Wireless LAN Based GPRS Support Node

Vincent W.-S. Feng, Lin-Yi Wu, Yi-Bing Lin, and Whai-En Chen
Department of Computer Science & Information Engineering
National Chiao Tung University
vincentfeng@itri.org.tw
{lywu, liny}@csie.nctu.edu.tw
cwe@pcs.csie.nctu.edu.tw

Abstract

This paper proposes WLAN-based GPRS Support Node (WGSN), a solution for integrating 3G and WLAN services. We show that the 3G mechanisms can be re-used for WLAN user authentication and network access without introducing new procedures and without modifying the existing 3G network components. We describe the WGSN features and show how they are designed and implemented. A WGSN prototype has been implemented in *Industrial Technology Research Institute* (ITRI) and *National Chiao-Tung University* (NCTU) Joint Research Center.

Key words: 3G, GPRS, SIP, UMTS, WLAN

1 Introduction

3rd Generation Partnership Project (3GPP) Technical Report 22.934 [1] conducts a feasibility study on *Third Generation* (3G) system and *Wireless LAN* (WLAN) interworking that extends 3G services to the WLAN environment. In this interworking, WLAN serves as an access technology to the 3G system, which scales up the coverage of 3G services. Six scenarios were proposed for incremental development of 3G and WLAN interworking. The service and operational capabilities of each scenario are described as follows.

Scenario 1 provides common billing and customer care for both WLAN and 3G mobile operators. That is, a customer receives single monthly billing statements combining both 3G and WLAN services. The customer also consults the same customer care center about the problems for both services.

Scenario 2 reuses 3G-access control and charging mechanisms for WLAN services. The WLAN customers are authenticated by the 3G core network without introducing a separate procedure. In addition, the roaming mechanism between 3G system and WLAN are supported. In this scenario, users can access traditional Internet services but cannot access 3G services (such as *Circuit-Switched* (CS) voice and GPRS data services) through WLAN.

Scenario 3 allows a customer to access 3G *Packet-Switched* (PS) services over WLAN. The PS services include *Short Message Service* (SMS), *Multimedia Message Service* (MMS), and *IP Multimedia Subsystem Service* (IMS). Customers equipped with both WLAN card and 3G module can simultaneously but independently access WLAN and 3G networks.

Scenario 4 allows a customer to change access between 3G and WLAN networks during a service session. The system is responsible for re-establishing the session without user

involvement. Service interruption during system switching is allowed in this scenario. *Quality of Service* (QoS) is a critical issue for service continuity. Since 3G and WLAN networks have different capabilities and characteristics, the user would gain different QoS grades in different networks. Therefore, QoS adaptation is required during system switching.

Scenario 5 provides seamless service switching (i.e., handover) between 3G system and WLAN. Techniques must be developed to minimize data lost rate and delay time during switching so that the customer would not experience significant interruption during handover.

Scenario 6 supports 3G CS services in the WLAN environment. The seamless continuity feature described in Scenario 5 is also required to support CS services when customers roam between different networks.

Our survey with several mobile service providers indicates that the Scenario 3 features are essential for commercial operation of 3G/WLAN interworking in the first stage deployment. Depending on the business strategies, the Scenario 4 features may or may not be deployed in the long-term commercial operation. Scenarios 5 and 6 are typically ignored because the benefits of the extra features might not justify the deployment costs. This paper proposes a *Universal Mobile Telecommunications System* (UMTS) and WLAN interworking solution called WGSN. The features of WGSN are described in Section 2. The design and implementation of WGSN components are elaborated in Section 3.

2 The WGSN Approach

This section describes the architecture and the features of the *WLAN-based GPRS Support Node* (WGSN). WGSN interworks *Universal Mobile Telecommunications System* (UMTS) [2] with WLAN to support Scenario 3 features described in Section 1.

Figure 1 illustrates the inter-connection between a UMTS network and a WLAN network through WGSN. The UMTS network (Figure 1 (1)) provides 3G PS services. The WLAN network (Figure 1 (2)) provides access to Internet. The customers are allowed to roam between the two networks as long as the *Mobile Station* (MS) is equipped with both a 3G module and a WLAN card.

