# 3G and WLAN Interworking Security: Current Status and Key Issues

Chou-Chen Yang[1], Kuan-Hao Chu[2], and Ya-Wen Yang[2]
*(Corresponding author: Chou-Chan Yang)*

Department of Management Information Systems, National Chung Hsing University[1],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C. (Email: cc.yang@nchu.edu.tw)
Graduate Institute of Networking and Communication Engineeing, Chaoyang University of Technology[2],
168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.

*(Invited Paper)*

## Abstract

The third-generation (3G) mobile communication systems provide great coverage, complete subscriber management and nearly universal roaming. Nevertheless, 3G systems are subject to the low data rates (2Mbps highest for WCDMA). WLAN (Wireless Local Area Network) provides hot spot coverage with high data rates (reaches 54Mbps while 802.11 a/g), but is subject to short range (reaches 100m the furthest) and lacking a roaming and mobility support. From the users' point of view, the Integration of WLAN and 3G systems will provide a convenient and attractive way for the user to access network. The users are able to access 3G mobile network while at high speed travel or access WLAN while moving slowly or entering a specific area. However, while integrating WLAN and 3G, there are still some problems that should be considered in terms of authentication and security (such as billing, service continuity and authentication delay). In this article, we focus on the UMTS (Universal Mobile Telecommunications System). First, we review the interworking scenarios and architecture of 3G and WLAN. Then, we review the standardized authentication protocol for 3G/UMTS and WLAN interworking; moreover, we will review some papers related to the security issues and solutions on interworking between 3G/UMTS and WLAN. We also further make some comparisons to these schemes on their features and performance. Finally, we conclude some future works for the interworking between 3G/UMTS and WLAN.

*Keywords: 3G, authentication, interworking, WLAN*

## 1 Introduction

The 3G [2, 3, 7, 16] mobile communication system has a large coverage, high speed mobility, complete subscriber management (billing system) and nearly universal roaming. The data transmission rate in 3G mobile communication systems is from 144Kbps to 2Mbps. Although the data transmission rate of 3G mobile system is superior to 2G mobile system, it compares poorly with WLAN. WLAN provides only hot spot coverage with a high data rate (reaching 54Mbps for 802.11 a/g). However, it is obvious that the WLAN lacks global roaming and mobility support. Thus, the integration of the two diverse networks [38] can make up for each other's weakness, and bring the utmost benefits to subscribers, 3G service providers, and WISPs (Wireless Internet Service Providers). With the integration service, the subscribers are able to access 3G mobile network while at high speed travel or WLAN while the users are moving slowly or entering a specific area. Therefore, the integration of WLAN and 3G systems [44] can provide a convenient and attractive way for the user to access networks. And in turn, speed up the recruitment of new customers for 3G service providers and WISPs.

In this paper, we first review the interworking scenarios and architecture. The interworking scenarios are introduced in [3]. Each scenario has its features, capabilities and requirements. While the scenario changes from 1 to 6, the relationship of the two heterogeneous networks become more and more tight. Thus, it also needs more requirements and mechanisms. We also present the reference models for Scenarios 2 and 3 because Scenario 4 and upwards are still under investigation. After, the standard protocols will be reviewed in Section 3. The 3GPP (3rd Generation Partnership Project) TS 33.234 [5] specifies the 3G and WLAN interworking security [28]. The EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement) [4, 10] protocol is based on the existing UMTS AKA method which is chosen by 3GPP to achieve network access security. Other protocols, such as EAP-MD5, EAP-TLS and EAP-SIM, are also introduced in Section 3. In addition, we

made some comparisons between them. In Section 4, we will review some related works, current issues and its solutions. The subjects in Section 4 includes the existing authentication [31], billing and non-repudiation services [32] issues, service continuity, session hijacking, and fast re-authentication. We introduce these protocols with their features and also make some comparisons about the functionalities and performance between these proposed protocols. Some proposals provide new features to existing architecture such as billing mechanism and non-repudiation service. It is especially for someone who is trying to access the Internet with an un-trusted network. It can prevent over charging from a dishonest operator. Furthermore, we conclude this paper and introduce some future works in Section 5. We discuss the drawbacks of the above mentioned protocols and show the perspectives for interworking between 3G and WLAN. Although some proposals are very useful for securing interwork between 3G and WLAN, but some of them use public key algorithms to achieve their goal. This is not beneficial for mobile devices because the mobile devices always equip lower-level hardware and has the burden of very heavy costs. Another issue is to provide a seamless handoff. In order to reduce the authentication delay, a localized authentication must be provided. If there is not such a mechanism, the authentication traffic must return to the user's home network and thus resulting in a longer delay time.

# 2 3GPP-WLAN Interworking

## 2.1 Interworking Scenarios

The 3GPP also brings up six interworking scenarios [3]. The six scenarios give us a flexible, scalable, and general way of the 3G-WLAN interworking. We will introduce the six scenarios briefly.

- **Scenario 1 - Common Billing and Customer Care**
  In this scenario, common billing is required. The common billing means a user will receive only one bill from a 3G operator regardless of how many WLANs he/she visits. This scenario does not need any real interworking between 3G and WLAN networks.

- **Scenario 2 - 3GPP System Based Access Control and Charging**
  In this scenario, the 3G-WLAN interworking uses 3GPP based access control and charging mechanisms. That is, the 3GPP system provides the authentication, authorization and accounting mechanisms while a 3G subscriber requests WLAN network access. This scenario provides a more secure way for a 3G user to access WLAN.

- **Scenario 3 - Access to 3GPP System Packet Switch Based Services**
  Since WLANs support a higher data transmission rate and lower cost, it is reasonable for a 3G user to access 3GPP packet switch based services, such as Multimedia Message Service, from WLAN. This scenario starts a real interwork between 3G. PLMN and WLAN network. Thus, some new components or mechanisms must be put into a 3G core network to achieve the functionality.

- **Scenario 4 - Service Continuity**
  Service continuity means if a user initiates a packet switch based service in 3G network and then moves to a WLAN, the initiated session will survive, and vice versa. This scenario requires mobility management and handoff mechanism to support the functionality.

- **Scenario 5 - Seamless Services**
  The functionality of seamless services is similar to Scenario 4, but it requires the mobility to be smoothened. That is, minimizing the data lost and handoff delay.

- **Scenario 6 - Access to 3GPP Circuit Switch Based Services**
  The goal of this scenario is to allow a 3G user to access 3G circuit switch based services, e.g. voice calls, from a WLAN network. Further, seamless mobility and user-transparent while a user is switching between the two networks is required.

The summarization of 3GPP-WLAN interworking scenarios [3] is shown in Table 1. As the 3G and WLAN are integrated from Scenario 1 to 6, the interwork between them become more frequent and more tight. This also needs more and more requirements and mechanisms. For example, when the scenario changes from Scenario 2 to 3, it needs packet data gateway and WLAN access gateway to provide access control and data routing mechanisms.

