Interworking between WLANs and 3G - Part 3: Loose coupling

Vijay Garg - November 12, 2010

[Part 1 begins with a look at interworking objectives and requirements, as well as interworking schemes to connect WLANs and 3G networks. Part 2 examines the tight coupling interworking approach, where the WLAN is connected to the 3GPP (GPRS) core network in the same way as any other radio access network.]

22.8 System Description with Loose Coupling

Figure 22.11 shows the system architecture with loose coupling. The WLAN 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.

In this architecture, SIM-based authentication can be supported in both the GPRS network and the WLAN to gain access to the operator's services. The architecture also supports integrated billing, via the billing mediator, in a common billing system. The WLAN 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.
Loose coupling utilizes standard IETF-based protocols for authentication, accounting, and mobility. Roaming can be enabled across all types of WLAN implementations, regardless of who owns the WLAN, solely via roaming agreements.

The WLAN access network connects to the GPRS data network like a different type of radio access network for interworking. This allows for the support of the legacy WLAN access networks, which commonly support RADIUS/ DIAMETER protocols in the WLAN access network. This approach defines some new interfaces with well-defined functions and commonly used protocols. The new interfaces are discussed below (see Figure 22.17).

- **$W_0/W_e$ interface.** This interface connects the WLAN access network with the visited 3GPP data network or the home 3GPP data network. The $W_e$ interface transports authentication, authorization, and other related information. The $W_s$ interface transports charging related information. The $W_e$ interface logically connects the WLAN capable user to the AAA server, which resides in the cellular operator home network. The WLAN capable user is authenticated and authorized by the AAA server. The WLAN related subscription information for the user are stored in home location register/home subscriber server (HLR/HSS). The extensible authentication protocol (EAP) is used for this purpose between the WLAN capable user and the AAA server. To accommodate the existing WLAN access networks, which support RADIUS or DIAMETER, the $W_0/W_e$ interface uses DIAMETER protocol toward the AAA server. The principle of authentication is mutual authentication. Two methods of mutual authentication are currently defined, EAP/SIM and EAP/AKA. The EAP/AKA is used for subscribers with USIM and EAP/SIM is used for subscribers with SIM. The existing SIM subscribers’ authentication in cellular networks is not based on mutual authentication. This is the reason that the authentication methods are different for SIM- and USIM-based WLAN users.

- **$W_n$ interface.** This interface transports tunneled WLAN user data toward the packet data gateway in the home network and vice versa. The $W_n$ interface is used to transport tunneled data between the home packet data gateway in the home network and the visited data border gateway in the visited network if the WLAN access network is not directly connected to the home network. It is also possible that the packet data is directly routed by the WLAN access network to the external IP network. This is the reason that this interface is service specific. If the packet data is routed by the packet data gateway then there are two ways of transporting the user packet data to the packet data gateway. One method is to establish a secure tunnel between the WLAN access network and the packet data gateway. This method is called network based tunneling as the WLAN user is not involved. The other method establishes a direct secure tunnel between the WLAN user client and
the packet data gateway. This method is referred to as client based tunneling. The $W_i$ interface is used to inform the WLAN access network about tunneling related information.

- **$W_i$ interface.** This interface connects the AAA server with HLR/HSS. The AAA server retrieves the authentication vectors over this interface from the HLR/HSS. The AAA server also retrieves the WLAN access-related subscriber information using this interface. This interface is also used by the AAA server to register itself for an authorized WLAN-capable user with the HLR/HSS. This interface also helps the AAA server to get an indication of subscription-related changes from the HLR/HSS. The AAA server generates temporary identifiers for the WLAN user for security. The temporary identifiers are used as far as possible over the WLAN radio access network by the WLAN user. This interface is quite similar to the mobile application part (MAP) $G_r$ interface defined between SGSN and HLR/HSS. This interface is based on the MAP or DIAMETER protocol.

