3GPP-WLAN Interworking using a Novel Access Control Mechanism

Ray-Guang Cheng, Shiao-Li Tsao

Department of Electronic Engineering
National Taiwan University of Science and Technology
Taiwan, R.O.C.

Dept. of Computer Science and Information Engineering
National Chiao Tung University
Taiwan, R.O.C.
crg@ieee.org, sltsao@csie.nctu.edu.tw

Abstract

The integration of WLANs and 3G networks has recently attracted much attention. To support seamless service between 3G and WLAN networks, low latency access control mechanisms of the two networks are highly required. This work presents a novel access control mechanism, which aims to support seamless services for an integrated 3G-WLAN network. The proposed method, based on a loose coupling architecture, employs a single set of procedures to authenticate the access to both WLAN and 3GPP, and ensures a low latency of the network access control procedures regardless of the traffic load of 3G and WLAN networks. It not only inherits the flexibility of a loose coupling approach, but also takes the advantage of a single method for controlling access to WLAN and 3GPP, based on tight coupling concept. Simulation results reveal that the proposed method can achieve a relative low WLAN attachment/re-attachment latency compared with existing methods.

Keywords : 3GPP-WLAN interworking, access control, loose coupling.

1 Introduction

Demand for ‘mobile information’ that everyone can access Internet at anytime from anywhere is increasing. With a well-established infrastructure, the 3rd generation (3G) system provides wide area wireless services with high mobility. The IEEE 802.11Wireless LAN (WLAN) system facilitates high-speed wireless services at relatively low cost but with limited service coverage and mobility. The integration of 3G and WLANs, which increases the coverage, bandwidth, and mobility of the individual networks, achieves the requirements of high-speed mobile information retrieval [1]. Interworking and integrating the two networks are regarded as very important to providing convenient access to both technologies in various environments, and to supporting seamless services between the two systems.

ETSI specified two generic methods for integrating WLAN and 3GPP systems, which includes GSM, GSM/GPRS and/or UMTS, known as loose coupling and tight coupling [2,3]. In loose coupling architecture [4-6], WLANs are deployed as an independent network complementary to the 3GPP systems, and WLAN and 3GPP are individually operated. EAP-SIM and EAP-AKA [4] over WLAN have been developed to obtain authentication and authorization for WLAN accesses, using subscriber information stored in the home location register/home subscriber server (HLR/HSS). Salkintzis [5] proposed two architectures for realizing interworking scenarios 2 and 3 defined in [7]. These architectures enable 3G subscribers to access WLAN and also provide WLAN subscribers with 3G packet-switched services. The importance and technique challenges of the session mobility were addressed; however, no solution was available yet. Shi, Shen, and Mark [6] proposed a WLAN service integration architecture to offer roaming in WLAN/cellular networks. An application layer end-to-end authentication and key negotiation was proposed to overcome the open air connection problem. However, application layer approaches often result in long handoff latency during the network/domain switching and thus, cannot ensure the service continuity. In these methods, the 3GPP functionalities are treated as residing behind the WLAN. Hence, the two networks share only a 3GPP subscriber database and WLAN access involves no 3GPP functionality, except for retrieving databases. The benefit of the loose coupling method is the flexibility of managing and operating the two networks. The shortcoming is that the presence of two access procedures results in the complicated design of user equipment (UE) and a high latency during 3GPP-WLAN handover.

The problem addressed herein is associated with the current loose coupling methods: a WLAN station (STA) must first pass through the WLAN access control procedure before it can perform a signaling procedure on the 3GPP network. To solve this problem, Salkintzis [8] proposed an EAP-GPRS protocol to eliminate the need for two access procedures, minimizing the 3GPP/WLAN handover latency in a tight coupling architecture. The tight coupling method treats WLAN as a radio access network which is tightly connected to a 3GPP backbone. The tight coupling method reduces signaling delays, minimizes handover latency between WLAN/3GPP, and eliminates the need of a mobile IP to support IP layer mobility. However, directly
connecting WLANs to a 3GPP CN removes the flexibility of independently managing WLAN and 3GPP networks. Implementing 3GPP protocols on top of a WLAN also increases the complexity of developing the WLAN card.

This work considers the interworking scenario 4 defined in [7], which focuses on the service continuity (or session mobility) for roaming between 3GPP systems and WLANs. Hence, we focus on a Class WA 3G-WLAN user equipment (UE) [9] operating under both WLAN and 3GPP coverage. This class of 3G-WLAN UE has both 3GPP and WLAN radio interfaces, can attach to both WLAN and 3GPP systems at the same time, when an interworking WLAN is available. Also it supports simultaneous access to both WLAN and 3GPP cellular network by activating both radio interfaces. Accordingly, a novel access control mechanism, which aims to minimize access latency for 3GPP-WLAN interworking, is developed. The access latency of a network is mainly introduced by the messages exchange during user authentication and authorization and user database query. In this paper, we adopt a single set of access control procedure for both WLAN and 3GPP to reduce the time for the user database query. Moreover, the proposed method reuses the existing 3GPP authentication procedures over secured 3GPP radio links to obtain the WLAN access privilege. Therefore, it avoids un-predictable access latency introduced by the authentication and authorization of WLAN access over a contention-based WLAN channel. The proposed approach not only inherits the high flexibility of a loose coupling approach, but also provides the advantage of a single access control method for accessing both WLAN and 3GPP, based on tight coupling.

