Security Performance Analysis and Enhancement of Authentication Protocol in Wireless Mobile Networks

Ja'afer AL-Saraireh

Applied Science University, Amman, Jordan, 11931
sarjaafer@yahoo.com

Abstract: Due to the rapid growth of wireless technology and wireless services, a detailed look at the issue of security is required. Mobile networks are protected by using authentication security mechanisms. The authentication protocol incurs overheads on the transmission process. These overheads affect the mobile network performance such as delay, bandwidth allocation efficiency and throughput. The main aim of this research is to improve authentication mechanism in mobile networks. In the proposed protocol, AKA has been enhanced by generating temporary key to enable visitor location register (VLR/SGSN) to authenticate mobile station (MS) without intervention of HLR/AuC. Therefore, the bottleneck at the authentication centre is avoided by reducing the number of messages between mobile and authentication centre. A fluid mobility model is used to investigate the performance of signaling traffic and load transaction messages between mobile databases, such as Home Location Register (HLR) and Visitor Location Register (VLR), for both the current protocol and the proposed protocol. The simulation results show that the authentication delay and current load transaction messages between entities and bandwidth are minimized as compared with the current protocol. Therefore, the performance and authentication delay time have been improved significantly. To validate the simulation results in this research work, the results have been compared and analyzed with the analytical results.

[Ja'afer AL-Saraireh. **Security Performance Analysis and Enhancement of Authentication Protocol in Wireless Mobile Networks.** Journal of American Science 2011;7(5):599-610]. (ISSN: 1545-1003). http://www.americanscience.org.

Keywords: 3G, Authentication, UMTS, AKA, Security, Mobile Station, and Bandwidth.

1. Introduction

Authentication is used to provide security services in wireless mobile networks, it is considered as an initial process to authorize a mobile terminal for communication through secret credentials (AL-Saraireh and Yousef, 2006). The authentication process provides a reasonable level of security, but it overloads the network with significant signalling traffic and increases the call setup time (AL-Saraireh and Yousef, 2006).

There are different approaches done to enhance UMTS authentication mechanisms, there are sets of approaches being discussed in Europe (Putz et al., 1998). The 1st scheme is proposed by Royal Holloway College. This protocol is a symmetric scheme, it works with a challenge response mechanism and it is offers a mutual authentication of the user and the network operator as well as confidentiality about the user identity towards the network operator. In general the mechanism consists of five messages, which are exchanged between the user, the network operator and the service provider. If the user has already logged on at the network operator who possesses a temporary identity, two of the five messages are dropped and the service provider is not involved. The 2nd scheme is proposed by Siemens. It is an asymmetric protocol. This protocol requires five messages, which are exchanged between the user, the network operator and a certificate server storing certified copies of the necessary public keys. Only three messages are required for this without a certificate server being involved. The 3rd scheme is proposed by KPN. It is a variant of the station-to-station (STS) protocol and similar to protocol that was developed by Siemens as far as the message flow and the mechanism of key exchange is concerned. The 4th scheme is proposed by Siegen University. This protocol is based on asymmetrical, certified based algorithms. By making use of Time Variant Parameters, digital signatures supply the authentication of the communicating partners.

The UMTS AKA protocol has the problem of the bandwidth consumption between SN and HN. It is attractive to choose a suitable length (L) value for AV in the third generation mobile networks. So, many techniques are developed to minimize the authentication signalling cost and network bandwidth consumption by selecting dynamic length (L) for an authentication vector (AL-Saraireh and Yousef, 2006), (AL-Saraireh and Yousef, 2007), (AL-Saraireh, 2011) and (3GPP, 2008). But with this improvement there is still bandwidth consumption (AL-Saraireh, 2011).

The technique of Lin and Chen basically estimated the number of authentication requests in current visited network based on the number in the previous visited network. Whereas the method of

AL-Saraireh and Yousef, estimated the number of authentication requests in current visited network based on the history of mobile movements and the arrival rate for events (AL-Saraireh and Yousef, 2007).

Juang and Wu proposed an efficient 3GPP AKA with robust user privacy. A temporary key to authenticate MS and prevent the location privacy attack is used. In this proposed protocol, the VLR initiates the authentication process by sending a random number to the MS without using any MAC (Juang and Wu, 2007). Therefore denial of services (DoS) attack is possible, additionally; the proposed protocol has seven steps.

A new UMTS AKA protocol called EAKAP is proposed in (Farhat et al., 2009). The EAKAP combines identification stage and AKA stage of UMTS AKA protocol. The problem in EAKAP is that the size of messages between MS, VLR/SGSN and HLR/AuC is increased. Therefore; the consumption of bandwidth is occurred. Subscriber identity/location confidential and non-repudiation services are solved by (Min-Shiang et al., 2010), the proposed scheme integrates symmetric and public key cryptosystem. An Enhancement for UMTS AKA protocol is proposed by Harn and Hsin used hash chaining technique instead of using AVs (Huang and Li, 2005).

Huang and Li (2005) proposed an extension of UMTS AKA protocol, called UMTS X-AKA, to overcome some of problems of UMTS AKA protocol. The UMTS X-AKA protocol used timestamp to manage re-freshness of the messages. A time synchronization infrastructure is required to use timestamp. So time-sync structure of the network has no security feature.

Daeyoung etal., proposed a privacy protecting UMTS AKA protocol is providing perfect forward secrecy. The proposed protocol used timestamp as X-AKA and used EC-based Diffie-Hellman key agreement protocol (Adi et al., 2007); therefore; the authentication time and setup time is increased.

Adi et al., proposed a technique for public key image authentication using fussy computations for El-Gamal authentication technique (Daeyoung et al., 2007), the security was enhanced while more computation overhead was incurred.

The current mechanism of security authentication in 3G system is known as AKA protocol. In this mechanism a secret key (K), and cryptographic algorithms are shared between MS and HN (AL-Saraireh and Yousef, 2006) and (Zhang and Fang, 2005).

AKA protocol has many weaknesses such as, the transmission between the HN and SN is usually expensive, the authentication vectors (AVs) consume network bandwidth for each transmission from authentication centre to SN (Lin and Chen, 2005), the storage space overhead occurs in SN, and bottleneck at HN, the HN is responsible for generating authentication vectors upon receipt of requests from all SN.