## 2.2 Interworking Architecture

3GPP TS 23.234 [6] described the interworking architecture between 3G and WLAN. It proposed some components in order to achieve interworking such as Packet Data Gateway and WLAN Access Gateway. The reference model of interworking architecture can be found in [6]. The presented reference model was only achieved in Scenario 3 since Scenario 4 and upwards are still under investigation. 3GPP TS 33.234 [5] specified the 3G and WLAN interworking security. The security architecture of 3GPP-WLAN interworking is based on the existing UMTS AKA method. The authentication procedure requires a MS to access its UICC smart card to run the USIM application, which implies that the WLAN-UE (User Equipment) must be equipped with a UICC smart card. Obviously, the WLAN-UE may have a dual-mode (WLAN-Cellular) UEs or a local interface to communicate with UICC (e.g. Bluetooth, IR or serial cable interface). On the other hand, the interworking mechanism enables a 3G mobile network subscriber to access

Table 1: 3GPP-WLAN interworking scenarios and their capabilities

| | Scenario 1 | Scena. 2 | Scena. 3 | Scena. 4 | Scena. 5 | Scena. 6 |
|---|---|---|---|---|---|---|
| Common Billing | Y | Y | Y | Y | Y | Y |
| Common Customer Care | Y | Y | Y | Y | Y | Y |
| 3GPP System Based Access Control | | Y | Y | Y | Y | Y |
| 3GPP System Based Access Charging | | Y | Y | Y | Y | Y |
| Access to 3GPP PS Based Services | | | Y | Y | Y | Y |
| Service Continuity | | | | Y | Y | Y |
| Seamless Service Continuity | | | | | Y | Y |
| Access to 3GPP CS Based Services | | | | | | Y |

WLAN which is administrated by different WLAN operators. Therefore, the appropriate roaming agreements (RAs) are necessary to be maintained between the home 3G home operator and various visited WLANs. Furthermore, to execute the UMTS AKA from the 3G system's home domain toward the WLAN user equipment, the AAA [23] architecture and EAP [19] technologies are necessary. The AAA architecture and the RADIUS or Diameter protocol are to be used as the bridge between the 3GPP system and the WLAN access network. EAP is a general protocol for point-to-point protocol (PPP) authentication, which can support multiple authentication mechanisms. Consequently, EAP-AKA provides a way to exchange WLAN-UE AKA authentication messages and avoid link layer modification. The network elements of the 3GPP-WLAN interworking Reference Model are described as follows:

- **The Home Environment (HE)**: The HE includes the 3GPP home AAA Server, and the PDG.(Packet Data Gateway) The 3GPP home AAA Server located within the 3GPP network retrieves authentication information from the HLR/HSS of the 3GPP subscriber's home 3GPP network. It is also responsible for executing the AKA procedure toward the WLAN-UE. PDGW acts as a gateway while the UE accesses 3GPP packet data service through the WLAN.

- **The Serving Network (SN)**: 3GPP AAA proxy, Access point (AP) and WAG (WLAN access gateway) all belong to the SN. The AAA proxy represents a logical proxying functionality, namely, it relays the AAA information between WLAN and the 3GPP home AAA Server. The AP is a hardware device, which terminates the radio that is connected with UE, and acts as a communication hub for UE to connect with a wired LAN. When UE accesses the 3GPP packet data service through WLAN, the traffic is routed to WAG.

- **WLAN-UE**: The WLAN-UE, generally, is a laptop computer or PDA with WLAN card, and further equipped with a UICC/USIM smart card for accessing the WLAN interworking service.

The following Figure 1 is the 3GPP and WLAN interworking architecture for Scenarios 2 and 3 (roaming case). In Scenario 2, the authentication traffic is routed via the visited network to the 3GPP home network. As the user equipment associates to a WLAN AP, the AP sends EAP request to the user. After the user responds with required parameters to AP, this response will be forwarded to 3G AAA server. While authentication procedure is completed, the user's data traffic is authorized and is able to reach the Internet. 3GPP AAA server takes charge of access control. In Scenario 3, The UE is authenticated by the 3G AAA server in a way as described above. If a user wants to access 3G packet switch based service like MMS from WLAN, the user's data traffic is routed via the WAN Access Gateway to the Packet Data Gateway of 3G home network. The WAG is located in a visited network, like WLAN, in order to route legal packet to PDG. In other words, WAG acts as a firewall and contacts other networks. The PDG provides a secure entry from a public IP network to the 3G core network.

# 3 3GPP-WLAN Security Architecture

## 3.1 3G-WLAN Security Architecture Overview

As regards to the security of WLAN, The IEEE 802.11-1999 standards specify the Wired Equivalent Privacy (WEP) [27] for link layer security. However, due to the publication of the standard, WEP has been addressed as having many existing weaknesses. Therefore, WEP is considered as not being useful today. As WEP is known to be vulnerable, the new security protocol IEEE 802.11i [18] is developed to offer the highest level of privacy. The 802.11i specification includes both the RC4-based encryption Temporal Key Integrity Protocol (TKIP) and the AES (Advanced Encryption Standard) -based algorithm Counter Mode CBC-MAC Protocol (CCMP) for encryption and integrity protection, and 802.1X [17] for authentication and key distribution. The TKIP is an interim solution to adjust the known problem with WEP, which is

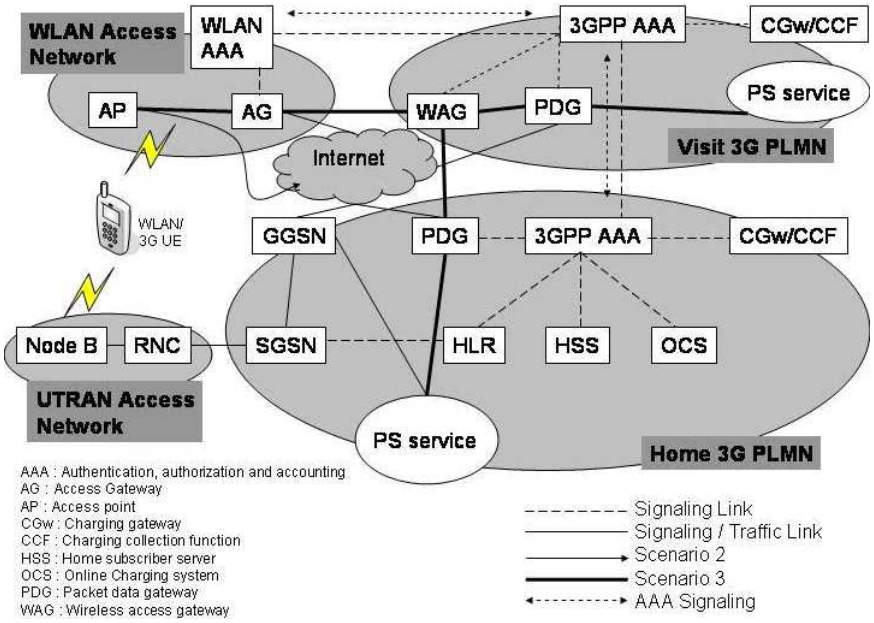


Figure 1: 3GPP and WLAN interworking reference model and network architecture

compatible with 802.11 products. Although TKIP is more secure than WEP, it is still not good enough compared with the AES solution. Consequently, the final standard of long-term solution for 802.11i is based on the Advanced Encryption Standard (AES). As mentioned above, the 802.11i Task Group (TGi) has decided to use IEEE 802.1X as the authentication framework. The 802.1X is a port-based network access control mechanism, which uses the Extensible Authentication Protocol (EAP) for end-to-end mutual authentication between a Mobile Station and an Authentication Server. In other words, the Access Point can filter the frames to/from non-authenticated stations. Before authentication is completed, only EAP-traffic is allowed to pass. Once the mobile station has successfully authenticated by the authentication server, the AP starts forwarding data packets to/from that station. The whole IEEE802.1X authentication mechanism includes EAP, EAP Over Lan (EAPOL), and Radius Protocol. EAP is a Point-to-Point protocol mainly used to provide extra authentication mechanism for remote logins. Based on different security requirements and users' requests, EAP provides different authentication mechanisms. The following are examples of EAP mechanisms.