The rest of the article is organized as follows. Section 2 describes the system architecture. The interworking architecture and the functions of each network element are described. Section 3 presents the procedures and message flows that implement the proposed 3GPP-based access control mechanism. Section 4 elucidates the session management and mobility management based on the proposed access control methods to achieve service continuity. Section 5 compares existing access control methods in detail. The performance of these approaches is also investigated. Finally, Section 6 draws conclusions.

2 System Architecture

Figure 1 depicts the loose coupling architecture for 3GPP-WLAN interworking considered herein. This architecture inherited the original one that was proposed by 3GPP [7]. Since the 3GPP network provides ubiquitous coverage, the service area of a WLAN is assumed to be under the umbrella of 3GPP. Without loss of generality, the de facto WLAN architecture presented in [3] is considered. A WLAN operator, which is uniquely identified by a WLAN public land mobile network identity (WLAN PLMN ID) [10], maintains a WLAN comprising access points (APs), and a WLAN access gateway (WLAN AG) [7]. The AP, which is uniquely identified by a basic service set identification (BSSID), is a layer-two device that bridges a wireless local area network and a wired local area network. The AP is also responsible for encryption data over WLAN radio links. The WLAN AG is an access gateway, which relays WLAN user authentication messages to a 3GPP AAA server or a 3GPP AAA proxy [7]. The cellular network considered herein is a 3GPP system. The 3GPP system, which is uniquely identified by a public land mobile network identity (PLMN ID), consists of base stations (BTS in GSM/GPRS or NodeB in UMTS), base station controllers (BSC in GSM/GPRS or RNC in UMTS), serving GPRS support nodes (SGSNs), gateway GPRS support nodes (GGSNs), a subscriber information database HLR/HSS, visiting location registers (VLRs), an authentication center (AuC), and a 3GPPP AAA server or a 3GPP AAA proxy. The HLR/HSS stores all users’ profiles and subscription information. The AuC is responsible for generating authentication vectors (AVs) for subscribers. The AV, which is a triplet for GSM/GPRS and a quintet for UMTS, contains temporary authentication and key agreement data that enable a SGSN/VLR to engage in authentication and key agreement (AKA) with a particular subscriber. The VLR keeps the partial subscriber information within a SGSN area. The SGSN routes traffic within the CN and the GGSN is the gateway to the external networks. The BSC/RNC controls at least one BTS/NodeB, which provides radio access service to the UEs. The 3GPPP AAA server or the 3GPP AAA proxy, which is uniquely identified by its IP or SS7 address, is responsible for either processing WLAN AAA messages or relaying WLAN AAA messages to HLR/HSS; authorizing the attachment of WLAN users, and distributing security keys. A WLAN user, who has been successfully authenticated by the network, can be authorized to attach to the AP, generate security keys on the basis of challenge data originated from the 3GPP AAA server, and then access the
Internet through WLAN. It is important to note that the proposed access control method does not introduce new network components, and it can be applied to the original 3GPP-WLAN framework defined in [7].

The 3G-WLAN UE, as shown in Figure 1, is a dual mode WLAN-3GPP system UE defined in [7] which handles all the 3GPP-WLAN interworking services that are offered to the user through either the 3GPP or the WLAN network. Unless other specified, a 3G-WLAN UE is also referred to herein as a station (STA) or, in short, as a UE. The UE can be a smart phone, a laptop computer or a personal digital assistant (PDA) equipped with a 3G-WLAN dual mode communication module. The UE can be also a pair of single-mode devices that communicate with each other through a wireless personal area network (WPAN). In both cases, the IMSI and the WLAN physical address (e.g., MAC address) can be used to uniquely identify WLAN and 3GPP modules, respectively. The UE needs a subscriber account to access WLAN. The account may be represented by a Network Access Identifier (NAI). The NAI, which includes a user name part, followed by the ‘@’ character and a realm part, identifies the user and the home network. The account information is stored in the USIM.

The architecture deal with the interworking scenario 4 defined in [7], which allows services to be survived during a change of access between WLAN and 3GPP systems. Accordingly, a user can access the 3GPP system, WLANs, or both networks using a single subscriber account. The IP session continuity or service continuity between the WLAN and the 3GPP system is handled by either mobile IP or application mobility methods such as session initiation protocol (SIP) mobility. Data packets may be forwarded and routed between packet data gateways (PDGs) and GGSNs for users who are roaming between WLAN and the 3GPP system. Based on the system architecture described above, the WLAN access control procedures with low access latency for supporting the service continuity in a 3GPP/WLAN integration network are developed below.