The UMTS network includes two sub-networks. The *UMTS Terrestrial Radio Access Network* (UTRAN; Figure 1 (3)) consists of *Radio Network Controllers* (RNCs) and Node Bs (i.e., base stations). The radio interface between a Node B and an MS is based on WCDMA radio technology [3]. The *UMTS core network* (i.e., GPRS network; Figure 1 (4)) consists of *Serving GPRS Support Node* (SGSN) and *Gateway GPRS Support Node* (GGSN), which provide mobility management and session management services to mobile users. An SGSN connects to the UTRAN by *Asynchronous Transfer Mode* (ATM) links, and communicates with the GGSN through an IP-based backbone network. The GGSN connects to the external *Packet Data Network* (PDN) by an IP-based interface Gi. Both SGSN and GGSN communicate with the *Home Location Register* (HLR) through the *Gr* and *Gc* interfaces, respectively. These two interfaces are based on the *Mobile Application*

Part (MAP) [4]. The HLR is the master database containing all user-related subscription and location information.

The WLAN radio network includes 802.11-based *Access Points* (APs) that provide radio access for the MSs. The WGSN acts as a gateway between the PDN and the WLAN node, which obtains the IP address for an MS from a *Dynamic Host Configuration Protocol* (DHCP) server and routes the packets between the MS and the external PDN. The WGSN node communicates with the HLR to support GPRS/UMTS mobility management following 3GPP Technical Specification 23.060 [5]. Therefore, the WLAN authentication and network access procedures are exact the same as that for GPRS/UMTS.

The WGSN node integrates both SGSN and GGSN functionalities. Like an SGSN, the WGSN communicates with the HLR through the Gr interface. On the other hand, like a GGSN, the WGSN communicates with the external PDN via the Gi interface. Therefore, for other GPRS/UMTS networks, the WGSN node and the corresponding WLAN network are considered as a separate GPRS network. The WGSN node can be plugged in any 3G core network without modifying the existing 3G nodes. To integrate the billing system for both UMTS and WLAN, WGSN communicates with the *Charging Gateway* using the same UMTS protocols (the *GPRS Tunneling Protocol* (GTP') protocol implemented in the Ga interface [5] or by FTP).

To access the WGSN services, the MS must be either a 3G-WLAN dual mode handset or a laptop/*Personal Data Assistant* (PDA) that equips with both WLAN *Network Interface Card* (NIC) and a 3G module.

WGSN provides automatic WLAN network configuration recovery. A WGSN MS can be a notebook, which is used at home or office with different network configurations. The network configuration information includes IP address, subnet mask, default gateway, WLAN *Service Set Identifier* (SSID), etc. When the MS enters the WGSN service area, its network configuration is automatically reset to the WGSN WLAN configuration if the MS is successfully authenticated. The original network configuration is automatically recovered when the MS detaches from the WGSN. This WGSN functionality is especially useful for those users who are unfamiliar with network configuration setup.

3. Implementation of WGSN

This section describes the implementation of WGSN [6]. We first introduce the protocol stack among MS, AP, WGSN, and HLR. Then we elaborate on the WGSN components for the WGSN network node and the MS. Figure 2 illustrates the WGSN protocol stack. In the current implementation, the lower-layer protocol between the MS and the WGSN node is IP over 802.11 radio (through WLAN AP). In the control plane, standard *GPRS Mobility Management* (GMM) defined in 3GPP Technical Specification 23.060 [5] is implemented on top of TCP/IP between the MS and the WGSN node. The standard UMTS Gr interface is implemented between the WGSN node and the HLR through *Signaling System Number 7* (SS7)-based MAP protocol [7]. The layers of the SS7 protocol include *Message Transfer Part* (MTP), *Signaling*

