國立臺北大學 資訊工程學系
NTPU, Department of Computer Science and Information Engineering

Chapter 14
Integration of WLAN and Cellular Networks

Prof. **Yuh-Shyan Chen**

Department of Computer Science and Information Engineering

National Taipei University

Outline

- 14.1 The WGSN Approach
  - 14.1.1 WGSN Network Architecture
  - 14.1.2 WGSN Features
- 14.2 Implementation of WGSN
- 14.3 Attach and Detach
- 14.4 WGSN Push Mechanism
- 14.5 IEEE 802.1X-based Authentication
  - 14.5.1 Related Protocols for IEEE 802.1X Authentication
  - 14.5.2 SIM-based IEEE 802.1X Authentication
  - 14.5.3 EAPOL Timers
- 14.6 Concluding Remarks
- 14.7 Questions

Abstract

- **Chapter 14** elaborates on WLAN-based GPRS Support Node (WGSN),
  - A solution for integrating cellular and WLAN networks.
  - WGSN was developed by the NCTU and the Industrial Technology Research Institute.
  - We address how the cellular/mobile mechanisms are re-used for WLAN user authentication and network access without introducing new procedures and without modifying the existing cellular network components.
  - We also describe the WGSN features and show how they are designed and implemented. Then we discuss how IEEE 802.1X authentication can be integrated in WGSN.

Introduction

- **3GPP TR 22.934** which conducts a feasibility study on cellular system and *Wireless LAN* (*WLAN*) interworking that extends mobile services to the WLAN environment.
- In this interworking, WLAN serves as an access technology to the cellular system, which scales up the coverage of mobile services.

Six scenarios were proposed for incremental development of cellular and WLAN interworking

Table 14.1 Interworking scenarios and service capabilities

Service Capabilities Scenario	1	2	3	4	5	6
Common Billing	Yes	Yes	Yes	Yes	Yes	Yes
Common Customer Care	Yes	Yes	Yes	Yes	Yes	Yes
Cellular-based Access Control	No	Yes	Yes	Yes	Yes	Yes
Cellular-based Access Charging	No	Yes	Yes	Yes	Yes	Yes
Access to Mobile PS Services	No	No	Yes	Yes	Yes	Yes
Service Continuity	No	No	No	Yes	Yes	Yes
Seamless Service Continuity	No	No	No	No	Yes	Yes
Access to Mobile CS Services with Seamless Mobility	No	No	No	No	No	Yes

Scenario 1

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

Scenario 2

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

Scenario 3

- **Scenario 3** allows a customer to access mobile *Packet Switched* (*PS*) services over the WLAN. The PS services include Short Message Service (SMS; see Chapter 1), Multimedia Messaging Service (MMS; see Chapter 11), and IP Multimedia Core Network Subsystem (IMS) Service (see Chapter 15). Customers equipped with both a WLAN card and a cellular (e.g., UMTS or GPRS) module can simultaneously but independently access WLAN and cellular networks.

Scenario 4

- **Scenario 4** allows a customer to change access between cellular and WLAN networks during a service session. The system is responsible for reestablishing 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 cellular 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

- **Scenario 5** provides seamless service switching (that is, handoff) between the cellular system and the WLAN. Techniques must be developed to minimize the data lost rate and delay time during switching so that the customer does not experience significant interruption during handoff.

Scenario 6

- **Scenario 6** supports mobile 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.

Cont.

- Our survey with several mobile service providers indicates that the Scenario 3 features are essential for commercial operation of cellular/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.

Cont.

- Scenarios 5 and 6 are typically ignored because the benefits of the extra features might not justify the deployment costs.

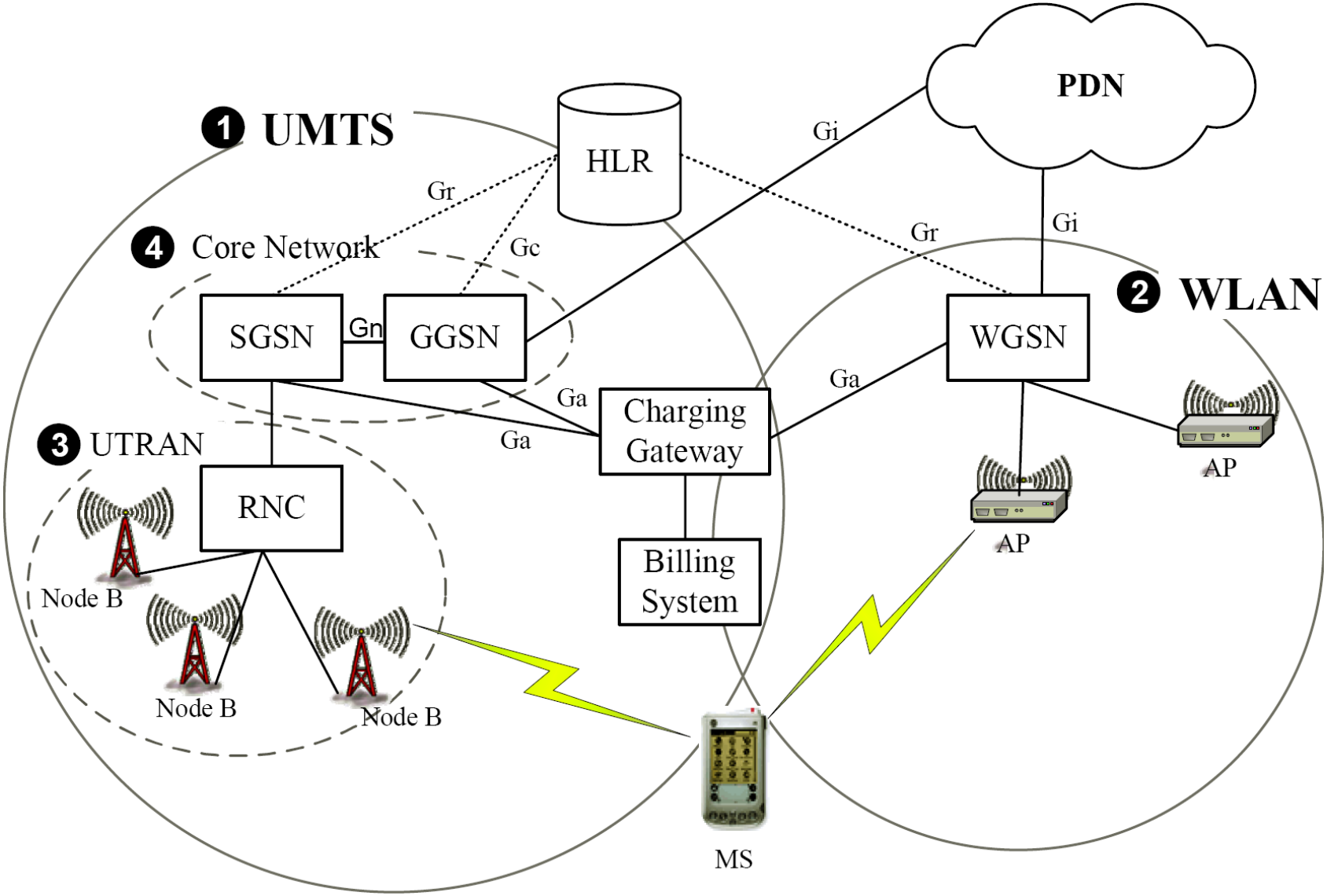
14.1 The WGSN Approach

- *WLAN-based GPRS Support Node* (***WGSN***) interworks UMTS with WLAN to support Scenario 3 features. This section describes the architecture and the features of WGSN.

14.1.1 WGSN Network Architecture

- Figure 14.1 illustrates the inter-connection between the UMTS and a WLAN network through WGSN.
- The UMTS network (Figure 14.1 (1)) provides mobile PS services.
- The WLAN network (Figure 14.1 (2)) provides access to the Internet.
- The customers are allowed to roam between the two networks as long as the Mobile Station (MS) is equipped with both a cellular module (for example, GPRS module) and a WLAN card.

Fig. 14.1 WGSN Architecture



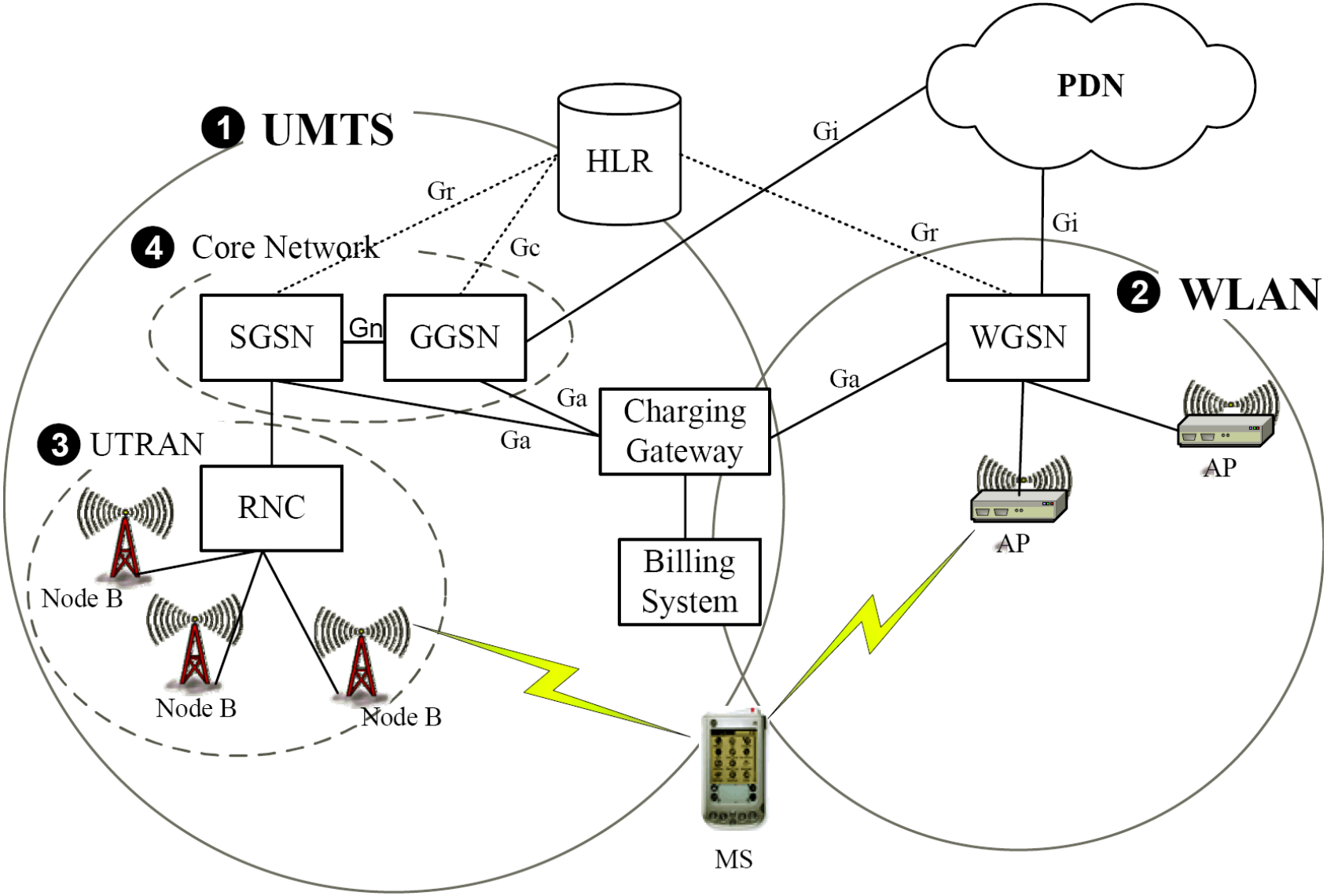
Cont.

- 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 *Packet Data Network* (*PDN*).
- The WGSN node communicates with the HLR to support GPRS/UMTS mobility management following **3GPP TS 23.060** as described in Chapter 2.
- Therefore, the WLAN authentication and network access procedures are exactly the same as that for GPRS/UMTS.