3 3GPP-based Access Control

This section describes procedures required to implement the 3GPP-based mechanism for controlling WLAN access. An access control mechanism may support mutual authentication to prevent illegal access; provide authorization to ensure users’ access privilege, and perform security functions for data exchange. In a 3GPP system, the 3GPP AKA procedure implements all of these features. The AKA procedure is a challenge/response protocol, which supports mutual authentication between users and the system. It also provides key materials to both the UE and the network to generate cipher key and integrity key.

IEEE 802.11i, which extends 802.11 with enhanced security, specifies a scalable authentication, access control, and key management framework based on the IEEE 802.1x standard [11]. 802.11i defines three authentication and key management architectures [12]. The ‘Open System’ and ‘Share Key’ architectures are defined for use in the context of wired equivalent privacy (WEP) and the ‘802.1x-based’ architecture is defined for the use in the context of a robust security network. Share key authentication is currently disfavored and the open system is the default authentication architecture for legacy equipment that does not support 802.1x. 802.1x defines a framework based on the EAP over LAN, also known as EAPoL. EAPoL provides a protected channel for exchanging EAP messages. The messages support mutual authentication between STAs and 3GPP AAA servers such that rouge APs and unauthorized STAs can be eliminated. The required attachment procedures, the user authentication and authorization procedures, the admission control policies, the security functions, and the detachment procedures for implementing 3GPP-based access control are developed below.

3.1 3GPP Attach

In either a WLAN or a 3GPP system, a UE must be attached to the network before it acquires network services. UEs may decide to be attached to the 3GPP network by performing 3GPP attachment or registration procedures [13]. During the attachment, the authentication, authorization and security procedures, which will be addressed later in this section, must be supported to protect the access rights of the subscriber. After successful attachment, the UE enters the discrete reception mode to reduce its power consumption and periodically updates its location information. A UE normally is permanently attached to the 3GPP network after power-on and so is reachable at anytime anywhere given the ubiquitous coverage of the 3GPP system.

3.2 WLAN Attach

In 802.11, an STA is attached to the WLAN by the association procedure. The authentication procedure may be executed during the attachment. Normally, the open system authentication and association procedures are used by a UE to negotiate security characteristics with the AP [12]. If 802.1x is further supported, an EAP type specific mutual authentication between the UE and the 3GPP AAA server will be executed. Since the WLAN service may be provided only in the hotspot, the UE may not be able permanently to be attached to a WLAN. The UE may, however, become attached to the WLAN, to meet the demand of the service. On-demand attachment prevents the UE from unnecessary frequency scanning and packet monitoring and so may considerably reduce the power consumption.
3.3 User Authentication and Authorization

We offer two alternative methods - ‘direct-authentication’ and ‘reverse-authentication,’ - to authenticate the UE for accessing WLAN. Both methods use current 3GPP authentication procedures over secured 3GPP radio links and can be applied to both open system and 802.1x-based architectures. Hence, the access latency are not be affected by the WLAN traffic load because the authentication and authorization messages are mainly exchanged over the 3GPP radio link.

The direct-authentication method, depicted in Figure 2(a), is similar to that in the case of a mobile-terminated (MT) call. The 3GPP AAA server triggers the authentication by providing the subscriber account (such as the NAI) and the identity of the WLAN module (such as the MAC) of the UE to the 3GPP network. The 3GPP AAA server will use the NAI to identify the home network to perform the authentication and the 3GPP network will use the NAI to identify the subscriber. The UE will use the MAC for verification during the 3GPP authentication procedure. The 3GPP AAA server may decide to communicate with the HLR/HSS over the SS7 network or the Internet. In either case, the 3GPP AAA server can use the NAI to obtain the routing path. If a SS7 network is available, the 3GPP AAA server will send the authentication request directly to the HLR/HSS. In this case, the HLR governs the triggering of the 3GPP authentication procedure. If no SS7 link is present between the 3GPP AAA server and the HLR, then the 3GPP AAA server may transmit the authentication request to the HLR through the Internet. In this case, the GGSN is responsible for triggering the authentication and the HLR serves as a subscriber database which resolves the IMSI and IP address of the serving SGSN, SGSNinUse, from the NAI.

The WLAN subscription information is assumed to be downloaded from the HLR and stored as a data entry in the VLR during the 3GPP attachment. Hence, the SGSN will query the VLR for authorization when it receives the request from the GGSN. The authentication information is then exchanged between the SGSN/VLR and the UE. The SGSN/VLR may retrieve the up-to-date AVs from the HLR/HSS and setup an RRC connection to the UE. The UE will check its MAC address during authentication to prevent fraudulent access. If verification fails, the UE must return a User Authentication Reject message, indicating the MAC error. Otherwise, the UE may request the SIM/USIM application to perform the AKA algorithm and return a User Authentication Response message with an expected user response. Finally, the 3GPP AAA server will be informed about the authentication result. Direct-authentication is similar to that associated with the methods adopted by the EAP-AKA/EAP-SIM, except in that the AKA of the direct-authentication is undertaken over the 3GPP radio link, rather than the unsecured WLAN radio link. Therefore, it can replace the EAP-AKA/EAP-SIM with minimal effort.

