Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2006, Article ID 98107, Pages 1–10
DOI 10.1155/WCN/2006/98107

A New Authentication Protocol for UMTS Mobile Networks

Ja'afer Al-Saraireh and Sufian Yousef

Faculty of Science and Technology, Anglia Ruskin University, Bishop Hall Lane, Chelmsford CM1 1SQ, UK

Received 28 November 2005; Revised 7 July 2006; Accepted 16 August 2006

Recommended for Publication by Kamesh Namuduri

This paper analyzes the authentication and key agreement (AKA) protocol for universal mobile telecommunications system (UMTS) mobile networks, where a new protocol is proposed. In our proposed protocol, the mobile station is responsible for generating of authentication token (AUTN) and random number (RAND). The home location register is responsible for comparison of response and expected response to take a decision. Therefore, the bottleneck at authentication center is avoided by reducing the number of messages between mobile and authentication center. The authentication time delay, call setup time, and signalling traffic are minimized in the proposed protocol. A fluid mobility model is used to investigate the performance of signalling traffic and load transaction messages between mobile database, 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 to current protocol. Therefore, the performance and the authentication delay time have been improved significantly.

1. INTRODUCTION

In order to provide security services in wireless networks, authentication is used as an initial process to authorize a mobile terminal for communication through secret credentials [1]. In authentication process, a mobile terminal is required to submit secret materials such as certificate or "challenge and response" values for verification [2]. Without strong authentication, mobile networks access is unprotected through the release of message contents, and modification of message or denial of service can be accomplished easily by an intruder.

There are different approaches done to enhance UMTS authentication mechanisms, there are four approaches being discussed in Europe [3]. The 1st scheme is proposed by Royal Holloway College. This protocol is a symmetric scheme, it works with a challenge response mechanism and it 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 the protocol that was developed by Siemens as far as the message flow and the mechanism of key exchange are 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.

In this paper, analysis model is used to investigate the performance of signalling traffic, load, and bandwidth that are generated by these protocols as well as the delay in the call setup time. Also, a new protocol is proposed to improve the performance of authentication by reducing the authentication times and signalling messages.

This paper is organized as follows. Section 2 specifies and describes the AKA protocol in 3G. In Section 3, the UMTS authentication protocol is analyzed. A proposed authentication protocol for UMTS mobile networks is described in Section 4. The traffic load in the proposed

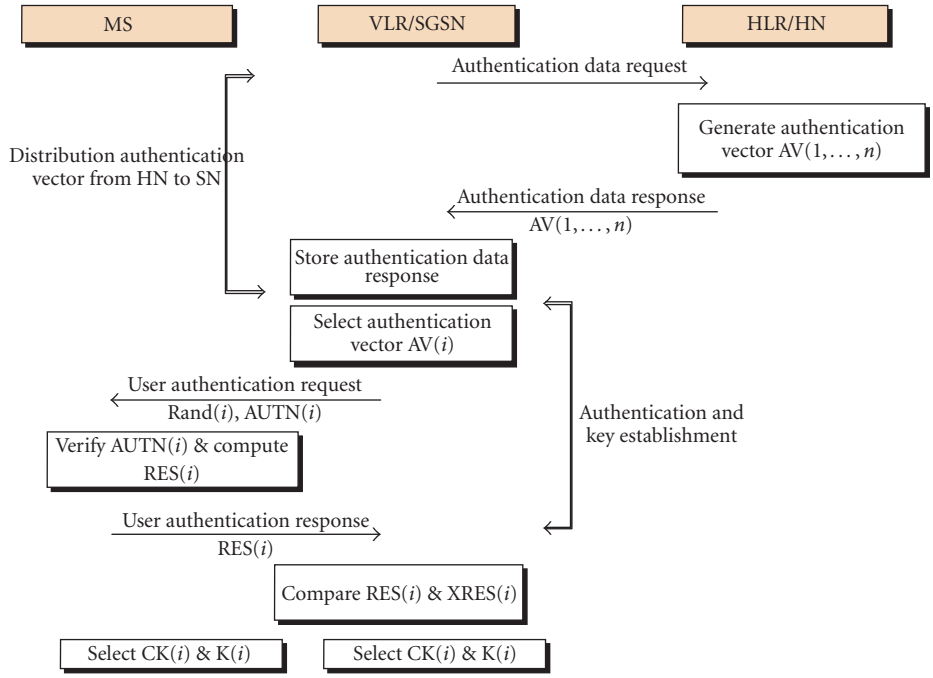

Figure 1: Authentications and key agreement protocol.

authentication protocol is analyzed in Section 5. In Section 6, simulation results, comparison, and discussion between the two protocols are presented. The paper is concluded in Section 7.

2. UMTS AUTHENTICATION PROTOCOL

In UMTS, three components participate in authentication.

(1) Mobile station (*MS*) and UMTS subscriber identity module (*USIM*).
(2) Base station (*BS*), mobile switching center (*MSC*), and visitor location register (*VLR*).
(3) Authentication center (*AuC*) and home location register (*HLR*).