In this paper the UMTS AKA illustrates in section 2. In section 3, the UMTS authentication protocol is analysed. The efficient and secure AKA scheme is described in section 4. Section 5 presents security performance analysis for the proposed protocol. Simulation results, comparison and discussion between the UMTS AKA protocol and proposed protocol are presented in section 6. In section 7, the statistical test and validation is presented. The paper is concluded in section 8.

2. UMTS Authentication Protocol

The current mechanism of security authentication in 3G system is known as AKA protocol. In this mechanism a secret key (K), and cryptographic algorithms - f_1, f_1^*, f_2, f_3, f_4, f_5 and f_5^* - are shared between MS and HN (AL-Saraireh and Yousef, 2006) and (Huang et al., 2009).

There are two phases in AKA protocol, the first phase is the generation and distribution authentication vectors from the HN to the SN, and the second phase is the authentication and key agreement procedure between the MS and the SN (AL-saraireh and Yousef, 2007) and (Zhang and Fang, 2005). An overview of UMTS AKA is given in figure 1 (AL-Saraireh, 2011).

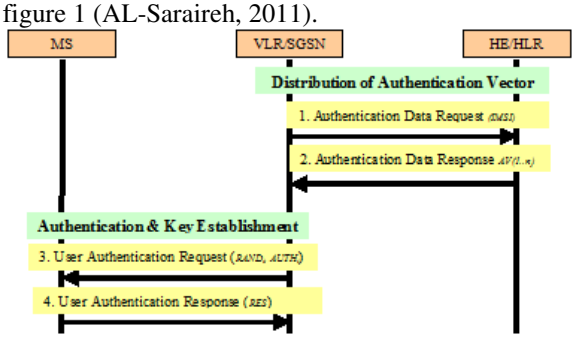

Figure 1. The Authentications and key agreement protocol.

Mobile station (***MS***) sends authentication request to the ***SN***, which includes International Mobile Subscriber Identity ***(IMSI)***. ***SN*** passes this authentication request to ***HN***. ***HN*** sends authentication data response to ***SN***, which include authentication vector (***AV***). Each authentication vector has five components: random number (***RAND***), expected response (***XRES***), cipher key (***CK***), integrity key (***IK***) and authentication token (***AUTN***). The authentication vectors are ordered by

the sequence number SQN_{HLR}. The authentication vector is generated according to the following steps (AL-Saraireh, 2011) and (Li et al., 2009):

i. ***HN*** set ***SQN*** to SQN_{HN} and generates ***RAND***.
ii. ***HN*** computes the following values: ***XRES***, ***CK***, ***IK***, ***AK,*** and ***MAC***
iii. ***HN*** assembles the authentication token ***AUTN = (SQN*** $\oplus$ ***AK*** $||$ ***AMF*** $||$ ***MAC)*** and the authentication vector (***RAND,XRES, CK, IK, AUTN***)
iv. ***HN*** increments SQN_{HLR} by 1.

SN is receiving response from ***HN*** and then storing ***AV***. The ***SN*** selects the i^{th} authentication vector ***AV(i)***, and sends (***RAND (i), AUTN(i)***) to ***MS***. Each authentication vector is efficient for one authentication process (AL-Saraireh, 2011).

MS is receiving ***RAND*** and ***AUTN*** from ***SN***. ***MS*** computes and retrieves the anonymity key ***AK***, ***SQN,*** expected message authentication code ***XMAC***. The ***MS*** compares ***XMAC*** with ***MAC*** which is included in ***AUTN***. If they are different, then ***MS*** sends failure message to the ***SN***. Otherwise, ***MS*** checks that the received ***SQN*** is in the correct range. If the ***SQN*** is not in the correct range, then ***MS*** sends failure message to the ***SN***. Otherwise, if the ***SQN*** in correct range, the ***MS*** computes ***RES*** and sends it to ***SN***. Lately, ***MS*** computes ***CK*** and ***IK.***

SN is receiving authentication response from ***MS***. ***SN*** compares the received ***RES*** with ***XRES*** in authentication vector. If ***RES*** is matching ***XRES***, then authentications is successfully completed and select the ***CK*** and ***IK*** from authentication vector. If ***RES*** is unequal ***XRES***, ***SN*** sends authentication failure to the ***HN***.

3. Analysis Of UMTS Authentication Protocol

In this research work, a fluid mobility model, as in (AL-saraireh and Yousef, 2006), (Mohan and Jain, 1994) and (Skehill and McGrath, 2004) is used to investigate and analyse the performance of signalling traffic, load, and bandwidth that are generated by UMTS authentication protocols, and the delay in the call setup time (AL-Saraireh and Yousef, 2006).

Different mobility models used to describe aggregate and individual user movement behaviour such as Fluid Mobility model, Gravity model, Gaussian model, Random Walk model, and Markov model.

The fluid flow model is suitable for this research study because it is characterizes aggregate movement behaviour as the flow of a fluid. Fluid flow model describes the mobility in terms of the average number of users crossing the boundary of a registration area. Fluid-flow model is more suitable for users with high mobility, infrequent speed, and direction changes.

The fluid mobility model has the following parameters (AL-Saraireh and Yousef, 2006):

i. User who is carrying mobile station (***MS***) is moving at an average velocity ***v***;
ii. Direction of ***MS*** movement is uniformly distributed over **[0, 2π]**;
iii. Mobile users are uniformly populated with the density ρ within the registration area;
iv. ***L*** is perimeter length Registration area (***RA***) boundary.

The rate of registration area crossing ***R,*** and the average number of active mobile crossing the registration area, is given by (AL-Saraireh and Yousef, 2006) and (Mohan and Jain, 1994):

$$R_{\text{Re gistration},RA} = \frac{\rho.v.L}{\pi} \qquad (1)$$

The signalling traffic for registration, origination, and termination of calls was calculated by using equation (1). Mobile traffic of the network depends on the ***MS*** user's movement. Table 1 summarises assumptions, which are made to perform numerical analysis (AL-Saraireh and Yousef, 2006) and (Porta et al., 1996).

Table 1. Assumption parameters.