Cont.

- The WGSN node integrates both SGSN and GGSN functionalities. Like an SGSN, the WGSN communicates with the HLR through the *Gr* interface.
- Conversely, 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.

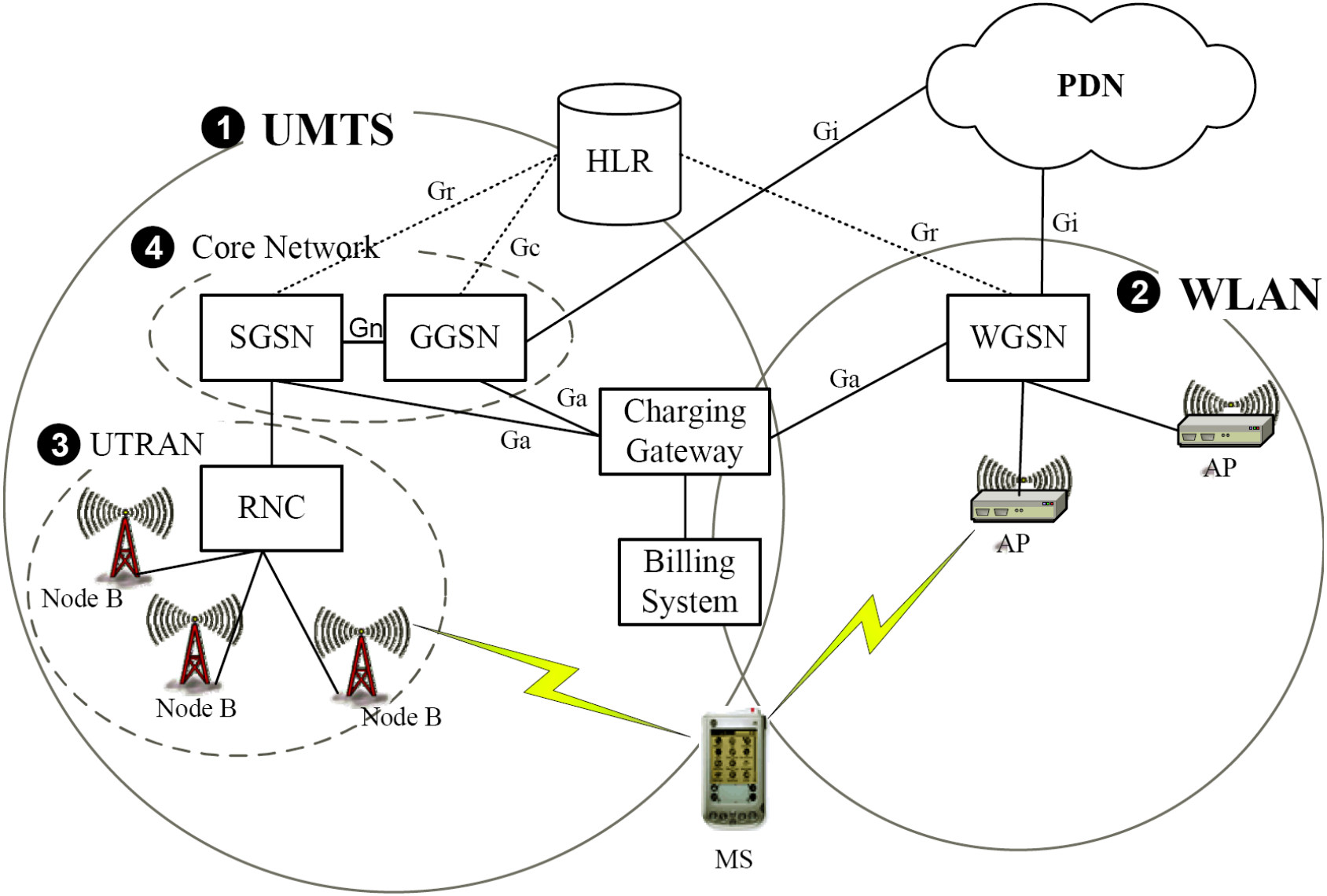
Fig. 14.1 WGSN Architecture



Cont.

- The WGSN node can be plugged in any UMTS core network without modifying the existing UMTS nodes (such as SGSNs and GGSNs).
- To integrate the billing system for both UMTS and WLAN, WGSN communicates with the charging gateway using the same UMTS protocols; that is, the GPRS Tunneling Protocol (GTP') implemented in the Ga interface (see Chapter 7) or by *File Transfer Protocol* (*FTP*).
- To access the WGSN services, the MS must be either a UMTS-WLAN dual-mode handset or a laptop/Personal Data Assistant (PDA) equipped with both a WLAN *Network Interface Card* (*NIC*) and a GPRS/UMTS module.

Fig. 14.1 WGSN Architecture



14.1.2 WGSN Features

- Based on the seven interworking aspects listed in 3GPP TS 22.934, we describe the features implemented in WGSN.

Service aspects:

- WGSN provides general Internet access and *Voice over IP* (*VoIP*) services based on *Session Initiation Protocol* (*SIP*; see Chapter 12).
- Since a *Network Address Translator* (*NAT*) is built into the WGSN node, the VoIP voice packets delivered by the *Real-Time Transport Protocol* (*RTP*) connection cannot pass through the WGSN node.
- This issue is resolved by implementing a *SIP Application Level Gateway* (*ALG*) in the WGSN node, which interprets SIP messages and modifies the source IP address contained in these SIP messages.

Cont.

- In UMTS, an MS must activate the *Packet Data Protocol* (*PDP*) context for VoIP service before a caller from the external PDN can initiate a phone call to this MS.
- Also, for both UMTS and WLAN, a SIP *User Agent* (*UA*) must be activated in an MS before it can receive any incoming VoIP call.
- Therefore, a *SIP-based Push Center* (*SPC*) is implemented in the WGSN node to provide MS terminated SIP services.

Cont.

- The SPC is implemented on iSMS, the SMS-based IP service platform described in Chapter 1.
- The SPC also provides a push mechanism through WLAN for a WGSN user who does not bring up the SIP UA.
- Therefore, the SIP terminated services (for example, incoming VoIP calls) can be supported in WGSN.

Access control aspects:

- WGSN follows standard UMTS access control for users to access WLAN services, where the existing **UMTS Subscriber Identity Module (SIM)** card and the **subscriber data** (user profile) records in the HLR are utilized.
- Therefore, the WGSN customers do not need a separate WLAN access procedure, and maintenance of customer information is simplified.
- User profiles for both UMTS and WLAN are combined in the same database (that is, the HLR).

Security aspects:

- WGSN utilizes the existing UMTS authentication mechanism (see Section 9.1).
  - That is, the WLAN authentication is performed through the interaction between an MS (using a UMTS SIM card) and the Authentication Center (AuC).
  - Therefore, WGSN is as secure as existing cellular networks. We do not attempt to address the WLAN encryption issue.

Cont.

- It is well known that WLAN based on IEEE 802.11b is not secure.
- For a determined attack, *Wired Equivalent Privacy* (*WEP*) is not safe, which only makes a WLAN network more difficult for an attacker to intrude.
- The IEEE 802.11 Task Group I has been investigating the current 802.11 *Media Access Control Address* (*MAC*) security.
- WGSN follows the resulting solution.

Roaming aspects:

- WGSN provides roaming between UMTS and WLAN. We utilize the standard UMTS mobility management mechanism described in Chapter 2 without introducing any new roaming procedures.

Terminal aspects:

- A terminal for accessing WGSN is installed with a ***Universal IC Card*** (*UICC*) reader
  - a smart card reader implemented as a standard device on the Microsoft Windows platform.
- The UICC reader interacts with the UMTS SIM card (i.e., the UICC containing the SIM application) to obtain authentication information for the WGSN attach procedure.

Naming and addressing aspects:

- WGSN user identification is based on the *Network Access Identifier* (*NAI*) format, following the 3GPP recommendation.
- Specifically, the **International Mobile Subscriber Identity (IMSI)** is used as WGSN user identification.

Charging and billing aspects:

- The WGSN acts as a router, which can monitor and control all traffics for the MSs. The WGSN node provides both offline charging and online charging (for pre-paid services) based on the *Call Detail Records* (*CDRs*) delivered to the charging gateway.

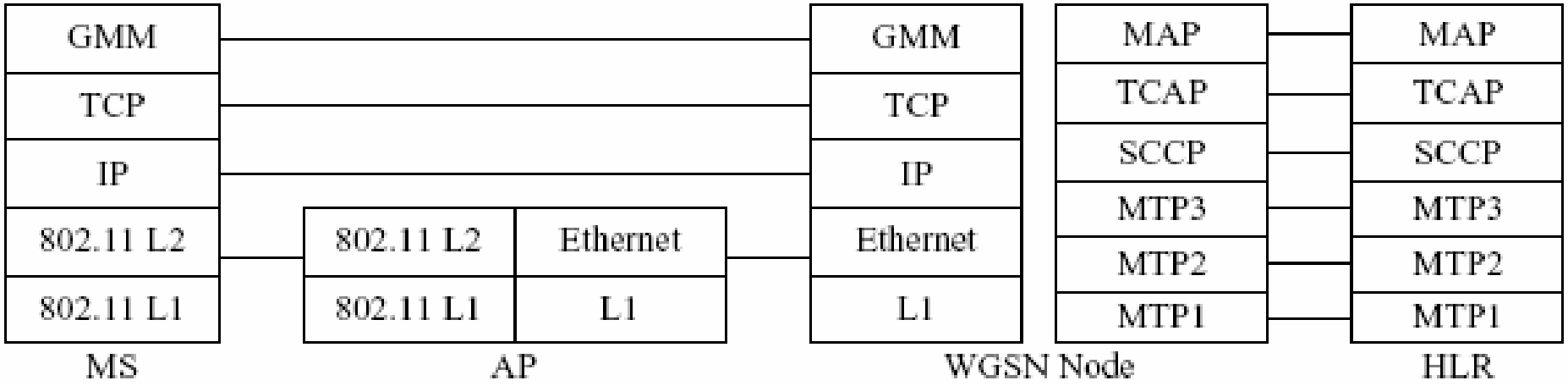
Cont.

- Besides the six aspects listed above, WGSN also provides automatic WLAN network configuration recovery.
- A WGSN MS can be a notebook, which is used at home or at the office with different network configurations.
- The network configuration information includes IP address, subnet mask, default gateway, WLAN *Service Set Identifier* (*SSID*), et cetera.

4.2 Implementation of WGSN

- This section describes the implementation of WGSN. 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 14.2 illustrates the WGSN protocol stack. In this figure, the lower-layer protocol between the MS and the WGSN node is IP over 802.11 radio (through WLAN AP).

WGSN Control Plane



(a) WGSN Control 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

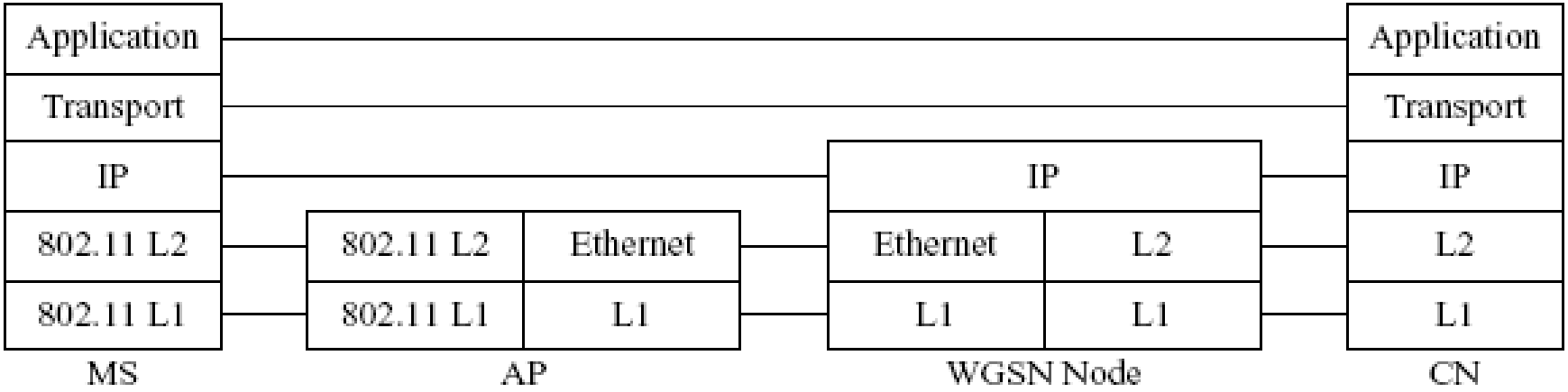
Cont.

