widely deployed in public locations, such as hotels and coffee shops, as well as in enterprises and homes. Specifically, WLAN networks will provide wireless data coverage by means of *hotspot* deployments. To generate revenue in the WLAN space with cellular customers, it is commonly believed that operators must provide a seamless user experience between the cellular and WLAN access networks. This calls for interworking mechanisms between WLANs and cellular data networks capable of providing integrated authentication, integrated billing, roaming, terminal mobility, and service mobility.

1070-9916/02/$17.00 © 2002 IEEE

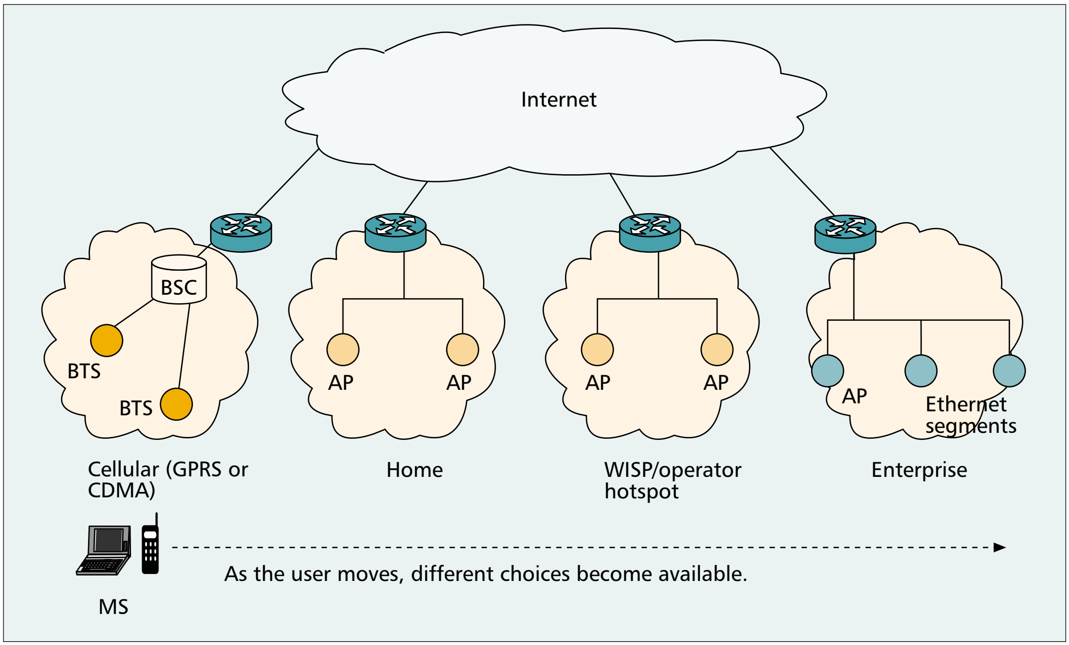


Figure 1. *Multiple access options in an integrated data environment.*

A cellular data network can provide relatively low-speed data service over a large coverage area. On the other hand, WLAN provides high-speed data service over a geographically small area. An integrated network combines the strengths of each.

In this article we focus on the above interworking mechanisms, which effectively combine WLANs and cellular data networks into integrated wireless data networks with very high data rate capabilities in hotspot locations. In the following section, we discuss the general aspects of integrated WLAN-cellular data networks, and in the next section we examine the generic interworking architectures that have been proposed in the technical literature. We then review the current standardization activities in the area of WLAN-cellular data network integration. We propose two different interworking architectures, and finally briefly compare their features and present our concluding remarks.

Integrated WLAN and Cellular Data Networks

A cellular data network can provide relatively low-speed (up to 100 kb/s per user) data service over a large coverage area. On the other hand, WLAN provides high-speed data service (up to 11 Mb/s with 802.11b and 54 Mb/s with 802.11a) over a geographically small area. An integrated network combines the strengths of each, resulting in a wide-area system capable of providing users with ubiquitous data service ranging from low to high speed in strategic locations.

Roaming

Figure 1 illustrates an integrated environment in which a subscriber has multiple access network options. There are two example configurations discussed here concerning the integration of WLAN and cellular networks. These configurations vary in the area of ownership/management of the WLAN. The first example is the case in which the cellular operator owns and manages the WLAN. The second is the case in which a wireless Internet service provider (WISP) or enterprise is the owner.

Consider a cellular data customer waiting in an airport where the cellular operator has deployed a WLAN. While waiting, the customer can take advantage of the high bandwidth and wireless connectivity of the WLAN to gain access to the data services provided by the operator. By augmenting their cellular data systems with WLANs, operators are able to enhance their data service capabilities with high-speed data connectivity in strategic locations such as airports and hotels. In doing this, the cellular operator is able to gain a competitive advantage by offering the ability for their current customer base to roam in these hotspots.

In operator-owned WLANs, the cellular operator has the advantage (over the WISP) of an established customer base to which they can market such capabilities. Additionally, operators have authentication and billing mechanisms in place for their users, which they can leverage in the WLAN space.

Although the mechanisms may be slightly different when the cellular operator does not own the WLAN, the same user experience may be achieved. A multilateral roaming agreement between WISPs and cellular operators may allow a cellular customer to use a WISP-operated WLAN. The billing and authentication services would continue to be provided by the cellular operator. The WISP may partake in revenue sharing with the cellular operator, based on the particular roaming agreements between the two parties.

In an enterprise WLAN, the enterprise may choose its own authentication and billing mechanisms. Most enterprises do not have any billing systems for data services, and have only limited authentication mechanisms. However, cellular and wireline operators have considerable interest in providing their customers service through the enterprise WLAN system. Such a service would be facilitated by mechanisms similar to that required for a WISP-owned WLAN.

Typically, no user intervention would be required to perform the switchover from WLAN to GPRS. Moreover, the user would not perceive this handover. When the user moves back into the coverage of a WLAN system, the flow would be handed back to the WLAN network.

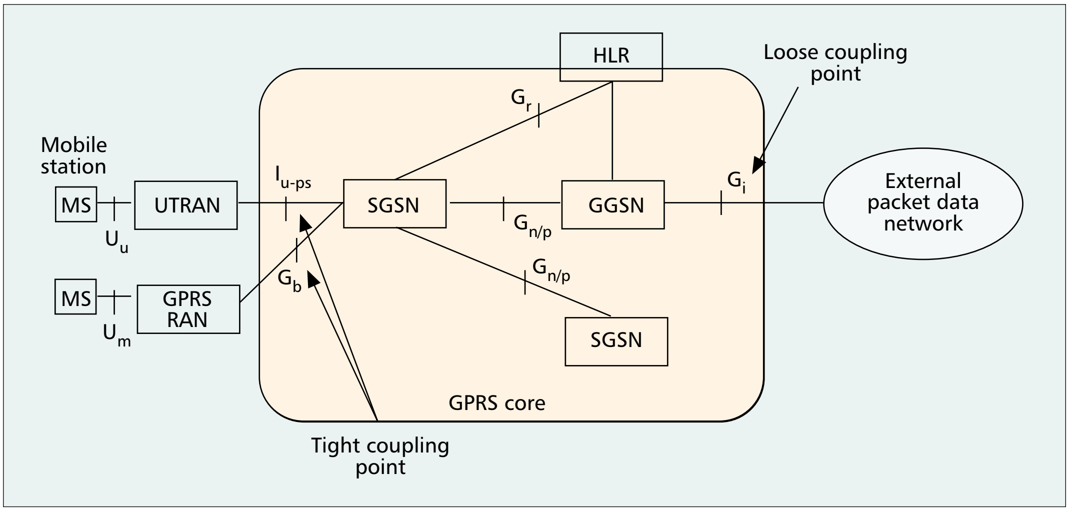


Figure 2. *A GPRS reference diagram showing the WLAN coupling points.*

Session Mobility

Session mobility may be seen as an evolutionary step from roaming in this integrated environment. Session is defined here as a flow of IP packets between the end user and an external entity; for example, an FTP or HTTP session. Consider, for instance, a mobile device capable of connecting to the data network through WLAN and cellular. This could be, for example, a laptop with an integrated WLAN-GPRS card, or a personal digital assistant (PDA) attached to a dual access card. The end user is connected to the data network and is in a session flow through one access network, say a WLAN. As the user moves out of the coverage of the WLAN system, the end device detects the failing WLAN coverage and seamlessly switches the flow to a GPRS network. The end-to-end session remains unaffected. Typically, no user intervention would be required to perform the switchover from WLAN to GPRS. Moreover, the user would not perceive this handover. When the user moves back into the coverage of a WLAN system, the flow is handed back to the WLAN network.