Parameter	Value
Total registration area (RA)	128
Square registration area size	$(8.65\text{km})^2$= $74.8225\ \text{km}^2$
Border length L	32.45 km
Mean density of mobile ρ	$328\ /\text{km}^2$
Total of MS	3.5 million
Average call origination rate	2/hr/user
Average call termination rate	2/hr/user
Average speed of user who is carrying mobile, v	5.95 km/hr

The rate of deregistration area crossing R is equivalent to the rate of registration (AL-Saraireh and Yousef, 2006).

$$R_{Registration,RA} = R_{Deregistration,RA} \qquad (2)$$

The total number of authentication request messages per second that arrive at the HLR/HN is [(AL-Saraireh and Yousef, 2006):

$$R_{Registration,HLR} = R_{registration,RA} * Total \quad number \quad of \quad RA \qquad (3)$$

The total number of authentication requests due to call origination per serving network (SN) is equivalent to the total number of authentications due to call termination per serving network. The total number of authentication requests due to call

origination per serving network ($R_{Call\ origination/SN}$) is calculated as follows (AL-Saraireh and Yousef, 2006):

$$R_{call\ Origination/SN} = Call\ \ Rate\ \ Per\ User$$
$$= Average\ Call\ Origination\ Rate * Total\ of\ MS \quad (4)$$

The number of calls origination per registration area ($R_{Call\ origination/RA}$) is calculated as (AL-Saraireh and Yousef, 2006):

$$R_{Call\ \ origination\ \ /RA} = \frac{R_{Call\ \ origination\ \ /SN}}{Total\ \ registarti\ \ on\ \ Area}) \quad (5)$$

The number of calls terminating per registration area ($R_{Call\ Termination/RA}$) is equivalent to the number of call originations per registration area, $R_{Call\ Termination/RA}$ (AL-Saraireh and Yousef, 2006).

The security performance for the current UMTS authentication and key agreement protocol was analyzed by (AL-Saraireh and Yousef, 2006) and the results are summarized as follows:

Table 2 summarizes the total authentication requests per VLR/SN and HLR/HN for each type of activity, as computed by (AL-Saraireh and Yousef, 2006).

Table 2: Total authentication requests per second (s) for VLR and HLR.

Activity	VLR/s	HLR/s	Total/s
Registration	5.60	716.80	722.40
Call Termination	15.19	1944.40	1959.59
Call Origination	15.19	1944.40	1959.59
Total/ Network	35.98	4605.60	4641.58

The signalling messages flow for each activity: registration, call origination, and call termination was summarised in (AL-Saraireh and Yousef, 2006), as shown in table 3.

Table 3: Signalling messages per authentication request for each activity.

Activity	AuC	HLR	VLR	Old VLR	Total
Reg.	2	4	5	1	12
Call Term.	2	4	5	0	11
Call Orig.	2	4	5	0	11
Total	6	12	15	1	

The total signalling traffic and load transaction messages between mobile databases (VLR/SN and HLR/HN) was computed by [1] as shown in table 4, based on the results from table 2 and table 3.

Table 4: Total signalling traffic and load transaction messages/s for each activity in UMTS

Activity	AuC	HLR	VLR	Old VLR	Total
Regist.	1433.60	2867.20	28.01	5.60	4334.41
Call Term.	3888.80	7777.60	75.95	0	11742.35
Call Orig.	3888.80	7777.60	75.95	0	11742.35
Total	9211.20	18422.40	179.91	5.60	

As shown in table 4, the relationships between the velocity of movement of users and the total authentication requests per VLR/SN and HLR/HN for the UMTS authentication process is directly proportional, and the relationship between the registration area and total authentication requests per VLR/SN and HLR/HN for the UMTS registration process is directly proportional. Table 5 has the authentication parameters that were used to compute the bandwidth for each activity (AL-Saraireh and Yousef, 2006).

Table 5: Authentication parameters.

Parameter	Length (bits)
IMSI	128
Key K	128
Random Challenge RAND	128
Sequence Number SQN	48
Anonymity Key AK	48
Authentication Management Field AMF	16
Message Authentication Code MAC	64
Cipher Key CK	128
Integrity Key IK	128
Authentication Response RES	32
Authentication token AUTN	128
Authentication vector AV as one record	544
Standard number of record in authentication vector	5
Location Area Identifier LAI	40
Service Request	8

The authentication delay is the time between the MS sends an authentication request until the MS receive the authentication response. Al-Saraireh and Yousef were assumed that the authentication time delay is T_{auth} and the time delay to access the VLR/SN database is the same as to access the HLR/HN database, and they let this time to be T_{DB} and the time between MS and VLR/SN is $T_{MS \leftrightarrow VLR/SNh}$. The authentication delay was computed by (AL-Saraireh and Yousef, 2006) as follows:

$$T_{Auth} = 4 * T_{DB} + 3 * T_{MS \leftrightarrow VLR/SN} \quad (6)$$

Table 6 summarises the bandwidth consumed between the MS and VLR/SN and between databases, as computed by (AL-Saraireh and Yousef, 2006).

Table 6: Bandwidth Consumptions between entities for AKA protocol.

Activity	Bandwidth between MS and VLR/MSC (Bytes/S)	Bandwidth between Databases(Bytes/S)	Total
Registration	324.80	2531.20	28560
Call Orig./Term.	881.02	6865.88	7746.90
Total/ Network	1205.82	9397.08	10602.90

4. The Proposed Efficient Authentication Protocol (E-AKA)

E-AKA is used to eliminate the security weakness involved with UMTS AKA. E-AKA is considered as a secure and an efficient authentication scheme. In the E-AKA scheme VLR/SN has the capability to authenticate the user without intervention of HLR/HN.

The E-AKA uses a new key generation functions called fx to generate the temporary key (TK). The fx function produces a 128 bits or higher bits to provide high level of security. In the proposed protocol, the SN is able to authenticate the MS after the initial authentication has been performed. The proposed authentication protocol contains two operation modes for initial and subsequent authentication. The first mode is registration and distribution of authentication information (Initial Authentication) and temporary key (TK) from the HLR/HN to the VLR/SN. The second mode is the authentication and key agreement procedure (Subsequent authentication) performed between the MS and the VLR/SN.

Figure 2 and 3 describe authentication mechanism for the proposed protocol. The authentication procedure is described as follow:

Step 1: Authentication Request Message: When MS needs authentication to network, to access or to use the network services, the initial authentication is carried out as follow:

1.1 ***MS*** generates random number ***($Rand_{MS}$)***,

1.2 ***MS*** computes the Message Authentication Code $MAC_{MS}= f_1(K, Rand_{MS})$,

1.3 ***MS*** sends ***IMS***, $Rand_{MS}$ and MAC_{MS} as authentication request to ***VLR/SN***.

Step 2: Authentication Request Message: ***VLR/SN*** passes this authentication request to ***HLR/HN***.