Connection Control Part (SCCP), and *Transaction Capabilities Application Part* (TCAP). Details of SS7 can be found in [7]. The WGSN node communicates with the charging gateway through the IP-based GTP' protocol which is not shown in Figure 2. In the future, the TCP/IP layers in the control plan will be replaced by *Extensible Authentication Protocol / EAP Over LAN* (EAP/EAPOL) [8, 9]. EAP/EAPOL operates over 802.11 MAC layer, which allows authentication of an MS before it is assigned an IP address. Therefore, the IP resource of WGSN system can be managed with better security. Also, between the WGSN node and the HLR, the lower-layer SS7 protocols (i.e., MTP and SCCP) will be replaced by IP-based *Stream Control Transmission Protocol* (SCTP) [10] to support all-IP architecture.

The WGSN user plane follows standard IP approach. That is, the MS and the WGSN node interact through the Internet protocol. The MS communicates with the *Corresponding Node* in the external PDN using the transport layer over IP. In the user plane, the WGSN node serves as a gateway between the WLAN network and the external PDN.

The WGSN MS must be either a 3G-WLAN dual mode handset or a laptop/PDA that equips with both WLAN *Network Interface Card* (NIC) and a 3G module. The UICC reader (which can be contained in the 3G module or a separate smart card reader) communicates with the standard SIM card to obtain the authentication information required in both 3G network and WLAN. In the current WGSN implementation, we use GPRS module instead of 3G module because 3G service is not available in Taiwan as of the writing time of this paper. The WGSN UICC reader is implemented as a standard device on the Microsoft Windows platform. The WGSN software modules are implemented on the Window 2000 and XP OS platforms for notebooks and WinCE for PDAs. A WGSN client is implemented to carry out tasks in the control plane. Several *Session Initiation Protocol* (SIP) [11] user agents are implemented for SIP-based applications in the user plane. The modules for WGSN client are described as follows.

SIM Handler (Figure 3 (1)): As in UMTS, a WGSN user is authenticated using the UMTS SIM card (or GPRS SIM card in the current implementation) before the user can access the WLAN network. Through the UICC smart card reader, the SIM Handler retrieves the SIM information (including IMSI, SRES and Kc) [12] and forwards the information to the GMM Handler.

GMM Handler (Figure 3 (2)): Based on the SIM information obtained from the SIM handler, the GMM handler communicates with the WGSN node to perform MS attach and detach. The authentication action is included in the attach procedure.

NIC Handler (Figure 3 (3)): The network configurations of different WLANs may be different. With the OS support, the NIC handler dynamically sets up appropriate network configurations when a WGSN user moves across different WLAN networks. WGSN utilizes *Dynamic Host Configuration Protocol* (DHCP) for IP address management. The WGSN MS must obtain a legal IP address and the corresponding network configuration through

the DHCP lease request. On the other hand, when the MS terminates a WGSN connection, it should send the IP release message to the WGSN node, and the IP address is reclaimed for the next WGSN user. The NIC handler then recovers the original network configuration for the MS. If the MS is abnormally terminated, the NIC handler cannot immediately recover the network configuration. Instead, the NIC handler offers a Window OS program called WGSN Service. When the MS is re-started, this service will check if the network configuration has been recovered. If not, the configuration previously recorded by the NIC handler is used.

User Interface (Figure 3 (4)): A user interacts with the WGSN system through the MS user interface. The user types the *Global System for Mobile communications* (GSM) / *General Packet Radio Service* (GPRS) pin number to initiate the WGSN connection. Like the usage of a GPRS handset, the pin number can be disabled. Based on the received command, the corresponding modules are instructed to carry out the desired tasks. During a WGSN session, the user interface indicates the status of the execution and displays the elapsed time of the WGSN connection.