The mobility function is distinct from roaming in that Mobility requires no user intervention and preserves any IP-based session during handovers between cellular data and WLAN. With roaming the switchover between WLAN and cellular data requires explicit user intervention and in most cases would result in teardown of any existing sessions.

Enhanced Mobile Applications

Given the possibility of cellular customers being connected to two different access networks, WLAN and GPRS,[1] a number of enhanced applications can be enabled. The applications could take advantage of the fact that the end user is always connected through a low-speed cellular network and sometimes connected through a high-speed WLAN. An example is a mobile email application that schedules the delivery of attachments or large files when the mobile is connected to the WLAN network, and delivers only synopses of emails when the mobile is connected to the GPRS network.

Interworking Architectures

Several approaches have been proposed for interworking between WLANs and cellular networks. The European Telecommunications Standards Institute (ETSI) specifies in [2] two generic approaches for interworking: so-called *loose coupling* and *tight coupling*. With loose coupling the WLAN is deployed as an access network *complementary* to the GPRS network. In this case, the WLAN utilizes the subscriber databases in the GPRS network but features no data interfaces to the GPRS core network. Considering the simplified GPRS reference diagram displayed in Fig. 2, we may argue that the loose coupling between the GPRS and the WLAN is carried out at the Gi reference point. This means that with loose coupling the WLAN bypasses the GPRS network and provides direct data access to the external packet data networks (PDNs). On the other hand, with tight coupling the WLAN is connected to the GPRS core network in the same manner as any other radio access network (RAN), such as GPRS RAN and UMTS terrestrial RAN (UTRAN). In this case, the WLAN data traffic goes through the GPRS core network before reaching the external PDNs. As shown in Fig. 2, with tight coupling the WLAN is connected to either Gb or Iu-ps reference points. Detailed descriptions of the GPRS reference diagram, including the reference points and the functional nodes, can be found in [1].

Reference [2] also describes a specific tight coupling architecture for interworking between HIPERLAN/2 [3] and GPRS networks. In this architecture, the HIPERLAN/2 RAN is connected to the standard Iu-ps interface. The loose coupling and tight coupling approaches are further discussed in subsequent sections, where we propose more specific architectures and describe them in detail.

Currently, the short-term trend is to follow the loose coupling approach and use (U)SIM-based authentication and billing. With this approach, a subscriber can reuse his Subscriber Identity Module (SIM) card or his User Services Identity Module (USIM[2]) card to access a set of wireless data

[1] *In the rest of this article, we focus explicitly on GPRS as a cellular data technology. Note that GPRS is a packet service in both 2.5G and 3G systems standardized by 3GPP. When we refer to GPRS, we refer to the packet service itself, which may be implemented with either 2.5G or 3G technology.*

[2] *Typically, GSM subscribers are equipped with a SIM card and UMTS subscribers with a USIM card.*

services over a WLAN. However, as explained later, this approach features limited session mobility capabilities compared to tight coupling.

Notable references to other interworking architectures are also [4–6], which describe five different architectures for implementing handover between GPRS and 802.11 WLAN networks [7]. However, all these architectures mainly refer to very high-level concepts and do not discuss any operational details. On the contrary, in this article we propose detailed architectures and thoroughly discuss their key functional aspects.

CURRENT STANDARDIZATION ACTIVITIES

Apart from the standardization activities in ETSI, which are summarized in Technical Report TR 101 957 [2] discussed above, other standardization bodies have recently been involved in the integration of WLANs and cellular telecommunication networks. Most of these activities are promoted by cellular operators, who want to benefit from the rapidly evolved WLAN technology and offer advanced high-speed data services to their subscribers with one subscription, one bill, one set of services, and so on. The goal of standardization activities is to define standard interworking interfaces and ensure interworking across multivendor equipments and across several types of WLANs and cellular networks.

Recently, several WLAN standardization bodies (in particular, ETSI BRAN, IEEE 802.11, IEEE 802.15, and MMAC) have agreed to set up a joint Wireless Interworking Group (WIG) to deal with the interworking between WLANs and cellular networks. This activity is being driven primarily from Europe by ETSI BRAN and the first meeting was planned for September 2002.

Recently, several WLAN standardization bodies have agreed to set up a joint Wireless Interworking Group (WIG) to deal with the interworking between WLANs and cellular networks. This activity is being driven primarily from Europe by ETSI BRAN.

The most intense standardization activities are currently taking place in the Third Generation Partnership Project (3GPP), a standardization body that maintains and evolves the GSM and UMTS specifications (see http://www.3gpp.org). 3GPP has recently approved a WLAN/Cellular Interworking work item, which aims to specify one or more techniques for interworking between WLANs and GPRS networks. This standardization work has recently started and is scheduled for completion in early 2003. In the context of this work, several interworking requirements have been specified and categorized into six interworking scenarios [8].

Scenario 1 — Common billing and customer care: This is the simplest form of interworking, which provides only a common bill and customer care to the subscriber but otherwise features no real interworking between the WLAN and GPRS network. For this reason, this scenario does not require any particular standardization activities.

Scenario 2 — 3GPP system-based access control and charging: This scenario requires authentication, authorization, and accounting (AAA) for subscribers in the WLAN to be based on the same AAA procedures utilized in the GPRS system. For example, a subscriber in a WLAN can use his SIM card for authentication, as he normally does in a GPRS environment. Also, authorization is provided by the GPRS system itself based on subscription data. This scenario basically enables IP connectivity via WLAN for GPRS subscribers. It is noted that no requirements are put on the set of services to be offered in the WLAN.

Scenario 3 — Access to 3GPP GPRS-based services: The goal of this scenario is to allow the cellular operator to extend access to its GPRS-based services to subscribers in a WLAN environment. For example, if an operator maintains a Wireless Application Protocol (WAP) gateway for providing WAP services to its subscribers, under interworking scenario 3, this WAP service should also be accessible to subscribers in a WLAN environment. In general, GPRS-based services include any service provided over the GPRS network such as IP multimedia services (as specified in [9]), location-based services, instant messaging, and presence-based services. Note that although the user is offered access to the same GPRS-based services over both the GPRS and WLAN access networks, no service continuity across these access networks is required in scenario 3.