Step 3: Authentication Response Message: Receiving the authentication request and then verification procedure is performed by ***HLR/HN***. A response message is generated. The following operations are carried by ***HLR/HN***:

3.1 Compares and computes expected message authentication code for mobile station $(XMAC_{MS})$ to verify the received message.

$XMAC_{MS}=f_1(K, Rand_{MS})$

$XMAC_{MS} ?= MAC_{MS}$

If mismatching occurs then the registration will fail otherwise it will execute the next steps.

3.2 Generates SQN_{HLR} and $RAND_{HLR}$.

3.3 Computes expected response $XRES_{HLR} = f_2(K,RAND_{HLR})$, Anonymity Key $AK_{HLR} = f_5(K,RAND_{HLR})$, Message Authentication Code $MAC_{HLR} = f_1(K,SQN||RAND_{HLR}||MAF)$, where ***MAF*** is Message Authentication Field and authentication token $AUTN_{HLR} = (SQN \oplus AK_{HLR}||AMF||MAC_{HLR})$ where $\oplus$ is exclusive OR operation.

3.4 Computes temporary key $TK = f_x(K,RAND_{HLR})$.

3.5 Sets response messages and sends it to ***VLR/SGSN***, including one authentication vector ***AV***. This ***AV*** consists of four components: $RAND_{HLR}$, $XRES_{HLR}$, ***TK*** and $AUTN_{HLR}$.

$AV = RAND_{HLR}|| XRES_{HLR}||TK|| AUTN_{HLR}$

Step 4: Authentication Response Message: Receiving the response message from ***HLR/HN***, ***VLR/SN*** will invoke the authentication to the ***MS***. ***VLR/SN*** will achieve the following:

4.1 Stores the ***TK***, $AUTN_{HLR}$ and generates $Rand_{VLR}$.

4.2 Computes $MAC_{VLR}=f_1(TK, MAC_{HLR}||Rand_{VLR})$ where the MAC_{HLR} retrieved from $AUTN_{HLR}$ which stored in previous step.

4.3 Computes $AUTN_{VLR} = (SQN_{HLR} \oplus AK_{HLR}||AMF||MAC_{VLR})$

4.4 ***VLR/SN*** sends $AUTH_{VLR}$, $Rand_{VLR}$ and $Rand_{HLR}$ to ***MS***

Step 5: Authentication Response Message: When ***MS*** receives the messages, the ***MS*** will achive the following:

5.1 Computes $TK=f_x(K, Rand_{HLR})$.

5.2 Verifies that the received sequence number ***SQN*** is in the correct range. If the ***MS*** considers the sequence number to be not in the correct range, it sends synchronization failure back to the ***VLR/SN*** including an appropriate parameter, and abandons the procedure.

5.3 Computes ***XMAC*** for ***HLR*** and ***VLR.***

$XMAC_{HLR} = f_1(K, AK_{MS} \oplus (SQN_{HLR} \oplus AK_{HLR})||Rand_{HLR}|| AMF)$ where $Rand_{HLR}$ and ***AMF*** are retrieved from $AUTN_{VLR}$

$XMAC_{VLR} = f_1(TK, XMAC_{HLR}||Rand_{VLR})$. If $XMAC_{VLR}$ is equal $XMAC_{VLR}$ then ***HLR/HN*** and ***VLR/SN*** are valid,

5.4 Computes an $XRES = f_2(TK, Rand_{VLR})$

5.5 Sends ***XRES*** to ***VLR/SN***. While, the ***MS*** computes an integrity key as $IK = f_3(TK, Rand_{VLR})$ and a cipher key as $CK = f_4(TK, Rand_{VLR})$ to realize securely communication with ***VLR/SN*** subsequently.

Step 6: Authentication Response Message: ***VLR/SN*** receives the messages from ***MS*** and verifies whether ***RES*** is identical to the ***XRES***. If it is true, the whole authentication is successfully completed. If it is false, the authentication is failed.

After the initial authentication, both the ***VLR/SN*** and ***MS*** obtain the authentication result from the ***HLR/HN*** and share some secret information. Here, the ***VLR/SN*** caches some authentication information, which can be used in subsequent authentication without intervention of ***HLR/HN***.

After initial authentication, the ***VLR/SN*** has the ability to authenticate the ***MS*** in subsequent authentication. If the ***MS*** remains in the same ***VLR/SN*** and requests services, then the user should ask for subsequent authentication. ***MS*** similarly generates an authentication request message, which should contain the information shared between the ***MS*** and ***VLR/SN***; the ***VLR/SN*** uses this information to authenticate the ***MS***. ***VLR/SN*** authenticates ***MS*** by using temporary key ***TK***.

As mentioned above, the ***VLR/SN*** has cached information needed to authenticate ***MS***. After authenticating the ***MS***, the ***VLR/SN*** sends a response message containing the authentication result to the ***MS***. The ***MS*** receives the response message and learns whether the authentication was successful or not. The subsequent authentication is described as follows:

Step 1: Authentication Request Message: ***MS*** sends authentication request to ***VLR/SN***

Step 2: Authentication Request Message: When ***VLR/SN*** receives the request message, ***VLR/SN*** will do the following:

2.1 Generates $Rand_{VLR}$

2.2 Computes authenticate token $AUTN = SQN \oplus AK \| AMF \| MAC$

Where $AK = f_5(TK, RAND)$, and $MAC = f_1(TK, SQN \| RAND \| MAF)$.

2.3 Sends ***AUTN*** and ***RAND*** to ***MS***.

Step 3: Authentication Response Message: When ***MS*** receives the response message, ***MS*** will achieve the following:

3.1 Computes and retrieves the $AK = f_5(TK, Rand)$, $SQN = (SQN \oplus AK) \oplus AK$, and $XMAC = f_1(SQN, RAND, AMF)$

3.2 Compares ***XMAC*** with ***MAC*** which is included in ***AUTN***. If ***XMAC*** is not equal to ***MAC*** then ***MS*** sends failure message to the ***VLR/SN***, else if ***XMAC*** is equal ***MAC*** then ***MS*** checks that the received ***SQN*** is in the correct range i.e. $SQN > SQN_{MS}$. If ***SQN*** is not in the correct range then ***MS*** sends failure message to the ***VLR/SN***, else if it is in the correct range, then ***MS*** computes the Response $RES = f_2(TK, RAND)$, and $CK = f_3(TK, Rand)$. After that, it sends ***RES*** to ***VLR/SN.***

Step 4: Authentication Response Message: ***VLR/SN*** receives the messages from ***MS*** and verifies whether ***RES*** is identical to the ***XRES***. If it is true, the whole authentication is successfully completed. If it is false, the authentication is failed.