Reverse-authentication is proposed to simplify the authentication process further. Figure 2(b) shows the message flows associated with the reverse-authentication method. Unlike the direct-authentication method, the reverse-authentication method triggers the authentication for its WLAN access via the UE, rather than the network. The Service Request message [13] with service type field indicating the WLAN access, is proposed herein to minimize the protocol modification of the 3GPP system. The message carries the W-APN of the WLAN operator and the MAC address of the UE such that the SGSN can use this information to configure the 3GPP AAA server. After it has received the Service Request from the UE, the SGSN may query the VLR for the authorization of the subscriber and then exchange the authentication information with the UE. If the authentication succeeds, the SGSN will respond to the UE with a Service Accept message to instruct the UE to attach itself to the WLAN. The SGSN also tells the 3GPP AAA server to activate the WLAN service for the specific MAC address according to the given W-APN. In the reverse-authentication method, the UE can perform WLAN attachment only after successful authentication. Accordingly, the WLAN will not be notified about the failure
authentication and the signaling load is reduced. Additionally, active attacks against the authentication server are prevented because the 3GPP AAA server will not request 3GPP authentication when it receives attachment requests from illegal UEs. The following paragraph elucidates the adaptation of the aforementioned methods to make them applicable to the authentication architectures defined by 802.11i.

The authentication procedure used for open system and 802.1x-based architectures are described below. For simplicity, only reverse-authentication is illustrated. Readers may refer to [14] for the application of direct-authentication-based procedures. Figure 3 presents the proposed reverse-authentication procedure for the open system architecture. According to 802.11i, the Open System Authentication is a null procedure and may not trigger any action. Therefore, the AP must be enforced to request 3GPP authentication. In the proposed procedure, the UE is authenticated by the reverse-authentication method through the 3GPP radio interface. After the authentication, the SGSN/VLR notifies the 3GPP AAA server about the authentication results, therefore, the 3GPP AAA server can process the Authentication Request from the AP. In such a case, the 3GPP AAA server may set a timer to tolerate the propagation delay between the 3GPP AAA server and the HLR, after the 3GPP AAA server receives a request form the AP.

Figure 4 presents the proposed reverse-authentication procedure for the 802.1x-based architecture. 802.1x and EAP have defined a framework to support the access control so the authorization procedure is similar to that in the cases of EAP-SIM and EAP-AKA. In the proposed procedure, the UE is authenticated through the 3GPP radio interface. The AP sends the EAP Access Request/Identity message that carries the MAC address of the UE to the 3GPP AAA server for authentication. Upon receiving the Service Activation command from the SGSN/VLR, the 3GPP AAA server indicates the success of the authentication by responding to the UE with an EAP Success message.

3.4 Admission Control Policies

The admission control in the WLAN ensures that the operator provides services only to legitimate users by discarding packets from illegal users. If 802.1x is supported, then the AP performs the admission control; otherwise, is the WLAN AG performed the control. Koien and Haslestad [15] presented three admission control methods at the WLAN link layer. The first enables filtering of the MAC address at the AP or WLAN AG. The drawback of this approach is that all AP must be configured using an exhaustive and static list of subscribers’ MAC addresses. The second and the third methods rely on WEP and 802.11i, respectively. Hence, they may not be applied to legacy APs and UEs that do not support WEP or 802.11i.

The problem of MAC filtering can be solved by configuring the APs or WLAN AGs dynamically using the 3GPP AAA server. In the proposed authorization procedures, the 3GPP AAA server will notify the WLAN AG and the AP of the MAC address of the authorized user. Therefore, a list of authorized MAC addresses can be dynamically updated. For legacy APs and UEs that rely on the open system architecture, WLAN AG performs the admission control. 3GPP AAA server generates a list of the authorized MAC addresses and notifies the WLAN AG via the Authentication Response message. For the APs and UEs that adopt the 802.1x-based architecture, the admission control will be provided by 802.1x, which will be independent of the chosen authentication and authorization procedures.

3.5 Security Functions

Two security issues must be resolved for 3GPP-WLAN interworking. The first is to ensure confidentiality and integrity over the radio link and the second is to protect subscribers’ AVs from unnecessary disclosure within the wired network. Confidentiality is aimed at protecting against inappropriate disclosure of system or user data, which can be achieved by providing symmetric key encryption. Integrity
aimed at protecting data from illegal modification and is realized by applying symmetric keyed cryptographic checksum functions.

