The ISC Int'l Journal of Information Security

July 2014, Volume 6, Number 2 (pp. 141–153)

http://www.isecure-journal.org

An Efficient Non-Repudiation Billing Protocol in Heterogeneous 3G-WLAN Networks

Ali Fanian [1,*], Fariba Alamifar [1], and Mehdi Berenjkoub [1]

[1] *Department of Electrical and Computer Engineering, Isfahan University of Technology (IUT), Isfahan, Iran*

ARTICLE INFO.

Article history:
Received: 14 January 2014
Revised: 11 July 2014
Accepted: 20 August 2014
Published Online: 25 August 2014

Keywords:
WLAN, Cellular Network, Heterogeneous Network, Authentication and Non-repudiation.

ABSTRACT

The wireless communication with delivering variety of services to users is growing rapidly in recent years. The third generation of cellular networks (3G), and local wireless networks (WLAN) are the two widely used technologies in wireless networks. 3G networks have the capability of covering a vast area; while, WLAN networks provide higher transmission rates with less coverage. Since the two networks have complementary properties, some attempts are made for their integration which could lead to an advantageous heterogeneous network. In such a heterogeneous network, provision of services like authentication, billing and quality of service are essential. In this article, a new mutual authentication protocol, namely, Non-Reputation Billing Protocol (NRBP) is proposed based on extensible authentication protocols. This authentication scheme provides a non-repudiation property for the billing problem. The proposed scheme is analyzed based on different security features and computation overhead. In comparison with previous approaches, this protocol contains all the considered security parameters. Moreover, the computation overhead of this protocol is less than other schemes.

© 2014 ISC. All rights reserved.

1 Introduction

The second generation of cellular networks provides global coverage and could fulfill the requirements of current user networks for voice channels. However, by the expansion of Internet usage, users like to connect to Internet through their mobile devices; hence, an increased tendency is applying the third generation of mobile networks. On the other hand, the wireless local area networks recently have been developed rapidly. The WLAN networks offer higher data rate in comparison with 3G networks, but cover smaller areas [1]. There are many public environments such as hospitals, shopping malls and universities covered with WLANs, so connecting to WLANs has become easy for mobile users, while the third-generation (3G) networks provide wider service areas and ubiquitous connectivity with low-speed data rate. In a sense, these two networks have complementary properties and integration of them is an important research area [2]. For integrating these two heterogeneous networks, several issues should be involved including quality of service, seamless handoff among WLAN and 3G, authentication and billing. In fact, integrating 3G and WLAN networks may offer subscribers high-speed wireless data services and ubiquitous connectivity. The first security requirement in integrating these two heterogeneous networks is authenticating users. After a successful authentication, the 3G mobile users can receive services

* Corresponding author.
Email addresses: a.fanian@cc.iut.ac.ir (A. Fanian), alamifar@ec.iut.ac.ir (F. Alamifar), brnjkb@cc.iut.ac.ir (M. Berenjkoub).

ISSN: 2008-2045 © 2014 ISC. All rights reserved.

from the WLANs. The second security requirement is the billing, where the data should be recorded in the accounting server of both the 3G's operator and the WLAN provider in such a manner, not only the users could repudiate their usage, but also the WLAN providers could not charge users more as well.

In this article, a mutual authentication protocol is proposed for 3G users who wish to authenticate themselves to the WLANs. This authentication scheme provides a non-repudiation property for the billing issue. In this protocol, the processing and power limitations of mobile devices are considered and the protocol is low cost. The remainder of this article is organized as follows: In Section 2, the heterogeneous network architectures and some authentication protocols are introduced. Then, the proposed protocol based on the extensible authentication protocol is introduced in Section 3. The performance analysis is presented in Section 4. Finally, some conclusions are given in Section 5.

2 Preliminary

The third-generation cellular networks and the WLANs have completely different properties; consequently, integration is a complicated and difficult task since they might have different service provider. Under these circumstances the authentication and the billing in the heterogeneous 3G, WLAN networks are important. It is necessary to have a flexible architecture for the integration of the two heterogeneous networks which could provide comprehensive services to users. In this section, first the architecture of the heterogeneous networks is introduced, and then the proposed authentication protocols for the 3G and the WLAN networks are briefly reviewed.

2.1 Heterogeneous Networks Architecture

The standardization efforts of the European Telecommunications Standards Institute (ETSI) and 802.11 work groups have introduced the two main architectures for the integration of the WLAN and the 3G networks [2, 3] namely the tightly coupled interworking and the loosely coupled interworking. As shown in Figure 1, there is an assumption in designing tightly coupled structure where the 3G and the WLAN networks depend on the same servers, that is the 3G provider design WLAN networks for their users. In the mentioned structure, since both the networks depend to the same provider, it cannot adapt the available WLAN networks. Therefore, this model is not scalable. In the loosely coupled structure, as shown in Figure 2, unlike tightly coupled structure, both may depend on different operators, that is, the two networks are connected to each other via the Internet network. This

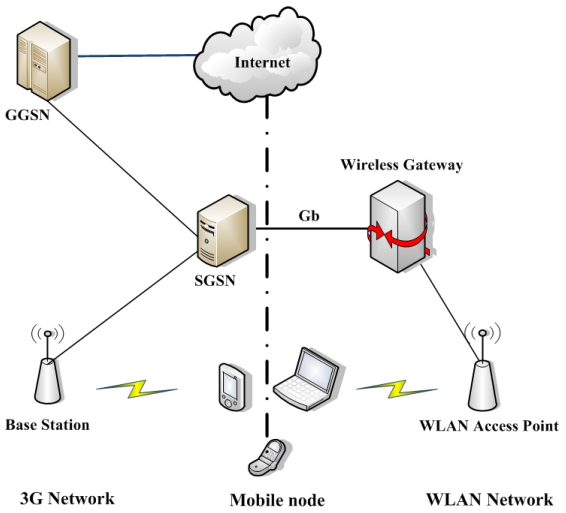

Figure 1. Tightly coupled structure in 3G and WLAN integrated network.

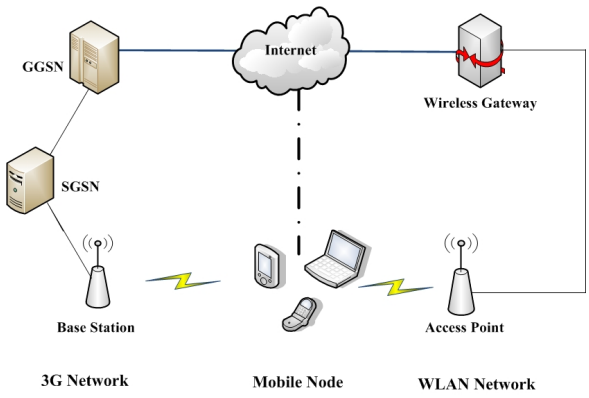

Figure 2. Loosely Coupled Architecture in 3G-WLAN integrated network

approach separates the data paths in the WLAN and the 3G networks completely. Moreover, the 802.11 data traffic is never injected into the 3G core network. Operators of 3G networks can benefit from other operators' WLAN deployments without extensive capital investments [3]. Since there is no limitation on the number of the 3G and WLAN networks that can connect to each other, the loosely coupled structure is more flexible and scalable in comparison to the tightly coupled structure. Furthermore, the 3GPP (Third Generation Partnership Project) standardization [4] has confirmed the loosely coupled structure for the integration of 3G and WLAN networks.