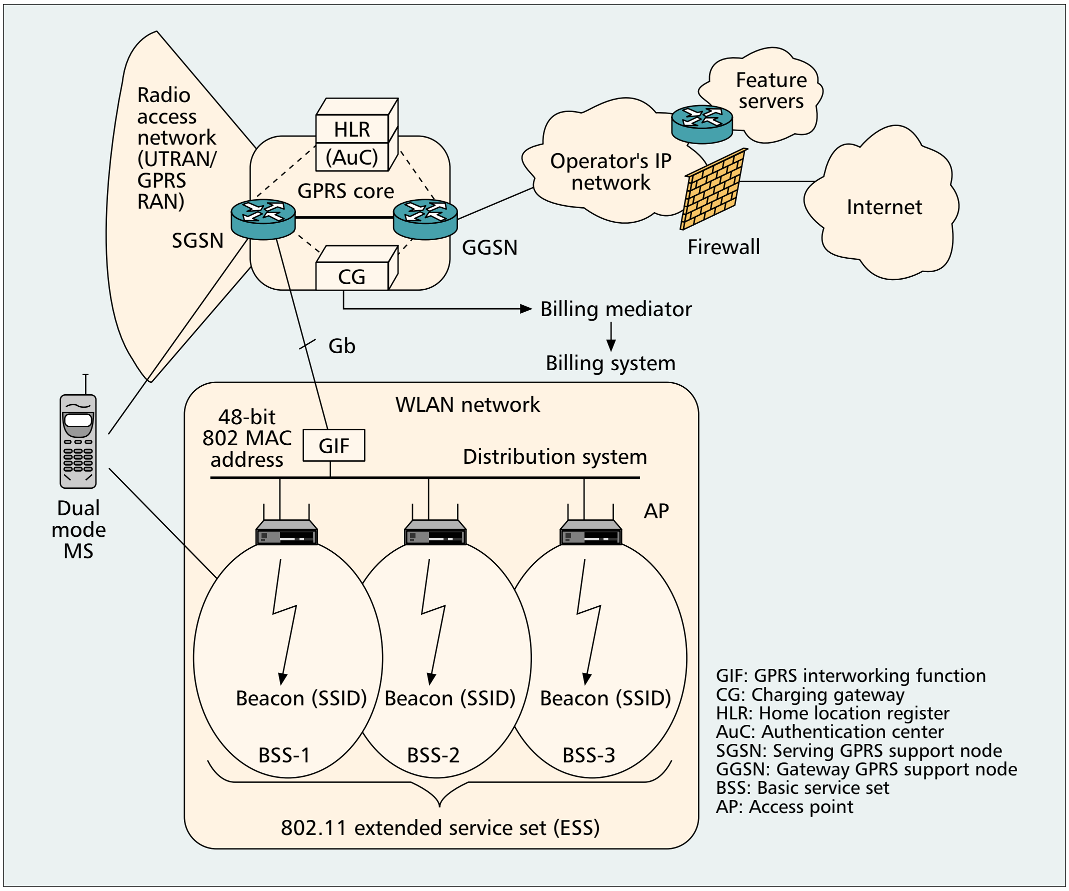
Scenario 4 — Service continuity: The goal of this scenario is to allow access to GPRS-based services as required by scenario 3, and in addition to maintain service continuity across the GPRS and WLAN systems. For example, a user starting to utilize WAP service from the GPRS radio network should be able to continue accessing WAP service after he/she moves to a WLAN system and vice versa. Although service continuity is required by scenario 4, the service continuity requirements are not very stringent. This means that under interworking scenario 4, some services may not be able to continue after a vertical handover to/from the WLAN (e.g., due to varying capabilities and characteristics of access technologies). A typical example could be, for instance, a GPRS-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 system. Also, under scenario 4, change in service quality is possible and may be a consequence of handover between WLAN and GPRS access technologies.

Scenario 5 — Seamless services: This scenario is one step further than scenario 4. Its goal is to provide *seamless* service continuity between GPRS and WLAN. That is, GPRS-based services should be utilized across the GPRS and WLAN access technologies in a seamless manner (without the user noticing any significant differences).

Scenario 6 — Access to 3GPP circuit-switched services: The goal of this scenario is to allow the operator to offer access to circuit-switched services (e.g., normal voice calls) from the WLAN system. Seamless mobility for these services should be provided.

After reviewing the most important standardization activities for interworking between WLANs and cellular networks, we present in the following sections two architectures for WLAN-GPRS integration.

The WLAN network is deployed as an alternative radio access network and connects to the GPRS core network through the standard Gb interface. From the core network point of view, the WLAN is considered as any other GPRS routing area in the system.



■ **Figure 3.** *WLAN-GPRS integration with tight coupling: system configuration.*

A Tight Coupling Architecture

In this section, we propose and discuss a tight coupling architecture that can fulfill the requirements of scenarios 1–4. Depending on the WLAN technology, and in particular on whether the WLAN can support quality of service (QoS) equivalent to the GPRS Release 1999 QoS (as specified in [10]), the proposed architecture might also satisfy the requirements of scenario 5.

The proposed architecture follows the principles of the aforementioned tight coupling approach, as described in [2]. However, in contrast to [2], the proposal specifies a tight coupling architecture for interworking between 802.11 WLAN (not HIPERLAN/2) and GPRS networks. In addition, the proposal assumes that the 802.11 WLAN is connected to the standard Gb interface (not Iu-ps), which is already deployed in live GPRS networks. It is noted that Gb is specified from GPRS Release 1997 and onward, whereas Iu-ps is specified from GPRS Release 1999 and onward. A discussion of the different GPRS Releases can be found in [11].

In general, the proposed tight coupling architecture provides a novel solution for interworking between 802.11 WLANs[3] and GPRS, and features many benefits, such as:

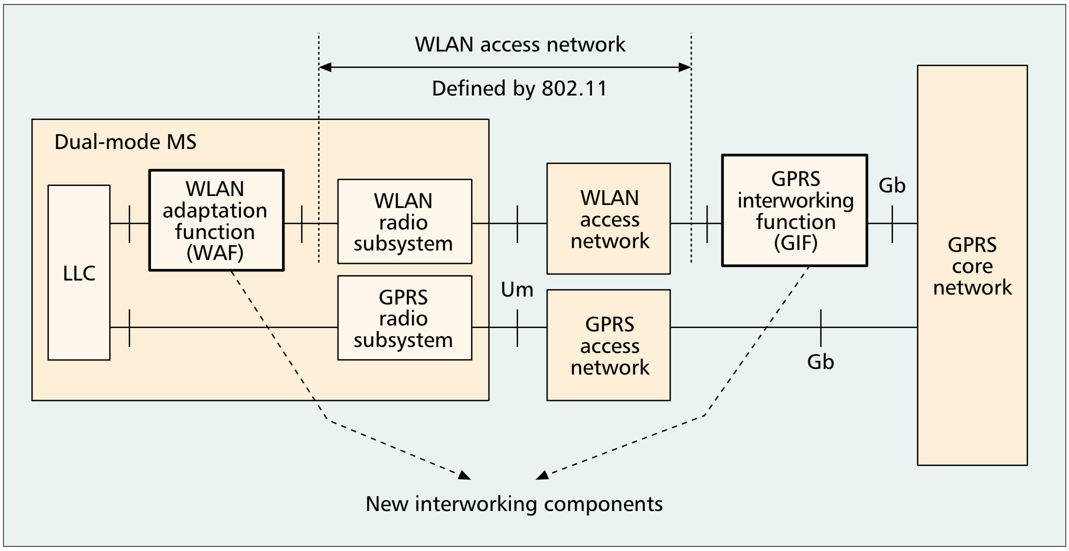
- Seamless service continuation across WLAN and GPRS. The users are able to maintain their data sessions as they move from WLAN to GPRS and vice versa. For services with tight QoS requirements, seamless service continuation is subject to WLAN QoS capabilities.
- Reuse of GPRS AAA.
- Reuse of GPRS infrastructure (e.g., core network resources, subscriber databases, billing systems) and protection of cellular operator's investment.
- Support of lawful interception for WLAN subscribers [12].
- Increased security, since GPRS authentication and ciphering can be applied on top of WLAN ciphering.
- Common provisioning and customer care.
- Access to core GPRS services such as short messaging service (SMS), location-based services, and multimedia messaging service (MMS).

System Description

Figure 3 illustrates the proposed system architecture. A WLAN network is deployed with one or more off-the-shelf access points (APs), which are connected by means of a distribution system (DS). In our system, the DS is a LAN, typically compliant with IEEE 802.3. The WLAN is deployed in an infrastructure configuration, that is, APs behave like base stations, and mobiles exchange data only with APs. The service area of one sole AP is termed a basic service set (BSS) [7]. Each WLAN is typically composed of many BSSs, which all together form an extended service set (ESS) [7].

The WLAN network is deployed as an alternative RAN and connects to the GPRS core network through the standard Gb interface. From the core network point of view, the WLAN is considered like any other GPRS routing area

[3] In the rest of this section, the term WLAN refers to IEEE 802.11 WLAN, unless otherwise specified.



■ **Figure 4.** *Tight coupling over Gb: a reference diagram.*

MSs are dual mode, i.e., they support both GPRS access and WLAN access in a seamless fashion. Seamless mobility is achieved by means of the RA update procedure, which is the core mobility management procedure in GPRS

(RA) in the system. In other words, the GPRS core network does not really identify the difference between an RA with WLAN radio technology and one with GPRS radio technology.