In the 3GPP system, the 3GPP AKA algorithm supports the confidentiality and integrity over the radio link. It enables the SGSN and the UE to derive the cipher and integrity keys separately. The entire 3GPP network is owned by a single operator, so the information exchange within the wired network is protected. In 802.11, 802.1x and the selected EAP method are responsible for supporting the radio link security. If EAP-AKA or EAP-SIM is adopted, both the STA and the 3GPP AAA server can individually derive a master key for protecting the message exchanged over the radio link. The key is derived from the AVs obtained from the HLR and the AKA or SIM algorithm defined by 3GPP. In these approaches, the 3GPP AAA server can query the HLR for the AVs whenever it needs. Therefore, the security of the AVs is not guaranteed if various operators own the WLAN and 3GPP networks.

In the proposed method, both the security of the radio link and the subscriber’s AVs are well protected because the mechanism reuses current 3GPP authentication procedures over secured 3GPP radio links to enable WLAN access. Accordingly, the 3GPP AKA algorithm provides the radio link security and the AVs need not be distributed to the 3GPP AAA server. Thus, a higher security level can be attained.

3.6 3GPP Detach

The dual-mode UE may decide to detach itself from the 3GPP network when its power is turned off. The standard 3GPP detach or de-registration procedure is used for detachment. Notably, the 3GPP will automatically trigger the WLAN detach procedure during the 3G detatchment if the UE remains attached to the WLAN.

3.7 WLAN Detach

The dual-mode UE may choose to detach from the WLAN when it finishes its WLAN service or exits the area covered by the WLAN. In the former case, the 3GPP AAA server must inform the 3GPP system of the detachment of the WLAN services. In the latter case, the UE and the 3GPP AAA server will be notified of the breaking of the WLAN link after a link-layer timer is expired. Hence, the UE and the 3GPP AAA server individually trigger the detachment procedure and the 3GPP AAA server must inform the 3GPP system of the detachment. The 3GPP system may trigger a periodic WLAN authentication or a combined 3GPP/WLAN authentication during WLAN access. If the authentication fails, then the 3GPP system may trigger the UE or the 3GPP AAA server to perform a WLAN detachment procedure, possible to increase the level of security of the user if the WLAN subscriber forgets to log out his/her account.

4 Service Continuity

This section further addresses service continuity. This work considers only the continuity of packet domain services. Two typical solutions are offered to support service continuity between WLAN and 3GPP networks. The first method relies on a mobile IP to provide a single IP session to applications and correspondent nodes. Therefore, the correspondent nodes communicate with the UE through the same IP address, while the UE moves from the WLAN to the 3GPP network or vice versa. Mobile IP mechanisms involved in WLAN and 3GPP networks manage the single IP address. The second method, which may involve SIP mobility, leaves the problem of service continuity to be solved by applications. The UE may register two IP addresses, one for WLAN and the other for 3GPP network, and signal the application server to switch the active IP address when the UE moves from one network to the other. The following paragraph presents the session management and mobility management based on the proposed access control methods to achieve service continuity.

4.1 Session Management

UEs can perform the 3GPP packet data protocol (PDP) context activation procedures defined in [13] to establish a 3GPP session and thus obtain IP service. SGSN and GGSN handle the 3GPP session in 3GPP networks. In WLAN, the UE can first attach itself to the WLAN based on WLAN attachment procedures defined above, and then it can receive an IP address from configuration protocols such as the dynamic host configuration protocol (DHCP). The WLAN sessions are IP sessions that are managed by a WLAN infrastructure. WLAN IP sessions can be independent of 3GPP IP sessions so that users can requests packet domain services through WLAN sessions and/or 3GPP sessions to meet their needs. If WLAN and 3GPP are dependent sessions, then application-level solutions are required to ensure service mobility. For instance, a WLAN user registers a SIP service and is conducting a SIP session. After the user moves to a 3GPP network, he obtains a new IP address. The user must send a Re-Invite SIP message with the new IP address to notify the application server that the change of the IP address.

Another scenario is that a user subscribes to a single IP service and wishes to have the same IP address while moving to visiting networks. In this scenario, a mobile IP must be implemented in WLAN and 3GPP networks. Figure 5 shows an example of the combination of mobile IP service with the proposed access control method. The example elucidates situations in which mobile IP version 4, without routing optimization, is offered.
If the subscribed IP address belongs to the WLAN and subscribers are attached to a 3GPP network, then the UEs have to send a Registration Request to the home agent in the WLAN to update its current care-of address (CoA). All packets sent to the WLAN home network are forwarded to the newly visited 3GPP network. However, if the subscribed IP address belongs to the 3GPP network and subscribers are attached to a WLAN, then the UE must also send the Registration Request to the home agent in the 3GPP network to update its CoA. Applying the mobile IP between WLAN and 3GPP networks ensures that IP sessions are not broken so applications and services session are maintained.

In summary, sessions in WLAN and 3GPP can be independent and/or mobile IP sessions. The proposed access control mechanisms introduce no extra procedures in session management nor differ from standard 3GPP access control methods, such as EAP-SIM or EAP-AKA.