2.2 Related Work

To integrate the 3G and WLAN networks, many approach of works have been proposed such as European Telecommunication Standard Institute (ESTI) in 3rd Generation Partnership Project (3GPP) [4]. In the 3GPP project, there is a complete description of 3G-WLAN integrated systems, where the architecture of

integrated networks, authentication and billing issues are discussed. In the last recorded studies on 3GPP, the 3G and WLAN providers first sign a roaming agreement for their users and then in the next step, an AAA (Authentication-Authorization-Accounting [5]) server is installed in 3G Home network and AAA proxies are installed in visited networks [4]. Eventually, all the integrated networks connect to the Internet via the operator's IP network. The 3GPP applies the EAP-AKA protocol for the authentication of users.

An authentication scheme has been presented in [3] based on Single Sign On (SSO), where an end user is able to roam between different administrative domains and access network technologies. This solution integrates some authentication methods and does not require any end-user interactions while roaming. Here, the end user should install a Smart Client on his/her device, which provides an interface for different authentication methods and hides all different authentication mechanism details from application and end users views.

In the related literature, different authentication methods have been proposed based on Extensible Authentication Protocol (EAP) [6, 7] for the integration of 3G and WLAN networks. EAP protocol provides a sub-structure for authentication of users to networks which lack IP layer in their architecture. This authentication protocol was practically expanded to be applied on top of PPP protocol, while in due time it was being implemented on wired networks like IEEE 802.3, wireless networks like IEEE 802.11i, IEEE 802.16e, and Cellular networks like GSM, UMTS and IKEv2. This protocol operates on the data link layer. There are several protocols based on the EAP protocol that include the EAP-AKA [8, 27], the EAP-TLS, and the EAP-TTLS [10] but each protocol have some problems that are mentioned in the latter.

The EAP-AKA scheme [8] is based on a symmetric key agreement between user and cellular network. Since, a great number of messages must be transmitted among the nodes, this protocol endures latency. The EAP-AKA is an authentication protocol based on EAP framework which encapsulates the AKA protocol. To integrate the EAP-AKA protocol in the loosely coupled architecture, the Cellular Authentication Gateway should host the AAA server for handling the client authentication requests from WLAN operators to 3G [24]. The EAP-AKA is compliant with the 3GPP security standard. In this protocol, although WLAN traffic directly goes to the Internet by avoiding the overhead in the tightly coupled approach, there exist some shortcomings as far as the authentication process is concerned. First, the authentication request has to be sent from the WLAN to the 3G-AAA server and then sent from it to the Home Location Register (HLR). The HLR will generate a challenge that needs to be sent through the 3G-AAA server to the AP from where it reaches the MS. In a similar manner, the response generated by the MS to the challenge has to make its way to the HLR. This method has some drawbacks of its own: if the MSs make handoffs to different WLANs on constant bases, this process could become a bottleneck. Second, the networks' side is never authenticated. Third, the MS identity is sent to the network without any protection [9].

The EAP-TLS protocol [10] is based on public key cryptography (PKC), in which no central server is required like the HLR that shares a secret key with the MS, hence this protocol is scalable. But, the EAP-TLS requires intensive computation with PKC. One major drawback of the EAP-TLS is that an MS needs to possess a public key certificate when the AP needs to authenticate the MS. Most of the MSs are not equipped with a digital certificate. Then the modified EAP-TTLS (Tunneled TLS) [10] and PEAP (Protected EAP) [11] that are similar to EAP-TLS have been developed. In these two protocols the client does not need to have digital certificate. There are two phases in these protocols: in the first phase, the server certificate is used for authenticating the server and exchanging security parameters for making a secure tunnel. Then the authentication traffic passes from this channel, hence, the user identity can be protected. In the second phase, user authentication, and session key agreement are done [10].

In [12], a protocol named local fast re-authentication (LFR) is proposed to enhance the EAP-AKA protocol. The objective of this protocol is to replace the re-authentication protocols in the EAP-AKA protocol with the localized protocol, known as, local fast re-authentication (LFR) protocol. This Protocol performs re-authentication locally within the WLAN domain instead of communicating with the 3G Home Network (3GHN). Hence the re-authentication is performed locally, and it reduces delays during re-authentication process.

In [9], a local authentication scheme, called LDSA, is proposed which does not need to directly communicate to HLR. LDSA is based on a dual signature scheme and can be implemented on a loosely coupled structure. To produce a dual signature (DS), the client identity (CI), and the usage information (UI) of the MS negotiated with WLAN are hashed to produce a client information message digest (CIMD) and usage information messages digest (UIMD). The CIMD and UIMD are concatenated and hashed again to produce the payment order message digest (POMD), and it is finally signed by the client's private key. The re-

sult is a Dual signature. The DS is concatenated with the CI and UIMD, and the result is encrypted. The encrypted part is encrypted to the 3G operator by using a digital envelope (DE). The DE is encrypted with a cipher such as AES with the shared secret key between the user and the 3G operator. The EP and DE are obtained by the WLAN operator and subsequently given to the designated 3G operator. The EP and the DE are used as an approval of the MS's usage for a payment from the 3G operator.

In [13], Tseng has proposed two authentication protocols for the integration of heterogeneous 3G-WLAN networks. One protocol utilizes a one-time password approach, and the other is constructed on a public-key-based system (i.e., certificates). One time-password protocol utilizes hash functions and symmetric cryptography to authenticate users but this protocol could not offer the non-repudiation property for the billing problem. Public-key-based protocol consists of two phases: in the first, the issued certificates from the Trusted Center and 3G operator communicate between components, and in the second, the mobile and WLAN authentication is done with the exchanged certificates in phase 1, and EAP-TLS protocol. Then mobile produces a random number and computes hash-chain values, signs this chain with its private key and sends it to WLAN, where, the non-repudiation property is provided while it requires more computation times.

Some of the proposed authentication protocols for the integration of heterogeneous 3G-WLAN networks operate based on estimating the next user region like [16] and [17]. In these protocols, in order to reduce the authentication time of moving users, the next region of user will be estimated through place-estimating algorithms and then user information is forwarded to that region. These protocols reduce the authentication time noticeably. For example, in the proposed protocol [18], some sensor nodes named as region server are broadcasted in the network area. Each mobile device communicates with the sensor nodes continuously and thus sensor nodes can estimate next user region. After estimating the next region, user authentication information is forwarded to that region and the authentication time is reduced. However, this method is costly and needs some lateral equipment.