The key functional element in the system is the *GPRS interworking function* (GIF), which is connected to a DS and to a serving GPRS support node (SGSN) via the standard Gb interface. The main function of the GIF is to provide a standardized interface to the GPRS core network and to virtually hide the WLAN particularities. The GIF is the function that makes the SGSN consider the WLAN a typical RA (composed of only one cell).

As discussed below, the existing GPRS protocols in the mobile are fully reused. In particular, the logical link control (LLC) [13], Subnetwork Dependent Convergence Protocol (SNDCP), GPRS mobility management (GMM), and session management (SM) are used in both a standard GPRS cell and a WLAN area. Therefore, the WLAN merely provides a new radio transport for these protocols.

When a mobile station (MS) is outside the WLAN area, its WLAN interface is in passive scan mode, that is, it scans a specific frequency band and searches for a beacon signal. When a beacon is received the service set identifier (SSID) may be checked and compared against a preconfigured SSID. The SSID serves as a WLAN identifier and can help mobiles attach to the "correct" WLAN. For example, an operator could use a unique SSID and request that its subscribers configure their mobiles to consider only this SSID valid.

When an MS detects a valid SSID, it performs the typical authentication and association procedures as specified in [7]. It then enables its WLAN interface, and further GPRS signaling is carried over this interface.

MSs are dual mode, that is, they support both GPRS and WLAN access in a seamless fashion. Seamless mobility is achieved by means of the RA update (RAU) procedure, which is the core mobility management procedure in GPRS [1]. Typically, when a mobile enters a WLAN area, a RAU procedure takes place, and subsequent GPRS signaling and user data transmission are carried over the WLAN interface. Similarly, when the mobile exits a WLAN area, another RAU procedure takes place, and the GPRS interface is enabled and used to carry further data and signaling traffic. From the core network point of view, handover between WLAN and GPRS is considered handover between two individual cells.

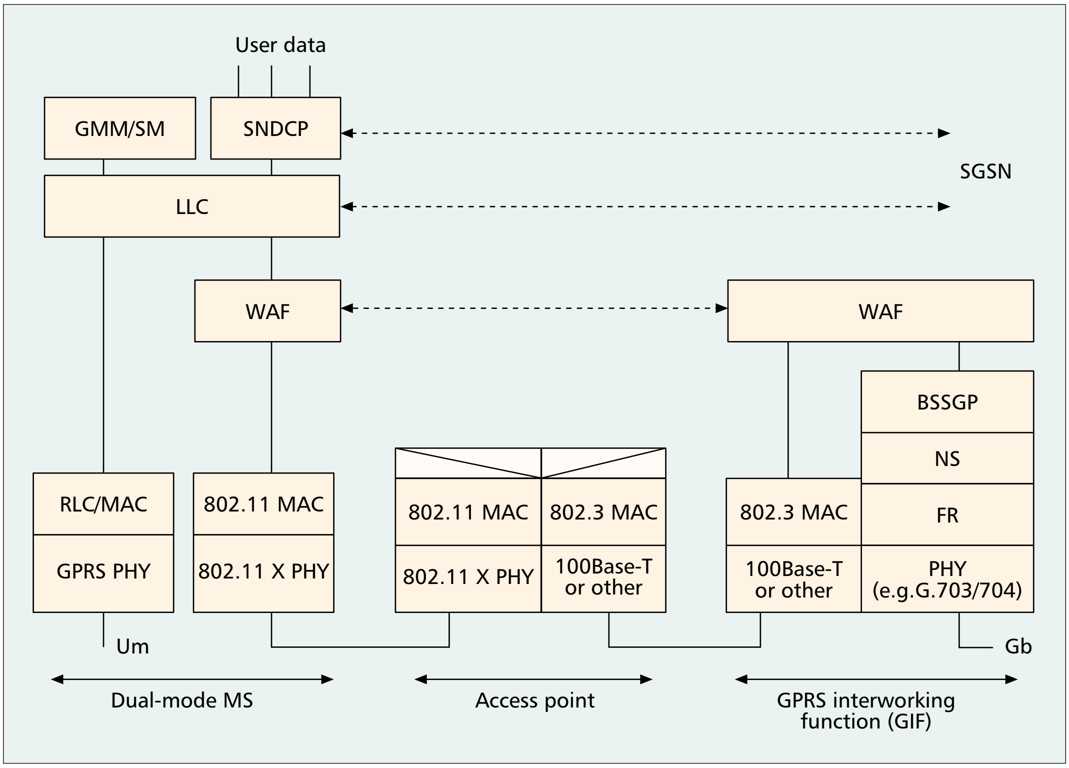
It is important to point out that in an 802.11 WLAN, mobile terminals use 48-bit IEEE 802 addresses as medium access control (MAC) addresses, which are hard-coded in their network interface cards. Such addresses are also used for addressing in the DS; therefore, terminals attached to DS (e.g., GIF) and WLAN terminals share the same address space. In the configuration shown in Fig. 3, MSs in the WLAN send uplink GPRS traffic to the MAC address of GIF; similarly, downlink GPRS traffic is sent from GIF to the MAC addresses of MSs. The way MSs discover the MAC address of GIF as well as the identity of the RA that corresponds to the WLAN is explained below.

The reference diagram of the proposed architecture is illustrated in Fig. 4. The MS has two radio subsystems, one for GPRS access and another for WLAN access. The WLAN adaptation function (WAF) identifies when the WLAN radio subsystem is enabled (i.e., when the MS associates with a valid AP) and informs the LLC layer, which subsequently redirects signaling and data traffic to the WLAN. Note that all standard GPRS protocols operating on top of LLC (SNDCP, GMM, SM) function as usual and do not identify which radio subsystem is used. WAF is a key component in MS and is discussed below in more detail.

Protocol Architecture

The protocol architecture is illustrated in Fig. 5. As shown, the MS supports two radio subsystems (or interfaces) for transporting GPRS signaling and user data. The first interface is implemented with the GPRS-specific radio link control (RLC)/MAC and physical layers, whereas the sec-

The main component in the proposed tight coupling system is the WLAN Adaptation Function, which is implemented in every dual mode MS and in the GIF, and supports the appropriate interworking functions. With the aid of WAF it becomes feasible to transport GPRS signaling and data over 802.11 WLANs.



■ **Figure 5.** *Tight coupling over Gb: protocol architecture.*

ond is implemented with the 802.11-specific MAC and physical layers. These two interfaces provide two alternative means for transporting of LLC packet data units (PDUs). Typically, when the MS is outside a WLAN area, LLC PDUs are transmitted over the GPRS interface (Um). However, when the mobile enters a WLAN area, LLC PDUs are transmitted over the WLAN interface. This switching is performed with the aid of WAF and could be completely transparent to the user and to upper GPRS layers.

As shown in Fig. 5, WAF operates in both MS and GIF. It provides an adaptation function for interworking between LLC and 802.11 MAC (in the mobile) and between 802.3 MAC and BSSGP (in the GIF). The signaling exchanged between the two WAF peers is described in the next section. Apart from WAF, also GIF implements the GPRS protocols specified on the Gb interface: frame relay (FR), network service (NS), and Base Station Subsystem GPRS Protocol (BSSGP) [1].

The access point (AP) implements the 802.11 and 802.3 protocols and a simple interworking function that provides bridging between them. Such APs are already available in the market.