- In the **control** plane, standard GPRS Mobility Management (GMM) defined in 3GPP TS 23.060 (see Chapter 2) 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 the Signaling System Number 7 (SS7)-based Mobile Application Part (MAP) protocol.
- The layers of the SS7 protocol include Message Transfer Part (**MTP**), Signaling Connection Control Part (**SCCP**), and Transaction Capabilities Application Part (**TCAP**), described in Chapter 8.

Cont.

- The WGSN node communicates with the charging gateway through the IP based GTP protocol described in Chapter 7.
- In Section 14.5, the TCP/IP layers in the control plan will be replaced by *Extensible Authentication Protocol / EAP over LAN* (*EAP/EAPOL*).
- EAP/EAPOL operates over the 802.11 MAC layer, which allows authentication of an MS before it is assigned an IP address. Therefore, the IP resource of the 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) can be replaced by the IP-based *Stream Control Transmission Protocol* (*SCTP*) to support all-IP architecture. See Chapter 8 for the SCTP description.

WGSN User 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

Cont.

- The WGSN **user** plane follows the standard IP approach. That is, the MS and the WGSN node interact through the Internet protocol. The MS communicates with a host 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 UMTS-WLAN dual-mode handset or a laptop/PDA equipped with both a WLAN NIC and a UMTS/GPRS module.

Cont.

- The UICC reader (which can be contained in the UMTS/GPRS module or a separate smart card reader) communicates with
- the standard SIM card to obtain the authentication information required in both the cellular network and the WLAN. The WGSN UICC reader is implemented as a standard device on the Microsoft Windows platform.
- The WGSN software modules are implemented on the Windows 2000 and XP OS platforms for notebooks, and on WinCE for PDAs. A WGSN client is implemented to carry out tasks in the control plane. Several SIP user agents are implemented for SIP-based applications in the user plane.

Fig. 14.3 The MS Architecture

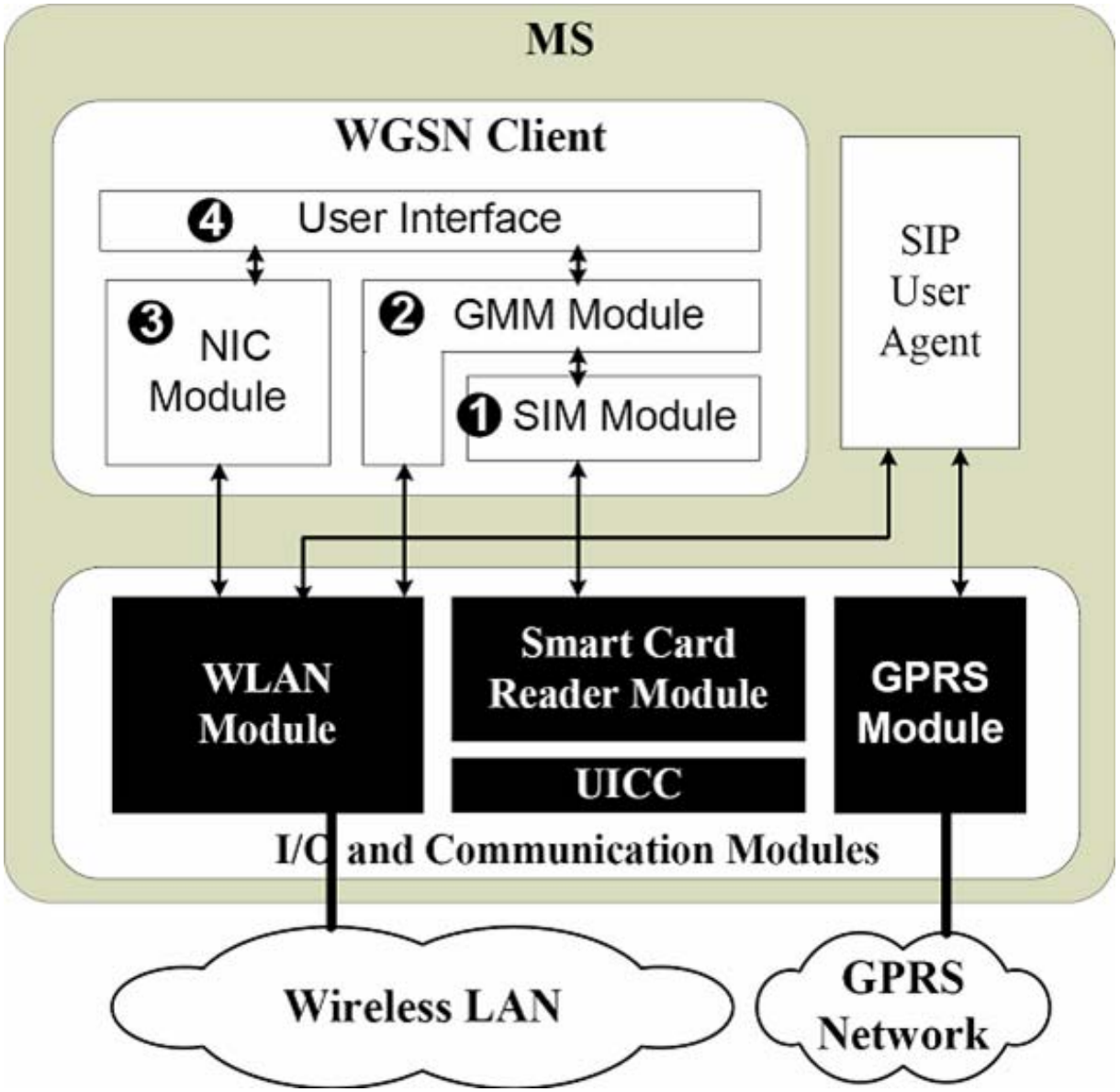
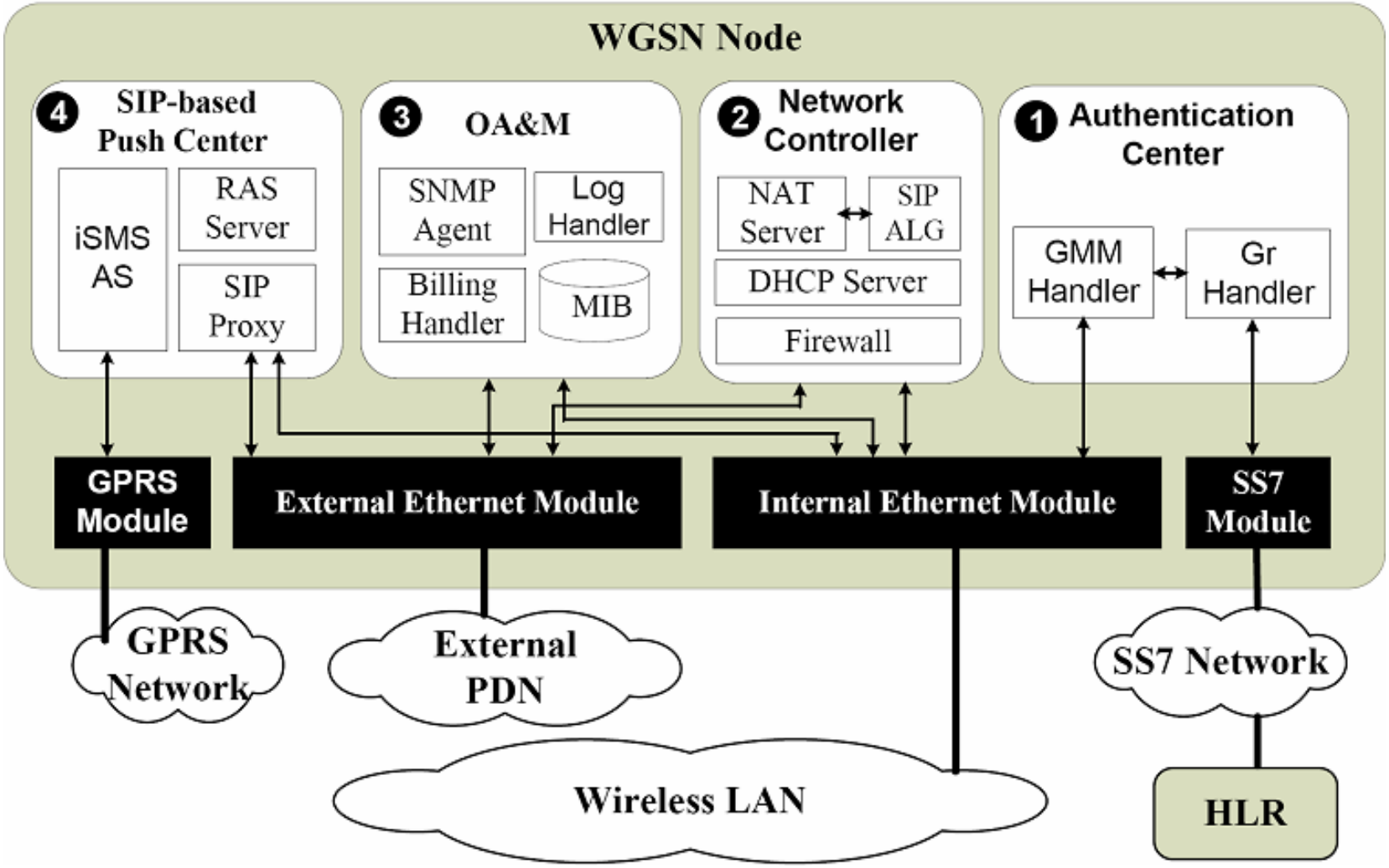


Fig. 14.4 The WGSN User Interface

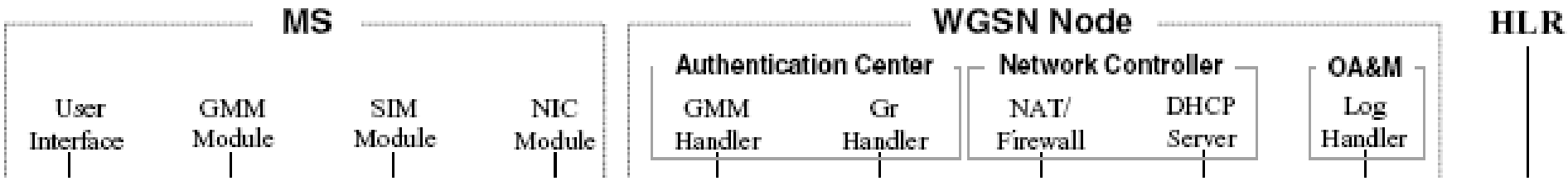
Fig. 14.5 The WGSN Node Architecture



14.3 Attach and Detach

- The attach procedure is illustrated in Figure 14.6, and consists of the following steps:

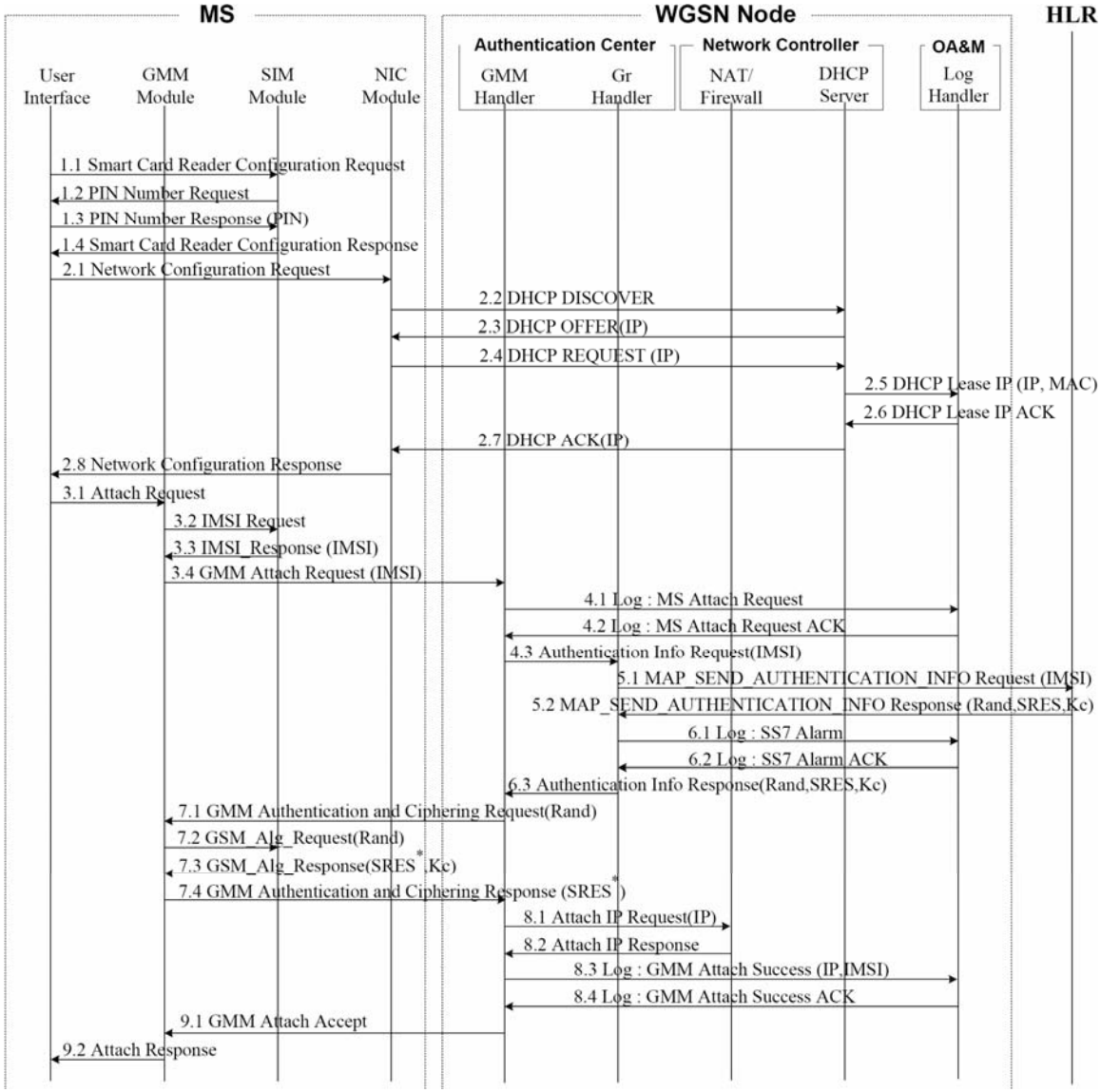
Fig. 14.6 Message Flow for the Attach Procedure



Step 1.

- When the WGSN user brings up the MS user interface, the SIM module is invoked to configure the smart card reader and (optionally) request the user to input the *Personal Identification Number* (*PIN*) number. The card reader authenticates the user through the pin number, just like a GPRS mobile phone.

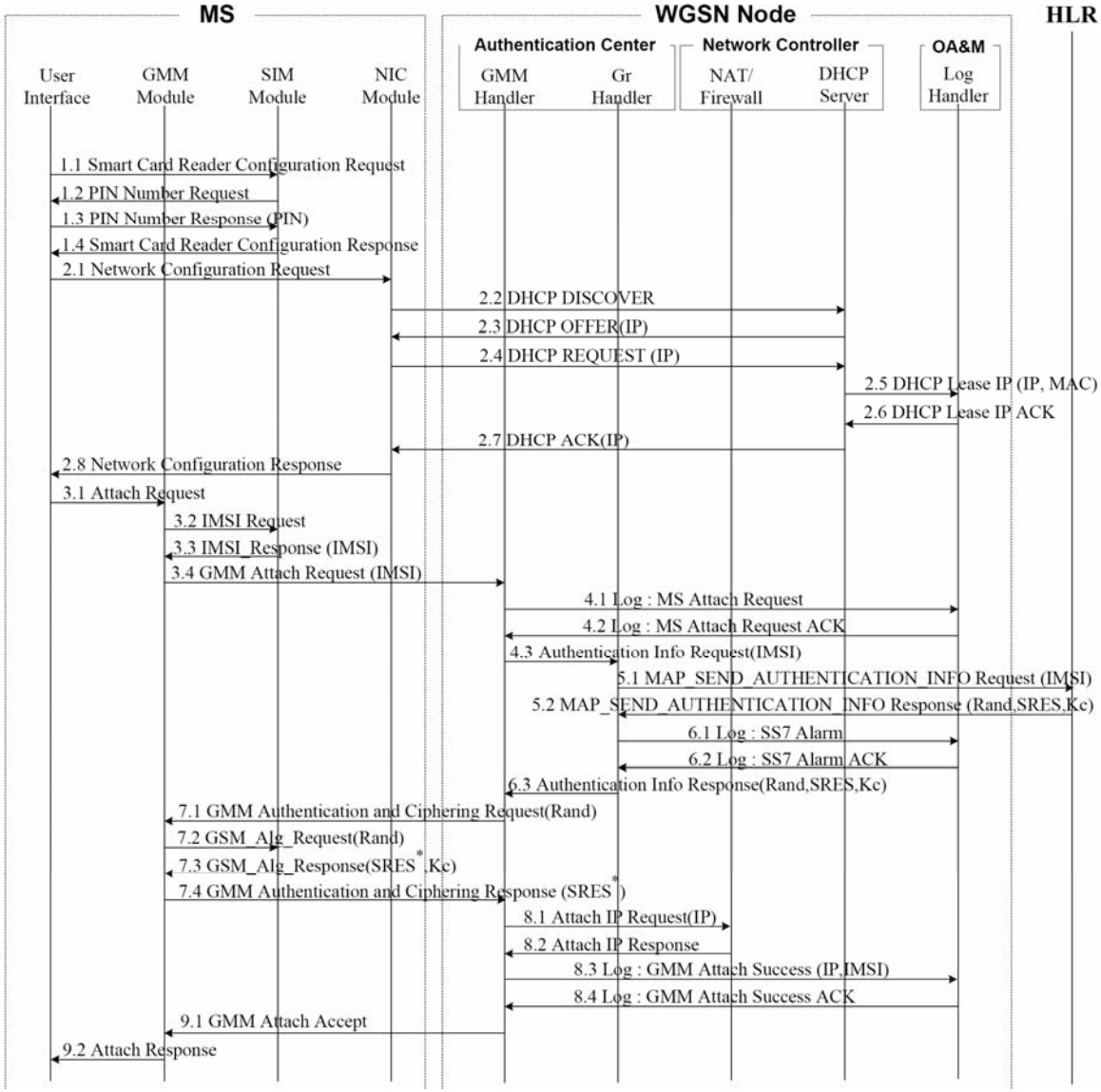
Fig. 14.6 Message Flow for the Attach Procedure



Step 2.

- The MS NIC module is invoked to store the current WLAN network configuration. To obtain the network configuration of WGSN, the MS broadcasts the DHCP Discover message on its subnet to look for a DHCP server.
- The DHCP server in the WGSN node replies to the MS with the DHCP Offer message, which includes an available IP address. Then the MS sends the DHCP Request message to the DHCP server and asks for the usage of an available IP address contained in the DHCP Offer message.
- If the DHCP server accepts the request, it reports the IP lease event to the Log Handler and sends the MS the DHCP Ack message with network configuration parameters. Finally, the MS NIC module sets up the new network configuration.

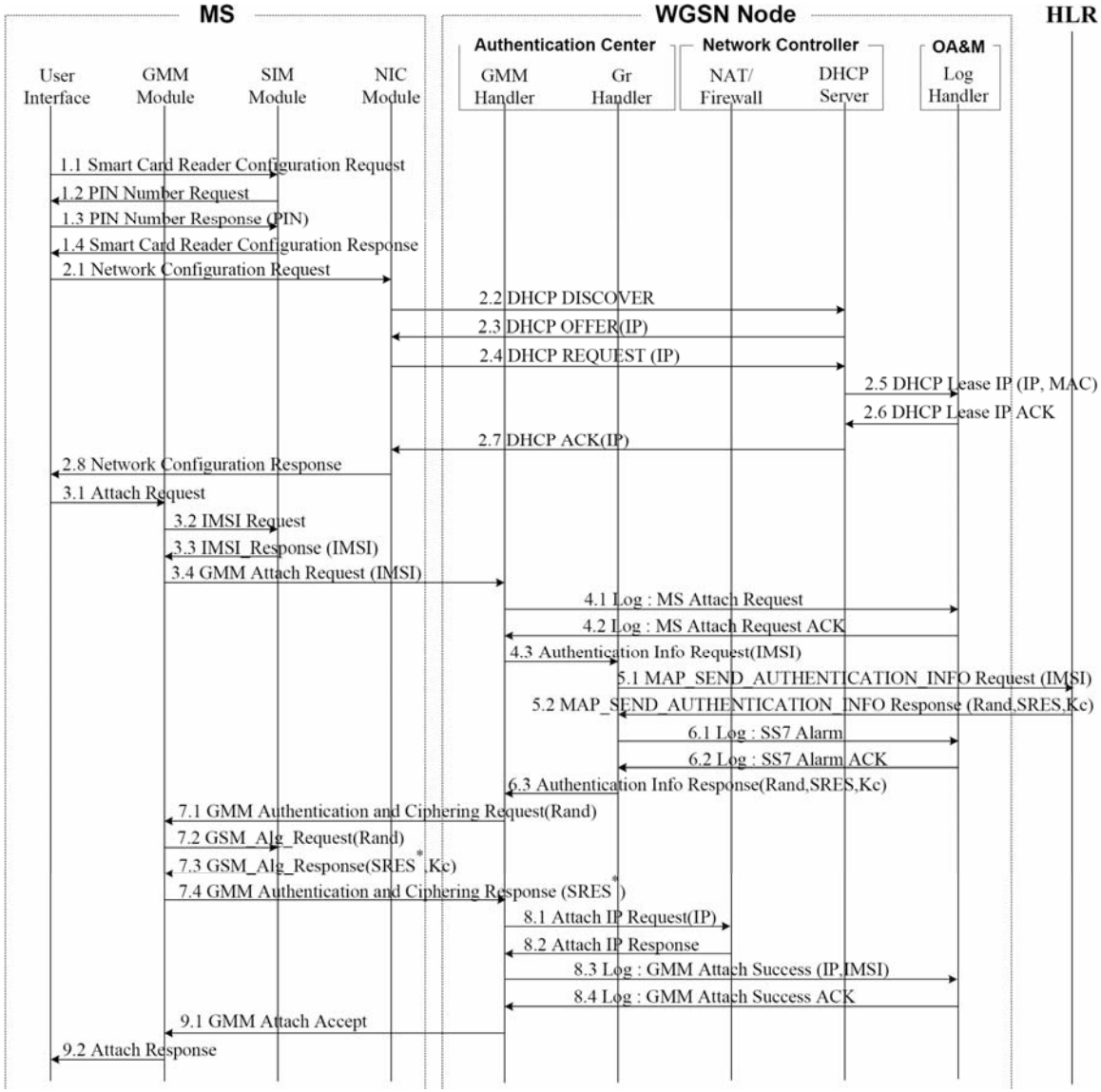
Fig. 14.6 Message Flow for the Attach Procedure



Step 3.

- The MS GMM module is invoked to perform the attach operation. The GMM module first obtains the IMSI from the SIM module. Then it sends the GMM Attach Request message (with the parameter IMSI) to the WGSN node.