In [19], Tseng proposed a protocol based on EAP-TLS, named as EAP-UTLS. In this protocol, the problem of sending mobile identity in a clear way is eliminated. Although, EAP-TTLS and PEAP protocols [10, 11] are developed to provide the MT identity protection, both are vulnerable against a Man-in-the-Middle attack [19]. In EAP-TTLS and PEAP protocols, a user cannot roam between WLAN and Cellular Networks. In EAP-UTLS, the symmetric-key based certificate distribution scheme combines with the EAP-TLS protocol to present a new USIM-based EAP-TLS protocol. This new EAP protocol provides mutual authentication, strong identity protection, and roaming capability between the cellular network and the WLAN networks.

In [23], two pre-authentication protocols in the UMTS-WLAN interworking architectures are proposed. These pre-authentication protocols contribute in reducing authentication delays during WLAN Horizontal Handover in UMTS-WLAN interworking architecture. The pre-authentication protocols authenticate the mobile user locally before handover takes place which results in a reduction in the handover delay. The proposed protocol is an enhanced version of EAP-AKA authentication protocol.

3 The Proposed Authentication and Non-Repudiation Billing Protocol

As mentioned before, the proposed protocol, NRBP, is an authentication and non-repudiation billing protocol, based on extensible authentication protocol for the heterogeneous 3G-WLAN network. The heterogeneous structure which will be utilized in this work is based on the loosely coupled heterogeneous structure presented in the 3GPP standardization [4, 28, 29] where an authentication center (AAA server) is added. As explained in Section 2.1, using the loosely coupled structure has several advantages, like imposing less change in the network's components. Therefore, in the NRBP protocol, the loosely coupled architecture in 3G-WLAN is applied.

The heterogeneous network structure used in this article is shown in Figure 3. The overview of the NRBP authentication protocol is as follows. When the mobile device enters a new region covered by a WLAN,

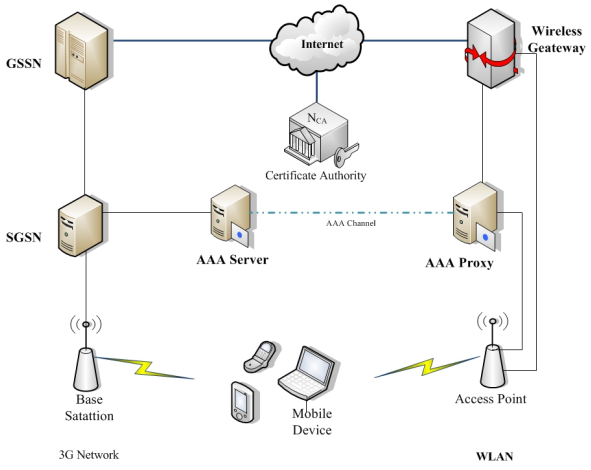

Figure 3. The heterogeneous network in NRBP protocol

it may choose to connect to WLAN and benefit from its services, and if so, the mobile device has to do the authentication process. Since, the mobile device is not registered in the WLAN, at first, it needs to contact to the AAA 3G server to request a WLAN ticket. The mobile has a shared key, called KeyU, with the AAA sever generated during the 3G authentication process. Equipped with this authentication ticket, the mobile device is able to connect itself to WLAN and utilize its services. Furthermore, as illustrated in Figure 3, in the NRBP protocol, an AAA server is added to the 3G network. The duty of this server is to provide public key authentication of the existing servers to the foreign servers. If some unauthenticated public keys are accessible, then the man-in-the-middle attack may occur. The authentication server can either be online such that it authenticates a server's public key upon receiving a request, or it can use the public key infrastructure to sign all servers' pubic keys and store them in a secured database. The NRBP conducts the authentication process in two phases. In the first phase, when mobile enters to a new WLAN network, it contacts to the AAA server to receive an authentication ticket. Also, in this phase, WLAN authentication server (AAA proxy server) receives some security parameter for subsequent authentications. The first phase is accomplished when mobile enters to a new WLAN or its authentication parameter is finished. In the second phase, the mobile and the WLAN network can authenticate each other, and then the mobile can use the network. This phase will be performed many times until the mobile's authentication parameters is finished. Authentication and billing services can be accomplished in this phase. The details of these phases are introduced in the next section.

The notation used in the proposed protocol is given in Table 1.

Table 1. Notation

Symbol	Description
ID_{WL}	WLAN identification number
ID_{3G}	3G network identifier
$EAPOL\text{-}START$	EAP Over LAN start (EAP message)
$EAP\text{-}Request\ ID$	EAP-Request-Identity (EAP message)
NAI	Identifier of mobile and its 3G network (Network Access Identifier)
r	Mobile random Number
r_s	3G Auc. random number
R_{WL}	WLAN Auc. Random number
$KeyU$	Pre-shared key between mobile and 3G network in order to authenticate the mobile
$DKey_{WL}$	Private Diffie-Hellman of WLAN AAA proxy server
$BlindKeyWL$	Blind Diffie-Hellman private key of WLAN authentication server ($g^{DKey_{WL}} \ mod\ p$)
$DKey_{3G}$	Private Diffie-Hellman of 3G AAA server
$DiHe_{Key}$	Diffie-Hellman key between AAA and AAA proxy servers
$ChainPar$	First value of a hash chain
$PrivKey_{3G}/PubKey_{3G}$	3G Private/Public keys
$Ticket_U$	Mobile ticket used for mobile authentication to the AAA proxy server
Ack_U	Mobile authentication parameter to AAA server
$Auth_U E$	Mobile authentication parameter to AAA proxy server
$Auth_W L$	WLAN authentication parameter to mobile user
N_u	Mobile nonce
$SKey$	Session key between mobile user and WLAN network
PMK	Master key in IEEE 802.11 protocol

3.1 Phase I: Authentication Ticket Request

Each access point broadcasts some information including the access point Service Set IDentifier (SSID). When a user enters a WLAN region, the mobile will recognize the new region by receiving this information. In the NRBP protocol, SSID or the WLAN identification number is shown by IDWL. If the user decides to connect to the WLAN, it first contacts the AAA server to receive an authentication ticket. The first phase of NRBP protocol is presented in Figure 4. As shown in Figure 4, first, the mobile sends an EAPOL-Start message to access point as a join request, and then the access point asks for the user identity by sending an EAP-Request-Identity message to the mobile. Once the mobile receives this message, it generates a random number r, and encrypts it together with the SSID derived from the access point's broadcast information, using the shared key among the user and its home 3G network (1).

$$\{ID_{WL}, r\}_{KeyU} \tag{1}$$

Now the mobile sends the encrypted message together with the network identifier (NAI) [20] to the access point in a message named EAP-Response/Identity (NAI). The user and network identifier is presented in equation (2).

$$NAI = TMSI@VLR_{ID}.3G_{Server} \tag{2}$$

Using the NAI, the user determines its authentication server's domain together with its identity in the do-