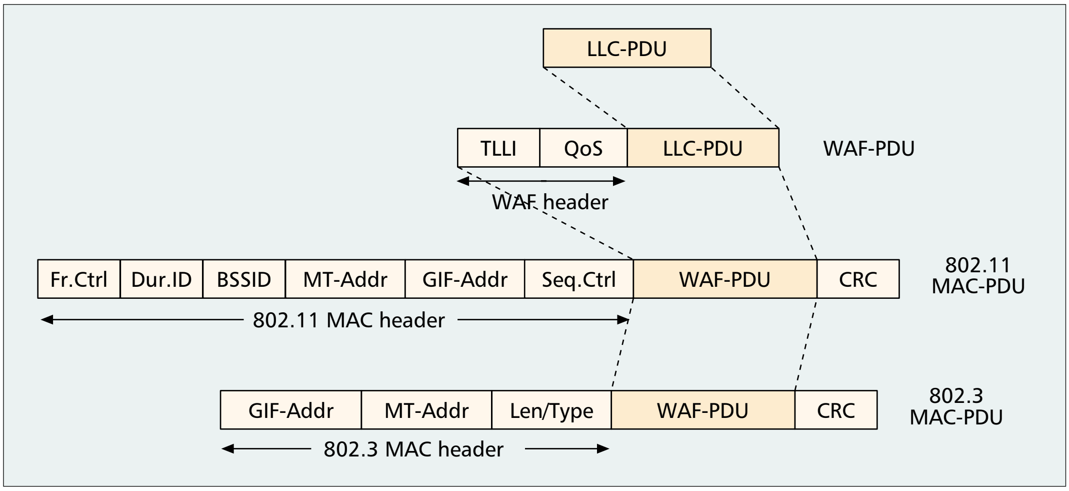
WLAN Adaptation Function

The main component in the proposed tight coupling system is the WAF, which is implemented in every dual mode MS and in the GIF, and supports the appropriate interworking functions. With the aid of WAF it becomes feasible to transport GPRS signaling and data over 802.11 WLANs.

WAF provides the following functions:

- It signals the activation of WLAN interface when the mobile enters a WLAN area. It also signals the change of RA to GMM when a mobile enters a WLAN area and gets associated with an AP.
- It supports the GIF/RAI discovery procedure (discussed below), which is initiated by MSs in order to discover the MAC address of GIF and the RA identity (RAI) of the WLAN.
- It supports the paging procedure on Gb, used when the SGSN needs to page an MS. During this procedure, WAF sends an appropriate signaling message to MS in order to alert it and respond to page.
- It transfers uplink LLC PDUs from the MS to the GIF by using the transport services provided by the 802.11 MAC. It also transfers downlink LLC PDUs from the GIF to mobiles.
- It supports QoS by implementing transmission scheduling in GIF and in the MS.
- It transfers the temporary logical link identifier (TLLI) and QoS information in the WAF header. The TLLI is a temporary MS identifier used by LLC layer for addressing purposes (see [13] for further details).

The encapsulation scheme used in the uplink direction as well as the format of a WAF PDU are illustrated in Fig. 6. Each LLC PDU is encapsulated into a WAF PDU, which includes TLLI and QoS in the header. TLLI is used by GIF to update an internal mapping table that correlates TLLIs with 802 MAC addresses. In order to support the paging procedure, GIF also needs to correlate IMSIs with 802 MAC addresses. The correlation between TLLIs and 802 MAC addresses is used for forwarding downlink LLC PDUs received on the Gb interface to the correct mobile on the WLAN. Note that the SGSN uses TLLI on Gb as address information, whereas the WLAN utilizes 802 MAC addresses.



■ **Figure 6.** *The encapsulation scheme.*

The correlation between TLLIs and 802 MAC addresses is used for forwarding downlink LLC PDUs received on the Gb interface to the correct mobile on the WLAN. Note that the SGSN uses TLLI on Gb as address information, whereas the WLAN utilizes 802 MAC addresses.

In the uplink direction, QoS contains the following attributes:

- Peak throughput
- Radio priority
- RLC mode [13, 14]

These QoS attributes are primarily used for scheduling in the MS and GIF. In the downlink direction, the QoS may be empty, since there is no need to transfer any QoS parameters to the mobile.

The 802.11 and 802.3 MAC headers shown in Fig. 6 are the standard headers specified by the 802.11 and 802.3 standards, respectively.

GIF/RAI Discovery Procedure

GIF/RAI discovery is a key procedure carried out immediately after an MS enters an 802.11 WLAN area and gets associated with an AP. The WAF in the MS initiates this procedure:

- To discover the 802 MAC address of GIF. All uplink LLC PDUs are subsequently transmitted to this MAC address.
- To discover the RAI that corresponds to the WLAN network.
- To send the MS's IMSI value to GIF. This value is subsequently used by GIF to support the GPRS paging procedure. By knowing the IMSI of a particular MS, GIF can forward subsequent paging messages from the SGSN.

Figure 7 illustrates the signaling flow during the GIF/RAI procedure. This procedure is initiated after the 802.11 MAC layer is enabled (i.e., after the mobile gets associated with a particular AP). The WAF layer in an MS sends a request to 802.11 MAC to transmit a PDU with source address (SA) equal to the MS's MAC address and destination address equal to *broadcast*. This PDU is a *GIF/RAI Discover Request* message that includes the IMSI value of the MS. The 802.11 MAC layer transmits an 802.11 MAC PDU with the appropriate address information (designated Addr1, Addr2, Addr3). Note that this PDU is directed to the AP with identity *BSSID*. The AP broadcasts this message to the DS and is finally received by the GIF, which associates the IMSI with the MS's 802 MAC address (designated MS). Subsequently, the WAF in the GIF responds with a *GIF/RAI Discover Response* that includes the RAI of the WLAN. The MS receives this response, stores the GIF address and the RAI, and notifies the GMM layer that the current GPRS RA has changed. In response, the GMM layer initiates the normal GPRS RAU procedure and notifies the SGSN that the MS has changed RA. After that, normal GPRS data and signaling is performed over WLAN.

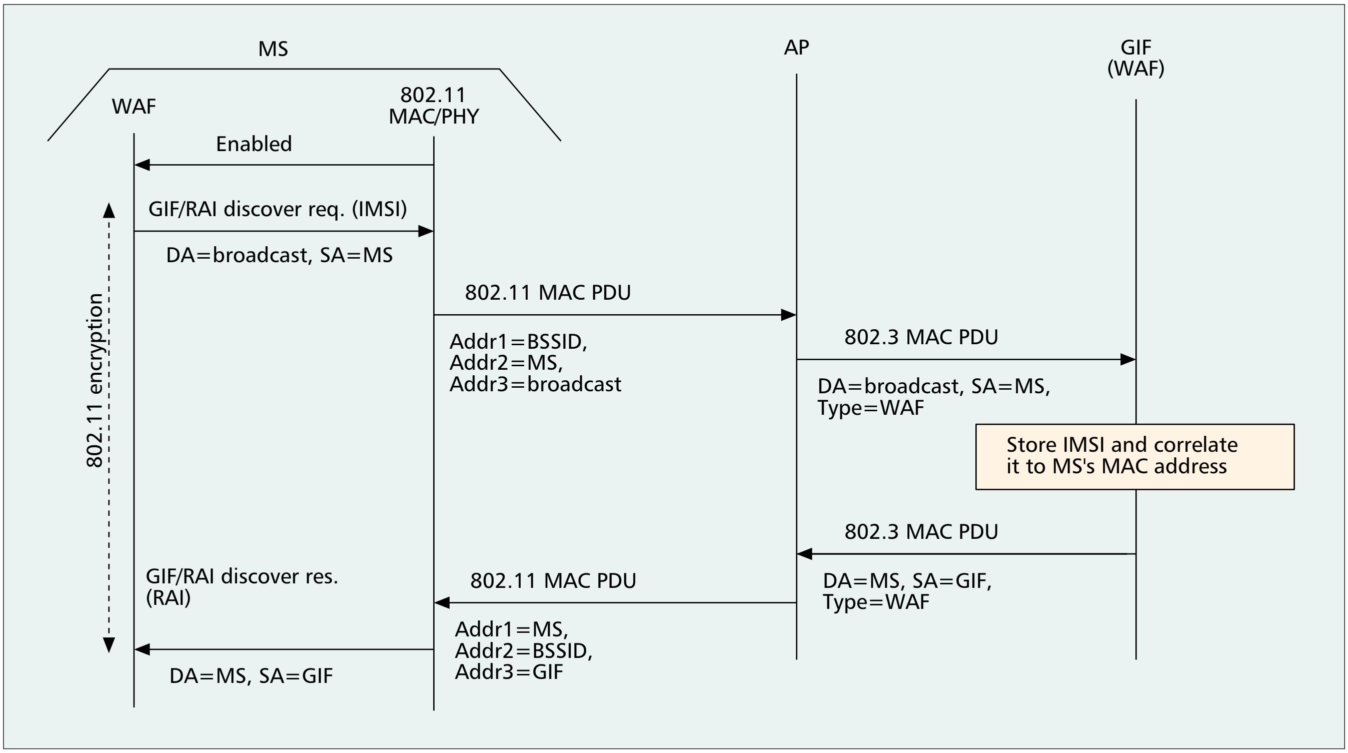
In conclusion, with the proposed tight-coupling system we have shown that, with the aid of WAF, MSs can seamlessly move between WLAN and GPRS radio access and use the normal GPRS procedures for mobility management.