EAP-SIM [15]: for GSM SIM-based authentication.

EAP-AKA [4, 10]: for UMTS USIM-based authentication.

EAP-TLS [22]: Base on SSL v3.0, for certificate-based authentication.

EAP-MD5 [13]: base on MD5-Challenge handshake authentication.

The EAP packet has four types (Request, Response, Success and Failure). Furthermore, IEEE802.1X defined a special frame format called EAP over LAN (EAPOL) to allow EAP message to be sent over the LAN before a higher layer protocol is employed. By using the EAPOL, an unauthenticated user can deliver an authentication packet to the AP for further authentication procedure. The EAP authentication takes place between the UE and the AS (Authentication Server) and is transparent to the AP. After the AP receives the EAP message, it will encapsulate the EAP message in an AAA protocol, such as in RADIUS or DIMETER, and forward to the AS. Once the authentication is successful, the AS will send a RADIUS/DIAMETER-Access Accept message to the AP. After AP makes the confirmation, it will then send EAP-Success message to the UE. As a result, the AP starts forwarding data to/from the UE.

### 3.2 The EAP-AKA Authentication Mechanism

In Figure 3, a basic successful full authentication exchange for EAP-AKA [4, 10] mechanism is given. Initially, a connection is established between the WLAN-UE and AP, and then the AP sends an EAP request/identity to the WLAN-UE. The WLAN-UE sends responses to either its IMSI, or a temporary identity (Pseudonym) complying with the Network Access Identifier (NAI) format [21]. The AP will forward the EAP message to the subscriber's 3GPP AAA-server based on the realm part of the NAI and the message may be routed by one or many AAA proxies. After obtaining the subscriber's identity, the 3GPP AAA-server checks whether there is an unused authentication vector (AV) available for that subscriber. If not, the 3GPP AAA-server will present the subscriber's IMSI to the HSS/HLR. According to the IMSI, the HSS/HLR can generate the AVs from the secret key K and send them to the 3GPP AAA-server. If the 3GPP AAA-server checks out that the subscriber's WLAN access profile is not available, the profile will be retrieved from HSS. After

the subscriber has been verified to be authorized to access WLAN service, the 3GPP AAA-server will store the AVs to fulfill the authentication mechanism. An ordered AV (RAND, AUTN, RES, CK, IK) based on SQN is selected, and the CK and IK will be used to derive the keying (critical/confidential) material. Several keys will be further generated from the keying material for different purposes, such as protecting EAP-AKA packets, link layer security, being a key of MAC [36] algorithm, or encrypting the pseudonym username or fast re-authentication identity. The 3GPP-AAA server then sends the RAND, AUTN, MAC, protected pseudonym, and next re-authentication ID to WLAN-UE. The RAND, AUTN and MAC values are used to provide replay protection. A keyed message authentication code (MAC) is calculated over the whole EAP packet with the key which is generated to form the keying material. Therefore, the integrity protection can be provided by the MAC as well. The pseudonym is used to protect user identity privacy and the re-authentication ID is used for re-authentication purposes. After obtaining the RAND, AUTN, MAC and the two user identities, the WLAN-UE runs the AKA algorithm on the USIM and verifies the AUTN and SQN. If these steps are successful, the WLAN-UE computes RES, IK and CK and uses IK and CK to derive the keying material to check the received MAC. If this passes through, the WLAN-UE computes a new MAC covering the whole EAP message with the new keying material, and sends the RES and MAC to 3GPP AAA-server to check the received MAC and compare the XRES with the received RES. If all these checks are passable, the 3GPP-AAA server sends the EAP-success message along with the keying material, which is generated for WLAN data layer security to the AP. The AP stores the keying material and sends EAP-success message to WLAN-UE. Finally, a mutual authentication is successfully fulfilled by the full EAP-AKA authentication exchange, and the WLAN-UE and the AP share the keying material for protecting user data confidentiality in the radio link.

### 3.3 The EAP-MD5 Authentication Mechanism

The EAP-MD5 [13] authenticates a user by a user name and a password. In EAP-MD5, a peer (WLAN-UE) and an EAP server must share a secret value, such as a password, and perform a MD5 operation as their hash function. After the above mentioned processes has been done, they can start an authentication procedure. First, peer establishes a connection with a WLAN-AP (wireless LAN access point), and the AP sends an EAP request/identity to the peer after. The peer responses its ID to the AP, and the AP relays this ID to an EAP server. While receiving this ID, the EAP server produces an EAP-Request/MD5-Challenge and responds to the peer. The peer then computes a hashed value which input includes an identifier, a shared secret, and a challenge value. The peer then sends it to the authentication server. The EAP server checks the legitimacy of this value. If it is a legitimate value, the WLAN can get the access right from the authorized resource. Contrarily, the peer can't access any resources because it has not been authenticated and authorized for any of them. The authentication procedure is shown in Figure 2. For simplification, we only show a peer and an EAP server in this figure. Because EAP-MD5 only authenticates the peer, it may suffer from the man-in-the-middle attack. Because of the challenge value and the identifiers are sent in plaintext, any one could obtain these values. So, the EAP-MD5 is also vulnerable to the dictionary attack.

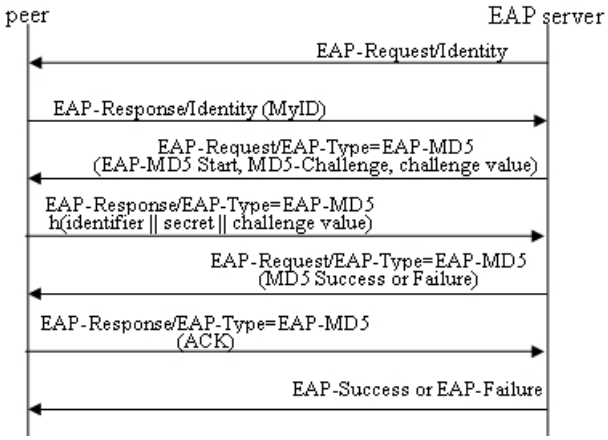


Figure 2: EAP-MD5 CHAP authentication

### 3.4 The EAP-TLS Authentication Mechanism

Many authentication mechanisms are only focused on how a server authenticates a client. That means these authentication mechanisms don't support mutual authentication and may suffer from the man-in-the-middle attack. Therefore, an authentication support mutual authentication is essential especially for commercial or sensitive behaviors. Transport Layer Security (TLS) provides some useful features such as mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two peers. EAP-TLS [22] also supports fragmentation, reassembly and session resumption. In the following, we'll describe how EAP-TLS work briefly. Initially, The EAP server and the peer (WLAN-UE) should send and receive each other's identity. After checking the identity, the EAP server sends a TLS Start, which is an EAP-Request packet excluding data, to the peer. The peer responds to this packet with TLS client_hello message which is an EAP-Response packet containing the client's TLS version number, a sessionId, a random number, and a set of ciphersuites supported by the peer. The EAP server then responds with an EAP-Request packet. This packet includes TLS Server_hello, TLS certificate, server_key_exchange, certificate request, and server_hello_done. The server_hello message contains the