This authentication protocol is using secret key K and cryptographic algorithms—including three message authentication codes f_1, f_1^*, and f_2 and four key generation functions f_3, f_4, f_5, and f_5^* [4–7] that are shared between *MS* and the *HLR/AuC*. This is known as authentication and key agreement protocol (*AKA*); also the *AuC* maintains a counter called sequence number (SQN_HLR), and user mobile station maintains a counter (SQN_{MS}), the initial value for these counters are set to zeroes [7–9].

There are three goals for the UMTS AKA [10]:

(1) the mutual authentication between the user and the network;
(2) the establishment of a cipher key and an integrity key upon successful authentication; and
(3) the freshness assurance to the user of the established cipher and integrity keys.

There are two phases in AKA protocol [11]:

(1) the distribution of authentication vectors from the *HLR/AuC* to the *VLR/MSC*;
(2) the authentication and key agreement procedure between the *MS* and the *VLR*.

As illustrated in Figure 1, UMTS authentication procedure works as follows.

(1) *MS* sends international mobile subscriber identity *(IMSI)* and authentication request to (*VLR/SGSN*) (visitor location register/serving GPRS support node).
(2) *VLR* passes this authentication request to *HLR*.
(3) *HLR* Generates authentication vectors $AV(1,\ldots,n)$ and sends the authentication data response $AV(1,\ldots,n)$ to *VLR/SGSN*. Each authentication vector is called a quintet. This *AV* consists of five components: the random number (*RAND*), the expected response (*XRES*), cipher key (*CK*), integrity key (*IK*) and authentication token (*AUTN*). The authentication vectors are ordered by the sequence number.
(4) *VLR* stores authentication vectors, selects authentication vector *AV(i)*, and sends authentication request (*RAND (i), AUTN(i)*) to *MS*. In the *VLR* one authentication vector is needed for each authentication instance. This means that the signalling between *VLR* and *HLR/AuC* is not needed for every authentication event.
(5) *MS* computes and retrieves the following:
    (a) $AK = F5\,(Rand, K)$, $SQN = ((SQN \oplus AK) \oplus AK)$, computes expected message authentication code $XMAC = f_1\,(SQN, RAND, AMF)$, and then

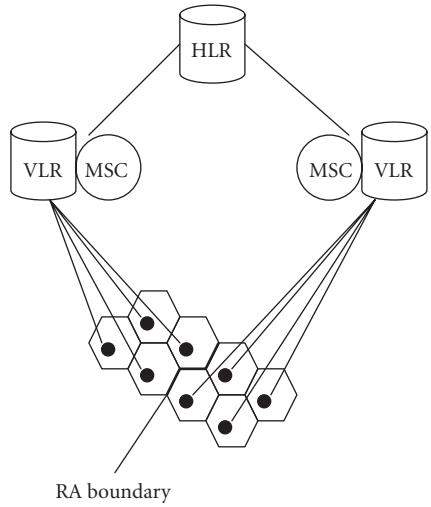

Figure 2: Location registration areas.

(b) compares *XMAC* with *MAC* which is included in *AUTN*. If *XMAC* is not equal to *MAC*, then *MS* sends failure message to the *VLR/SGSN*, else if *XMAC* is equal to *MAC*, then *MS* checks that the received *SQN* is in the correct range, that is, $SQN > SQN_{MS}$. If *SQN* is not in correct range, then *MS* sends failure message to the *VLR/SGSN*, else if it is in the correct range, then *MS* computes the Response $RES = f_2\ (K, RAND)$, and $CK = f_3\ (K, Rand)$, after that it sends *RES* to *VLR/SGSN*.

(6) *VLR* compares the received *RES* with *XRES*. If they match, then authentication is successfully completed.

3. ANALYSIS OF UMTS AUTHENTICATION PROTOCOL

The mobile station is continuously listening to the broadcast message from MSC/VLR to identify the location area by using location area identity (LAI), the MS is comparing the LAI which is received with the LAI stored in the USIM. When the LAI is different then the MS requires a new registration. Figure 2 illustrates registration area boundary.

The registration occurs when the mobile is switched on, or when it has moved from one registration area to a new one. Movement of MS within the same registration area will not generate any registration messages. The authentication processes is done in every registration, call originating, and call terminating. Figure 3 illustrates the signalling messages flow for registration activity. Figure 4 illustrates the signalling message flow for call origination and termination.

In our analysis, a fluid mobility model is used to investigate and analyze the performance of signalling traffic, load, and bandwidth that are generated by these protocols and the delay in the call setup time. In this model, we have the following parameters:

(1) user who is carrying mobile station (*MS*) is moving at an average velocity v;

(2) direction of *MS* movement is uniformly distributed over $[0, 2\pi]$;

(3) mobile users are uniformly populated with the density ρ within the registration area;

(4) registration area (*RA*) boundary is of length L.

Then the rate of registration area crossing R, the average number of active mobile crossing the registration area, is given by

$$R = \frac{\rho \cdot v \cdot L}{\pi}. \tag{1}$$

From (1), we can calculate the signalling traffic for registration, origination, and termination call. Mobile traffic of network depends on the *MS* user's movement. Table 1 summarizes assumptions which are made to perform numerical analysis.