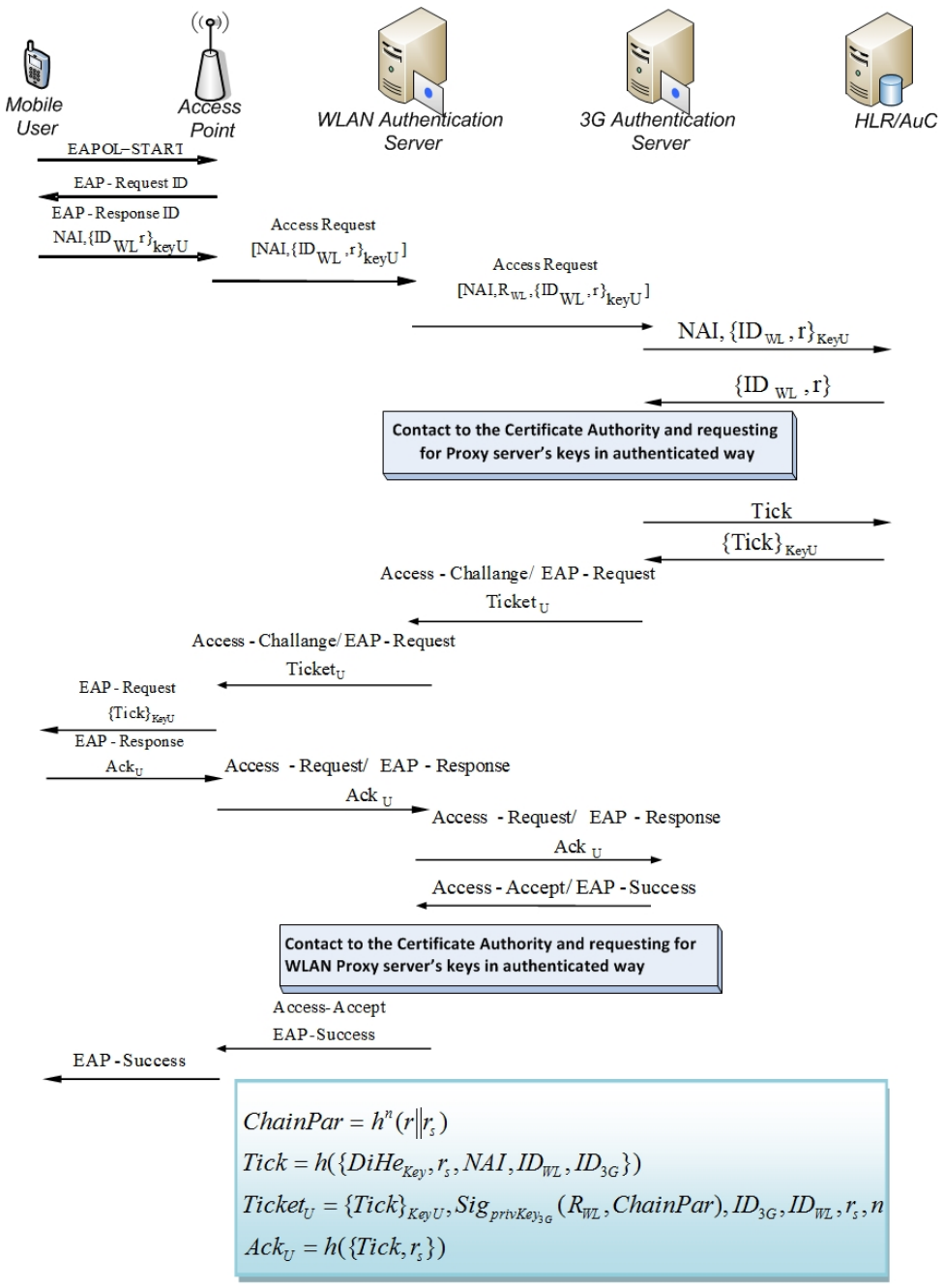

Figure 4. The first phase in NRBP protocol

main. Consequents, when the AAA proxy server (the authentication server in WLAN) receives the user's NAI, it will know to which server the message should be forwarded. The access point puts the message into an AAA message (Access Request message) and sends it to the AAA proxy server. The server adds a random number (RWL) to the data and sends them to the corresponding Visitor Location Register (VLR). The VLR uses the received TMSI to get the mobile's identity (IMSI) and sends it to the 3G AAA server. Since, the generated NAI will be used in phase 2 for many times, it should be saved in mobile.

The AAA server sends this information to the authentication unit of the cellular network (AuC). The AuC authenticates the user using its IMSI and extracts its KeyU from the database. Then, it decrypt the user's message with KeyU and sends the decrypted message ($\{ID_{WL}, r\}$) to the AAA server. Indeed, there should always be a secured communication channel between AuC and AAA server. At this point, the AAA server retrieves the WLAN public and blind Diffie-Hellman private key from the trust center in an authenticated message. The AAA server gets access to the blind private key of the AAA proxy server, BlindKeyWL,

and calculates the Diffie-Hellman shared key according to (3). Also, the AAA proxy server can compute this Diffie-Hellman key when the verification of the authenticity of the AAA server becomes necessary.

$$\begin{aligned} DiHe_{Key} &= BlindKey_{WL}^{DKey_{3G}} mod\ p \\ &= (g^{DKey_{WL}} mod\ p)^{DKey_{3G}} mod\ p \\ &= g^{DKey_{WL} \times DKey_{3G}} mod\ p \\ where\ \ DKey_{3G} &\in \{0, 1, \ldots, p-2\} \end{aligned} \tag{3}$$

The AAA server, upon receiving the mobile's random number (r), will generate its own random number (r_s). Then, it performs one way hash function on ($r||r_s$) for n times to achieve chain's 1st parameter according to (4). This authentication chain will be used in phase 2 for authenticating user to the WLAN.

$$ChainPar = h^n(r||r_s) \tag{4}$$

Then, the 3G authentication server will sign the produced authentication chain along with the produced random number (R_{WL} by its private key ($PrivKey_{3G}$), and public key as follows:

$$Sig_{Privkey_{3G}}(R_{WL}, ChainPar)$$

This signed value is used for proving the freshness of the message to the AAA proxy server. The 3G authentication server will calculate the user ticket by performing one way hash function on user identification (NAI), WLAN ID, r_s, 3G identification, and $DiHe_{Key}$ according to (5).

$$Tick = h(DiHe_{Key}, r_s, NAI, ID_{WL}, ID_{3G}) \tag{5}$$

The authentication server will send this ticket securely to the HLR/AuC. The HLR/AuC will encrypt the ticket with KeyU, and then will send it to the 3G authentication server again, and then will send it to the 3G authentication server again. The 3G authentication server will send the encrypted value along with 3G ID, WLAN ID and r_s inside a message called as EAP-Request. Then, it will encapsulate this message to Access Challenge message, AAA message protocol, and will send it to the proxy server. The value of $Ticket_U$ message is presented in (6).

$$\begin{aligned} Ticket_U = \{&\{Tick\}_{KeyU}, \\ &Sig_{Privkey_{3G}}(R_{WL}, ChainPar), ID_{3G}, ID_{WL}, r_s, n\} \end{aligned} \tag{6}$$

The AAA proxy server will save some information of $Ticket_U$ and will send $\{Tick\}_{KeyU}, r_s$ to the user. The saved parameters in AAA proxy server will be used for obtaining security parameters at the end of phase 1 of the protocol when the user is already authenticated by the AAA server. The saved parameters by the proxy server are as follows:

$$Sig_{Privkey_{3G}}(R_{WL}, ChainPar), ID_{3G}, r_s, NAI$$

The user will obtain the $Tick$ value by decrypting the $\{Tick\}_{KeyU}$. Then, to authenticate itself to the AAA server, it will generate Ack_U according to (7), and send it to the AAA server.

$$Ack_U = h(Tick, r_s) \tag{7}$$

This value, under EAP protocol will be enclosed in EAP-Response message, then under the AAA protocol it will be enclosed in Access-Request message.