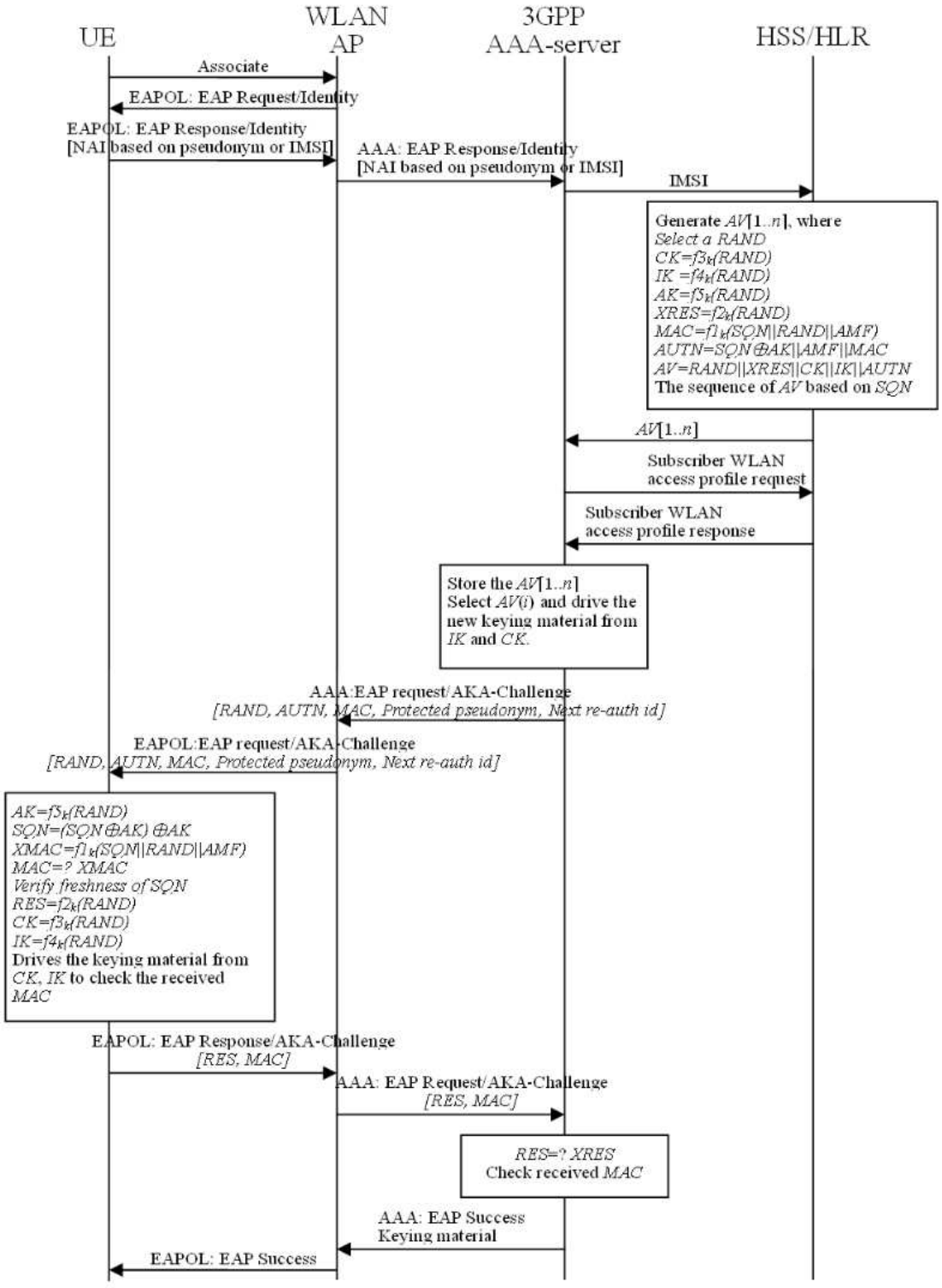


Figure 3: Authentication based on EAP AKA scheme

server's TLS version number, another random number, a sessionId, and a ciphersuite supported by the server. The peer sends an EAP-Response to the EAP server after it receives the request. If this is a new session, the EAP-Response contains a TLS change_cipher_spec, a TLS certificate, a client_key_exchange, a certificate_verify, and a TLS finished message. If this is a resumption of a previous session, the EAP-Response only contains a change_cipher_spec and a TLS finished message. While receiving the EAP-Response sent by a peer, the EAP server checks the validity of the peer's certificate and signature [35]. If the verification has passed, the peer can then access authorized resources right away. Otherwise, the peer can restart an authentication procedure. Since the peer and the EAP server know each other's certificate, mutual authentication can be provided. The detailed procedure is shown in Figure 4.

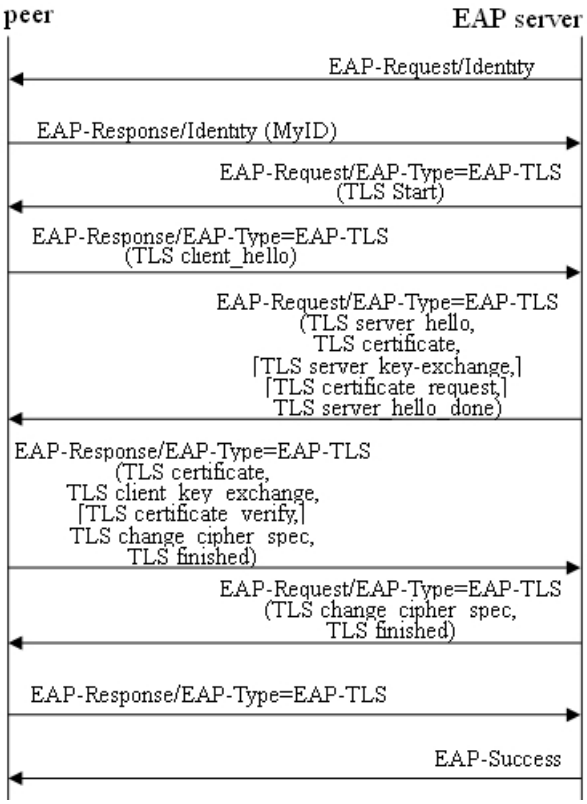


Figure 4: EAP-TLS authentication

### 3.5 The EAP-SIM Authentication Mechanism

For GSM users, SIM based authentication can't be changed. Furthermore, we can predict the combination of GSM and wireless LAN will be a new trend for a mobile device to get a reasonable service. Thus the EAP-Subscribe Identity Modules (EAP-SIM) [15] is developed for the existing unchanged GSM style authentication. We'll introduce the EAP-SIM authentication steps briefly.

At first, the authenticator sends an identity request to the peer to query who the peer is. While receiving the identity request, the peer responds with its identity. This identity may be an International Mobile Subscriber Identifier (IMSI) or a pre-negotiated pseudonym they have negotiated before. The authenticator checks the identity's validity and sends an EAP-Request/SIM/Start message to the peer. It also contains a list of EAP-SIM version in AT_VERSION_LIST which are supported by the authenticator. The peer responds to an EAP-Response/SIM/Start to the authenticator. The EAP-Response also contains a nonce value and a selected EAP-SIM version from the AT_VERSION_LIST sent by authenticator. After receiving the EAP-Response/SIM/Start, the EAP server connects to the AuC (Authentication Centre which belongs to the GSM network) to obtain GSM triplets. The GSM triplets contain RAND, SRES, and Kc. The uses of the triplets are a random challenge value, an expected response value computed with the secret key and the RAND, and a session key. Then, the EAP server sends EAP-Request/SIM/Challenge which contains RAND and a message authentication code. After receiving the EAP-Request/SIM/Challenge message, the peer performs a regular GSM algorithm and checks the validity of the received MAC. If the MAC which is computed by the peer matches the received one, the peer responds to EAP-Response/SIM/Challenge message, including SRES, to the EAP server. The EAP server then verifies the MAC's correctness. If the verification has passed, the EAP server sends the EAP-Success message to the peer. And the peer can access authorized resources. The detailed procedure is shown in Figure 5.