The traffic due to authentication request at registration is generated by mobile moving into new registration area, this equals the number of deregistration (registration cancellations). The rate of registration area crossing R is given by

$$\begin{aligned} R_{\text{registration},RA} &= \frac{\rho \cdot v \cdot L}{\pi}, \\ R_{\text{registration},RA} &= \frac{328 * 5.95 * 32.45}{1\,\text{h} * 60\,\text{min} * 6\,\text{s} * \pi} = 5.60\,/\text{s}. \end{aligned} \tag{2}$$

The rate of deregistration area crossing R is equivalent to the rate of registration

$$R_{\text{Deregistration},RA} = 5.60\,/\text{s}. \tag{3}$$

The total number of authentication request message per second that arrives at the *HLR* is

$$\begin{aligned} &R_{\text{registration},HLR} \\ &\quad = R_{\text{registration},RA} * \text{Total number of registration area}, \\ &R_{\text{registration},HLR} = 5.60 * 128 = 716.8\,/\text{s}. \end{aligned} \tag{4}$$

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 ($R_{\text{Call orignation}/SN}$) is calculated as follows:

$$\begin{aligned} &R_{\text{call origination}/SN} \\ &\quad = \text{call rate per user} \\ &\quad = \text{average call origination rate} * \text{total of MS}, \\ &R_{\text{call origination}/SN} = \frac{2 * 3.5\ \text{million}}{1\,\text{h} * 60\,\text{min} * 60\,\text{s}} = 1944.4\,/\text{s}. \end{aligned} \tag{5}$$

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

The number of calls origination per registration area ($R_{\text{Call orignation}/RA}$) is calculated as follows:

$$\begin{aligned} R_{\text{Call orignation}/RA} &= \frac{R_{\text{Call orignation}/SN}}{\text{Total registartion area}}, \\ R_{\text{Call orignation}/RA} &= \frac{1944.4}{128} = 15.19\,/\text{s}. \end{aligned} \tag{6}$$

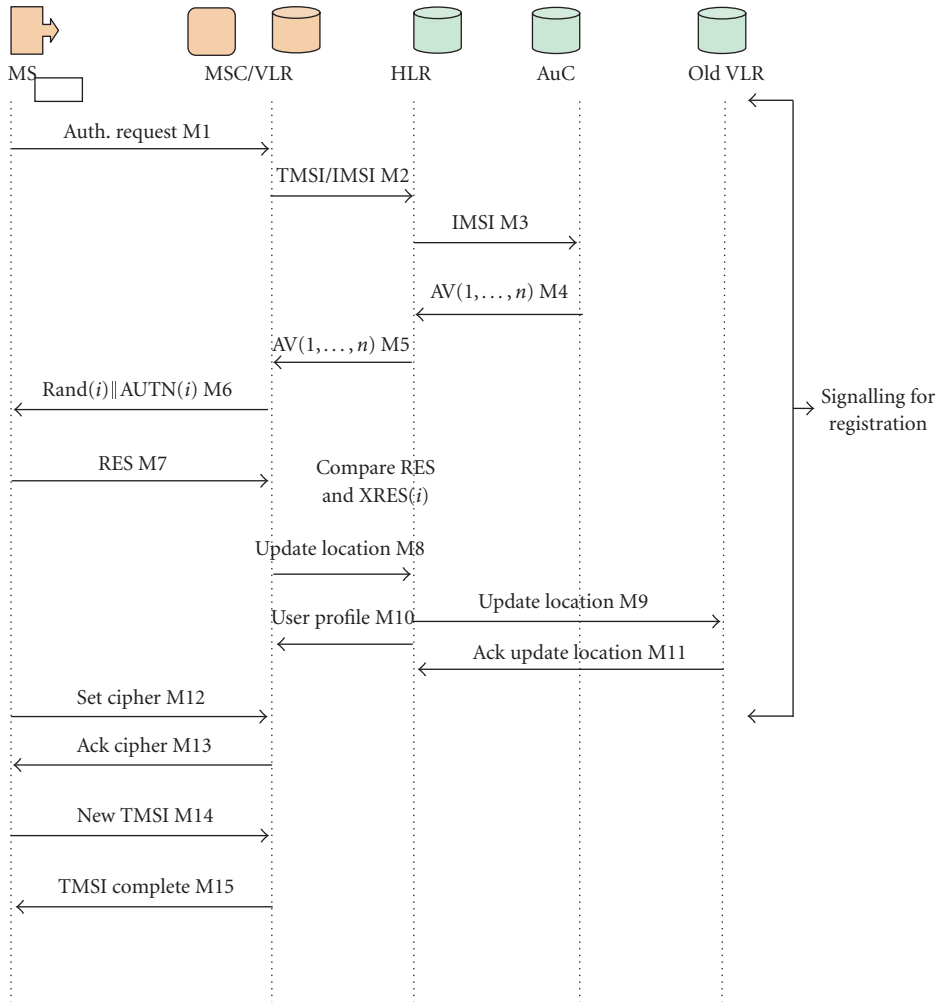

Figure 3: UMTS signalling messages flow for registration.

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

Table 2 summarizes the total authentication requests per VLR and HLR for each type of activity as computed above. From Figures 3 and **??**fig:4 it can be summarized that the signalling messages flow for each activity registration, call origination, and call termination as shown in Table 3. The total signalling traffic and load The transaction messages between mobile databases (VLR and HLR) are shown in Table 4 which are calculated from the values in Tables 2 and 3.