Upon receiving Ack_U, the AAA server can validate the received value by calculating it again. If two values are similar, the server will send the EAP-Success to the user. At this stage, the proxy server realizes that the user is authenticated by the AAA server, therefore, the previous exchanged parameters and saved data are true. The AAA proxy server can generate or restore required security parameters including: the public key of the 3G AAA sever ($PubKey_{3G}$), the blind Diffie-Hellman private key of the AAA server ($BlindKey_{3G}$), and decrypt 3G signature on $R_{WL}, ChainPar$ by public key of the AAA server. Having the R_{WL} (the Random number generated in proxy server), the correctness of the received message will be validated. As a result, the proxy server will accept the value of the presented in (4) as the seed of mobile authentication chain. Now, according to (8), the proxy server can reproduce the common Diffie-Hellman key using 3G blind key, and its private Diffie-Hellman key.

$$DiHe_{Key} = BlindKey_{3G}^{Dkey_{WL}}\ mod\ p \tag{8}$$

After these operations, the WLAN authentication server is able to calculate the $Tick'$ using the received parameters, and the produced parameters by itself according to (9). Then, it saves $Tick'$ and $ChainPar$ as security parameters in a table, corresponding to the user NAI, to be used in phase 2.

$$Tick' = h(DiHe_{Key}, r_s, NAI, ID_{WL}, ID_{3G}) \tag{9}$$

Finally, the proxy server sends *EAP-Success* message to the access point and from there, it will be forwarded to the user terminal.

Up to this point, the user is not able to use network resources, since no common key is agreed between the user and the access point. Consequently, the second phase of the authentication protocol should be processed. After this phase, the user will receive an IP address and it would be able to connect to Internet via the access point.

3.2 Phase II: User Authentication to the WLAN Network

The first phase of the NRBP authentication protocol is only performed once. Then, the user can authenticate himself to the WLAN for n times using the obtained ticket from the first phase. To this end the user exchanges the following messages with the authentica-

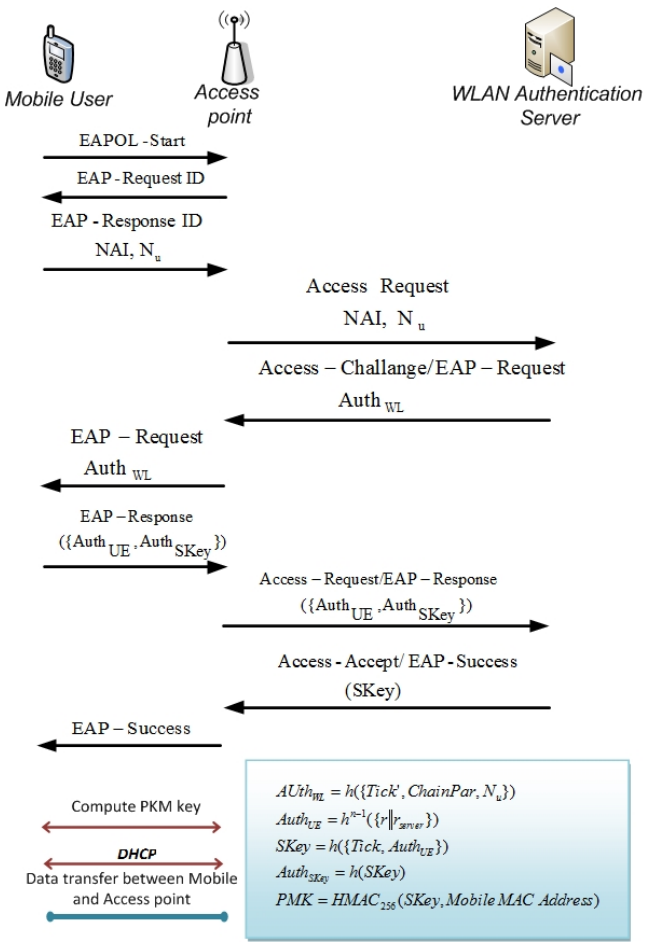

Figure 5. The Second Phase Steps of NRBP Authentication Protocol.

tion server in WLAN. The Figure 5 illustrates how the authentication messages are exchanged in Phase II.

In the first message, the user will announce his presence in the network by sending an EAPOL-Start message to the access point. In the second message, the access point will request the user's NAI. To respond to this request, the user sends its NAI together with N_u to the access point and then it will be forwarded to the proxy server from there. Receiving the user NAI, WLAN authentication server will restore the information obtained from the first phase and then, to authenticate itself to the user, it will generate $Auth_{WL}$ according to (10).

$$Auth_{WL} = h(Tick', ChainPar, N_u) \qquad (10)$$

where, N_u is the user's nonce which is used by the proxy server to prove the message freshness. The proxy server will send the $Auth_{WL}$ by the EAP-Request message to the user. Then, the user will calculate the $Auth'_{WL}$ according to (10), and compares it with the received $Auth_{WL}$ from the AAA proxy server. The AAA proxy is authenticated to the user if the two values are similar. The user, in order to authenticate itself to the proxy server, needs to have the previous parameter of the one way hash value of the chain. This parameter is called $Auth_{UE}$ and is calculated according to (11).

$$Auth_{UE} = h^{n-1}(r||r_s) \qquad (11)$$

For this purpose, the session key, $SKey$, can be drawn by (12).

$$SKey = h(Tick, h^{n-1}(r||r_s)) = h(Tick, Auth_{UE}) \qquad (12)$$

The user needs to demonstrate to the proxy server that it has a valid session key. Therefore, it calculates the one-way function of the produced session key and sends the result together with the authentication parameter, $Auth_{UE}$, to the proxy server in an EAP-Response message as shown as follows:

$$Auth_{SKey} = h(SKey)$$
$$Mobile \rightarrow ProxyServer.\{Auth_{UE}, Auth_{SKey}\}$$

The proxy server can easily calculate the one-way function of the received $Auth_{UE}$ and check if it is equal to $ChainPar = h^n(r||r_s)$.