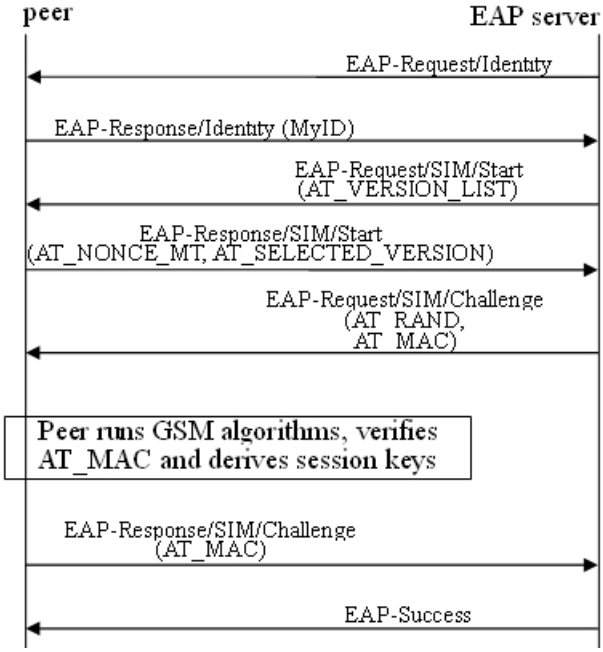


Figure 5: EAP-SIM authentication

### 3.6 Authentication Mechanisms Comparison

After we introduce the four standard protocols. We further compare them with their features in Table 2. EAP-MD5 is easy to implement but it is not secure enough. Since challenge value is not protected and the identity is a public value, it is vulnerable to dictionary attack. Further, because mutual authentication is not supported, it is possible to perform a Man-In-The-Middle attack on it. EAP-TLS offers a strong authentication protocol but it requires client certificates and much more computation costs. EAP-AKA also provides strong authentication, but some weakness of EAP-AKA will be discussed in the next section.

## 4 Current Issues

### 4.1 Authentication

The UMTS Authentication and Key Agreement (AKA) is discussed in some researches. One drawback of the UMTS AKA is that it needs several message rounds to complete its procedure. This may cause large authentication latency especially when interworking. Since the 3G core network is far away from the 802.11 WLAN network, the authentication latency will obviously increase. This is unfavorable especially for real time applications. Further, the EAP-AKA reveals user's identity to WLAN. Hence, the user's privacy can not be provided. Although the identity privacy problem can be solved by using a pseudonym, but a pseudonym can still be used to track a user's roaming tracks.

In [11], Cheng et al. mentioned the identity privacy problem in [9]. In addition, a WLAN station must pass through the WLAN access control procedure and perform a signaling procedure with 3G core network [41]. Hence, they proposed a scheme that a user performs authentication and authorization via 3G radio interface regardless of roaming or not. This scheme has several advantages. First, all of the authentication procedures are highly secured since all messages are exchanged through the 3G network. Further, a roaming user doesn't need to reveal his/her identity and protects the user privacy. Another research, Lin et al. [33] proposed a one-pass authentication procedure for 3GPP IP multimedia core network subsystem (IMS) in order to reduce the message round.

Tseng et al. [43] proposed an efficient authentication protocol which adopts the hash-chain technique. There are three components in their scheme, including the authentication server of 3G network (3G-AS), authentication server of WLAN (WLAN-AS), and mobile terminal (MT) which has dual interfaces to connection with UMTS or WLAN. When a MT reaches a WLAN AP, it sends the WLAN access request to the 3G-AS. Then, 3G-AS decrypts the message and computes a parameter for MT using hash-chain technique. MT sends the parameter to the WLAN-AS after it receives the parameter. WLAN-AS then uses the parameter to authenticate the MT. Their scheme can withstand the security weaknesses of WEP and authenticates a MT efficiently.

Since SSL/TLS provides stronger security, Gupta et al. [14] gives some experiments in implementation SSL with handheld devices. Further, AKA procedure can be implemented with SSL [29]. The integration between 3G and Public Key Infrastructure (PKI) [26] is also discussed in [1]. Thus, in [30], Kambourakis et al. proposed another solution to deal with the authentication problems for the WLAN-3G interworking by hiring SSL/TLS based technique. Their scheme is called EAP-TLS AKA. A MT and an AAA server authenticate each other using EAP-TLS through an access point supporting EAP-TLS. After authenticating each other, they change cipher specification and create session-keys respectively. The SSL/TLS based scheme benefits the end-to-end security by the nature of the asymmetric cryptography algorithm. As opposed to this solution, EAP-AKA provides hop-by-hop security.

While a 3G user wants to access a WLAN network, the authentication traffic always needs to return to the 3G core network through WLAN. This results in authentication delay especially the 3G core network is far from the WLAN. Thus, a localized authentication mechanism is needed to minimize the authentication delay.

We have introduced [39] in the above section. It provides a localized authentication protocol which is achieved by the use of a certificate. The main idea of this protocol is the use of a certificate. The certificate, includes the user's public key, which is signed by a 3G operator and can be authenticated by a WLAN operator to perform localized authentication. The certificate uses the public key cryptography. The adverse effect of using the public key cryptography is the computational overhead. It is not desirable for a mobile device burden with such an overhead as a mobile device is often equipped with a lower computing power and less memory space. In addition, this may also consume more battery power.

### 4.2 Billing and Non-repudiation Service

While 3G and WLANs are integrated, billing agreements or billing mechanisms must be provided. The billing mechanisms should support non-repudiation service. This is a very important issue especially when the 3G network and the WLAN network are administrated by different operators. If there's not such a mechanism provided, operators may deceive each other. Moreover, the two operators can collude with each other and over charge a victim. Therefore, Prasithsangaree et al. [39] proposed a dual signature scheme, called Localized Dual Signature Authentication, to achieve these requirements and it works in a loose coupling approach [8, 41]. Their scheme also provides localized authentication protocol which can reduce the latency from the message between two networks and provide user anonymity. In their protocol, the user anonymity is provided by using some identification not related to personal information. Although this

Table 2: Supported functionality of standard protocols

| | EAP-AKA | EAP-MD5 | EAP-TLS | EAP-SIM |
|---|---|---|---|---|
| Mutual Authentication | YES | NO | YES | YES |
| Key Derivation | YES | NO | YES | YES |
| Integrity Protection | YES | NO | YES | YES |

won't reveal personal information, the user's movements may be tracked. The localized authentication protocol is achieved by the use of the user's public key [40] certificate. Since the public key certificate can be authenticated by a WLAN operator, the user is authorized to access WLAN resources. Also, the user's public key is used for key exchange. The dual signature scheme is standardized in the Secure Electronic Transaction (SET) protocol [42]. The main idea of dual signature is that a WLAN operator is unable to know the roaming user's true identity, provide client anonymity, but can obtain a roaming user's usage information. A user which has a certificate signed by 3G operator's certificate authority. This certificate can be used to authenticate a user locally by a WLAN operator. The user signs a payment order message digest (POMD) which includes network usage and client information message digest (protected user ID) for the WLAN operator. WLAN can use POMD to collect money from the 3G operator.