From the above equations and calculations, it has been found that the relationships between velocity of movement of users and the total authentication requests per VLR and HLR for UMTS authentication process is directly proportional, and the relationship between the registration area and total authentication requests per VLR and HLR for UMTS registration process is directly proportional.

The authentication delay is the time between the MS starting to create a registration request until the completion of the registration after the last successful signature verification by the mobile node. Assume that the authentication time delay is T_{Auth} and the time delay to access VLR database is the same as to access HLR database, and let this time be T_{DB} and let the time between MS and MSC be $T_{MS\text{-}MSC}$. From Figure 3, it can be seen that there are four messages between databases (M2, M3, M4, and M5), and three messages between MS and VLR/MSC (M1, M6, and M7). Then T_{Auth} can be computed as follows:

$$T_{\text{Auth}} = 4 * T_{DB} + 3 * T_{MS\text{-}MSC}. \tag{7}$$

Table 5 has the authentication parameters that enable us to compute the bandwidth for each activity.

The size of messages between *MS* and *VLR/MSC* can be calculated as follows.

(i) M1 is the 1st message which contains the parameters *IMS/TMSI*, *Service Request*, and *LAI*, the length (L) of M1, $LM1 = L(IMSI/TMS) + \text{L}(Service\ Request) + L(LAI)$,

$$\text{LM1} = 128 + 8 + 40 = 176\,\text{bits}. \tag{8}$$

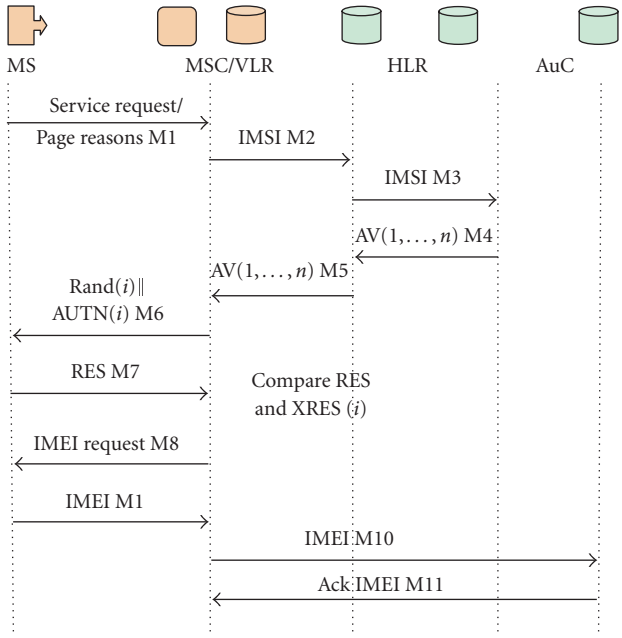

Figure 4: UMTS call origination/termination signalling messages flow.

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 /h/user
Average call termination rate	2 /h/user
Average speed of user who is carrying mobile, v	5.95 km/h

Table 2: Total authentication request per VLR and HLR.

Activity	VLR/S	HLR/S	Total
Registration (*Reg.*)	5.60	716.8	722.4
Call termination (*Term.*)	15.19	1944.4	1959.59
Call origination (*Orig.*)	15.19	1944.4	1959.59
Total/network	35.98	4605.6	4641.58

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

AuC	HLR	VLR	Old VLR	Total
2	4	5	1	12
2	4	5	0	11
2	4	5	0	11
6	12	15	1	—

Table 4: Total Signalling traffic and load transaction messages per second for each activity in UMTS entity.

Activity	AuC	HLR	VLR	Old VLR	Total
Registration	1433.60	2867.20	28.00	5.60	4334.4
Call termination	3888.8	7777.6	75.95	0	11742.35
Call origination	3888.8	7777.6	75.95	0	11742.35
Total	9211.2	18422.4	179.9	5.60	—

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 records in authentication vector K	5
Location area identifier *LAI*	40
Service request	8

(ii) M6 is the sixth message which contains the parameters *Rand* and *AUTN*, where

$$AUTN = (SQN \oplus AK \| AMF \| MAC), \tag{9}$$

and the length of $AUTN = \max[L(SQN), L(AK)] + L(AMF) + L(MAC)$,

$$\begin{aligned} L(AUTN) &= 48 + 16 + 64 = 128\,\text{bits}. \\ L(\text{M6}) &= L(\text{Rand}) + L(AUTN) \\ &= 128 + 128 = 256\,\text{bits}. \end{aligned} \tag{10}$$

(iii) M7 is the seventh message which contains only *Res*. $L(M7) = L(Res) = 32$ bits.

The size of the authentication messages between *MS* and *VLR/MSC* is calculated as follows:

$$\begin{aligned} (\text{L}_{MS\text{-}MSC}) &= \text{L(M1)} + \text{L(M6)} + \text{Lm(7)} \\ &= 464\ \text{bits} = 58\ \text{bytes}. \end{aligned} \tag{11}$$

The size of messages between databases can be calculated as follows.