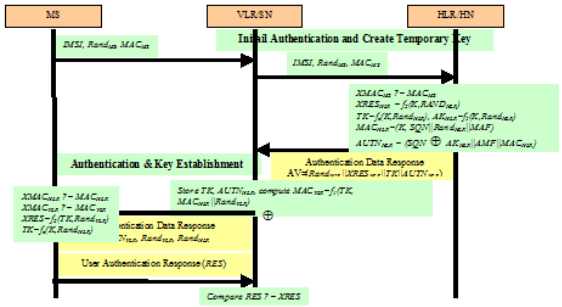

Figure 2. Registration and distribution of authentication information (Initial Authentication) in EAKA

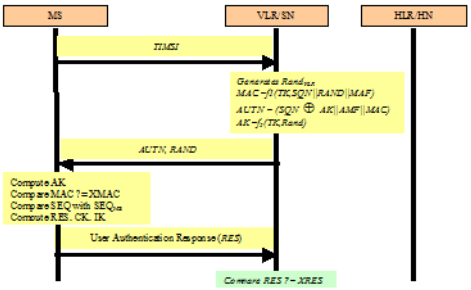

Figure 3. Subsequent authentications in EAKA

5. Analysis of the Proposed Protocol

Figure 4 illustrates the signalling messages flow for registration activity in the proposed protocol. The signalling messages flow for call origination and termination (i.e., subsequent authentication) is represented in figure 5.

The total signalling traffic and load transaction messages between the mobile database (VLR/SN and HLR/HN) are shown in table 8, and are calculated from the values in tables 2 and 7. The rate of registration area crossing R is calculated by using equation (1):

$$R_{registration,RA} = \frac{328 * 5.95 * 32.45}{1hr * 60\min * 60\sec * \pi} = 5.60/\sec$$

By using equation (2), the rate of deregistration area crossing R is equivalent to the rate of registration.

$$R_{Deregistration,RA} = 5.60/\sec$$

The total number of authentication request messages per second that arrive at the HLR by using equation (3)

$$R_{registration,HLR} = 5.60*128 = 716.8/\sec$$

The total number of authentication requests due to call origination per serving network (SN) is equivalent to the total number of authentications due to call termination per serving network. The total number of authentication requests due to call origination per serving network ($R_{Call\ origination/SN}$) is calculated by using equation (4) as follows:

$$R_{call\ Origination/SN} = \frac{2*3.5million}{1hr*60\min*60\sec} = 1944.4/s$$

The total number of calls terminated $R_{Call\ termination/SN} = 1944.4/s$.

By using equation (5), the number of calls origination per registration area ($R_{Call\ origination/RA}$) is:

$$R_{Call\ origination/RA} = \frac{1944.4}{128} = 15.19/s$$

The number of calls terminating per registration area ($R_{Call\ Termination/RA}$) is equivalent to the number of call originations per registration area, $R_{Call\ Termination/RA} = 15.19/s$.

From figures 4 and 5, the signalling messages per authentication for each activity registration, call origination, and call termination is summarised table 7. The total signalling traffic and load transaction messages between the mobile database (VLR/SN and HLR/HN) are shown in table 8, and are calculated from the values in tables 2 and 7.

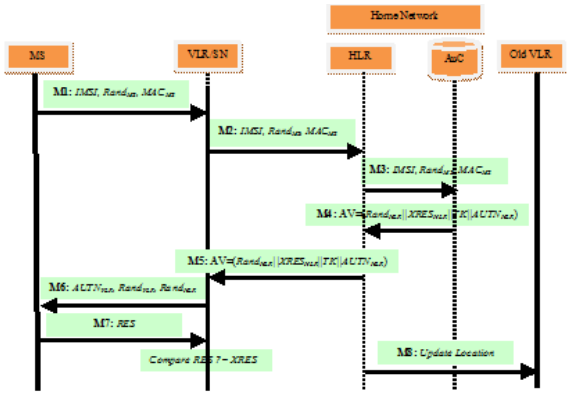

Figure 4. Signalling messages flow for the E-AKA protocol (Registration, initial Authentication).

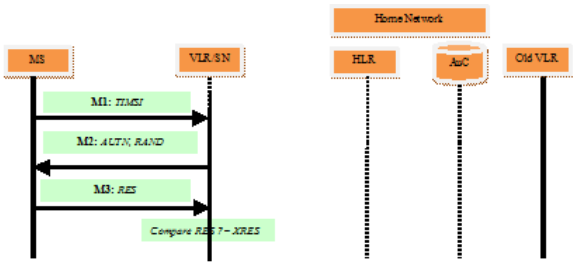

Figure 5. Signalling messages flow for the E-AKA protocol (Subsequent Authentication).

Table 7. Signalling messages per authentication request in the proposed protocol.

Activity	AuC	HLR	VLR	Old VLR	Total
Reg.	2	4	5	1	12
Call Term.	0	0	3	0	3
Call Orig.	0	0	3	0	3
Total	2	4	11	1	

Table 8. Total signalling traffic and load transaction messages per second for each activity in the

Activity	AuC	HLR	VLR	Old VLR	Total
Regist.	1433.60	2867.20	28.01	5.60	4334.41
Call Term.	0	0	45.57	0	45.57
Call Orig.	0	0	45.57	0	45.57
Total	1433.60	2867.20	119.20	5.60	

For registration and distribution of authentication (i.e., initial authentication), the authentication delay for the proposed protocol $T_{Initial\ Auth}$ is computed as follows:

$$T_{Initial\ Auth} = 4*T_{DB} + 3*T_{MS\leftrightarrow VLR/SN} \quad (7)$$

While for subsequent Authentication, the authentication delay for proposed protocol $T_{Subsequent\ Auth}$ is:

$$T_{Subsequent\ Auth} = 3*T_{MS\leftrightarrow VLR/SN} \quad (8)$$

The average of authentication delay for proposed protocol $T_{Avgl\ Auth}$ is:

$$T_{Avg\ Auth} = \frac{(T_{Initial\ Auth} + T_{Subsequent\ Auth})}{2} \quad (9)$$

In initial authentication to compute the bandwidth, there are seven messages to authenticate MS, three of them between the MS and VLR/SN, and the other four are between databases. For subsequent authentication, there are three messages between MS and VLR/SN.