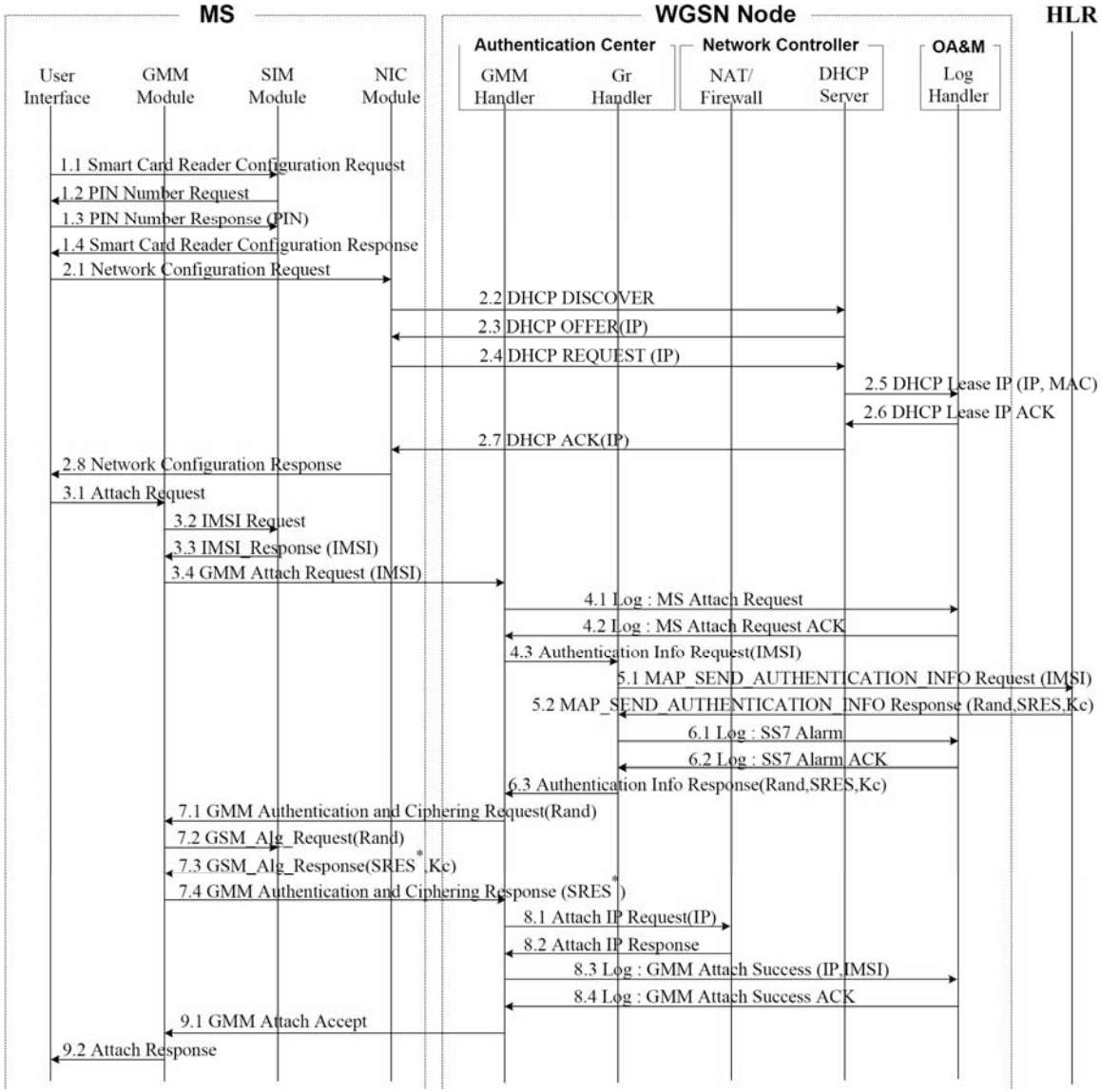
Fig. 14.6 Message Flow for the Attach Procedure



Step 4.

- When the GMM Handler of the WGSN node receives the attach request, it reports this event to the Log Handler, and sends the authentication information request to the Gr Handler.

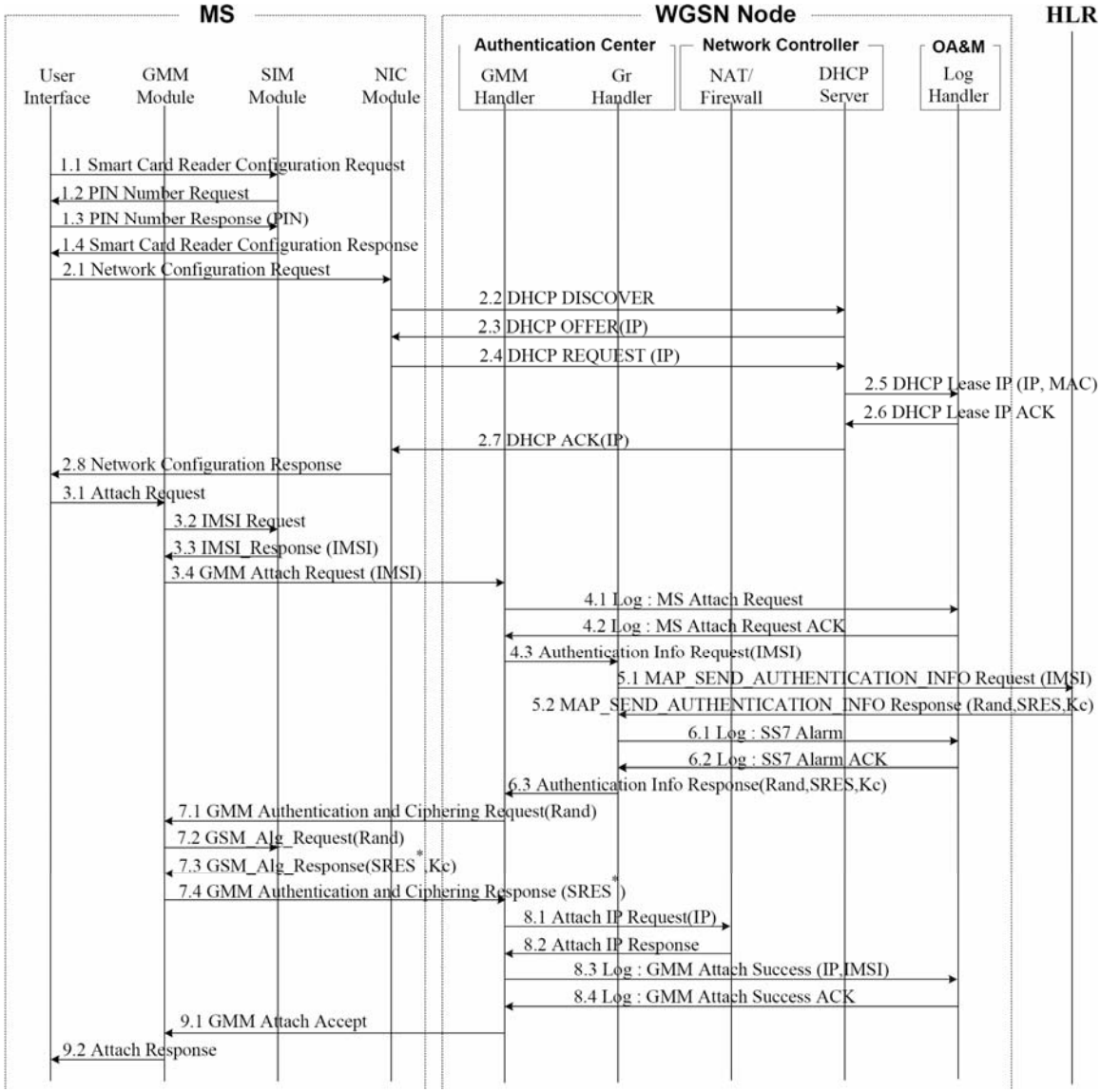
Fig. 14.6 Message Flow for the Attach Procedure



Step 5.

- The Gr Handler sends the Send Authentication Info Request message (with the argument IMSI) to the HLR. The HLR returns the authentication vector (RAND, SRES, Kc) through the Send Authentication Info Response message.

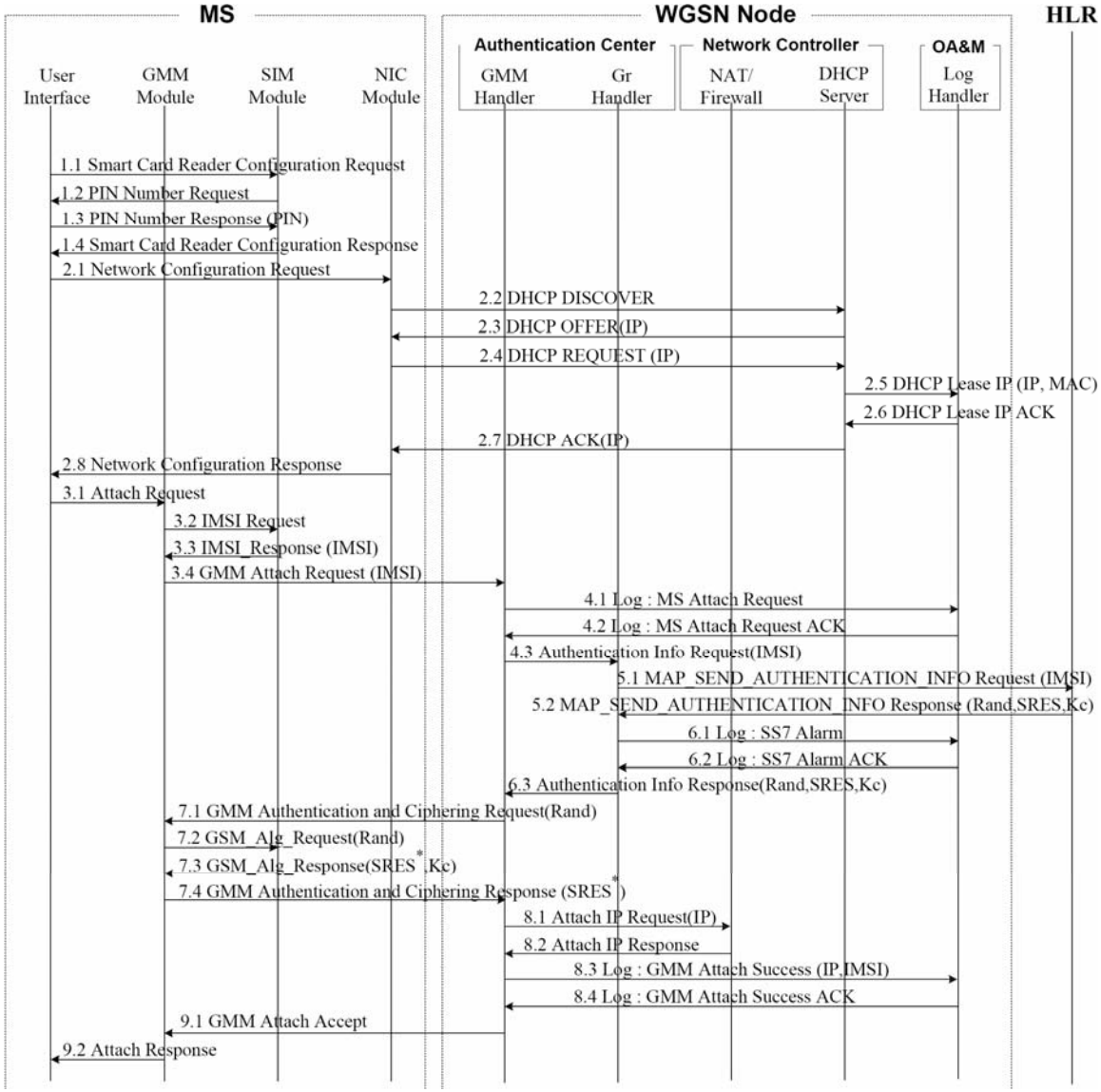
Fig. 14.6 Message Flow for the Attach Procedure



Step 6.