(i) M2 is the 2nd message which contains the parameters *IMS/TMSI*, *Service Request*, and *LAI*; the length of M2 is equal to the length of $M1 = 176$ bits.

(ii) M3 is the 3rd message which contains the same parameters as M2 the L(M3)= 176.

Table 6: Bandwidth that is used between entities for current protocol.

Activity	Bandwidth between MS and VLR/MSC (B/S)	Bandwidth between databases (B/S)	Total
Registration	324.8	2531.2	2856
Call *Orig./Term.*	881.02	6865.88	7746.9
Total/network	1205.82	9397.08	10602.9

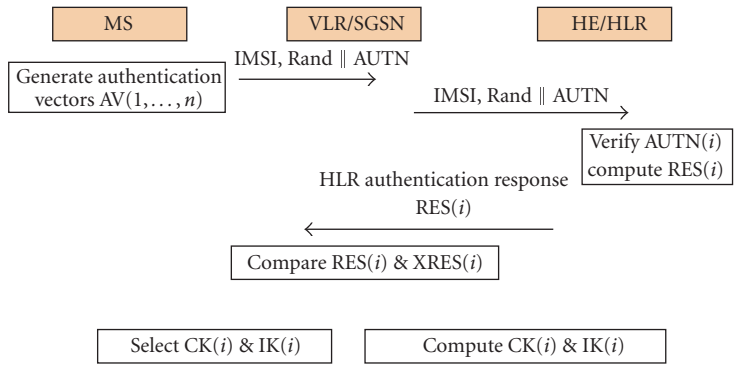

Figure 5: The proposed authentications and key agreement protocol.

(iii) M4 is the 4th message which contains only *AV*. The length of each *AV* is

$$L(AV) = L(Rand) + L(XRes) + L(CK) + L(IK) + L(AUTN) = 128 + 32 + 128 + 128 + 128 = 544 \text{ bits}. \quad (12)$$

For each AV generated from *AuC* that contains 5 records, the total size is

$$L(AV) = 5 * 544 = 3072 \text{ bits}. \quad (13)$$

The size of authentication messages between databases is calculated as follows:

$$(L_{DB}) = 176 + 176 + 2720 = 3616 \text{ bits} = 452 \text{ bytes}. \quad (14)$$

The total size of messages in the authentication process is $L_{Auth} = 464 + 3616 = 4080$ bits $= 510$ 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 6 summarizes the bandwidth used between MS and VLR/MSC and between databases.

4. THE PROPOSED AUTHENTICATION PROTOCOL FOR UMTS MOBILE NETWORKS

The secret key K, the cryptographic algorithms f_1, f_1^*, and f_2, and the four key generation functions f_3, f_4, f_5, *and* f_5^* are shared between *MS* and the *HLR/AuC*. The proposed protocol here works as follows.

(1) *MS* generates authentication vector $AV(1,\ldots,n)$ and sends *IMSI, RAND*, and *AUTN* as authentication request to *VLR/SGSN*.
(2) *VLR* passes this authentication request to *HLR*.
(3) *HLR* computes and retrieves the following:
   (a) $AK = F5(Rand, K)$, $SQN = ((SQN \oplus AK) \oplus AK)$, and the expected message authentication code $XMAC = f_1(SQN, RAND, AMF)$;
   (b) compares *XMAC* with *MAC* which is included in *AUTN*. If *XMAC* is not equal to *MAC* then *HLR* sends failure message to the *VLR/SGSN*, else if *XMAC* equals *MAC*, then *HLR* checks that the received *SQN* is in the correct range, that is, $SQN > SQN_{HLR}$. If *SQN* is not in the correct range, then *HLR* sends failure message to the *VLR/SGSN*, else if it is in the correct range, then *HLR* computes response $RES = f_2(K, RAND)$, and $CK = f_3(K,Rand)$, after that it sends *RES* to *VLR/SGSN*.
(4) *VLR* compares the received *RES* with *XRES*. If they match, then authentication is successfully completed.

Figure 5 illustrates the proposed UMTS authentication protocol.

5. ANALYSIS OF THE PROPOSED AUTHENTICATION PROTOCOL

From Figure 6, we can summarize the signalling messages per authentication for each activity registration, call origination, and call termination as illustrated in Table 7. The total signalling traffic and load transaction messages between mobile