In this case, the proxy server can validate the user's authentication, and stores the $h^{n-1}(r||r_s)$ as new ChainPar for the next authentication. On the other hand, the proxy after producing the SKey, can confirm that the user owns a valid key by examining the AuthSKey.

If the proxy server can successfully authenticate the user, an EAP-Success message is sent to the user. However, in order to encrypt the message to be securely communicated over the wireless channel, the access point should possess the produced session key. Therefore, the proxy server sends the session key to the access point, as well. According to (13), the access point is able to produce the PMK [14] (both mobile user and access point derive a symmetric key called PMK from master key in 802.11 protocol) using the one-way HMAC function (13), where the user and the access point can be authenticated with each other. Then, an IP address is allocated to the user using the DHCP protocol. From now on, the user can begin using the network resources.

$$PMK = HMAC_{256}(SKey, Mobile\ MAC\ Address) \qquad (13)$$

In the next stages of the authentication process, the user uses the next parameter in the one-way hash chain alternatively to authenticate itself to the proxy server as follows.

$$h^{n-i}(r||r_s), \quad i = 1, 2, \ldots, n$$

Since, only the AAA server in 3G network and the user can generate these tickets, it is guaranteed that the user without using the network resources will not be charged by the AAA proxy.

4 Security Analysis and Performance Evaluation

The security analysis and performance evaluation of the proposed protocol are presented and compared with similar protocols.

4.1 Security Evaluation

The comparison among the proposed protocol and some of the available protocols based on the following criteria are presented in Table 2.

Mutual Authentication: In wireless networks, the user and wireless network should authenticate each other. Otherwise, user might connect to a fake network and request for a service. The fake network may tell the user that he/she is successfully authenticated; hence, it may get valuable information from the user. To prevent this attack, in the NRBP protocol, user and network must mutually authenticate each other. For our purposed the WLAN authenticates itself to user by making $Auth_{WL} = h(Tick', ChainPar, N_u)$ and sends it to the user, that is, the user has received the $Tick$ in the first phase in a secure manner. Therefore, if the WLAN authentication server can produce suitable $Tick'$ according to (9), it can authenticate itself to the user, and the user in its turn must authenticate himself to the AAA proxy server. As observed in (6), the AAA proxy server has received $ChainPar$ from AAA server in an authenticated manner as the 1st hash value from a hash chain. Therefore, if the user can generate the next element in the hash chain, as introduced in (11), which can be verified by the available value in the AAA proxy server, he can authenticate himself. The WLAN performs hash function on this amount and compares the result with the amount generated from 3G server previously, and if they are similar, the user is authenticated to the WLAN.

Non-Repudiation: In the first phase, according to (6), the AAA server has signed some parameters such as the first element of a hash chain that is to be used for user authentication in the step 2. Since, this parameter is signed by this server after user authentication to the 3G network, none of the user and the 3G server cannot repudiate access to the WLAN service. In the second phase, it is important that the user cannot repudiate its usage and WLAN can impose additional cost to the user. As shown in (11), the user can authenticate himself by producing the next parameter in the hash chain. Since, only the legitimate user can produce verifiable hash values, he cannot repudiate the received service. Moreover, the user can consume a specific capacity of the WLAN network after each authentication. If he needs more request, he must authenticate himself again. Therefore, the number of generated hash value indicates the amount of consumed services by the user. The WLAN network, however, cannot charge the user more than the number of generated hash value by the user. Therefore, the proposed protocol has non-repudiation property during step two which is used many times.

User anonymity: In both phases of the NRBP protocol, as shown in (2), the temporary ID based on TMSI of the mobile is used instead of the real ID (IMSI) in order to protect against eavesdropping the real ID and tracing the mobile device.

Session Key Freshness: As shown in (12), the session key between the user and the WLAN network is generated based on the hash value which is not revealed before. Therefore, the session key is changed during each user authentication.

Replay Attack: Since the session key is continuously changing , this attack cannot take place. For making the new session key, the previous chain parameter is needed. A fake user cannot obtain this parameter, and in some situations, the random number is used to prevent replay attack. Moreover, in both the phases, authentication protocol is based on challenge/response protocols.

Necessity to make a secure channel: In the proposed protocol, all of the parameters are either encrypted before being transported to the network, or cannot be repeated. Therefore, there is no need to make a separate secure channel.

4.2 Performance Evaluation

In the NRBP protocol, a mobile client does not have to do public-key operations. For connecting to WLAN, the mobile needs some security parameters which are produced by 3G cellular networks. In this protocol, the WLAN network gets these parameters from 3G, and forwards them to UE. Whereas, in most similar protocols, mobile users should first contact the 3G and get a ticket for connecting to the WLAN. In this subsection the performance of the NRBP protocol and some similar protocols regarding the processing overhead and time cost are evaluated.

4.2.1 Processing Overhead

The NRBP protocol has non-repudiation property without forcing the mobile user to do high computations such as public key operations. In the proposed protocol, the 3G-AAA server signs the chain parameter instead of user, and the user only computes hash functions and some symmetric cryptography operations. In the phase I of the protocol, the mobile computes one hash function and two symmetric cryptogra-

Table 2. Comparison between security parameters of NRBP protocol and other 3G-WLAN authentication protocols

	NRBP	LFR	EAP-UTLS	Tseng Protocol (Password-based)	Tseng Protocol (Public-Key)	3GPP
No necessity to make a secure channel	√	√	√	-	√	-
No necessity to synchronize networks	√	√	√	-	-	√
Mutual Authentication	√	√	√	√	√	√
Non-Repudiation Billing	√	-	-	-	√	-
Session Key Freshness	√	√	-	-	-	√
User Identity Protection	√	√	√	-	√	-

phies and in phase II, the user should only compute three hash functions. However, in the Tseng protocol (public-key based), user must compute three asymmetric operations of EAP-TLS protocol. Moreover, since in 802.11 protocols and the EAP-TLS authentication mechanism need almost 800ms to operate [10], using this authentication mechanism in wireless networks might cause some problems due to having high latency [21].

In Table 3, the NRBP protocol is compared to the Tseng, EAP-UTLS and LFR protocols in case of the required number of operations. In the analysis here, the Advanced Encryption Standard (AES) [26] algorithm is used for encryption and decryption. The MD5 [25] is used for hash function and uses the DSA with 1024 bits public/private key size for digital signature. Also, the size of parameters is set as follows: the NAI, ID_{WL}, ID_{3G} are 8 bytes, and the Key_U and random numbers are 16 bytes. The selected mobile device is Compaq iPAQ H3950 with WinCE 3.0 to execute programs in Ewe virtual machine v1.3 [30].

The time-average needed for asymmetric and symmetric operations and one way hash chain function in such device are presented in Table 4. Therefore, considering the results of Table 3 and Table 4, the required processing times on mobile for one-time full authentication and re-authentication, for different protocols is presented in Table 5 and 6, respectively.