- **$W_f$ interface.** This interface connects the AAA server with the 3GPP charging control function or charging gateway function. This interface transports charging data toward the 3GPP charging control/gateway function. The charging data is collected by the AAA server from either the packet data gateway over the $W_m$ interface or the $W_i$ interface from the WLAN access network or both. This interface is based on DIAMETER or GPRS tunneling protocol (GTP).

- **$W_c$ interface.** This interface connects the AAA server with the 3GPP on-line charging system for credit control checks for the WLAN-capable user. This interface is based on DIAMETER protocol.

- **$W_m$ interface.** This interface connects the AAA server with the packet gateway for transport of charging, related information and tunneling related information to the AAA server from packet data gateway. This interface is based on DIAMETER protocol.

- **$W_I$ interface.** This interface connects the packet data gateway with the packet data network. The packet data network may be an external public or private data network or an operator's internal packet data network. The protocol for this interface is dependent upon the packet data network.

**Authentication**

An authentication similar to GPRS may occur within the WLAN, depending on the implementation. Where the GPRS operator owns the WLAN, it is likely that the operator will reuse SIM-based authentication or 3GPP-based USIM authentication 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 can be used.

To reuse the 3GPP subscription, 3GPP interworking WLAN terminals will need access to UICC smart cards with SIM/USIM applications. A WLAN equipped with a SIM/USIM smart card is called WLAN UE. Given the need for dual-mode (WLAN-cellular) UEs, SIM/USIM will be available in those UEs. The architecture of interworking WLAN access reusing 3GPP USIM/SIM and HSS is shown in Figure 22.12.
Figure 22.12 WLAN system architecture reusing the 3GPP subscription.

The authentication procedure shown in Figure 22.13 is based on the deployment of IEEE 802.1X with 802.11.

Figure 22.13 SIM-based authentication over WLAN.

The cellular access gateway provides the AAA server functionality in the cellular operator's IP core. The access gateway interworks with the home location register (HLR) to obtain the authentication parameters used to create the authentication challenge to the UE and validate the response to the challenge. The EAP is used in the WLAN to perform authentication of the UE, passing the subscriber identity, SIM-based authentication data, and encrypted session key(s) to be used for encryption for the life of the session [3,4].

The authentication process starts after the UE has associated with an AP. The UE 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 UE is obtained with standard EAP-Request/Response messages (see Figure 22.13).

Next, the AP initiates a RADIUS dialog with the access gateway by sending an Access-Request message that contains the identity reported by UE. In the SIM-based authentication, this identity
typically includes the IMSI value stored in the SIM card. The access gateway uses IMSI and other information included in the identity (i.e., a domain name) to derive the address of the HLR/HSS that contains subscription data for that particular UE.

In steps 5 and 6, the access gateway retrieves one or more authentication vectors from the HLR/HSS. These could be either UMTS authentication vectors (if the UE is equipped with a USIM) or GSM authentication vectors. 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 challenges sent to the UE, 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 the access gateway and compared against the corresponding XRES value received from the HSS. 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 UE. 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 for configuring the session key in the UE.

Note that the authentication and authorization in the above procedure is controlled by UE’s home environment (i.e., home GPRS network). The AP in the visited WLAN implements 802.1X and RADIUS but relies on the HSS in the home environment to authenticate the user. Figure 22.14 shows the protocol architecture for the authentication process. The UE is ultimately authenticated by HSS by means of either the GSM AKA or the UMTS AKA mechanisms.

![Figure 22.14 A loosely coupled WLAN control plane for authentication.](image_url)

The WLAN access network is connected to a 3GPP AAA proxy via the W, reference point. The W, reference point is used for authentication and key agreement signaling, and the protocols in this reference point are extensible authentication protocol (EAP) over DIAMETER or RADIUS (see Figure 22.15).
3GPP AAA proxy forwards authentication signaling between the WLAN access network and the 3GPP AAA server over the $W_s$ reference point. The 3GPP AAA server verifies if the subscriber is authorized to use WLAN. The authorization information and authentication vectors needed in the authentication protocols are stored by the HSS. The 3GPP AAA server retrieves this information over the $W_s$ reference point.