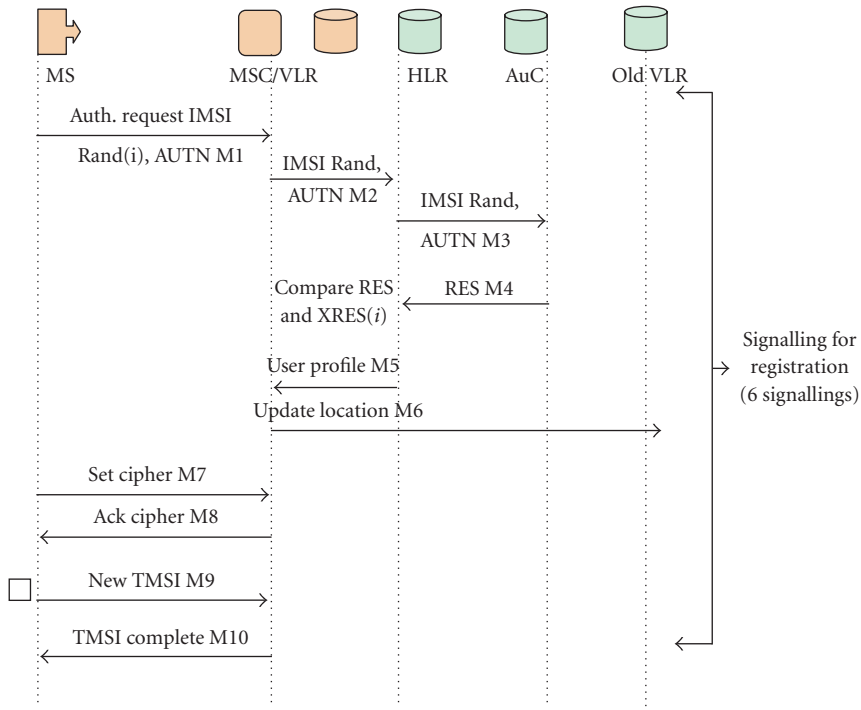

Figure 6: Signalling messages flow for the proposed authentications protocol.

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

Activity	AuC	HLR	VLR	Old VLR	Total
Regist.	1	2	2	1	6
Call Term.	1	2	2	0	5
Call Orig.	1	2	2	0	5
Total	3	6	6	1	—

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

AuC	HLR	VLR	Old VLR	Total
716.8	1433.6	11.2	5.60	2161.6
1944.4	3888.8	30.38	0	5863.58
1944.4	3888.8	30.38	0	5863.58
4605.6	9211.2	71.96	5.60	—

databases (VLR and HLR) are shown in Table 8 and are calculated from the values in Tables 2 and 7.

The authentication delay for the proposed protocol T_{Auth} is computed as follows:

$$T_{\text{Auth}} = 3 * T_{DB} + 1 * T_{MS\text{-}MSC}. \tag{15}$$

To compute the bandwidth, there are four messages to authentication; one of them is between *MS* and *VLR/MSC* and the other three are between databases, the sizes of these messages can be computed as follows.

The size of messages between MS and VLR/MSC can be calculated as follows.

(i) M1 is the 1st message which contains the parameters *IMS/TMSI*, *Service request*, *LAI*, *Rand*, and *AUTN*, the length (L) of M1,

$$\begin{aligned} LM1 &= \text{L}(IMSI/TMS) + \text{L}(Servicerequest) \\ &\quad + \text{L}(LAI) + \text{L}(Rand) + \text{L}(AUTN), \\ LM1 &= 128 + 8 + 40 + 128 + 128 = 432\,\text{bits}. \end{aligned} \tag{16}$$

The size of the authentication messages between *MS* and *VLR/MSC* is calculated as follows:

$$(\text{L}_{MS\text{-}MSC}) = 432\,\text{bits} = 54\,\text{bytes}. \tag{17}$$

The size of messages between databases can be calculated as follows.

(i) M2 is the 2nd message in which the length of M2 is equivalent to the length of M1 = 432 bits.
(ii) M3 is the 3rd message which contains the same parameters as *M*2 the L(M3) = 432 bits.
(iii) M4 is the 4th message which contains only *RES*, where the length M4 = 32 bits.

The size of authentication messages between databases is calculated as follows.

$$(\text{L}_{DB}) = 432 + 432 + 32 = 896\,\text{bits} = 112\,\text{bytes}. \tag{18}$$

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

Activity	Bandwidth between MS and VLR/MSC (B/S)	Bandwidth between databases (B/S)	Total
Registration	302.4	627.2	929.6
Call Orig./Term.	820.26	1701.28	2521.54
Total/network	1122.66	2328.48	3451.14

Table 10: Comparing signalling messages between the current and the proposed authentication protocol.

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

Table 11: Comparing 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
Registration	1433.6	2867.2	28	5	716.8	1433.6	11.2	5.6
Call Term./Orig	3888.8	7777.6	75.95	0	4876.19	3888.8	30.38	0

The total size of messages in the authentication process is $L_{Auth} = 54 + 112 = 166$ 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 summarizes the bandwidth used between MS and VLR/MSC and between databases.

6. SIMULATION RESULTS (COMPARISON AND DISCUSSION)

The simulation study has been carried out in order to analyze signalling traffic performance and load transaction messages and bandwidth that is consumed between mobile networks entities. The simulation is carried out by using different mobility rate.

The software we have 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 written in C++ and OTcl.

The proposed authentication protocol preserved the same security as such as the security available in the current UMTS. The authentication and privacy are preserved. The MS is still authenticated using the secret key and the authentication result is computed first in the mobile SIM card then it is sent to the AuC for verification and validation.

In the proposed protocol, the signalling messages are reduced between the mobile networks entities. Tables 10, 11, 12, and 13 illustrates the differences between current UMTS authentication protocol and the proposed protocol. The current protocol needs 12 messages between mobile networks entities to perform registration or call termination, but the proposed protocol needs 6 messages only to perform registration or 5 messages for call termination.