For Initial authentication, the size of these messages between MS and VLR/SN can be computed as follows:

(i) M1 is the first message which contains the following parameters: IMSI/*TMSI,Service request, and LAI*. The length of message 1 is computed as follow:

$$Length(M1) = Length(IMSI / TMSI) + Length(Service\ \ Request) + Length(LAI) + Length(Rand_{MS}) + Length(MAC_{MS}) \quad (10)$$

$$Length(M1) = 128 + 8 + 40 + 128 + 64 = 368 \quad bits$$

(ii) M6 is the sixth message which contains the parameters: $AUTN_{VLR}$, $Rand_{VLR}$, $Rand_{HLR}$, the length of message six is:

$$Length(M6) = Length(AUTN_{VLR}) + Length(Rand_{VLR}) + Length(Rand_{HLR}) \quad \ldots\ldots\ldots (11)$$

$$Length(M6) = 128 + 128 + 128 = 384 \quad bits$$

(iii) M7 is the seventh message between ***MS*** and ***VLR/SN*** which contains only *RES*. The length of M7 is:

$$Length(M7) = Length(RES) = 32 bits \quad (12)$$

The total size of authentication messages between MS and VLR/SN is calculated as follows:

$$Length\ (MS \xleftarrow{messages} VLR\ /\ SN) = Length\ (M1) + Length\ (M6) + Length\ (M7) \quad (13)$$

$$= 368 + 384 + 32 = 784 \quad bits = 98 \quad bytes$$

The size of messages between databases for initial authentication is computed as following:

(i) M2 is the second message which contains the following parameters: IMSI/*TMSI,Service request, LAI,* $Rand_{MS}$, and MAC_{MS}).

$$Length(M2) = Length(M1) = 368 \quad bits \quad (14)$$

(ii) M3 is the third message, which contains the same parameters as M1 and M2.

$$Length\ (M3) = Length\ (M2) = Length\ (M1) = 368 \quad bits \quad (15)$$

(iii) M4 is the fourth message, which contains only one *AV*.

$$Length(M4) = Length(AV) = Length(Rand_{HLR}) + Length(XRES_{HLR}) + Length(TK) + Length(AUTN_{HLR}) \quad (16)$$

$$= 128 + 32 + +128 + 128 = 416 \quad bits$$

(iv) M5 is the fifth message, which contains parameter same as M4.

$$Length(M5) = Length(M4) = 416 \quad bits \quad (17)$$

The total size of authentication messages between databases is:

$$Length(VLR / SN \xleftarrow{messages} HLR / HN + HLR / HN \xleftarrow{messages} AuC / HN) = Length(M2) + Length(M3) + Length(M4) + Length(M4) \quad (18)$$

$$= 368 + 368 + 416 + 416 = 1568 \quad bits = 196 \quad bytes$$

The total size of messages in the initial authentication process is:

$$Length(InitialAuth) = 98 + 196 = 294 \quad bytes$$

For subsequent authentication, the size of these messages between ***MS*** and ***VLR/SN*** can be computed as follows:

(i) M1 is the first message which contains the following parameters: IMSI/*TMSI,Service request, LAI,* $Rand_{MS}$, and MAC_{MS}). The length of M1 is:

$$Length(M1) = Length(IMSI / TMSI) + Length(Service\ \ Request) + Length(LAI) \quad (19)$$

$$Length(M1) = 128 + 8 + 40 = 176 \quad bits$$

(ii) M2 is the second message includes *AUTN* and *Rand*. The length of M2 is:

$$Length(M2) = Length(AUTN) + Length(Rand) \quad (20)$$

$$Length(M2) = 128 + 128 = 256 \quad bits$$

(iii) M3 is the third message includes *RES*. The length of M3 is:

$$Length(M3) = Length(RES) = 32 \quad bits \quad .(21)$$

The total size of messages in the subsequent authentication process is:

$$Length\ (Subsequent\ \ Auth) = Length\ (M1) + Length\ (M2) + Length\ (M3) \quad (22)$$

$$= 176 + 256 + 32 = 464 \quad bits = 58 \quad bytes\ .$$

The average total size of messages in proposed authentication protocol is:

$$Length(Avg.Auth) = \frac{Length(InitialAuth) + Length(SubsequentAuth)}{2} \quad (23)$$

$$= \frac{294 + 58}{2} = 176 \quad bytes$$

As shown in table 2, for registration activity there are 5.60 authentication requests and for origination/termination call activity there are 15.19 authentication requests. Table 9 summarises the bandwidth used between the MS and VLR/SN, and between databases.

Table 9. Bandwidth that is used between entities for proposed protocol.

Activity	Bandwidth between MS and VLR/MSC (Bytes/S)	Bandwidth between Databases(Bytes/S)	Total
Registration	548.80	1097.60	1846.40
Call Orig./Term.	881.02	0	881.02
Total/ Network	1429.82	1097.60	2527.12

6. Simulation Results and Discussion

To analyze signalling traffic performance, load transaction messages and bandwidth, the simulation study has been carried out. Different simulation scenarios are carried out by using different mobility rates. The software that has been used to simulate the current and proposed authentication protocol is network simulator (NS-2). NS-2 is an object-oriented, discrete event driven network simulator developed at UC Berkely.

In the proposed protocol, the signalling messages are reduced between the mobile network entities. Tables 10, 11, 12, and 13 illustrate the differences between current UMTS authentication protocol and the proposed protocol. The current protocol needs 12 messages between mobile network entities to perform registration or 11 messages for call origination/termination, but proposed protocol needs only 12 messages to perform registration or 3 messages for call origination/termination.

The results show that the authentication delay and current load transaction messages between entities and bandwidth are minimised when compared with the current protocol, as illustrated in figures 6, 7, 8, and 9. Therefore, the performance and the authentication delay time have been improved significantly. As shown in table 12, the percentage of improvement is more than 67.55%. From equations 6, 7, 8, and 9, where it is assumed that TDB = 1ms, the proposed protocol has less delay than the current UMTS protocol as shown in figure 6.

Table 10. Compare signalling messages between current and proposed authentication protocol.

	Current Protocol				Proposed Protocol			
Activity	AuC	HLR	VLR	Old VLR	AuC	HLR	VLR	Old VLR
Registration	2	4	5	1	2	4	5	1
Call Term./Orig	2	4	5	0	0	0	3	0

Table 11. Compare total signalling traffic and load messages per second between entities for each activity.