### 4.2 Mobility Management

Regarding of mobility between WLAN and 3GPP networks, management procedures can be separated into 3GPP intra-system mobility, WLAN intra-system mobility, and 3GPP-WLAN inter-system mobility. 3GPP intra-system mobility management remains unchanged since the proposed access control method adds only few parameters to current 3GPP procedures without introducing new message flows in into the 3GPP system.

In WLAN environment, the WLAN intra-system mobility management mechanisms must be addressed. A UE moves from one AP to another AP; if the network domain of the two APs are the same, then the UE can still access the network with the help of WLAN mobility management, incorporating, for example, the inter-access point protocol (IAPP). As the UE moves from one AP to another AP in different WLAN domains, the UE first detects the changes of the W-APN via network probe or the broadcast messages. The information reveals that the UE must be attached to the WLAN again in order to gain the network access rights. The new WLAN attachment should again perform direct-authentication or reverse-authentication, as described in Section 3. Figure 6 shows the message sequence chart according to which a UE moves from one AP to another AP when the two APs belong to two different WLAN domains. Figure 6 also depicts the flows of mobile IP messages between the UE and APs. Mobile IP can be applied to provide IP session continuity.

The third scenario is that of WLAN-to-3GPP and 3GPP-to-WLAN inter-system mobility management. An example is considered in which a UE accesses a WLAN, moves out of the WLAN and tries to continue to receive the packet domain services through a 3GPP network. The UE can activate PDP sessions in the 3GPP network; terminate WLAN sessions, and access the packet domain service again using the new IP address. If the user has subscribed the mobile IP service, the UE can activate new PDP sessions and send mobile IP messages to the home agent and correspondent hosts via the new PDP session; the IP sessions and service can thus be retained. The case is similar to that of 3GPP-to-WLAN handover, as depicted in Figure 5.

The above analysis reveals that the proposed access control method can be applied to manage the mobility of 3GPP networks, WLANs and between WLAN and 3GPP networks. The proposed method has a lower signaling complexity than that associated with separating WLAN control over WLAN, and 3GPP control over 3GPP, which methods are normally adopted in current access control methods, since the proposed method embeds both WLAN and 3GPP control in 3GPP radio links. The next section compares various access control methods.

### 5 Comparison of Existing Approaches

Table 1 compares different 3GPP-WLAN interworking approaches at a high level. The advantages of the proposed method are summarized below:

a. Reuse of existing 3GPP signaling: Extensions of information elements allow 3GPP control messages to be used to control WLAN access. Integrating the access control of WLAN and 3GPP reduces the signaling complexity of network nodes.

b. 802.1x infrastructure is not mandatory: the proposed...
method can be deployed over WLANs with or without the 802.1x infrastructure. In EAP-SIM and EAP-AKA, 802.1x infrastructure is required. The proposed method benefits existing WLANs in which 802.1x has not yet been implemented.

c. Secure infrastructure: all authentication and authorization messages and procedures are carried and exchanged over a 3GPP secured infrastructure. This is the main difference among EAP-SIM, EAP-AKA, EAP-GPRS and the proposed method. EAP-SIM, EAP-AKA and EAP-GPRS exchange authentication and authorization information over WLANs. WLANs operate on an unlicensed spectrum, so an adversary may easily retrieve authentication information and initiate active attacks, introducing a potential security hole. However, carrying authentication and authorization information over 3GPP radio links and networks reduces potential security problems. Additionally, the proposed access control mechanism exchanges authentication information within the private 3GPP CN and the HLR may not need to share subscribers’ information with the 3GPP AAA server. This approach reduces the effort required to manage the network and is beneficial for 3GPP operators.

The proposed method provides an alternative access control method in the 3GPP-WLAN interworking environment. It not only inherits the high flexibility of a loose coupling approach, but also provides the advantage of the single access control method in both WLAN and 3GPP, based on a tight coupling concept. More importantly, all of the proposed access control procedures are exchanged over a secured 3GPP infrastructure.

Simulations based on NS2 [16] are conducted to examine the maximal throughput and the access (i.e., attachment/re-attachment) latency of a UE. EAP-AKA, EAP-GPRS and the proposed reserve-authentication are investigated. Figure 7 presents the simulation environment. In the figure, a WLAN network consists of an 802.11 access point (AP), a WLAN AG, and a gateway (GW) to the Internet. A 3G network has an authentication server (3GPP AAA server), an HLR, a Node B, an RNC, a SGSN, and a GGSN connecting to the Internet. Three types of UE, a WLAN-UE, a 3G-UE and a 3G-WLAN UE, are defined here and are considered in the following simulations. A WLAN-UE is a single-mode terminal that accesses WLANs only. A 3G-UE is also a single-mode terminal that accesses 3G cellular networks only. A 3G-WLAN UE is a dual-mode terminal that simultaneously connects to the 802.11 AP and the Node B. In order to simulate the background traffics generated by WLAN-UEs accessing the same 802.11 AP and 3G-UEs accessing the same Node B, a WLAN-UEs emulator and a 3G-UEs emulator are configured into the simulation environment in Figure 7. The emulators generate constant bit rate (CBR) UDP packets to the Internet. Similarly, a 3G-Node Bs emulator and an 802.11-APs emulator are introduced in order to produce background UDP traffics from other 3G Node Bs to the same RNC and other 802.11 APs to the same WLAN AG, respectively. In the tightly coupling approach, 802.11 APs are directly connected to the RNC and thus, the dash links between the 802.11 APs and the RNC shown in the figure only exist for