A Loosely Coupled Architecture

As mentioned previously, loose coupling is another approach that provides interworking between GPRS and WLAN at the Gi interface (Fig. 2). In this section we propose a specific loosely coupled interworking architecture and explain its key aspects.

Figure 8 illustrates the proposed loosely coupled architecture. As can be seen, the WLAN network is coupled with the GPRS network in the operator's IP network. Note that, in contrast to tight coupling, the WLAN data traffic does not pass through the GPRS core network but goes directly to the operator's IP network (and/or Internet). In this architecture, SIM-based authentication may be supported in both the GPRS and WLAN networks to gain access to the operator's services. This architecture also supports integrated billing, via the billing mediator, in a common billing system. The WLAN network may be owned by a third party, with roaming/mobility enabled via a dedicated connection between the operator and the WLAN, or over an existing public network, such as the Internet (although only one method of roaming is required, both connections are shown in Fig. 8 for completeness).

Loose coupling utilizes standard IETF-based protocols for authentication, accounting, and mobility. It is therefore not necessary to introduce cellular technology into the WLAN network, as it is with tight coupling. Roaming can be enabled across all types of WLAN implemen-

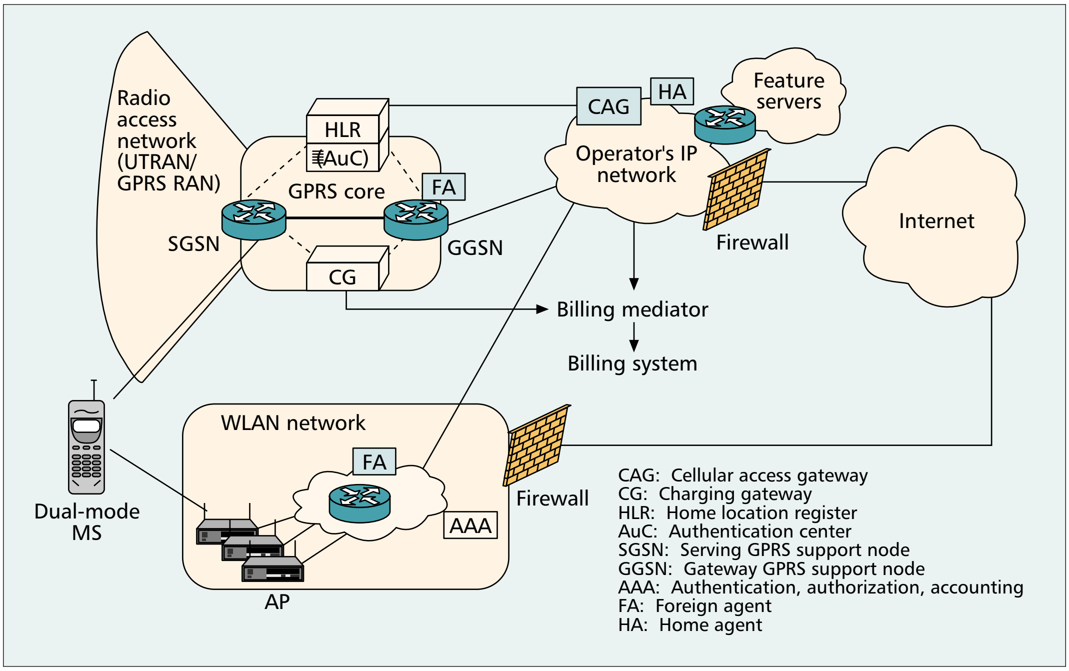


■ **Figure 7.** *Signaling flow during a GIF/RAI discovery procedure.*

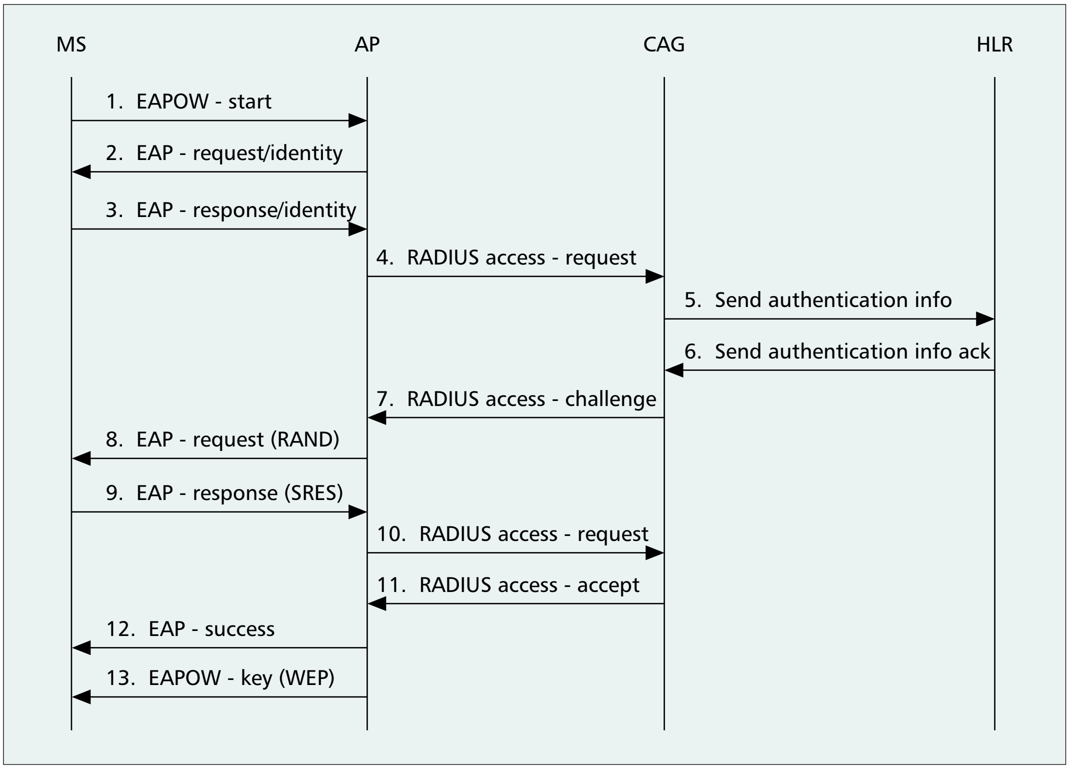
tations, regardless of who owns the WLAN, solely via roaming agreements. The following sections describe the key aspects of security, billing, and mobility of this architecture in more detail.

Authentication

An authentication similar to GPRS may occur within the WLAN network, depending on the particular implementation. Where the GPRS operator owns the WLAN, it is most likely that the operator will want to reuse SIM-based authentication (or USIM-based for UMTS subscribers) within the WLAN environment. Similarly, for a subscriber to access services provided by a GPRS operator over any WLAN access network, regardless of whether the WLAN is owned by a GPRS operator, (U)SIM-based authentication may be used. The architecture proposed here, and illustrated in Fig. 9, supports (U)SIM-based authentication in much the same way as in



■ **Figure 8.** *WLAN-GPRS integration with loose coupling: system configuration.*


MS
AP
CAG
HLR
1. EAPOW - start
2. EAP - request/identity
3. EAP - response/identity
4. RADIUS access - request
5. Send authentication info
6. Send authentication info ack
7. RADIUS access - challenge
8. EAP - request (RAND)
9. EAP - response (SRES)
10. RADIUS access - request
11. RADIUS access - accept
12. EAP - success
13. EAPOW - key (WEP)

■ **Figure 9.** *SIM-based authentication over WLAN.*

GPRS. The cellular access gateway (CAG) acts as an authenticator for WLAN users.