- The WGSN Gr Handler issues the SS7 Alarm message to the Log Handler, and the event is logged. The Gr Handler returns the authentication vector to the GMM Handler.

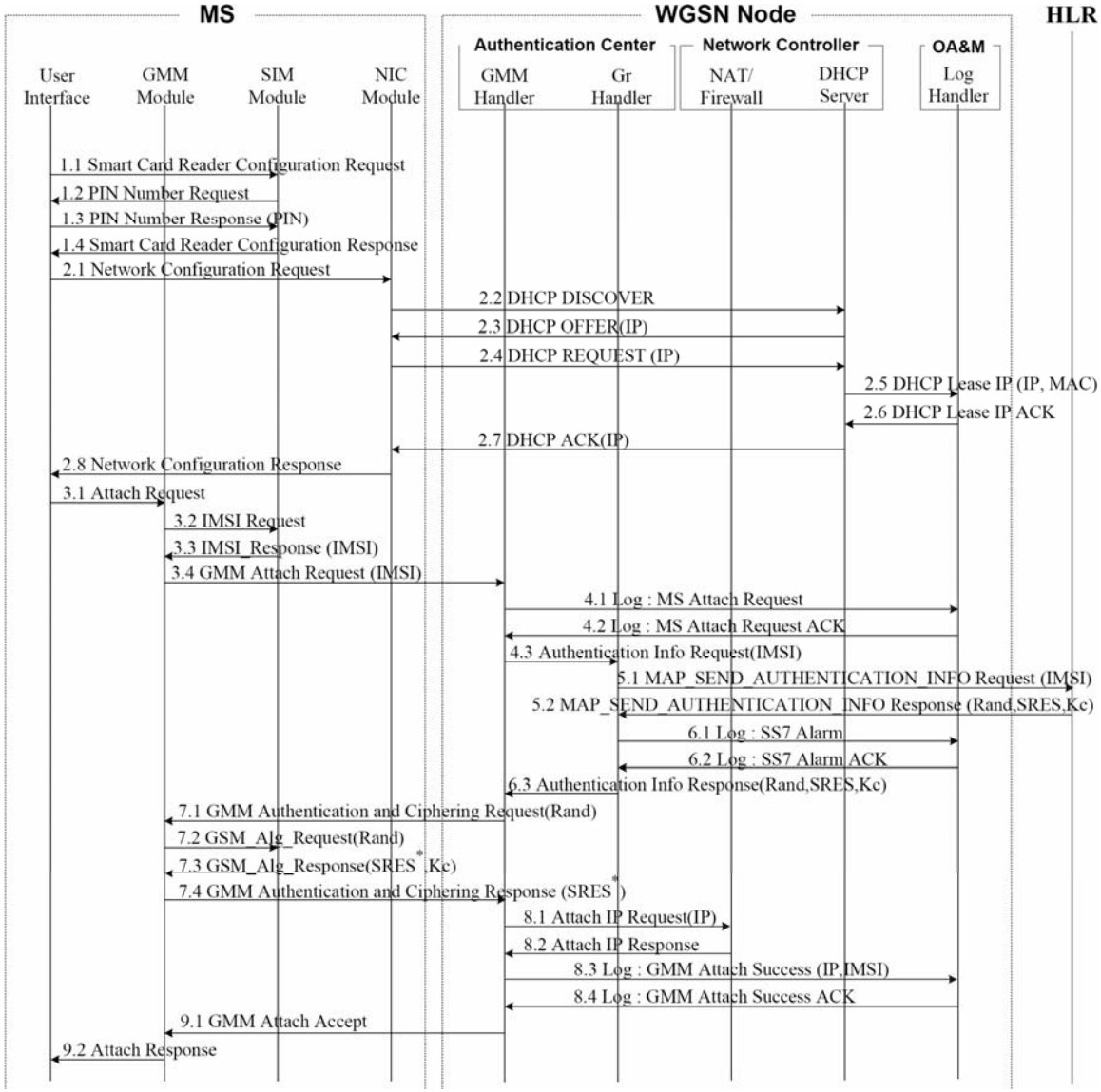
Fig. 14.6 Message Flow for the Attach Procedure



Step 7.

- The GMM Handler sends the GMM Authentication and Ciphering Request message (with the parameters IMSI and RAND) to the GMM module of the MS.
- The GMM module passes the random number (RAND) to the SIM module, and the SIM module computes the signed result (SRES∗) and the encryption key (Kc) based on the received RAND and the authentication key (Ki) stored in the SIM card.
- These results are returned to the GMM module. The GMM module returns the computed SRES∗ to the GMM Handler of the WGSN node using the GMM Authentication and Ciphering Response message (with the parameters IMSI and SRES∗).
- The GMM Handler compares SRES with SRES∗. If they match, the authentication is successful.

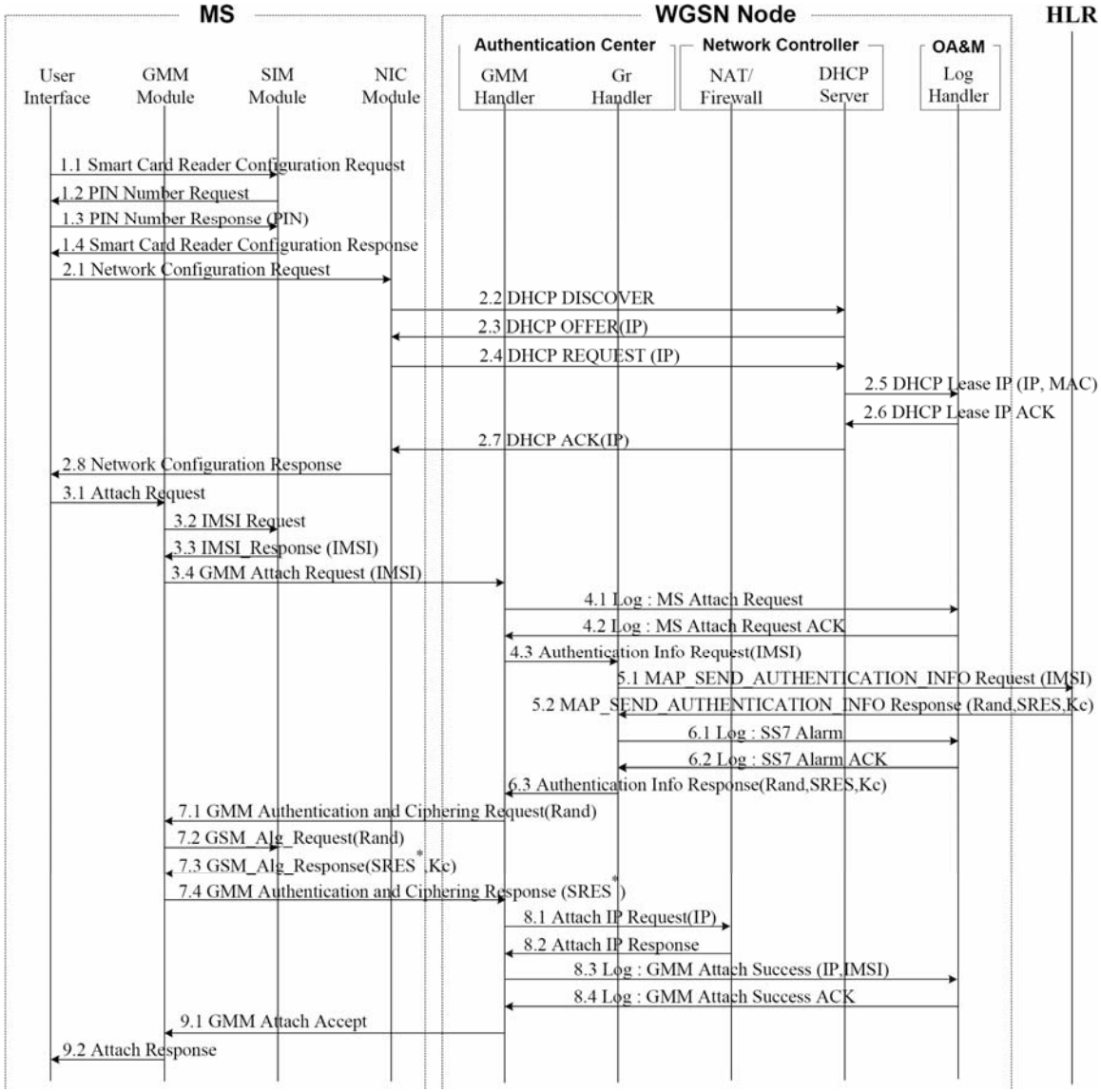
Fig. 14.6 Message Flow for the Attach Procedure



Step 8.

- The GMM Handler sends the Attach IP message to the firewall, which will allow the packets of this IP address to pass the WGSN node. Then the GMM Handler reports to the Log Handler that the attach is successful (with the corresponding IMSI and IP address).

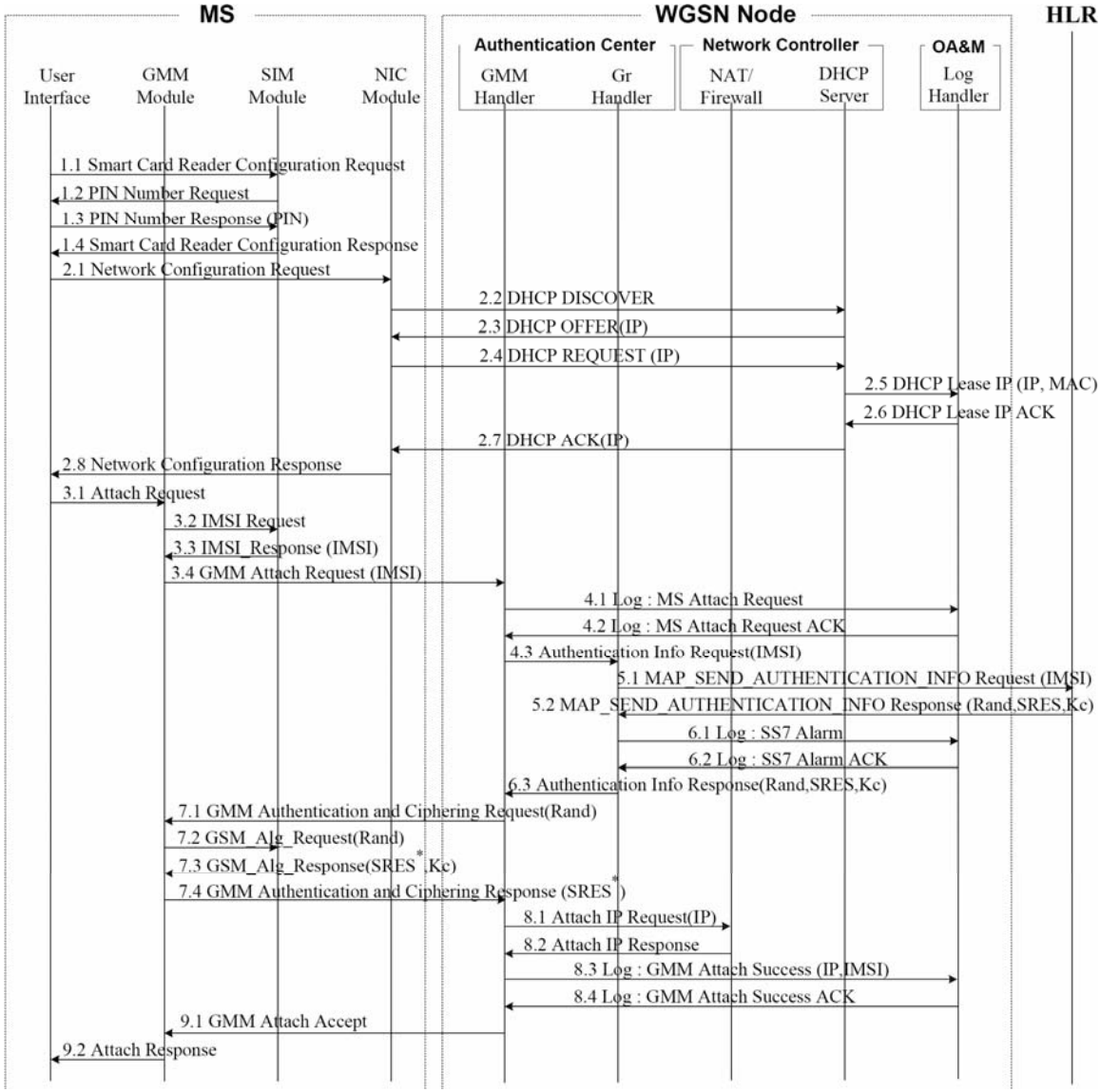
Fig. 14.6 Message Flow for the Attach Procedure



Step 9.