### Table 1 Comparison of control and data planes of different 3GPP-WLAN interworking approaches

<table>
<thead>
<tr>
<th>3GPP-WLAN interworking approaches</th>
<th>Tight coupling</th>
<th>Loose coupling</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(EAP-GPRS)</td>
<td>3GPP approach</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(EAP-SIM, EAP-AKA)</td>
</tr>
<tr>
<td>control plane</td>
<td>3GPP signaling over WLAN</td>
<td>WLAN signaling over WLAN</td>
</tr>
<tr>
<td>data plane</td>
<td>Packet through WLAN and 3GPP CNs to Internet</td>
<td>Packet through WLAN to Internet</td>
</tr>
<tr>
<td>3GPP</td>
<td>3GPP signaling over 3GPP networks</td>
<td></td>
</tr>
<tr>
<td>data plane</td>
<td>Voice/packet through 3GPP networks to external networks</td>
<td></td>
</tr>
</tbody>
</table>

![Figure 7 3GPP-WLAN simulation environment](image-url)
EAP-GPRS simulations.

The throughput of the 3G-WLAN UE is first investigated, where \( n \) 3G-WLAN UEs are served by one 802.11 AP. In this simulation, the traffic loads of the WLAN CN, the 3G CN and the 3G radio access network (RAN) are all considered. The background load of the 3G CN is CBR UDP packets generated from the 3G-Node Bs emulator to the 3G CN. This is to simulate that other Node Bs competes the bandwidth of the 3G CN. The background load of the WLAN CN simulates that other APs are competing the bandwidth of the CNs. The background load is also the CBR UDP packets generated from the 802.11-APs emulator through data path I or data path II in Figure 7. The data paths are routing paths of packets from a 3G-WLAN UE to the Internet once the 3G-WLAN UE obtains the access right of the WLAN network. The data path I is the path for the proposed approach and EAP-AKA, adopting the loose coupling architecture, in which packets are routed through AP, WLAN AG and GW to the Internet. The data path II is the path for EAP-GPRS, utilizing the tight coupling architecture, in which packets are routed through AP, RNC, SGSN and GGSN to the Internet. The data paths of EAP-AKA and EAP-GPRS are the same as their signaling paths, but the data path and signaling path are different in our proposed method. We exchange AAA messages over 3G RRC links and route data packets to the WLAN CN once the WLAN access is granted. It can be found in Fig. 8 that EAP-GPRS achieves the lowest average throughput among all 3G-WLAN UEs and 3G-UEs in the tightly coupling architecture. On the other hand, both the proposed approach and EAP-AKA route WLAN traffic through WLAN CNs and direct 3G traffic to 3G CN, therefore, the better performance is attained.

The latency introduced by a WLAN attachment process is then studied. The attachment latency considers only the network transmission delay and assumes that the nodes exhibit no message-processing delay, including AVs retrieval, database query and key generation. Another assumption of both EAP-GPRS and the proposed method is that 3GPP RRC links are already established; therefore, the time required to establish 3GPP RRC links has not been taken into account. Figure 9 shows the simulation results of the WLAN attachment latency of a UE, where only the background load of a WLAN access network (W-AN) is considered. The W-AN background load is generated by the WLAN-UEs emulator and sent to the 802.11 AP. It is to emulate that the bandwidth of the 802.11 AP is shared by a number of WLAN UEs. Figure 9 demonstrates that all three methods have a low attachment latency of less than 500 ms when the background load is under 1Mbps. It is also found that EAP-GPRS performs best among the three methods under this condition because EAP-GPRS is based on a tight coupling approach, in which 3G CN nodes can directly route and process messages received from the APs. The simulation results also show that the proposed method achieves a better performance if the W-AN background load is higher than 600Kbps. It is because EAP-GPRS and EAP-AKA exchanges AAA messages over the WLAN, which is a contention-based medium. On the other hand, increasing the W-AN background load does not excessively affect the attachment latency of the proposed approach since most of the attachment messages go through a 3GPP RRC link, which is a dedicated control channel.