On the network side, the WGSN node is implemented on the Advantech Industrial Computer platform S-ISXTV-141-W3. The black boxes in Figure 4 illustrate the WGSN communication modules, which include

- A SS7 module for communications with the HLR (through the SS7 network). In this module, the MTP, SCCP and TCAP layers (see Figure 2 (a)) are based on Connect7 2.4.0-Beta version software developed by SS8 Networks Cooperation.
- An internal Ethernet module for communications with the WLAN APs
- An external Ethernet module for communications with the external PDN

The software architecture of the WGSN node includes four major components:

Authentication Center (Figure 4 (1)) consists of the GMM and the Gr handlers. Through the internal Ethernet module, the GMM handler receives the GMM messages from the WGSN MS, and dispatches the corresponding tasks to the other WGSN modules. The Gr handler implements the standard GMM primitives for the Gr interface [5]. Through the SS7 module, the Gr handler interacts with the HLR for MS network access and authentication. Specifically, it obtains an array of authentication vectors (including a random number Rand, a signed result SRES, and an encryption key Kc) from the GPRS authentication center (which may or may not be co-located with the HLR). The size of authentication array can be dynamically adjusted (see [12] for the details). Each time the WGSN MS requests for authentication, the Gr handler uses an authentication vector to carry out the task as specified in 3GPP Technical Specification 33.102 [13]. Furthermore, when an MS detaches, the Gr handler should inform the HLR to update the MS status. The current WGSN version has implemented two MAP service primitives: the MAP_SEND_AUTHENTICATION_INFO and MAP_PURGE_MS services. These primitives are implemented on MAP version 1.4 software developed by Trillium Digital Systems Inc.

Network Controller (Figure 4 (2)) provides the following functions for Internet access:

- IP address management: A DHCP server is implemented in the WGSN node to distribute private IP addresses to the MSs. An NAT server performs address translation when the IP packets are delivered between the private (WLAN) and the public (external PDN) IP address spaces.
- Internet access control: The WGSN node only allows the authenticated users to access Internet services. Unauthorized packets will be filtered out by the firewall.
- SIP application support: To support SIP-based applications under the NAT environment, the WGSN node implements a SIP Application Level Gateway (ALG)[14] that modifies the formats of SIP packets so that these packets can be delivered to the WGSN MSs through the WGSN node.

Operation, Administration and Maintenance (OA&M; see Figure 4 (3)) controls and monitors individual WGSN user traffics. WGSN utilizes *Simple Network Monitoring Protocol* (SNMP) as the network management protocol. With *Management Information Base* (MIB), every managed network element is represented by an object with an identity and several attributes. An SNMP agent is implemented in the WGSN node, which interacts with the managed network element through SNMP. For example, the traffic statistics of an AP can be accessed by the OA&M (through the corresponding MIB object) and displayed in a web page using *Multi Router Traffic Grapher* (MRTG 2.9.22). The SNMP agent can also detach an MS through the MIB object of the MS. A log handler is implemented in the OA&M to record all events occurring in the WGSN node. A billing handler generates CDRs, which communicates with the billing gateway through the GTP' protocol or *File Transfer Protocol* (FTP).

4. Conclusion

This paper proposed WGSN, a solution for integrating 3G and WLAN services. We described how the 3G mechanisms are re-used for WLAN user authentication and network access without introducing new procedures and without modifying the existing 3G network components. We described the WGSN features and showed how they are designed and implemented. A WGSN prototype has been implemented in Industrial Technology Research Institute (ITRI) and National Chiao Tung University (NCTU) Joint Research Center.

Acknowledgement

This work was sponsored in part by the MOE Program for Promoting Academic Excellence of Universities under grant number 89-E-FA04-1-4, Chair Professorship of Providence University, IIS/Academia Sinica, CCL/ITRI, National Telecommunication Development Program, the Lee and MTI Center for Networking Research/NCTU.

Reference

[1] 3GPP, “Services and System Aspects; Feasibility Study on 3GPP System to Wireless Local Area Network (WLAN) Interworking,” 3GPP TR 22.934, 2002.

[2] Lin, Y.-B., Haung, Y.-R., Pang, A.-C., and Chlamtac, I., “All-IP Approach for UMTS Third Generation Mobile Networks,” *IEEE Network*, 16(5), pp. 8-19, 2002.