- The GMM Handler sends the GMM Attach Accept message to the GMM module of the MS, and the GMM module passes the Attach Response message to the user interface.
- At this point, the attach procedure is completed.

Fig. 14.6 Message Flow for the Attach Procedure



Detach Procedure

Fig. 14.7 Message Flow for the MS-Initiated Detach Procedure

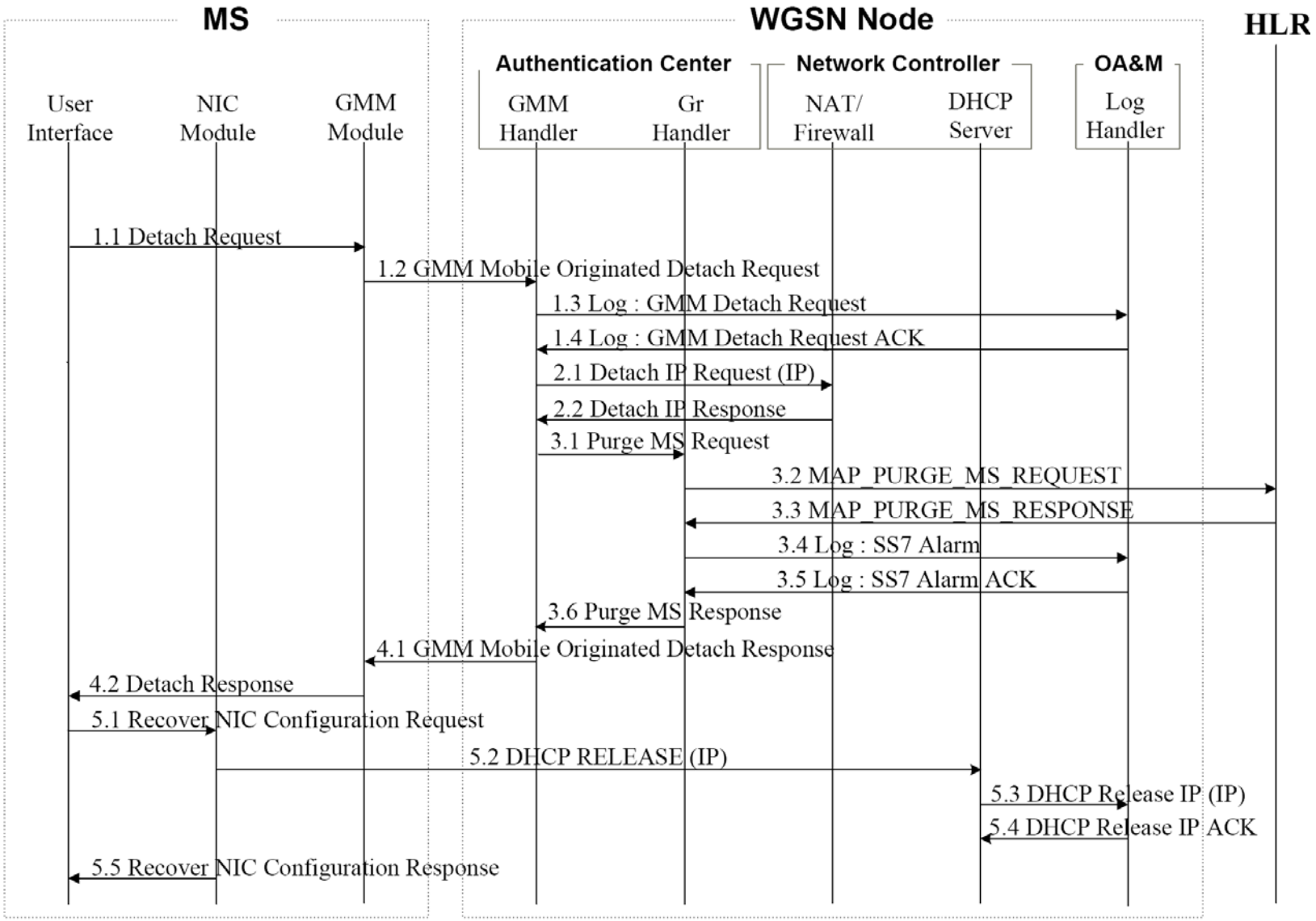


Fig. 14.8 The FSM State Transition Diagram for the SPC Status Record

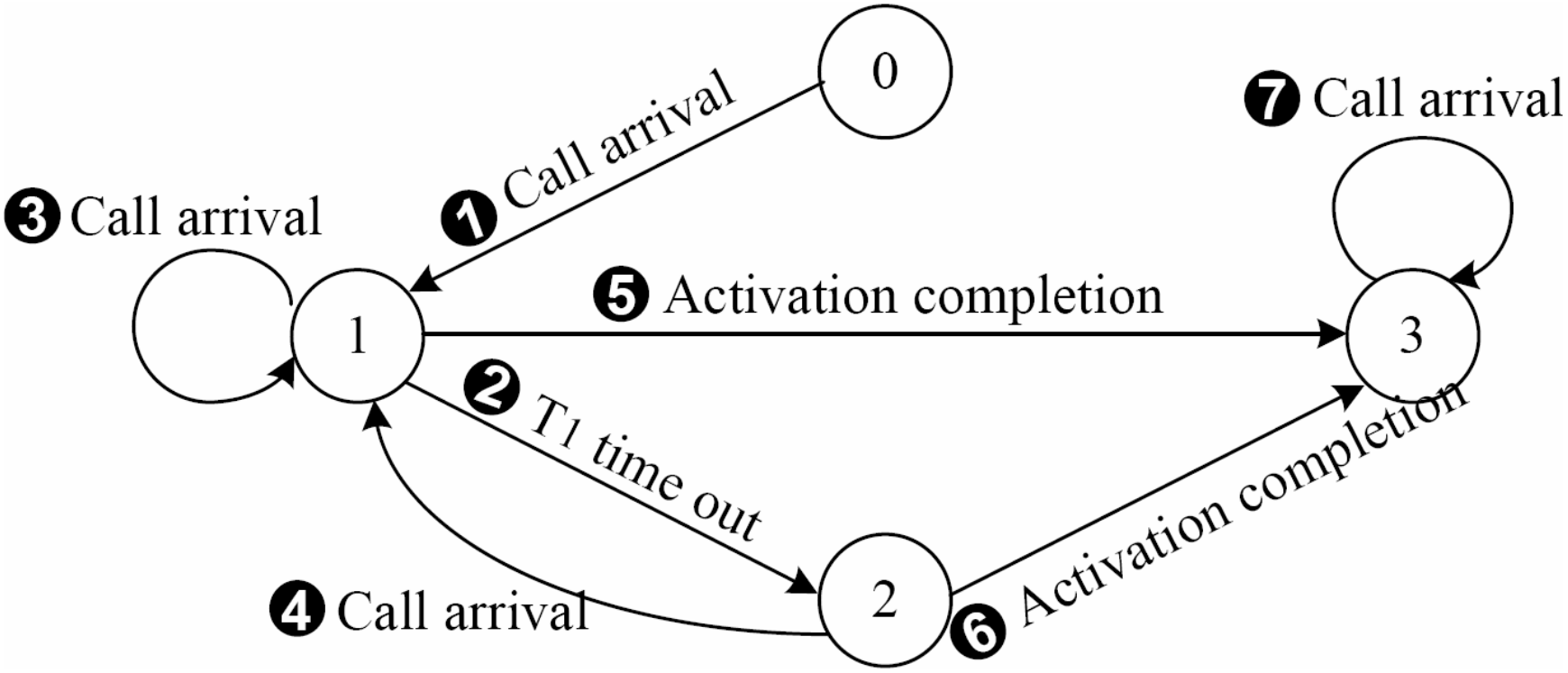