4.2.2 Time Cost

Another important parameter in performance evaluation is the mobile authentication delay. Here, the authentication delay (D_{auth}) of different protocols are computed. The D_{auth} consists of three delay elements: the processing, transmission, and propagation delays: $D_{auth} = D_{proc} + D_{trans} + D_{prop}$

The transmission delay, D_{trans}, is the delay for transmitting an EAP message. This delay is insignificant compared with the processing and propagation delays [9], therefore it is not included in the calculation of D_{auth} in the analysis.

The processing delay, D_{proc}, is the delay experienced by each node while processing a message. The cryptographic operations account for most of the processing delay. This delay depends mainly on the processing capabilities held by each node like the speed of the central processing unit (CPU) and the amount of memory. Since, most servers like the AAA servers are usually equipped with adequate CPU power and a large stack of memory, the processing delays in these devices are insignificant. Nonetheless, mobile users have limited processing capabilities and could incur substantial processing delays; hence, in the analysis here only the mobile user processing delays are considered [12]. The propagation delay, D_{prop}, is the round-trip time delay and the time needed until the frame becomes ready for processing at the receiver. Some notions used in delay analysis are presented in Table 7. The NRBP propagation delay is computed as follows:

Full Authentication

$$D_{prop(NRBP)} = 12 \times D_{prop(UE-AP)} + 8\times D_{prop(AP-WAAA)} + 4 \times D_{prop(WAAA-HAAA)} = 900ms$$

Re-Authentication

$$D_{prop(NRBP)} = 6 \times D_{prop(UE-AP)} + 4\times D_{prop(AP-WAAA)} = 300ms$$

Tseng propagation delay id computed as follows:

Full Authentication

$$D_{prop(NRBP)} = 15 \times D_{prop(UE-AP)} + 12\times D_{prop(AP-WAAA)} + 3 \times D_{prop(WAAA-HAAA)} = 1125ms$$

Re-Authentication

$$D_{prop(NRBP)} = 12 \times D_{prop(UE-AP)} + 10\times D_{prop(AP-WAAA)} = 750ms$$

Table 3. Comparison of the performance of the mobile terminal

	NRBP	LFR	EAP-UTLS	Tseng Protocol (Password-based)	Tseng Protocol (Public-Key)
Digital Sign	0	0	0	0	1
Hash chain generation	1	0	0	0	1
Hash Function	3	5	1	0	0
Symmetric Cryptography	2	2	0	1	2
Asymmetric Cryptography	0	0	4	1	3

Table 4. The time-average needed for encrpting, decrypting and hash chain function

Hash Chain Function	Digital Signature	Asymmetric Encryption (Public-Key)	Symmetric Decryption	Symmetric Encryption
16.8ms	18672ms	300ms	240ms	400ms

Table 5. Processing time for first authentication

NRBP	TSENG	EAP-UTLS	EAP-AKA
702.2ms	20128ms	1210ms	650ms

Table 6. Processing time for first re-authentication

NRBP	TSENG	EAP-UTLS	EAP-AKA
67.2ms	19588.8ms	600ms	605ms

Table 7. Some notions used in delay analysis

Symbol	Description
D_{auth}	Authentication Delay
D_{trans}	Transmission Delay
D_proc	Processing Delay
$D_{prop(AP-WAAA)}$	Propagation delay between the AP and WLAN-AAA-Server (WAAA)
$D_{prop(WAAA-3G)}$	Propagation delay between the 3G-AAA-server and WAAA
$D_{prop(UE-AP)}$	Propagation delay between mobile user and AP
$D_{prop(X)}$	The propagation delay of protocol X

EAP-UTLS propagation delay id computed as follows:

Full Authentication

$$D_{prop(NRBP)} = 10 \times D_{prop(UE-AP)} + 8\times D_{prop(AP-WAAA)} + 2 \times D_{prop(WAAA-HAAA)} = 750ms$$

Re-Authentication

$$D_{prop(NRBP)} = 5 \times D_{prop(UE-AP)} + 5\times D_{prop(AP-WAAA)} = 375ms$$

LFR propagation delay is computed as follows:

Full Authentication

$$D_{prop(NRBP)} = 5 \times D_{prop(UE-AP)} + 4\times D_{prop(AP-WAAA)} + 4 \times D_{prop(WAAA-HAAA)} = 600ms$$

Re-Authentication

$$D_{prop(NRBP)} = 5 \times D_{prop(UE-AP)} + 4\times D_{prop(AP-WAAA)} = 300ms$$

In this article, for computing different protocol delays, the delay amounts given in [9] and [22] are used.

$$D_{prop(AP-WAAA)} = 75ms$$
$$D_{prop(WAAA-HAAA)} = 75ms$$

The propagation delay between mobile user and AP($D_{prop(UE-AP)}$) is insignificant, hence, it is not included in these computations. The authentication delay between different protocols is presented in Table 8. The results indicate that the authentication delay of the NRBP protocol for first time authentication is just more than the authentication delay of the LFR protocol, while the NRBP protocol support non-repudiation service but LFR cannot support it. Furthermore, the NRBP protocol has the least re-authentication delay in comparison with other authentication delays. The LFR protocol cannot protect the mobile user identity, while this problem is solved in the NRBP protocol by using the temporary identity of the mobile user. The EAP-UTLS protocol is based on the EAP-TLS protocol and is able to solve EAP-TLS problems. Although, the EAP-UTLS does not support non-repudiation property, this protocol has more authentication delay in comparison to our presented protocol.

In Tseng protocol (public-key based), the mobile user has to sign the chain parameter, thus, it has the most authentication delay. For solving this problem, in the NRBP protocol, this operation is transferred from mobile users to 3G-Servers.

Table 8. Comparison of authentication delays between different protocols

	NRBP	EAP-UTLS	LFR	Tseng Protocol (Public-Key)
First Time Authentication	1607.2ms	1960ms	1205ms	21253.8ms
Re-Authentication	367.2ms	975ms	905ms	20338.8ms

5 Conclusions

In this article, a new non-repudiation authentication protocol is presented for heterogeneous WLAN-3G loosely coupled architecture networks, called NRBP, which is based on the EAP protocol. In the proposed protocol, the authentication process runs in two phases. In the first phase, which is executed only once in a network for a long time, the mobile node contacts the AAA server to receive an authentication ticket by transferring the EAPOL messages. In this phase, the node receives a ticket encrypted by the key shared between the user and its home 3G network. In the second phase, the node can authenticate itself to the WLAN for n times using the ticket obtained from the first phase. In the NRBP protocol, the mobile node does not have to do any public-key operations. The performance and security analysis indicates a better result over the previous protocols. Moreover, unlike most of the proposed protocols, the non-repudiation service is supported in the NRBP protocol without using any asymmetric cryptographic operation in the mobile users' side.

References

[1] [1] Institute of Electrical and Electronics. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," ISO/IEC 8802-11:1999(E), ANSI/IEEE Std 802.11, 1999, http://standards.ieee.org.

[2] [2] Institute European Telecommunications Standards., "Requirements and Architectures for Interworking Between HIPERLAN/2 and 3rdGeneration Cellular Systems," TR 101 957, Aug. 2001, http://www.etsi.org.