Tseng et al. [44] also proposed an authentication and billing protocol which contains two kinds of techniques (i.e., password based protocol and public-key based protocol). In a password based protocol, after being authenticated by 3G-AS (3G authentication server), MT (mobile terminal) can send WLAN(Wireless Local Area Network) access request to 3G-AS. When 3G-AS receives the request, it computes a parameter which can be used to be authenticated by a WLAN operator and a billing procedure starts. Since non-repudiation can't be provided by this protocol, they further proposed a public-key based protocol. In public-key based protocol, 3G and WLAN service provider must register with a trust center (TC) which may be a government or other just organizations. The 3G operator also signs certificates for MT and WLAN operator respectively. While a MT needs WLAN services, it sends WLAN access request to 3G-AS. Then, 3G-AS and WLAN-AS (WLAN authentication server) authenticates each other by public-key based authentication and key agreement protocols. 3G-AS further delivers MT's identity and certificate to the WLAN-AS. Afterward WLAN-AS creates MT's identifiable record in its database. 3G-AS sends encrypted certificate belonging to WLAN-AS to the MT. After receiving that, MT can negotiate with the WLAN-AS and a session key is established in the EAP-TLS protocol. Recording WLAN's network usage related to a MT relies on a hash-chain technique. Therefore, the authentication and billing procedure is accomplished.

## 4.3 Service Continuity

Since the interworking Scenario 4 and upwards are still under investigation, there're some proposals for the service continuity issue. The most important issue is how to secure a transfer service from one network to another. Furthermore, if a user changes the access network after he/she initiates a service or a session in 3G or WLAN network, the service might be terminated. This is caused by various factors. For example, an enterprise employee may want to use Virtual Private Network technology in order to access his/her enterprise network. The VPN technique also protects the user's traffic between a user and his/her enterprise network. But the security association like IPsec or Virtual Private Network will be terminated and needs to renegotiate security parameters for a new security association due to the user's roams between networks and changes IP address. Further, VPN can result in a significant overhead, and the user may not need to secure all the traffic. In [12], proposed a Secure Universal Mobility (SUM) which can support seamless mobility, and the user doesn't need to maintain an always-on VPN association by introducing dynamic VPN establishment mechanism. The dynamic VPN is achieved by using double tunneled mobile IP (MIP) [25] which needs two home agents, an internal home agent and an external home agent. One tunnel is from the mobile user to the external home agent, the other one is from external home agent to internal home agent. While the two MIP tunnels are established, a corresponding node or a mobile user can initiate a communication by sending Session Initiation Protocol (SIP) [24] INVITE message and the receive side check if there is an existing VPN session. If there's no existing VPN session, they use Internet Key Exchange (IKE) [20] to negotiate security parameters and establish a new VPN session.

## 4.4 Session Hijacking

Since we are in the transition stage of 2G migrating to 3G, a mobile terminal may have the ability to access 2G and 3G network. In addition, a mobile terminal has dual interface to access 3G and WLAN network. Hijacking could be achieved no matter if a 3G user roams to WLAN [37] or a 3G user uses 2G network [34], it is a serious problem. The context transfer means a context of service(s) is transferred from a network to another and the service is continued in the new network. Interworking between UMTS and WLANs causes context transfer while a mobile user moves between the two networks. [37]

pointed out some drawbacks in the context transfer between UMTS and 802.11 WLAN, and pointed out that context transfer could be hijacked through the middle of a communication session since the 802.11 WLAN's security architecture is not robust enough. They further proposed an architecture to secure the context transfer by introducing the one time session key generation protocol (OTSKGP). OTSKGP is designed to create a secure context transfer between a mobile user and an access point in order to protect the traffic for a UMTS user roams to 802.11 WLAN. Although these situations are corrected in [34] and [37], similar circumstances are possible to appear again in different aspects. We shall pay close attention to this problem and avoid suffering from the session hijacking attack.

### 4.5 Fast Re-authentication

In certain situations, the full EAP-AKA authentication process has to be performed frequently. Whereas the full EAP-AKA authentication processes need to run the UMTS AKA algorithm, and retrieve fresh authentication vectors from the HSS/HLR, it will result in a high network load when being used frequently. Hence, an EAP-AKA fast re-authentication was developed to lighten the authentication process, which does not perform the UMTS AKA algorithm and does not need to retrieve the AV from the HSS/HLR. Fast re-authentication re-uses the keys which are derived from the previous full authentication. Only a new master session key used in the link layer protection has to be generated. Figure 6 depicts the exchange of the EAP-AKA fast re-authentication protocol. When the 3GPP AAA-server receives the re-authentication identity, it sends a counter, nonce, MAC and next re-authentication ID to WLANE-UE. Among the above mentioned values, the counter, nonce and next re-authentication ID are encrypted by the old key which is generated from the keying material derived from the previous full authentication. The counter can protect the subscriber and 3GPP AAA-server from reply attack and limit the number of successive re-authentication exchange without full authentication (The counter will be initialized to one in the full authentication). The fast re-authentication identities are one-time identities. If the WLAN-UE is not able to receive the new re-authentication identity, it shall be forced to initiate full authentication. The random nonce is generated by the 3GPP AAA-server, which works as the RAND in the UMTS AKA. The MAC in the WLAN-UE's response is calculated over nonce to provide challenge/ response authentication scheme. The MAC contains a message authentication code over the packet. After receiving the counter, nonce, MAC and next re-authentication ID, the WLAN-UE verifies if the MAC is correct and the counter value is greater than any previously used value. Then the WLAN-UE stores the next re-authentication ID for later use. If all checks prove to be correct, the WLAN responds to the message with the same counter values and the MAC which calculates over the nonce. If these checks are successful, the EAP success message is forwarded to the WLAN-UE. The fast re-authentication has been completely finished. The detailed procedure is shown in Figure 6.