Fig. 14.9 The Timing Diagram I

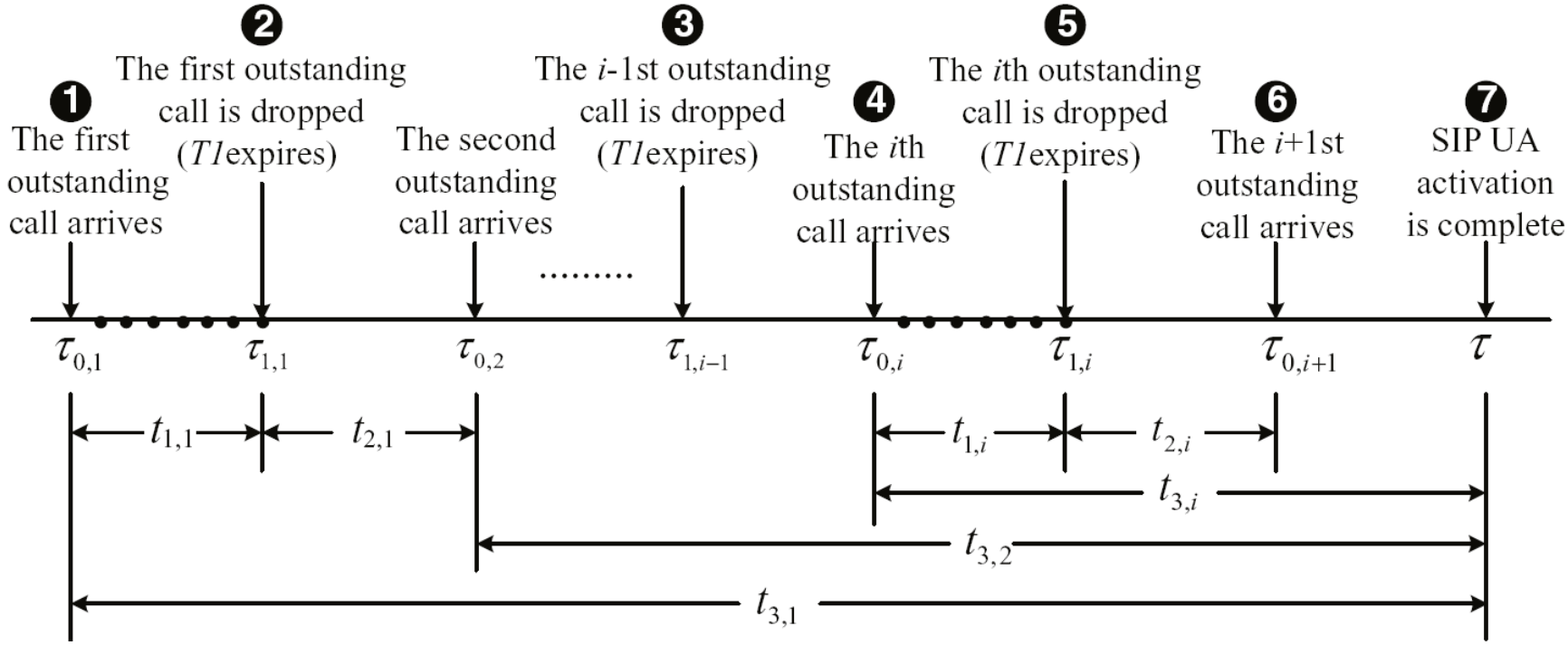


Fig. 14.10 A WLAN and Cellular Integration Environment

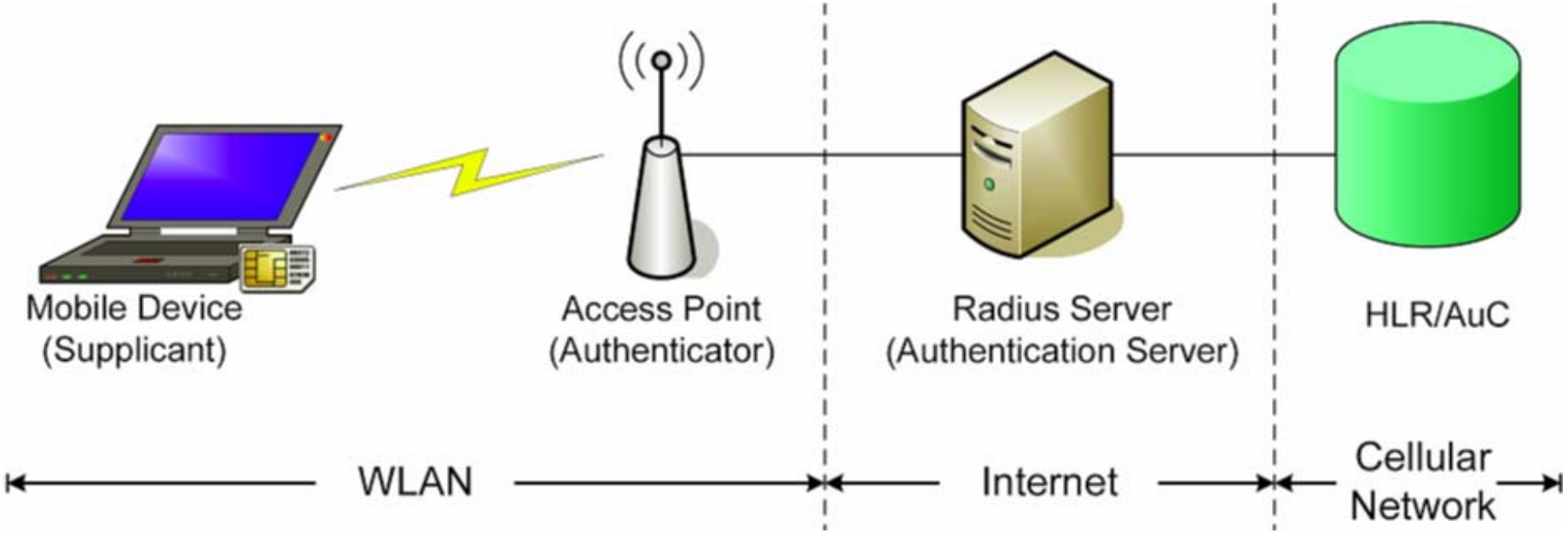


Fig. 14.11 IEEE 802.1X Protocol Stack

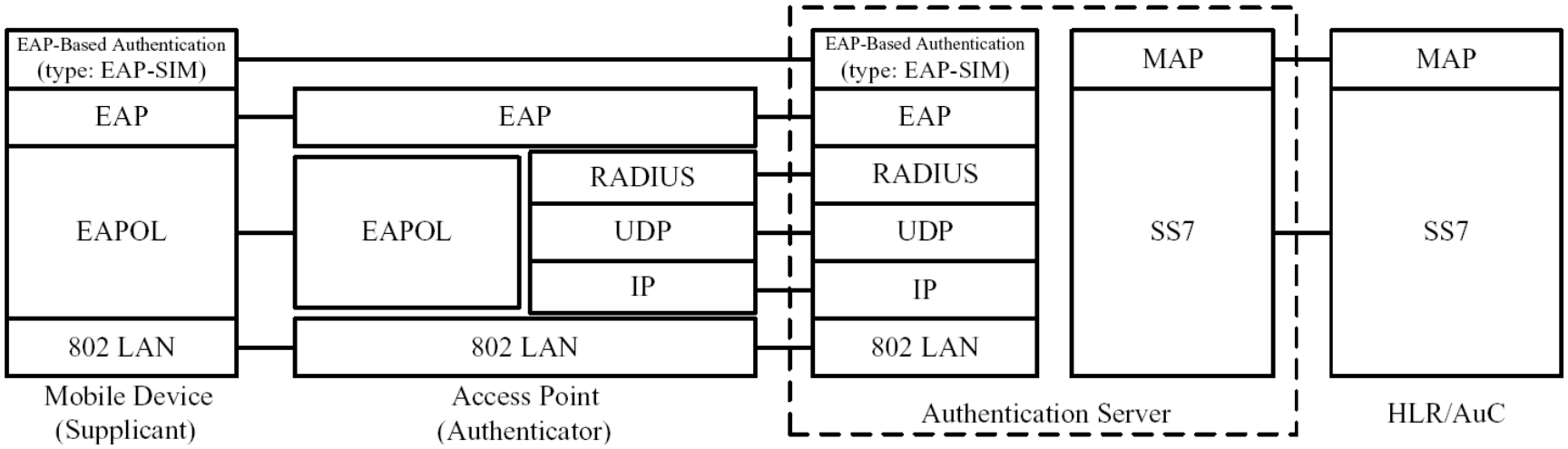


Fig. 14.12 EAP Header Format

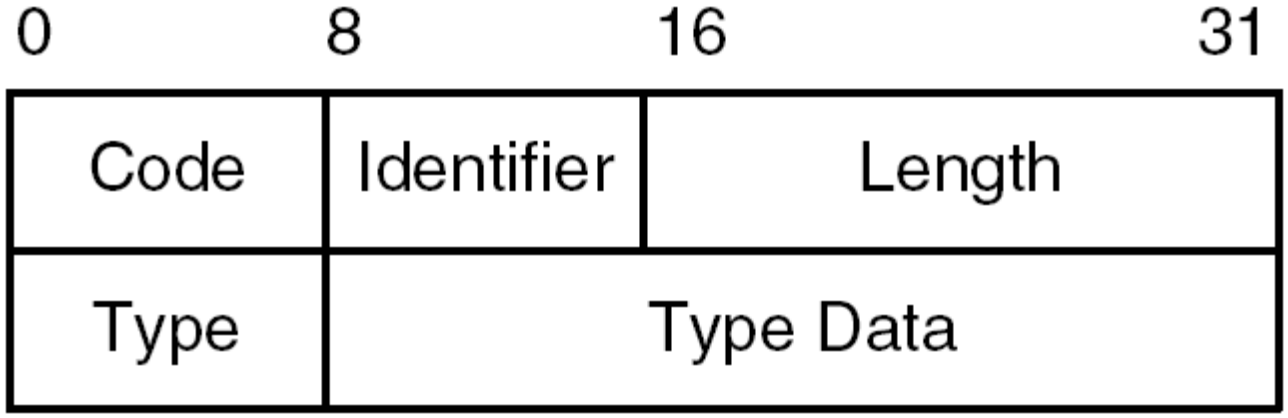


Fig. 14.13 EAPOL Frame Format

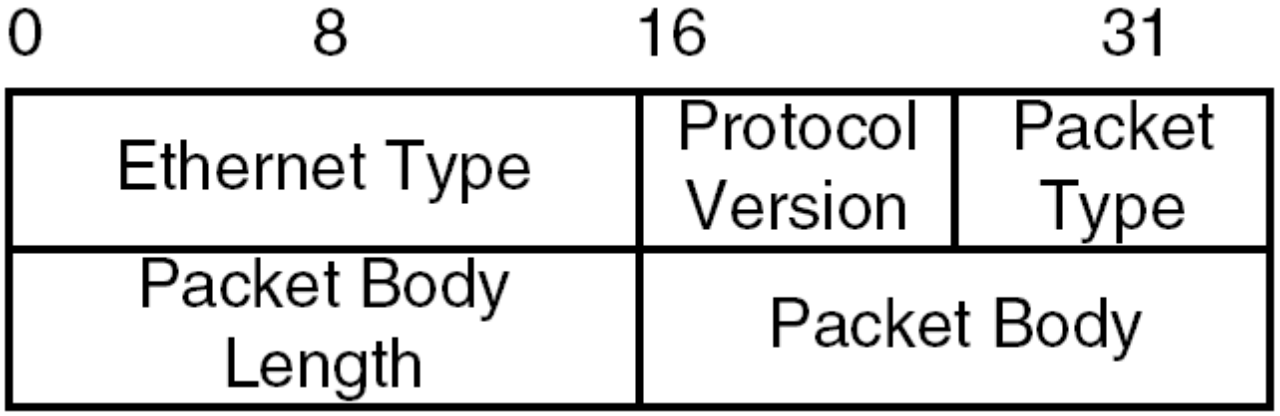


Fig. 14.14 RADIUS Packet Format

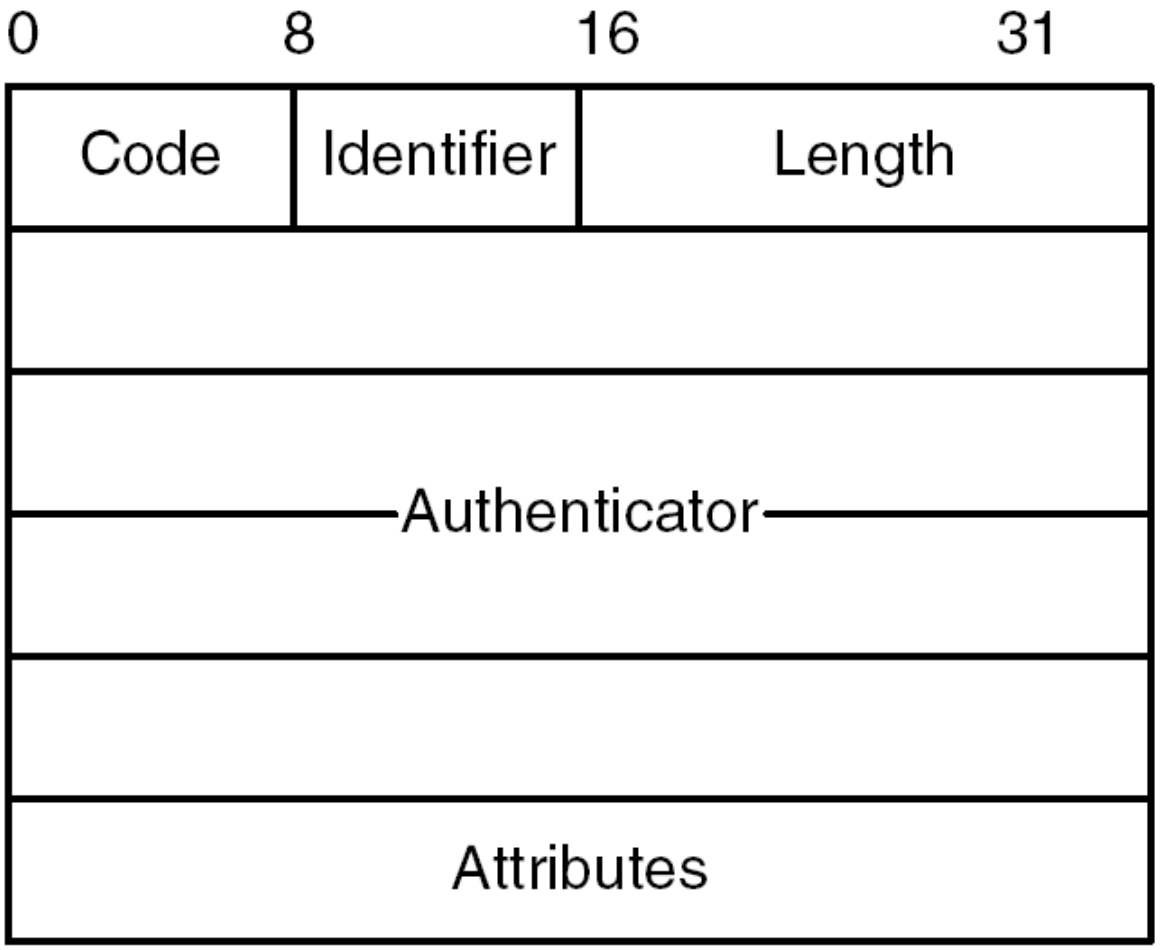


Fig. 14.15 IEEE 802.1X Authentication Message Flow