[3] M. Zivkovi, M. M. Buddhikot, K. Lagerberg and J. V. Bemme, "Authentication Across Heterogeneous Networks", Bell Labs Technical Journal, pages 3956, 2005.

[4] 3GPP TR 22.934, V2.0.0 Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) internetworking (Release 6), 2004.

[5] C. D. Laat, G. Gross, L. Gommans, J. Vollbrecht and J. Vollbrecht, "Generic AAA Architecture", RFC 2903, August 2000.

[6] L. Blank, J. Vollvrecht, "PPP Extensilble Authentication Protocol (EAP)", RFC 2284, IETF, March 1998.

[7] B. Aboba, L. Blunk, J. Vollbrecht, J. Carleson and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[8] J. Arkko and H. Havcrinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)". RFC 4187, January 2006.

[9] P. Prasithsangaree and P. V. Krishnamurthy, "A New Authentication Mechanism for Loosely Coupled 3G-WLAN Integrated Network", Proceeding of 59th IEEE Vehicular Technology Conference (VTC), vol. 5, pp. 2998-3003, May 2004.

[10] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)", Internet Draft, Work in Progress,¡draft-funk-eap-ttls-v1-01.txt¿, March 2006.

[11] H. Andersson, S. Josefsson, G. Zorn, D. Simon and A. Palekar, "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-08.txt, July 2004.

[12] Ali A. Shidhani and Victor C. M. Leung, "Local fast re-authentication for 3G-WLAN interworking", Security and Communication Networks, vol. 1, no. 4, pp. 309-323, 2008.

[13] Yuh-Min Tseng, Chou-Chen Yang and Jiann-Haur Su, "Authentication and Billing Protocols for the Integration of WLAN and 3G Networks," Wireless Personal Communications, vol. 29, no. 3, pp. 351-366, June 2004.

[14] Constantinos F. Grecas, Sotirios I. Maniatis and Iakovos S. Venieris, "Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration", Mobile Networks and Applications, vol. 8, no. 2, pp. 145-150, April 2003.

[15] M. Shi, X. Shen, J. W. Mark, D. Zhao and Y. Jiang, "User authentication and undeniable billing support for agent-based roaming service in WLAN/cellular integrated mobile networks", Computer Networks, vol. 52, no. 9, pp. 16931702, June 2008.

[16] M. Lee, G. Kim, S. Park, S. Jun, J. Nah and O. Song, "Efficient 3G/WLAN Interworking Techniques for Seamless Roaming Services with Location-Aware Authentication", IFIP International Federation for Information Processing,

LNCS 3462, pp. 370381, 2005.
[17] M. Shin, J. Ma and W. A. Arbaugh, "The Design of Efficient Internetwork Authentication for Ubiquitous Wireless Communications", Technical Report CS-TR-4617, Digital Repository at the University of Maryland, January 2006.
[18] K. Sethom, H. Afifi and G. Pujolle, "Secure and Seamless Mobility Support in Heterogeneous Wireless Networks", IEEE GLOBECOM, vol. 6, pp. 3407-3412, December 2005.
[19] Y. Tseng, "USIM-based EAP-TLS authentication protocol for wireless local area networks", Computer Standards & Interfaces, vol. 31, no. 1, pp. 128136, January 2009.
[20] B. Aboba, M. Beadles, J. Arkko and P. Eronen, "The Network Access Identifier", Network Working Group, RFC 4282, December 2005.
[21] A. Mishra, M. Shin and W. A. Arbaugh, "Proactive Key Distribution using Neighbor Graphs", IEEE Wireless Communications Magazine, vol. 11, no. 1, pp. 26-36, February 2004.
[22] H. Kwon, K. Cheon, K. Roh and A. Park, "USIM based authentication test-bed for UMTS-WLAN handover.", In Proceedings of IEEE INFOCOM, Barcelona, Spain, April 2006.
[23] A. A. Shidhani and V. C. M. Leung, "Pre-Authentication Schemes for UMTS-WLAN Interworking", EURASIP Journal on Wireless Communications and Networking, vol. 2009, pp. 1-16, 2009.
[24] G. Kambourakis, A. N. Rouskas and S. Gritzalis, "Advanced SSL/TLS-based authentication for secure WLAN-3G internetworking", IEE Communication Magazines, vol. 151, no. 5, pp. 501-506, October 2004.
[25] H. Dobbertin, "The status of MD5 after a Recent Attack", In CryptoBytes, vol. 2, no. 2, pp. 16, 1996.
[26] J. Nechavatal, Report on the Development of Advanced Encryption Standard (AES), NIST, Oct. 2000.
[27] C. Ntantogian and C. Xenakis, "One-Pass EAP-AKA Authentication in 3G-WLAN Integrated Networks", Wireless Press Communication, vol. 48, pp. 569584, 2009.
[28] X. Li, X. Lu, J. Ma, Z. Xu and Y. Park, "Authentications and Key Management in 3G-WLAN Interworking", Mobile Network Application, vol. 16, pp. 394407, 2011.
[29] Y. Deng, G. Wang and J. Cao, Practical Unified Authentication for 3G-WLAN Interworking, Journal of Information & Computational Science, vol. 9, no. 7, pp. 19912000, 2012.
[30] M.L. Brereton, "Ewe Virtual Machine", Retrieved from http://www.ewesoft.com/

Ali Fanian received his B.S. and M.S. degrees in computer engineering (hardware and computer systems architecture) in 1999 and 2001, respectively, and the Ph.D. degree in computer networks in 2011, all from Isfahan University of Technology (IUT), Isfahan, Iran. He started his work in the same department as an assistant professor since then. Different aspects of computer architecture and network security are his research interests; specially, network, security and distributed systems.

Fariba Aalamifar is currently a Ph.D. student at the Electrical and Computer Engineering (ECE) Department of the University of British Columbia. She did two internships with Powertech Labs Inc. in Surrey, BC, Canada where she helped with the WiMAX capacity planning for smart grid realization in 2013–2014. She completed her Master's degree in ECE program at Queen's University in 2012. Her Master's thesis was on the "Viability of Power Line Communication for the Smart Grid" which has received notable academic and industrial interests. She has received her Bachelor's degree in information technology engineering from Isfahan University of Technology in 2009.

Mehdi Berenjkoub received his Ph.D. degree from the Department of Electrical and Computer Engineering, Isfahan University of Technology in 2000. The title of his dissertation was "two-party key distribution protocols in cryptography. He started his work in the same department as an assistant professor since then. Graduate courses presented by him include Fundamentals of Cryptography, Cryptographic Protocols, Network Security, and Intrusion Detection. He has supervised more than a dozen M.S. students and Ph.D. candidates in related areas. He also was one of the founder members of the Iranian Society of Cryptology in 2001. He has continued his cooperation with the society as an active member. He along with his colleagues established a research group on security in networks and systems in IUT. He also is responsible for an established academic CSIRT in IUT. He is an associate professor and his current research interests are advanced security protocols, wireless network security, authentication protocols and intrusion detection systems.