The authentication procedure shown in Fig. 9 is based on deployment of IEEE 802.1X [15] with 802.11 [7]. In this architecture, the CAG provides the AAA server functionality in the cellular operator's IP core. The CAG interworks with the home location register (HLR) to obtain the authentication credentials used to create the authentication challenge to the MS and validate the response to the challenge. To do this, the CAG must interact with the HLR similar to the way SGSN interacts with the HLR in the standard GPRS authentication procedure. The Extensible Authentication Protocol (EAP) [17] is used in the WLAN to perform authentication of the MS, passing the subscriber identity, SIM-based authentication data, and encrypted session key(s) to be used for encryption for the life of the session. Where it is undesirable to use SIM-based authentication in the WLAN system, standard username/password procedures may be used.

The signaling diagram in Fig. 9 conforms to the principles in 802.1X and to GSM/AKA authentication as specified in [17]. The authentication flow starts right after the MS has associated with an AP. At first, the MS sends an EAP-Over-WLAN (EAPOW) Start message to trigger the initiation of 802.1X authentication. In steps 2 and 3 the identity of the MS is obtained with the standard EAP-Request/Response messages defined in [16]. Next, the AP initiates a RADIUS [18] dialog with the CAG by sending an Access-Request message that contains the identity reported by MS. In our case (we consider SIM-based authentication), this identity typically includes the IMSI value stored in the SIM card. CAG uses IMSI and possibly other information included in identity (e.g., a domain name) to derive the address of the HLR that holds subscription data for that particular MS. In steps 5 and 6, the CAG retrieves one or more authentication vectors from the HLR. These could be either UMTS authentication vectors (if the MS is equipped with a USIM) or GSM authentication vectors (see [1] for their differences). In both cases, a random challenge, RAND, and an expected response, XRES, is included in every authentication vector. In steps 7 and 8, the random challenge is sent to the MS, which runs the authentication algorithm implemented in the (U)SIM card and generates a challenge response value (SRES). In steps 9 and 10, SRES is transferred to CAG and compared against the corresponding XRES value received from the HLR. If these values match, a RADIUS Access-Accept is generated in step 11 (otherwise, a RADIUS Access-Reject is generated). This instructs AP to authorize the 802.1X port and allow subsequent data packets from the MS. Note that the RADIUS Access-Accept message may also include authorization attributes, such as packet filters, which are used for controlling the user's access rights in the specific WLAN environment. In step 12, the AP transmits a standard EAP-Success message and subsequently an EAPOW-Key message (defined in [15]) for configuring the session key in the MS.

Note that the authentication and authorization in the above procedure is controlled by the MS's home environment (i.e., home GPRS network). The AP in the visited WLAN implements 802.1X and RADIUS but relies on the HLR in the home environment to authenticate the user.

EAP is used in the WLAN to perform the authentication of the MS, passing the subscriber identity, SIM-based authentication data, and encrypted session key(s) to be used for encryption for the life of the session. In the case where it is undesirable to use SIM-based authentication in the WLAN system, standard username/password procedures may be used.

The functionality of the billing mediator is to convert accounting statistics from both the GPRS and WLAN access networks into a format native to the particular billing system used by the operator. The billing system may be an existing GPRS system, or a standard, IP based system used primarily by wireline ISPs.

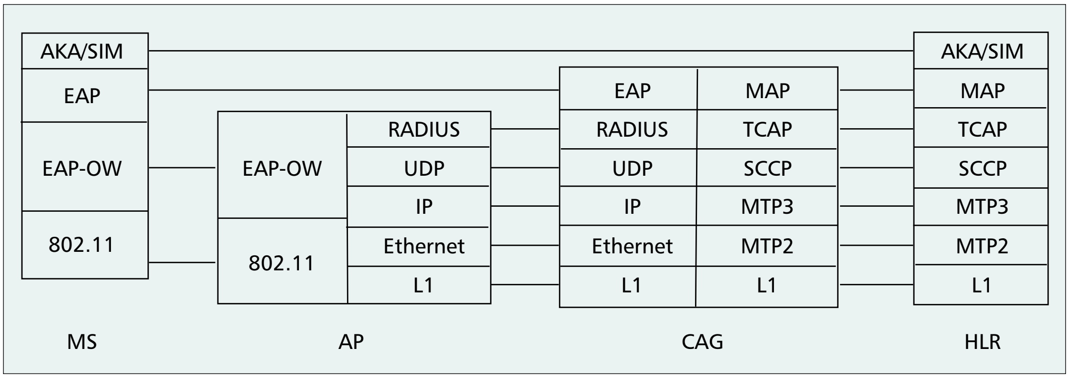


Figure 10. *A loosely coupled WLAN control plane for authentication.*

As shown in Fig. 10, which illustrates the protocol architecture for the aforementioned authentication, the MS is ultimately authenticated by HLR by means of either GSM AKA or UMTS AKA mechanisms.

Encryption

A commonly believed weakness of the 802.11 WLAN standard is in its encryption technology. Wired Equivalent Privacy (WEP) has been shown to be a relatively inefficient encryption scheme, if used as is as the only form of encryption. With the use of EAP, WEP may be enhanced by the use of a unique session key for each user of the WLAN. Typically, a WEP-encrypted channel may be compromised in a matter of hours due to its weak encryption algorithm and the standard practice of a universal key, shared by all users of the WLAN network. By implementing 802.1X, the sharing of keys is no longer necessary, since a new key is derived on a per-user per-session basis. Even if the session duration exceeds the amount of time for a breech to occur, the attacker may only use the key to decrypt data of the session to which the key belongs, and only for the remaining duration of that session, while all other sessions remain secure. To further enhance security, the WLAN system may support the more advanced encryption schemes specified in [19].

Billing

Integrated billing is achieved via the billing mediator function in the loosely coupled architecture of Fig. 8. The AP in the WLAN network may report accounting statistics to the CAG via standard AAA procedures (e.g., RADIUS accounting), which will subsequently report these statistics to the billing mediator. Similarly, the GPRS core (i.e., SGSN/GGSN) will report accounting statistics pertaining to GPRS usage. The functionality of the billing mediator is to convert accounting statistics from both the GPRS and WLAN access networks into a format native to the particular billing system used by the operator. The billing system may be an existing GPRS system, or a standard IP-based system used primarily by wireline ISPs.

Session Mobility

In contrast to tight coupling approach, which uses GPRS mobility management for session mobility, in the loose coupling approach, Mobile IP (MIP) can be used to provide session mobility across GPRS and WLAN domains. The MIP framework [20] consists of a MIP client (the MS), a foreign agent (FA), and a home agent (HA). As shown in Fig. 8, the FA in the GPRS network resides in the GGSN, while the FA in the WLAN can reside in an access router. On the other hand, the HA is located in the operator's IP network. When the MS moves from GPRS to WLAN, it performs a MIP registration via the FA that resides in the WLAN. The FA completes the registration with the HA, by providing a care-of address to the HA to be used as a forwarding address for packets destined to the MS. The FA then associates the care-of address with that of the MS and acts as a proxy on behalf of the MS for the life of the registration. This way, the MS does not need to change its IP address when it moves to WLAN (the same holds true when the MS moves from WLAN to GPRS). A more detailed description of MIP operation can be found in [20].

Concluding Remarks

With no doubt, the recent evolution and successful deployment of WLAN systems worldwide has fueled the need for interworking mechanisms between WLANs and cellular data networks such as GPRS. In response to this need, several fora and standardization bodies worldwide have initiated various activities on exploiting WLAN technology and integrating this technology into cellular data networks. One of the most notable examples is 3GPP, which is currently addressing this kind of integration within the recently approved work item on WLAN-cellular interworking.

As mentioned before, there are two generic approaches for WLAN-cellular integration: tight coupling and loose coupling. In Table 1 we show a brief comparison between these two coupling methods.