	Current Protocol				Proposed Protocol			
Activity	AuC	HLR	VLR	Old VLR	AuC	HLR	VLR	Old VLR
Regist.	1433.60	2867.20	28.01	5.60	1433.60	2867.20	28.01	5.60
Call Term./Orig	3888.80	7777.60	75.95	0	0	0	45.57	0

Table 12. Compare total signalling traffic and load messages per second between entities.

Entity	Current Protocol	Proposed Protocol	% improvement
AuC	9211.20	1433.60	84.44
HLR	18422.40	2867.20	84.44
VLR	179.91	119.15	33.77
Average of Improvement %			67.55

Table 13: Compare the bandwidth for each activity between database and VLR/MSC.

	Bandwidth Between MS and VLR and Between Data Bases					
	Current Protocol			Proposed Protocol		
Activity	VLR	Database	Total	VLR	Database	Total
Registration	324.80	2531.20	2856.00	548.80	1097.60	1646.40
Call Term./Orig	881.02	6865.88	7746.90	8281.02	0	881.02

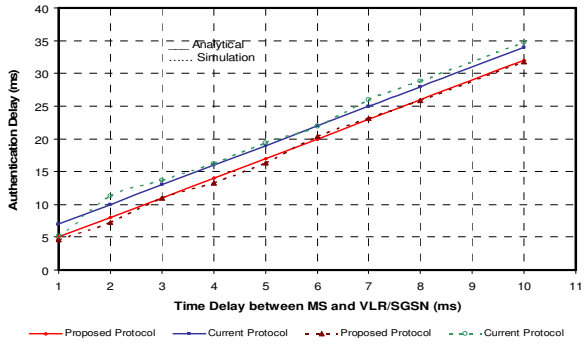

Figure 6. Authentication delay when $T_{DB} = 1ms$

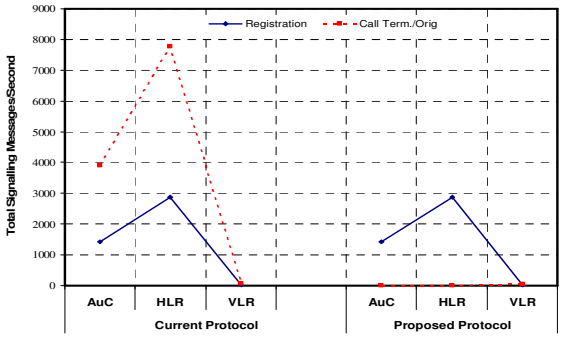

Figure 7. Load transaction messages per second between entities.

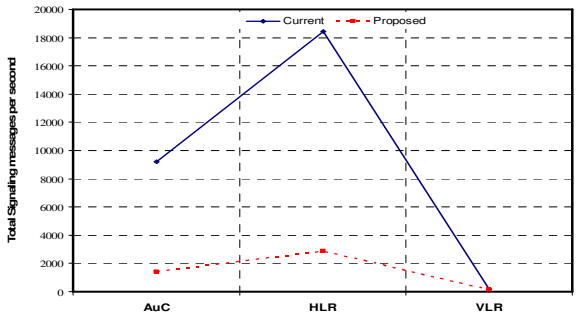

Figure 8. Total signalling messages/second for all activity in current and proposed protocol.

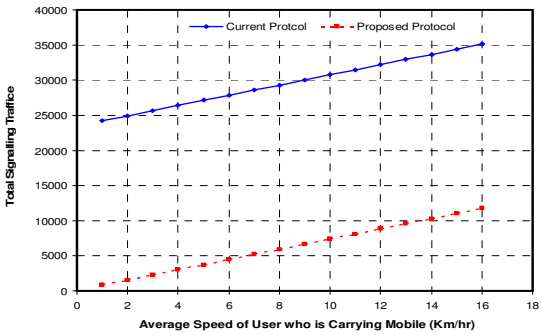

Figure 9. Network signalling traffic with different mobility rate.

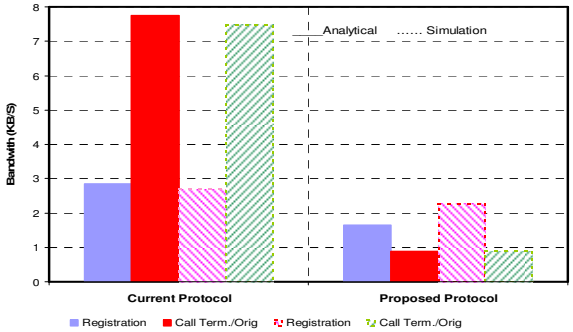

Figure 10. Comparing the bandwidth for each activity between current and proposed protocol.

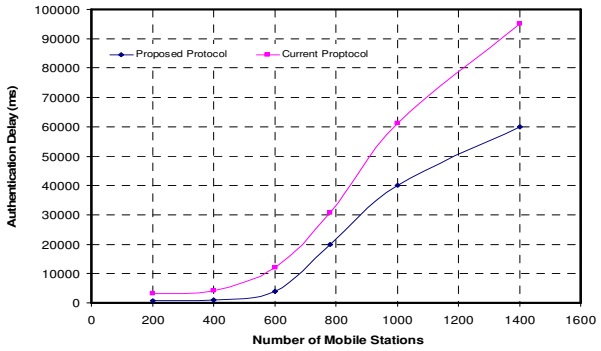

Figure 11. Authentication delay when the number of MS increased (simulation results).

7. Statistical Tests And Validation

The analysis of variance (ANOVA) method was used to compare the difference current and proposed protocol, and between analytical and simulation results, whether significant or insignificant.

For analytical results, the average authentication delay for the proposed protocol is (15.80) and current protocol is (17.80), by using the T-test showed a significant difference at (0.05) level of significance. For simulation results, the average authentication delay for the proposed protocol is (15.60), while the average of the current protocol is (18.14), by using the T-test showed a significant difference at (0.05) level of significance.

For the proposed protocol, when comparing the average authentication delay between the analytical results (15.80) and the simulation results (15.60), an insignificant difference was found. That was based on the statistical test, which was done using an independent T-test at (0.05) level of significance. When comparing the average authentication delay between the analytical results (17.80) and the simulation results (18.14) for current protocol, an insignificant difference was found. That was based on the statistical test, which was done using an independent T-test at (0.05) level of significance.