Then, the impact of the 3G CN background load, which is generated by the 3G-Node Bs emulator and is routed to the 3G CN through path III, is further investigated. Figure 10 depicts the WLAN attachment latency of a UE under different 3G CN background loads, where W-AN background loads of 64kpbs and 2048kpbs are still considered. It is found that both EAP-GPRS and the
proposed method are influenced by the 3G CN background load because the attachment messages of the two methods go through a 3G CN. Instead, EAP-AKA sends the attachment messages via the WLAN CN and thus, the performance are not affected. The simulation results also reveal that the attachment latencies of both EAP-GPRS and the proposed method become longer than that of EAP-AKA while the 3G CN is almost fully occupied. Fortunately, the insufficient bandwidth problem of the CN can be solved by increasing the bandwidth of network links between 3G CN nodes. Similar experiment is conducted by considering the background load of the 3G access network (3G-AN). The 3G-AN background load is generated by the 3G-UEs emulator, producing CBR UDP packets to the same Node B. It is to simulate that UEs in the same cell are competing the radio interface resource. Figure 11 demonstrates the WLAN attachment latency of a UE under different 3G-AN background loads. Simulation results show that all the three methods are not influenced by the 3G-AN background load. The reasons are different for EAP-AKA, EAP-GPRS, and the proposed method. In EAP-AKA and EAP-GPRS, authentication and authorization messages are not transferred over 3G radio links. In the proposed method, although authentication and authorization messages are exchanged over a 3G radio link, these messages are transferred over a dedicated 3G RRC link, which is not shared with other UEs. Figures 10 and 11 reveal that the attachment latencies of EAP-AKA and EAP-GPRS are significantly influenced by the W-AN background load because the two methods exchange messages over the WLAN. On the other hand, the proposed method is insensitive to both W-AN and 3G-AN background loads since it exchanges most of the signaling messages over a dedicated 3G RRC link.

6 Conclusion

This work presented a novel access control mechanism for 3GPP-WLAN interworking. Unlike other methods, the proposed mechanism suggests performing authentication and authorization via a 3GPP radio interface. The advantages of the proposed method are summarized below. First, the proposed method achieves a relative low WLAN attachment/re-attachment latency compared with existing methods. Secondly, the method uses only one, rather than two access control procedures for WLAN and 3GPP networks. In comparison with the current approaches, the proposed method reduces the complexity of the system. Thirdly, the proposed method reuses the existing 3GPP procedures and messages to minimize the effort in developing the new WLAN access control scheme. Fourthly, the WLAN authentication and authorization are highly secured because the messages and information are exchanged over 3GPP radio links and through a 3GPP CN. Additionally, operators need not disclose their user information to the 3GPP AAA servers owned by the WLAN operators. Furthermore, the proposed method can be deployed over WLANs with or without the 802.1x infrastructure. The method eliminates the barrier to integrating WLAN and 3GPP networks without 802.1x APs.
References


Acknowledgment

The authors would like to thank the National Science Council, and Computer and Communications Laboratories (CCL), Industrial Technology Research Institute (ITRI), of the Republic of China, Taiwan for their financially supporting this research under Contract Numbers NSC 92-2218-E-011-005, NSC 93-2218-E-011-030, and ITRI T2-93039-5, respectively.
Biographies

Ray-Guang Cheng received the BS, MS, and Ph.D. degrees in communication engineering from National Chiao Tung University, Taiwan, in 1991, 1993, and 1996, respectively. From 1997 to 2000, he was with Advance Technology Center, CCL, ITRI as a researcher and a project leader. From 2000 to 2003, he joined BenQ Mobile System Inc. as a senior manager of R&D division. Since 2003, he joined the Department of Electronic Engineering, National Taiwan University of Science and Technology, Taiwan, as an assistant professor. His research interests include broadband multimedia communications and wireless networks. He received the Best Industrial-based Paper Award from Ministry of Education in 1998, the Research Achievement Awards of ITRI in 2000, and Advanced Technologies Award of Ministry of Economic Affairs of R.O.C. in 2001. He is a member of IEEE and Phi Tau Phi scholastic honor society.

Shiao-Li Tsao received B.S., M.S., and Ph.D degrees in engineering science from National Cheng Kung University, Taiwan, in 1995, 1996 and 1999 respectively. His research interests include mobile communication and wireless network, embedded software and system, and multimedia system. From 1996 to 1997, he was a research assistant of Institute of Information Science, Academia Sinica. He visited Bell Labs, Lucent technologies, NJ, USA, in the summer of 1998. From 1999 to 2003, Dr. Tsao joined CCL, ITRI as a researcher and a section manager. Dr. Tsao is currently an assistant professor of computer science and information engineering of National Chiao Tung University. Prof. Tsao has published more than 40 international journal and conference papers, and held or applied 10 US, 3 Germany, 11 R.O.C. patents. Prof. Tsao received the Research Achievement Awards of ITRI in 2000 and 2004, the Outstanding Project Award of Ministry of Economic Affairs (MOEA) of R.O.C. in 2003, the Advanced Technologies Award of MOEA of R.O.C. in 2003, and the Research Paper Award of ITRI in 2002. He is a member of IEEE and IEEE ComSoc.