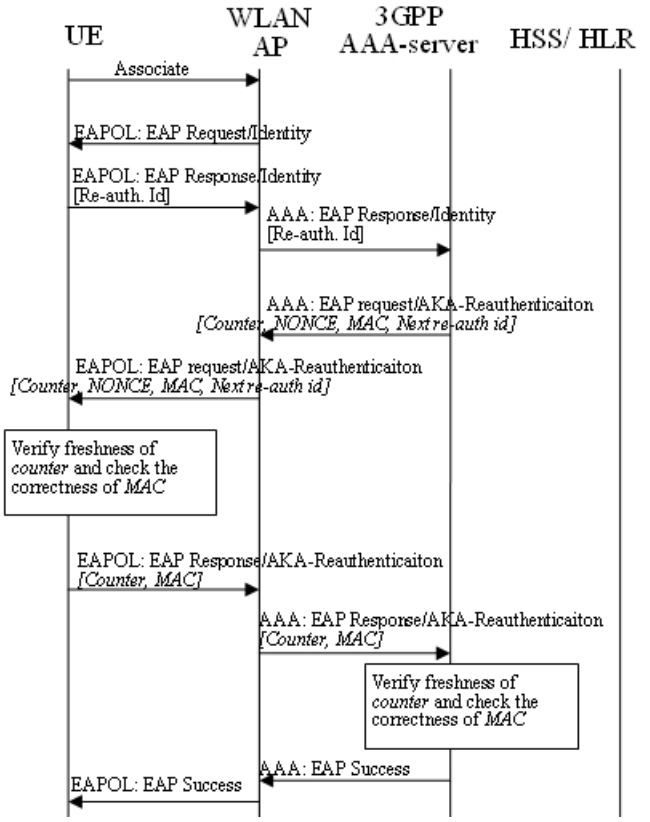


Figure 6: EAP-AKA fast re-authentication

### 4.6 Comparisons

Here we present the comparisons between the proposed authentication protocols with [11, 30, 39, 43, 44] their features are mentioned in Table 3. Mutual authentication between a mobile terminal and a wireless network is an important factor to security. Since mutual authentication and proper protocol are provided, session hijacking, man-in-the-middle attack, and masquerade are difficult to carry out. Localized authentication is required to provide lower authentication delay. This is very important for real time applications. Non-repudiation is provided with billing mechanisms to prevent over charging, colluded operators or a dishonest user. If public-key algorithms are introduced to a protocol, the computational overhead on both mobile terminal and authentication servers are increasing rapidly. This is more important for a mobile terminal because the mobile terminal often equips lower level hardware such as slower CPU, less memory and less storage. Identity privacy is also an important issue while interworking is provided. The user would like to keep his/her identity and actions in private. But without

protected identity it will reveal a great deal of information about a user. If a protected identity is changeless, an eavesdropper can still know the actions and roaming tracks of a user.

# 5 Conclusion and Future Works

We have shown the interworking architecture and scenarios. The functionalities of each scenario are also discussed. We also introduce standardized protocols and compare the provided functionalities of them. There are still weakness and limitations in these protocols. Some improvements or enhancements can be found in current issues. For example, billing mechanism is not supported in standardized protocols. Plus, non-repudiation should be provided in a billing mechanism. Thus, the improved protocol is proposed in [39]. Although these proposals improve the shortage of standardized protocol, there are still some drawbacks in these proposals. Hence, we discuss some future works in order to improve these protocols such as the reduction of the computational cost and the smooth transmission of a transferred service. The future works are discussed below.

- **Performance and Computational cost**
  It is always desirable to make an authentication protocol more efficient. First, the message round between two entities should be reduced and made acceptable. A duplicated process should be simplified to reduce cost. In [33], the one-pass authentication protocol is proposed to reduce the message round from a duplicated AKA protocol but the protocol missed the key agreement. We should provide a protocol that can reduce the message round in order to reduce authentication latency, network resource consumption, and doesn't miss the features provided by existing protocol. Then, a protocol should introduce algorithms with less cost. This is particularly important to a mobile environment since mobile devices usual equip low-level computational power, less memory and limited battery power.

- **Billing mechanism**
  Billing is an important issue especially when the integrated two networks belong to different operators. As mentioned in the previous section, [39] provides a billing mechanism which also achieves roaming user's privacy. However, this scheme introduced the public key algorithm, also known as asymmetric algorithm, to achieve their goal. The public key algorithm does cause high computational cost and is not suitable for mobile devices. Unfortunately, the devices that are used whilst mobile always have these characteristics. Therefore, we should make an effort on reducing the computational cost and make it suitable for mobile devices to give the users acceptable services. Further, the billing mechanism should provide the user non-repudiation in order to prevent an operator cheating another one or the victim will pay more money than was used.

- **Fast re-authenticationm**
  A fast re-authentication protocol can benefit real time applications particularly. If there is no fast re-authentication protocol provided, the user application, such as voice over IP or video communication, may result in obvious delay. The delay will increase as the distance between the 3G network and the WLAN network grows. Fortunately, the EAP-AKA provides a fast re-authentication mechanism. This mechanism, however, does not support billing mechanism, identity privacy and repudiation problem. It is desirable to combine these functionalities to a authentication protocol and even supports fast re-authentication.

- **Localized authentication**
  Localized authentication is introduced in [39]. If a localized authentication mechanism is not provided, whilst a user roams to a visit network, the existing sessions will suffer from long delays caused by the authentication procedure. The delay may become worse, when a home network is far from the visited network or even the home network is off-line. In a worst case, the session will be terminated and users will need to restart new sessions by themselves. Thus, the localized authentication is preferred due to the lower delay. Again, the public key algorithm is introduced in this protocol, and will result in another delay due to large computational cost.

- **Mobility Management**
  It is very important to provide secure handoff mechanisms. While a user changes his/her access network, ongoing sessions or services should be transferred smoothly in order to achieve service continuity. [12] is a pertinent example of seamless handoff. It uses make-before-break to achieve seamless mobility, it also uses dual tunneled mobile IP and dynamic establishes VPN tunnel to continue an existing VPN session. In this way, a user won't need to beak and re-establish a new VPN tunnel, and the VPN service is continued smoothly. Since the protocol introduced dual tunneled mobile IP, it needs two home agents. This costs more implementation and complicates the network topology. There are still some applications needed to treat the handoff smoothly, we need to create a generic solution for similar applications.

# Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC93-2213-E-005-033.

Table 3: Supported functionalities of proposed protocols

| | Mutual Authentication | Localized Authentication | Non-repudiation | Public-key Algorithm | Identity Privacy | Billing Mechanism Support |
|---|---|---|---|---|---|---|
| Chang et al. [15] | YES | NO | NO | NO | YES | NO |
| Tseng et al. [31] | NO | NO | NO | NO | NO | NO |
| Kambourakis et al. [22] | YES | NO | NO | YES | NO | NO |
| Prasithsangaree et al. [30] | YES | YES | YES | YES | YES | YES |
| Tseng et al. [32] | YES | NO | YES | YES | NO | YES |

# References


[1] 3GPP TSG, *Architecture Proposal to Support Subscriber Certificates, Discussion and Approval Document*, Technical Report, TDOC s2-022854, Oct. 2002.

[2] 3GPP TSG Core Network, *GPRS Tunneling Protocol (GTP) Across the GN and GP Interface*, Technical Report, 3G TS 29.060 v.6.6.0 (2004-09), Sept. 2004.

[3] 3GPP TSG Service and System Aspects, *Feasibility Study on 3GPP System to Wireless Local Area (WLAN) Interworking (release 6)*, Technical Report, 3G TS 22.934 v. 6.2.0 (2003-09), Sept. 2003.

[4] 3GPP TSG Services and System Aspects, *3G Security: Security Architecture (release 6)*, Technical Report, 3GPP TS 33.102 V6.3.0, Dec. 2004.

[5] 3GPP TSG Services and System Aspects, *3G Security: Wireless Local Area Network (WLAN) Interworking Security (release 6)*, Technical Report, 3GPP TS 33.234 V6.5.1, (2005-6), June 2005.

[6] 3GPP TSG Services and System Aspects, *3GPP System to Wireless Local Area Network (WLAN) Interworking: System Description (release 6)*, Technical Report, 3G TS 23.234 v. 6.5.0 (2005-06), June 2005.

[7] 3GPP TSG Services and System Aspects, *General Packet Radio Service (GPRS): Service Description*, Technical Report, 3G TS 23.060 v. 6.9.0 (2005-06), June 2005.

[8] K. Ahmavaara, H. Haverinen, and R. Pichna, "Interworking architecture between 3GPP and WLAN systems," IEEE Communications, vol. 41, no. 11, pp. 74–81, Nov. 2003.

[9] J. Ala-Laurila, J. Mikkonen, and J. Rinnemaa, "Wireless LAN access network architecture for mobile operators," IEEE Communications, vol. 39, no. 11, pp. 82–89, Nov. 2001.