With tight coupling the WLAN connects to the SGSN either via an already standardized interface (e.g., Gb or Iu-ps) or a new interface, specified for optimal performance with WLANs. Tight coupling indeed provides firm coupling between WLAN and GPRS, and its main advantage is enhanced mobility across the two domains, which is entirely based on GPRS mobility management protocols. In addition, tight coupling offers reuse of GPRS authentication, authorization, and accounting, and protects

Category	Tight coupling	Loose coupling
Authentication	• Reuse GPRS authentication for WLAN user • Reuse GPRS ciphering key for WLAN encryption	Cellular access gateway to provide SIM-based authentication interworking. RADIUS (only) based authentication is an alternative
Accounting	Reuse GPRS accounting	Billing mediator to provide common accounting
WLAN-cellular mobility	SGSN is the call anchor, and intra-SGSN handovers provide mobility	Home agent is the call anchor, and Mobile IP handovers between GGSN and access router provide mobility. Home sgent could be collocated at the GGSN or CAG, or somewhere in an external network.
Context transfer	Fine-grained context information is available, e.g., QoS parameters, information about multiple flows, etc.	Limited context transfer possible between GGSN and WLAN through current draft proposals in IETF Seamoby working group
System engineering	Impact of high-speed WLAN network on existing GSN from bearer and signaling standpoint is an issue	WLAN and GPRS networks can be engineered separately
New development	• WLAN terminal modifications for GPRS signaling • Modifications in WLAN network or modifications in SGSN	• CAG for SIM-based authentication • Billing mediator for accounting
Standardization	A new interface in the SGSN might be required, specifically for connecting to WLANs.	EAP-SIM and EAP-AKA is being pursued in IETF PPPext working group
Target usage	Applies primarily to WLAN networks owned by cellular operators. Has limited application when WISP is different from cellular operator.	Applies more broadly

Table 1. *Loose vs. tight coupling: a side-by-side comparison.*

The recent evolution and successful deployment of WLAN systems has fueled the need for interworking mechanisms between WLANs and cellular data networks. In response, several forums and standardization bodies worldwide have initiated several activities for exploiting WLAN technology and integrating this technology into cellular data networks.

the operator's investment by reusing the GPRS core network resources, subscriber databases, billing systems, and so on. Moreover, it can support GPRS core services such as SMS and lawful interception for WLAN subscribers.

Nevertheless, tight coupling is primarily tailored for WLANs owned by cellular operators and cannot easily support third-party WLANs. Also, there are some cost and capacity concerns associated with the connection of a WLAN to an SGSN. For example, the throughput capacity of an SGSN could be sufficient for supporting thousands of low-bit-rate GPRS terminals but could not be sufficient for supporting hundreds of high-bit-rate WLAN terminals. More important, tight coupling cannot support legacy WLAN terminals, which do not implement the GPRS protocols. These are some of the reasons that account for the current trend toward loose coupling.

Loose coupling is mainly based on IETF protocols, which are already implemented in live WLANs. Consequently, it imposes minimal requirements on WLANs. However, it mandates the provisioning of new equipment by the cellular operator — mainly, specific AAA servers for interworking with WLANs. It also requires the implementation of MIP for supporting mobility across the two access networks. The typical high latency associated with MIP registrations is an issue and might not permit seamless session handovers for some demanding applications.

In general, the choice of the optimal interworking architecture should be determined by a number of factors. For example, if the wireless network is composed of a large number of WLAN operators and cellular operators, the loosely coupled architecture would be the best choice. On the other hand, if the WLAN network is exclusively owned and operated by a cellular operator, the tightly coupled architecture might become more attractive. Independent of the choice of architecture, WLAN technology can and will play an important role in supplementing wide-area cellular data networks and enabling IP multimedia services in hotspots.

References

[1] 3GPP, "General Packet Radio Service (GPRS); Service Description," Tech. spec. 3GPP TS 23.060 v3.12.0, June 2002; http://www.3gpp.org/ftp/specs/2002-06/R1999/23_series/23060-3c0.zip).

[2] ETSI, "Requirements and Architectures for Interworking between HIPERLAN/3 and 3rd Generation Cellular Systems," Tech. rep. ETSI TR 101 957, Aug. 2001.

[3] ETSI, Broadband Radio Access Networks (BRAN); HIPERLAN Type 2, System Overview, ETSI TR 101 683, Feb. 2000.

[4] K. Pahlavan *et al.*, "Handoff in Hybrid Mobile Data Networks" *IEEE Pers. Commun.*, Apr. 2000.

[5] P. Krishnamurthy *et al.*, "Handoff in 3G Non-Homogeneous Mobile Data Networks," *Euro. Microwave Week*, Oct. 1998.

[6] P. Krishnamurthy *et al.*, "Scenarios for Inter-Tech Mobility," WiLU tech. rep., Jan. 1998.

[7] IEEE 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.

[8] 3GPP, "Feasibility Study on 3GPP System to WLAN Interworking," Tech. rep. 3GPP TR 22.934 v1.2.0, May 2002.

Independent of the choice of the architecture, WLAN technology can and will play an important role in supplementing wide-area cellular data networks and enabling IP multimedia services in hotspots.

[9] 3GPP, "IP Multimedia Subsystem; Stage 2," Tech. spec. 3GPP TS 23.228 v5.5.0, June 2002.

[10] 3GPP, "QoS Concept and Architecture," Tech. spec. 3GPP TS 23.107 v5.5.0, June 2002.

[11] A. K. Salkintzis, "Chapter 3: Network Architecture and Reference Model," *Broadband Wireless Mobile — 3Gwireless and Beyond*, Wiley, to be published.

[12] 3GPP, "3G Security; Lawful Interception Architecture and Functions," Tech. spec. 3GPP TS 33.107 v3.5.0, Mar. 2002.

[13] 3GPP, "Logical Link Control Layer Specification," 3GPP TS 04.64 v8.7.0, Dec. 2001.

[14] 3GPP, "BSS GPRS Protocol," 3GPP TS 08.18 v8.10.0, May 2002.

[15] IEEE 802.1X, "Port-Based Network Access Control," 2001.

[16] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," IETF RFC 2284, Mar. 1998.

[17] J. Arkko and H. Haverinen, "EAP AKA Authentication," Internet draft draft-arkko-pppext-eap-aka-04, June 2002.

[18] C. Rigney *et al.*, "Remote Authentication Dial In User Services (RADIUS)," IETF RFC 2138, Apr. 1997.

[19] IEEE 802.11i/D2.3, "Specification for Enhanced Security," Aug. 2002.

[20] C. Perkins, "IP Mobility Support for IPv4," IETF RFC 3220, Jan. 2002.

Additional Reading

[1] 3GPP, "3GPP System to WLAN Interworking; Functional and Architectural Definition," Tech.rep. 3GPP TR 23.934 v0.3.0, June 2002.

Biographies

APOSTOLIS K. SALKINTZIS (a.k.salkintzis@ieee.org) received his Diploma in 1991 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. 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 of the Advanced Systems Institute of British Columbia, Canada, and 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, working on the design and standardization of modern telecommunication networks, such as GPRS and UMTS. He has served as principal guest editor in many special issues and has published over than 40 papers in IEEE journals and international conferences. His primary research activities lie in the area of wireless digital communication networks, and he is particularly interested in mobility management, IP multimedia over mobile telecommunication networks, mobile channel modeling, diversity techniques in multipath fading channels, radio modem design with DSPs, and multiple access and data link protocols. Currently, he is most active in the design and standardization of GPRS and UMTS, networks and is an active participant and contributor in 3GPP.

CHAD FORS [M] (chad.fors@motorola.com) is a principal staff engineer at Motorola, Inc., Arlington Heights, Illinois. Since he began with Motorola in May 1995, he has worked in the areas of second- and third-generation cellular voice and data networks, with more recent emphasis on architecture, analysis, and design of cellular/IP hybrid networks. Since mid-2001 he has focused on the integration of WLAN and cellular systems, including common authentication, billing, and mobility mechanisms across technologies. He earned his B.Sc. degree in electrical engineering, specializing in communications systems, from Iowa State University in 1995. He holds one U.S. patent.

RAJESH PAZHYANNUR (rajesh.pazhyannur@motorola.com) received his Ph.D. in electrical and computer engineering from the University of Wisconsin-Madison in 1996. Since 1996 he has been part of the Network Advanced Technology group in Motorola. His research interests include performance analysis of cellular networks with focus on flow control algorithms and QoS. He has worked on designing IP-based radio access networks for cellular systems transporting voice and data. More recently, he has been investigating 802.11-based WLANs focusing on architectural and performance issues.