After the user has been successfully authenticated and authorized for network access, the WLAN access network grants UE access to an IP network. In the simplest case, the IP network is the public Internet, and the user data is directly routed from the WLAN access network to the Internet.

**User Data Routing and Access to Services**

The IP network selection is based on a parameter called WLAN access point name (W-APN) similar to the APN parameter used in GPRS. The UE indicates the desired IP network with W-APN. The network authorizes the request, or verifies that the user has the right to use the W-APN.

After selecting the IP network, appropriate tunnels are established to route the user data to the selected IP network. The tunnel is terminated in the home operator packet data gateway (PDG). The PDG is similar to the GGSN used in GPRS. The $W_i$ reference point between the PDG and the remote network is similar to the $G_i$ reference point used between GGSN and the remote IP networks in GPRS. In the visited 3GPP network, the WLAN access gateway (WAG) is required to implement tunneling. The reference points $W_n$, $W_m$, $W_w$, and $W_i$ are used to convey the user data plane, and $W_g$ and $W_m$ are used for control (see Figure 22.16).
22.8.3 3GPP-based Charging for WLAN
The WLAN charging architecture is shown in Figure 22.17. Charging information about WLAN is collected at the WLAN access network and forwarded to the 3GPP visited and home networks. The AAA server in the home 3GPP network authorizes each user's access to a WLAN.

Before authorizing a prepaid user to access the WLAN for direct Internet access, the 3GPP AAA server makes a credit reservation from the user's prepaid amount in the OCS (online charging system) over the W_{ref} reference point. The 3GPP AAA server monitors the received accounting information from the WLAN access network. When the downloaded credit is exhausted a new credit request from OCS is triggered to cover the forthcoming accounting reports from the WLAN access network. At the termination of the WLAN connection, the 3GPP AAA server returns any unused credit back to the OCS.

After authorization to access the WLAN access network is completed, a user-specific accounting session is established between the WLAN access network and the 3GPP home network. The
accounting session is established with standard AAA accounting signaling, and the reference point for this signaling is $W_1$.

At the establishment of the accounting session the 3GPP AAA server indicates to the WLAN a suitable set of accounting criteria, such as an accounting unit (e.g., amount of transferred kilobytes) and reporting threshold to be utilized. After the accounting session establishment the WLAN collects accounting information and reports it to the 3GPP AAA server over the $W_1$ reference point.

All associated IP flows traverse through the PDG; thus, more accurate and service-specific charging information can be collected at the PDG. The resource consumption by each IP flow can be monitored and collected internally at the PDG. For charging of the traversing IP flows, the PDG is also connected to the OCS by the $G_y$ reference point and to the CG (charging gateway) by the $G_z$ reference point. At the establishment of a certain IP flow via the PDG, the PDG requests credit for IP flow charging from the OCS over the $G_y$ reference point in a similar way as the 3GPP AAA server does over the $W_1$ reference point for WLAN access charging.

22.8.4 Session Mobility
In the loose coupling, mobile IP is used to provide session mobility across GPRS and WLAN. This is in contrast to the tight coupling approach in which the GPRS mobility management procedure is used. When the UE moves from GPRS to WLAN, it performs a mobile internet protocol (MIP) registration via the FA that resides in the WLAN. The FA completes the registration with the HA to be used as a forwarding address for the packet destined to the UE. The FA then associates the CoA with that of the UE and acts as a proxy on behalf of the UE for the life of the registration. This way, the UE retains its IP address when it moves from the WLAN to GPRS.

References:


Printed with permission from Morgan Kaufmann, a division of Elsevier. Copyright 2007. "Wireless Communications & Networking" Vijay Garg. For more information about this title and other similar books, please visit www.elsevierdirect.com.

Related links:
Interworking between WLANs and 3G - Part 1: Introduction, interworking objectives & approaches | Part 2: Tight coupling approach
An introduction to networking - Part III: Network and Transport layers