[10] J. Arkko and H. Haverinen, *Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)*, Technical Report, draft-arkko-pppext-eap-aka-14, Nov. 2004.

[11] R. G. Cheng and S. L. Tsao, "3G-based access control for 3GPP-WLAN interworking," in *IEEE 59th Vehicular Technology Conference, VTC 2004-Spring*, vol. 5, pp. 2967–2971, May 2004.

[12] A. Dutta, T. Zhang, S. Madhani, K. Taniuchi, K. Fujimoto, Y. Katsube, Y. Ohba, and H. Schulzrinne, "Secure universal mobility for wireless Internet," in *Proceedings of the 2nd ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, pp. 71-80, Oct. 2004.

[13] P. Funk, *EAP MD5 Authentication*, Technical Report, draft-funk-eap-md5-tunneled-00.txt, Mar. 2003.

[14] V. Gupta and S. Gupta, "Experiments in wireless Internet security," in *Proc. IEEE Wireless Communications and Networking Conf. (WCNC)*, vol. 1, pp. 859–863, Mar. 2002.

[15] H. Haverinen and J. Salowey, *EAP-SIM Authentication*, Technical Report, draft-haverinen-pppext-eap-sim-15.txt, Nov. 2004.

[16] H. Holma and Eds. A. Toskala, *WCDMA for UMTS*, Wiley, 2000.

[17] IEEE, *IEEE Standard for Local an Metropolitan Area Networks-port-based Network Access Control*, Technical Report, IEEE STD 802.1X, July 2001.

[18] IEEE, *Draft Supplement to Standard for Telecommunications and Information Exchange between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security*, Technical Report, STD 802.11i/D7.0, Oct. 2003.

[19] IETF, *PPP Extensible Authentication Protocol (EAP)*, Technical Report, RFC 2284, Mar. 1998.

[20] IETF, *The Internet Key Exchange (IKE)*, Technical Report, RFC 2409, Nov. 1998.

[21] IETF, *The Network Access Identifier*, Technical Report, RFC 2486, Jan. 1999.

[22] IETF, *PPP EAP TLS Authentication Protocol*, Technical Report, RFC 2716, Oct. 1999.

[23] IETF, *Generic AAA Architecture*, Technical Report, RFC 2903, Aug. 2000.

[24] IETF, *Session Initiation Protocol*, Technical Report, RFC 3261, June 2002.

[25] IETF, *IP Mobility Support for IPV4*, Technical Report, RFC 3344, Aug. 2002.

[26] ISO/IEC, *Information Technology - Open Systems Interconnection - the Directory: Authentication*

*Framework*, Technical Report, ISO/IEC 9594-8 ITU-T Recommendation X.509, 1997.

[27] ISO/IEC, *Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications*, Technical Report, ISO/IEC 880211 ANSI/IEEE STD 802.11 (E) Part 11, 1999.

[28] G. M. Koien and T. Haslestad, "Security aspects of 3G-WLAN interworking," *IEEE Communications*, vol. 41, no. 11, pp. 82–88, Nov. 2003.

[29] G. Kormentzas, G. Kambourakis, A. Rouskas, and S. Gritzalis, "Using SSL in authentication and key agreement procedures of future mobile networks," in *Proceedings of the 4th International Conference on Mobile and Wireless Communication*, pp. 152–156, Sept. 2002.

[30] G. Kormentzas, G. Kambourakis, A. Rouskas, and S. Gritzalis, "Advanced SSL/TLS-based authentication for secure WLAN-3G interworking," *IEE Proceedings - Communicatios*, vol. 151, pp. 501–506, Oct. 2004.

[31] L. Lamport, "Password authentication with insecure communication," *Communication of ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[32] H. Y. Lin and L. Harn, "Authentication protocols with nonrepudiation services in personal communication systems," *IEEE Communications Letters*, vol. 3, no. 8, pp. 236–238, 1999.

[33] Y. B. Lin, M. F. Chang, M. T. Hsu, and L. Y. Wu, "One-pass GPRS and IMS authentication procedure for UMTS," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 1233–1239, June 2005.

[34] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS," in *Proceedings of the 2004 ACM Workshop on Wireless Security*, pp. 90–97, Oct. 2004.

[35] NIST, *Digital Signature Standard (DSS)*, Technical Report, FIPS PUB 186-1, Dec. 1998.

[36] NIST, *The Keyed-Hash Message Authentication Code (HMAC)*, Technical Report, FIPS PUB 198, Mar. 2002.

[37] Y. C. Ouyang and C. H. Chu, "A secure context transfer scheme for integration of UMTS and 802.11 WLANS," in *IEEE International Conference on Networking, Sensing and Control*, vol. 1, pp. 559–564, Mar. 2004.

[38] R. Pazhyannur A. Salkintzis, C. Fors, "WLAN-GPRS integration for next-generation mobile data networks," *IEEE Wireless Communications*, vol. 9, pp. 112–124, 2002.

[39] P. Prasithsangaree and P. Krishnamurthy, "A new authentication mechanism for loosely coupled 3G-WLAN integrated networks," in *IEEE 59th Vehicular Technology Conference, VTC 2004-Spring*, vol. 5, pp. 2998–3003, May 2004.

[40] R. L. Rivest, A. Shamir, L. Adlemsn, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 332–340, Feb. 1987.

[41] A. K. Salkintzis, "The EAP-GPRS protocol for tight integration of WLANS and 3G cellular networks," in *IEEE 58th VTC 2003-Fall,* vol. 3, pp. 1793–1797, Oct. 2003.

[42] SET, *Secure Electronic Transaction Specification, Book 1: Business Description, version 1.0*, Technical Report, May 1997.

[43] Y. M. Tseng, C. C. Yang, and J. H. Su, "An efficient authentication protocol for integration WLAN and cellular networks," in *Proceedings of the 6th International Conference on Advanced Communication Technology*, vol. 1, pp. 416–420, 2004.

[44] Y. M. Tseng, C. C. Yang, and J. H. Su, "Authentication and billing protocols for the integration of WLAN and 3G networks," *Wireless Personal Communications*, vol. 29, pp. 351–366, June 2004.

**Chou-Chen Yang** received his B.S. in Industrial Education from the National Kaohsiung Normal University, in 1980, and his M.S. in Electronic Technology from the Pittsburg State University, in 1986, and his Ph.D. in Computer Science from the University of North Texas, in 1994. From1994 to 2004, Dr. Yang was an associate professor in the Department of Computer Science and Information Engineering, Chaoyang University of Technology. Currently, he is a professor in the Department of Management Information Systems, National Chung Hshing University. His research interests include network security, mobile computing, and distributed system.

**Kuan-Hao Chu** was born in Chiayi, Taiwan, Republic of China, on October 20, 1981. He received the B.S. in Information Management from Ming Hsin University of Science and Technology, Hsinchu, Taiwan, in 2004. He is pursuing his M.S. in Networking and Communication Engineering from Chaoyang University of Technology. His current research interests include network security and mobile communications.

**Ya-Wen Yang** was born in Chiayi, Taiwan, Republic of China, on August 31, 1976. She received the B.S. in Information Management from Ming Hsin University of Science and Technology, Hsinchu, Taiwan, in 2003; the M.S. in the Graduate Institute of Networking and Communication Engineering from Chaoyang University of Technology, Taichung, Taiwan, in 2005. Her current research interests include wireless network authentication, network security and cryptography.