For analytical results, the average bandwidth for the proposed protocol is (1.26) and for the current protocol is (5.30), by using the T-test showed a significant difference at (0.05) level of significance. When compare the average bandwidth for the proposed protocol (1.59) with the average of the current protocol (5.09) for the simulation results, by using the T-test showed a significant difference at (0.05) level of significance.

For the current protocol, when comparing the average bandwidth between the analytical results (5.30) and the simulation results (5.09), an insignificant difference was found. That was based on the statistical test, which was done using an independent T-test at (0.05) level of significance. When comparing the average bandwidth between the analytical results (1.26) and the simulation results (1.59) for the proposed protocol, an insignificant difference was found. That was based on the statistical test, which was done using an independent T-test at (0.05) level of significance.

It can be concluded from the above analysis of the authentication delay and bandwidth consumption that there are very little differences between the simulation and analytical results, and there is an enhancement from the current protocol.

8. Conclusion

In this research work, the UMTS authentication and key agreement protocol, and the signalling traffic that is generated by registration, call termination, and call origination, have been investigated and analysed. There has also been an analysis of the bandwidth that is used between MS and VLR, and between database registers. The proposed authentication protocol has improved the performance of authentication by reducing the authentication times, setup time and data sizes. In addition, the proposed authentication mechanism has less signalling traffic, and consequently the bottleneck at authentication centres is avoided by reducing the number of messages between mobiles and authentication centres.

The proposed authentication for UMTS has been generated with the aim of not only keeping the complexity of this function as low as possible, but also keeping a high level of security and efficiency for the bandwidth used.

Corresponding Author:
Dr. Ja'afer AL-Saraireh
Applied Science University, 11931
Amman, Jordan,
E-mail: sarjaafer@yahoo.com

References

1. Al-Saraireh J. & Yousef S., (2006) "A New Authentication Protocol for UMTS Mobile Networks", EURASIP Journal on wireless communications and networking, Vol. 2006, pp1-10.
2. Putz S., Schmitz R., Tonsing F., (1998) "Authentication Schemes for Third Generation. Mobile Radio Systems", Personal, Indoor and Mobile Radio Communication., The 9th IEEE International Symposium on Personal, vol. 1, Page(s): 126-130
3. Al-Saraireh J. & Yousef S., (2007) "Analytical Model: Authentication Transmission Overhead between Entities in Mobile Networks", Elsevier, Computer Communications Journal, Vol. 30, No. 9, pp1713-1720.
4. Al-Saraireh J., (2011) "Efficient and Secure Authentication and Key Agreement Protocol", International Journal of UbiCom (IJU), Vol. 2, No. 2.
5. 3GPP TS 33.102 V8.0.0, (2008) "3GPP Technical Specification Group Services and System Aspects, 3G Security, Security Architecture (Release 8)", 3rd Generation Partnership Project.
6. Juang W.S. & Wu J.L., (2007) "Efficient 3GPP Authentication and Key Agreement with Robust User Privacy Protection", IEEE Communications Society, Proceedings of the WCNC.
7. Farhat F., Salimi S. & Salahi A., (2009) "An Extended Authentication and Key Agreement Protocol of UMTS", Information Security Practice and Experience, Lecture Notes in Computer Science, Vol. 5451/2009, pp230-244, DOI: 10.1007/978-3-642-00843-6_21
8. Min-Shiang H., Song-Kong C. & Hsia-Hung O., (2010) "On the security of an enhanced UMTS authentication and key agreement protocol", European Transactions on Telecommunications. DOI: 10.1002/ett.1460
9. Harn L. & Hsin W., (2003) "On the security of wireless network access with enhancements", in Proceedings of the 2003 ACM workshop on Wireless security, San Diego, USA, Sep. 19 2003, pp88–95.
10. Huang C. & Li J., (2005) "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption", AINA2005, 19th International Conference on Advanced Information Networking and Applications (AINA'05), Vol. 1, pp392-397.
11. Adi W., Dawood A., Mabrouk A. & Musa S., (2007) "Low complexity image authentication for mobile applications", IEEE South East Conference, Richmond, USA. pp20-20.
12. Daeyoung K., Younggang C., Sangjin K. & Heekuck O., (2007) "A Privacy Protecting UMTS AKA Protocol Providing Perfect Forward Secrecy",Computational Science and Its Applications – ICCSA 2007, Lecture Notes in Computer Science, Vol. 4706/2007, pp. 987-995, DOI: 10.1007/978-3-540-74477-1_88
13. Zhang M. & Fang Y., (2005) "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol", IEEE Transactions on wireless communications, Vol. 4, No. 2, pp734–742.
14. Lin Y & Chen Y., (2003) "Reducing Authentication Signaling Traffic in Third-Generation Mobile Network", IEEE Transactions on Wireless Communications, Vol. 2, No. 3, pp493-501.
15. Huang Y., Shen Y., Shieh S., Wang H. & Lin C., (2009)"Provable Secure AKA Scheme with Reliable Key Delegation in UMTS", Secure Software Integration and Reliability Improvement, 2009. SSIRI 2009. Third IEEE International Conference, Vol. 2009, pp243-252.
16. Li H., Guo S., Zheng K., Chen Z. & Cui J., (2009) "Improved Adoptable Scheme for Authentication and Key Agreement", IEEE International Conference on Management and Service Science (MASS 2009), pp. 1-4, print ISBN: 978-1-14244-4638-4, DOI: 10.1109/ICMSS.2009.5301997
17. Mohan S., and Jain R. (1994), "Two User Location Strategies for Personal Communication Services", IEEE Personal Communications, vol. 1, no. 1, Page(s): pp 42-50.
18. Skehill R., and McGrath S. (2004), "PCS location area optimisation using an aggregate mobility model", 15th IEEE International Personal, Indoor and Mobile Radio Communications (PIMRC 2004), vol. 3, Page(s): 2212-2217.
19. Porta T.F., Veeraraghavan M., and Buskens R.W., (1996) "Comparison of signaling loads for PCS systems", IEEE/ACM Transactions on Networking, vol. 4, no. 6, Page(s): 840-856.

Ja'afer AL-Saraireh received the BSc degree in computer science from Mu'tah University, Karak, Jordan, in 1994. He received the MSc degree in computer science from University of Jordan, Amman, Jordan, in 2002. Since 2002 he has been member in the computer engineering department. He received PhD degree in computer science from Anglia Ruskin University, UK, in 2007. His research interests include mobile, wireless network security and database. He is currently working as assistant professor in computer science at applied science university, Jordan.

3/5/2011