[3] Holma, H., and Toskala, A., *WCDMA for UMTS*, John Wiley & Sons, 2000.

[4] ETSI/TC, ”Mobile Application Part (MAP) Specification, ” GSM 09.02, v. 7.3.0, 2000.

[5] 3GPP, “Technical Specification Group Services and Systems Aspects; General Packet Radio Service; Service Description; Stage 2,” 3GPP TS 23.060, 2001.

[6] Feng, V., “System Requirement Specification of WLAN-based GPRS Support Node (WGSN),” Technical report, ITRI and NCTU Joint Research Center, 2003.

[7] Lin, Y.-B., and Chlamtac, I., *Wireless and Mobile Network Architectures*. Wiley, 2001.

[8] Blunk, L., and Vollbrecht, J., “PPP Extensible Authentication Protocol (EAP),” IETF RFC 2284, Mar. 2003.

[9] IEEE, “IEEE Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control,” IEEE Std 802.1X-2001, 2001.

[10] Stewart, R., et al., “Stream Control Transmission Protocol,” IETF RFC 2960, Oct. 2000.

[11] Rosenberg, J., et al., “SIP: Session Initiation Protocol,” IETF RFC 3261, Jun. 2002.

[12] Lin, Y.-B., and Chen, Y.-K., “Reducing Authentication Signaling Traffic in Third Generation Mobile Network,” *IEEE Trans. on Wireless Commun.*, 2003.

[13] 3GPP, “Technical Specification Group Services and Systems Aspects; 3G Security; Security Architecture,” 3GPP TS 33.102, V3.7.0 (2000-12), 2000.

[14] 3COM Inc., “A SIP Application Level Gateway for Network Address Translation,” IETF draft-biggs-sip-nat-00, Mar. 2000.

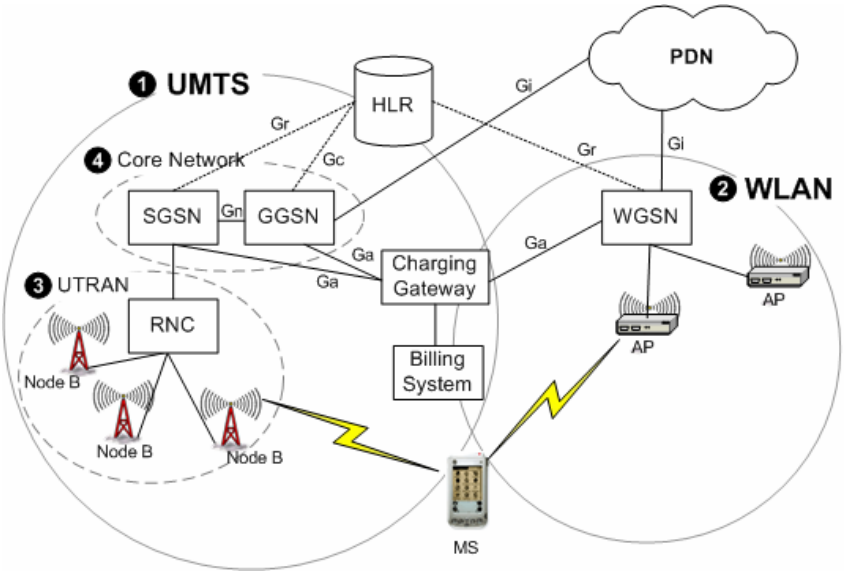
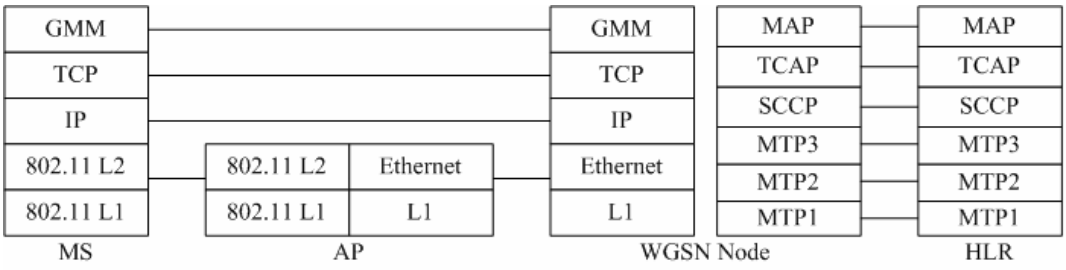
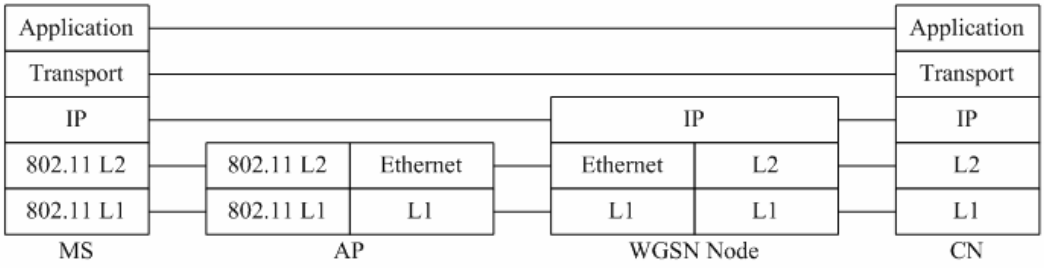