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

Entity	Current protocol	Proposed protocol	% improvement
AuC	9211.2	4605.6	50
HLR	18422.4	9211.2	50
VLR	179.9	71.96	40
Total	27813.5	23171.56	50

The simulation results show that the authentication delay and current load transaction messages between entities and bandwidth are minimized comparing to current protocol, as illustrated in Figures 7, 8, 9, 10, and 11. Therefore, the performance and the authentication delay time have been improved significantly.

As shown in Table 12—which is extracted from Tables 4 and 8—the percentage of improvement is more than 50%. From (7) and (15), where it is assumed that TDB = 1, the proposed protocol has less delay than the current UMTS protocol as shown in Figure 7.

Varying the MS mobility rate (the speed of movement), it can be seen in Table 14 that the proposed scheme is maintaining the same level of improvement in terms of total network signalling which is around 50 percent compared to the conventional UMTS approach.

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

	Bandwidth between MS and VLR and between databases					
	Current protocol			Proposed protocol		
Activity	VLR/MSC	Database	Total	VLR/MSC	Database	Total
Registration	324.8	2531.2	2856	302.4	627.2	929.6
Call Term./Orig	881.02	6865.88	7746.9	820.26	1701.28	2521.54

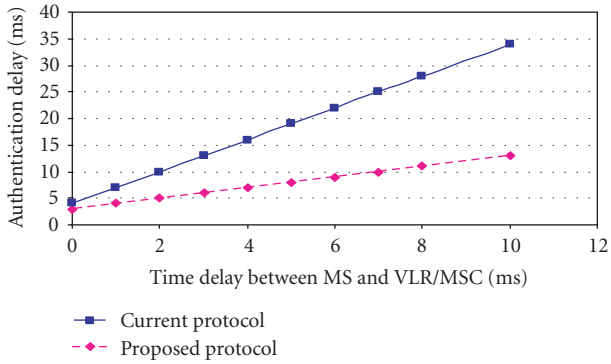

Figure 7: Authentication delay.

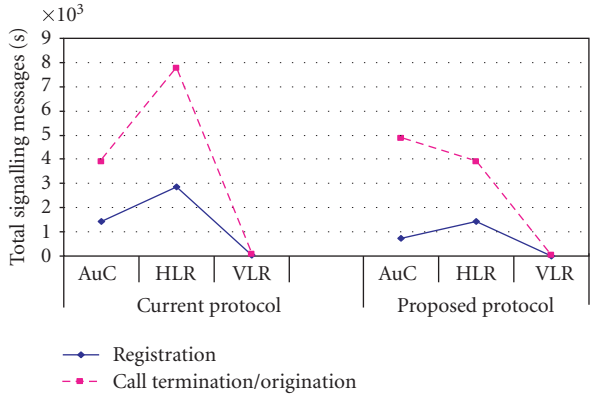

Figure 8: Load transaction messages per second between entities.

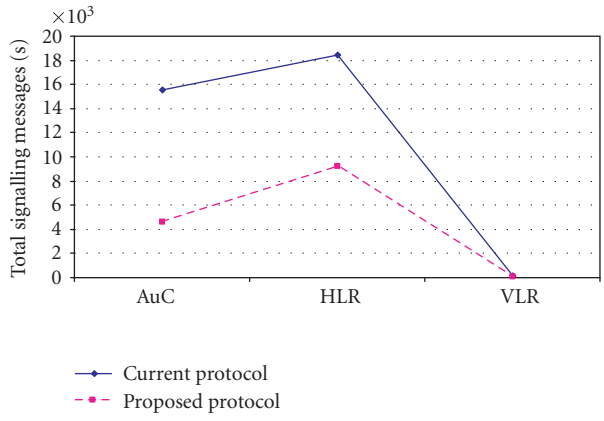

Figure 9: Total signalling messages/second for all activity in current and proposed protocol.

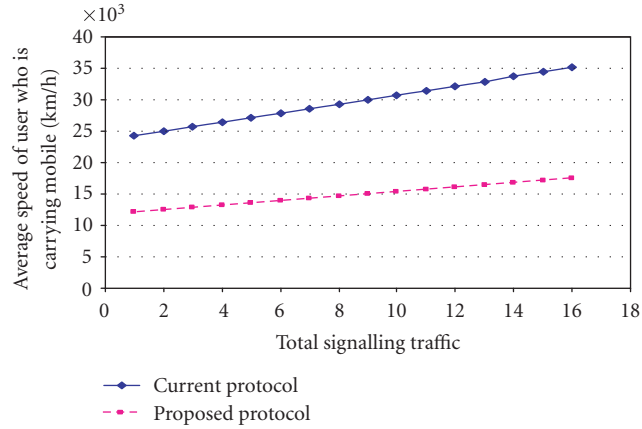

Figure 10: Network signalling traffic with different mobility rate.

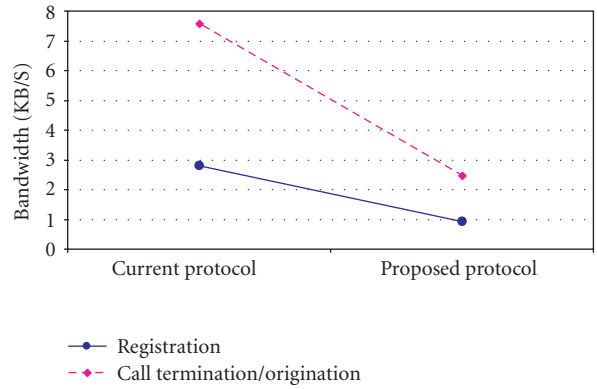

Figure 11: Comparing the bandwidth for each activity between current and proposed protocol.