Figure 1: WGSN Architecture (dashed lines: signaling; solid lines: data and signaling)



(a) WGSN Control Plane



(b) WGSN User Plane

MS: Mobile Station
AP: Access Point
WGSN Node: WLAN-based GPRS Support Node
HLR: Home Location Register
CN: Corresponding Node

GMM: GPRS Mobility Management
TCP: Transmission Control Protocol
IP: Internet Protocol
MAP: Mobile Application Part
TCAP: Transaction Capabilities Application Part
SCCP: Signaling Connection Control Part
MTP: Message Transfer Part

Figure 2: WGSN Protocol Stack

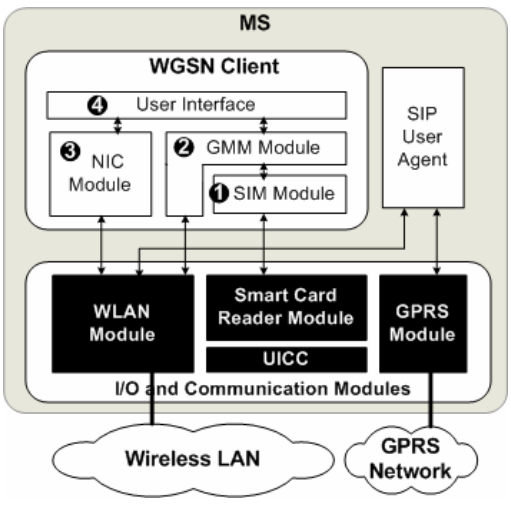


Figure 3: The MS Architecture

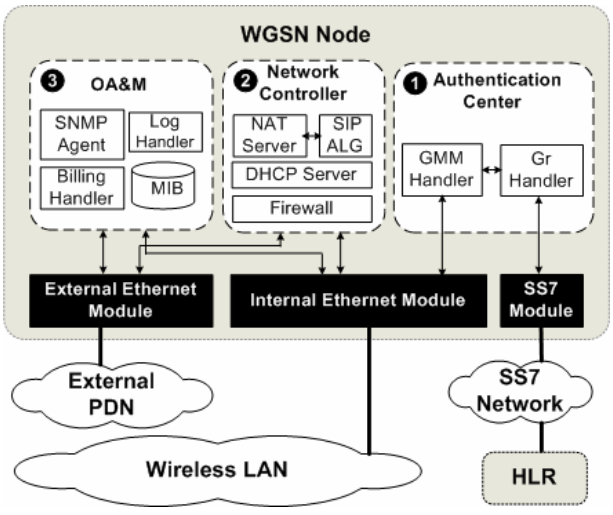


Figure 4: The WGSN Node Architecture