The advantage of the proposed scheme is the structure itself which is a very important issue in this analysis study. In the current UMTS AKA, the challenge response is based on challenging the MS after preparing the authentication vector in the AuC. Then the VLR has to send the RAND number to the MS and waits for the response (SRES), and upon comparison the authentication decision is taken. Our design concept is based on the general form of the authentication definition. The proposed protocol starts from preparing the authentication result in the MS, then sending it to the AuC for verification and validation in three messages only. Deregistration of the old VLR in the proposed protocol is faster than the current UMTS authentication protocol, which is vital in decreasing the total delay.

Table 14: Network signalling traffic with different mobility rate.

		Current protocol				Proposed protocol			
Speed	Rate	AuC	HLR	VLR	Total	AuC	HLR	VLR	Total
2	1.88	8259.06	16518.12	161.32	24938.50	4129.53	8259.06	64.53	12453.12
4.5	4.24	8863.22	17726.44	173.09	26762.75	4431.61	8863.22	69.23	13364.06
5.95	5.6	9211.38	18422.76	179.91	27814.65	4605.6	9211.2	71.96	13889.03
10	9.42	10189.30	203786	198.98	30766.88	5094.65	10189.3	79.59	15363.54
14	13.18	11151.86	2303.72	217.81	33673.39	5575.93	11151.86	87.12	16814

7. CONCLUSION

In this paper, the UMTS authentication and key agreement protocol and the signalling traffic that are generated by registration, call termination, and call origination have been investigated and analyzed as well as the bandwidth that is used between MS and VLR and between databases registers. The proposed authentication protocol has improved the performance of authentication by reducing the authentication times, setup time, and data sizes. Also, the proposed authentication mechanism has less signalling traffic and consequently, the bottleneck at authentication center is avoided significantly by reducing the number of messages between mobile and authentication center. The proposed protocol is tight for security, because no data-authentication vector (AV) is stored in VLR/MSC and the AV is generated in the mobile for each authentication request.

The proposed authentication for UMTS has been generated while keeping in mind that the complexity of this function is as low as possible while keeping a high level of security and efficiency of the used bandwidth.

REFERENCES

[1] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "Efficient authentication and key distribution in wireless IP networks," *IEEE Personal Communication on Wireless Communication*, vol. 10, no. 6, pp. 52–61, 2003.

[2] P. R. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," April 2005.

[3] S. Putz, R. Schmitz, and F. Tonsing, "Authentication schemes for third generation mobile radio systems," in *Proceedings of the 9th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 1, pp. 126–130, Boston, Mass, USA, September 1998.

[4] 3GPP TS 35.205. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 1: General.

[5] 3GPP TS 35.206. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 2: Algorithm specification.

[6] 3GPP TS 35.207. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 3: Implementors test data.

[7] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Transactions on Wireless Communications*, vol. 4, no. 2, pp. 734–742, 2005.

[8] 3GPP TS 21.133. 3GPP Security; Security Architecture.

[9] J. Al-Saraireh, S. Yousef, and M. Al Nabhan, "Analysis and enhancement of authentication algorithms in mobile networks," *Journal of Applied Sciences*, vol. 6, no. 4, pp. 872–877, 2006.

[10] J. AL-Saraireh and S. Yousef, "Authentication transmission overhead between entities in mobile networks," *International Journal of Computer Science and Network Security*, vol. 6, no. 3B, 2006.

[11] J. AL-Saraireh and S. Yousef, "A new authentication protocol for GSM and UMT networks," in *Proceedings of the 17th IASTED International Conference on Modeling and Simulation (MS '06)*, Montreal, Canada, May 2006.

Ja'afer AL-Saraireh received the B.S. degree in computer science from Mu'tah University, Karak, Jordan, in 1994. He received the M.S. degree in computer science from the University of Jordan, Amman, Jordan, in 2002. Since 2002, he has a been Member in the Computer Engineering Department. He is currently a Ph.D. student in the Faculty of Science and Technology at Anglia Ruskin University, UK. His research interests include mobile, wireless network security and database.

Sufian Yousef received his B.S. degree from Baghdad University, Engineering College, in 1977 and his M.S. degree in telecommunication systems management in 1994 from Anglia Ruskin University (ARU). He started his research activities at ARU during his Ph.D. research studies in modeling and simulation of asynchronous transfer mode (ATM), where he modeled the busty arrivals of heterogeneous sources using a 4-phase MMPP model. He was appointed as a Research Fellow in 1998 and then as Senior Lecturer at ARU. Currently, he is the Head of the Telecommunication Engineering Research Group (TERG). The main interest of the group is wireless mobile networking simulation, protocols, security, and bandwidth management, ad hoc wireless networks, wireless LANs and MANs, wireless fading modeling and measurements, and distributed computing and databases in wireless environments.