# Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 6 (4): 872-877, 2006
ISSN 1812-5654


# Analysis and Enhancement of Authentication Algorithms in Mobile Networks

Ja'afer AL-Saraireh, Sufian Yousef and Mohammad AL Nabhan
Faculty of Science and Technology
Anglia Ruskin University
Chelmsford -UK

**Abstract:** The present reserch investigated the existing authentication mechanisms for mobile communications and analyses these mechanisms as a step to propose enhancement to authentication. Specifically, the authentication signalling in GSM and UMTS mobile networks is minimized and consequently the bottleneck at authentication centre is avoided, by reducing the number of messages between mobile and authentication centre (i.e., reducing the procedures of authentication) and then reducing the authentication times, setup time and data sizes. The replay attacks and guessing attack are infeasible because the subscriber uses different key to request for authentication.

**Key words:** Mobile communication, authentication, UMTS, authentication center, security

## INTRODUCTION

First generation analogue phones were susceptible to user traffic eavesdropping and cloning. Against this background, 2nd generation system such as GSM were developed. GSM was introduce integrated cryptographic mechanisms for authentication and confidentially. These mechanisms have provided good protection against user traffic eavesdropping. But suffers from security problems such as weak authentication and encryption algorithms, short secret key length (only 32 bits) with no network authentication. This could lead to false base station attack and lack of data integrity, allowing denial of service attacks.

Third generation (3G) mobile systems such as UMTS was built on the success of GSM and other 2nd generation system by introducing new and enhanced security features that are designed to stop threats (William, 2004; Mark, 2002). These include: Mutual Authentication which allows the mobile user and serving network to authenticate each other.

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 (Salgarelli *et al*., 2003).

There are different approaches done to enhance authentication mechanisms. The 1st proposed authentication protocol for GSM network (named the KAY protocol) and it can achieve less signalling traffic and better call set up time (Al-tawil *et al*., 1998). But the proposed protocol is not very secure; because it only achieves authentication between MS and HLR. Also the 2nd proposed authentication protocol which is able to reduce the network traffic, but also to reduce mobile station power consumption (Min Shing Hwang *et al*., 2000), this technique has high performance than KAY protocol, but the security is still insufficient.

Royal Holloway College proposed scheme for UMTS authentication. It uses challenge response mechanism to achieve mutual authentication between MS and network.

In this study GSM and UMTS current authentication mechanism are investigated and a new authentication mechanism for GSM and UMTS is proposed.

## GSM AUTHENTICATION MECHANISM

In GSM, the mobile stations (MS) communicate with the base station (BS) through radio link, BS are connected to the mobile switching center (MSC). For each MSC, there are home location register (HLR) stores information about users registered in this GSM network and current location of users; and the other one is the visiting location register (VLR) which stores the information for visiting users (Lin, 1999). Authentication center (AUC) is the important component in mobile networks because it contains user's secret key information and generates some random number for authentication process. Figure 1 describes GSM network structure (Ari, 2005).

**Corresponding Author:** Ja'afer AL-Saraireh, Faculty of science and Technology, Anglia Ruskin University, Chelmsford, UK
Tel: 447766454438

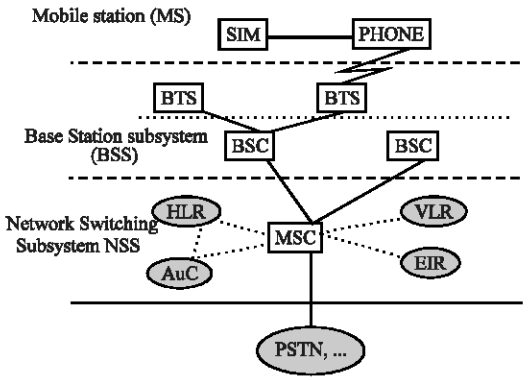


Fig. 1: GSM network structure

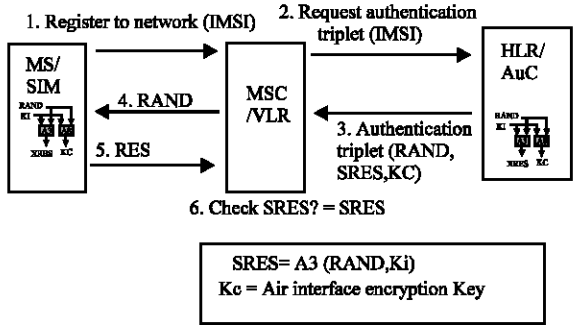


Fig. 2: Authentication in GSM network

GSM authenticate user to network, not network to user. It is based on secret key ($K_i$ 128 bits) which resides only on SIM card and in private database in AUC and used challenge response method for authentication. Figure 2 describes authentication in GSM Network (Ari, 2005).

Also in the SIM card and HLR/AuC there are hash functions known as A3 for authentication, A8 function for generated session key $K_c$ (cipher Key) and A5 function for encrypted data transfer. The following pseudo codes describe the procedure of authentication.

If initial authentication then
MS send IMSI to VLR
VLR send IMSI to AuC
AuC generate Random Number (RAND) and calculate the following:
SRES=A3(Rand, $K_i$)
$K_c$= A8(Rand, $K_i$)
AuC send $K_c$, RAND, XRES to VLR
VLR send RAND to MS
MS calculate RES=A3(Rand, Ki) and send RES to VLR
If RES = SRES then
Authentication is successful
Send Location Area Identifier ($LAI_1$), Temporary Mobile Subscriber Identity ($TMSI_{ms:1}$) to MS.
If Re-authentication with the same VLR then
MS send $LAI_1$, $TMSI_{ms:n}$ to VLR
VLR send RAND to MS
MSC send SRES to VLR
If RES = SRES then
Authentication is successful
VLR send $LAI_1$, $TMSI_{ms:n+1}$ to MS
If Re-authentication with handover to new $VLR_2$ then
MS send $LAI_1$, $TMSI_{ms:n}$ to $VLR_2$
$VLR_2$ send $LAI_1$, $TMSI_{ms:n}$ to $VLR_1$
$VLR_1$ send $TMSI_{ms:n'}$, $IMSI_{MS}$, $K_c$, RAND,SRES to $VLR_2$
$VLR_2$ send RAND to MS
MS send RES to $VLR_2$
If RES = SRES then
Authentication is successful
$VLR_2$ send $LAI_2$, $TMSI_{ms:n+1}$ to MS

In above algorithm there are two problems:

- The number of messages between MS, VLR and HLR/AuC are five messages then the signall traffic on the network could be very high and hence the authentication delay is very high.
- The challenge response message is transmitted unprotected in the signalling network and there are only authentication between MS and HLR/AuC, there is no any authentication between VLR and HLR/AuC.

Here, we will analysis authentication delay that 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. Let assume that the delay time between MS and VLR, is $DT_{MS\ to\ VLR}$ and this time equivalent to delay time between VLR and MS, delay time between VLR and HLR/AuC is $DT_{VLR\ to\ AuC}$ and it is equivalent to delay time between HLR/AuC and VLR.

The delay time for authentication can be computed as:

$$Td_{auth} = 3 * DT_{MS\ to\ VLR} + 2 * DT_{VLR\ to\ AuC}$$

## PROPOSED AUTHENTICATION MECHANISMS FOR GSM NETWORKS

The first mechanism is aimed reduce the signal traffic load on the networks, delay time for authentication, in this mechanism all component participate in the computation and provide level of security between component.

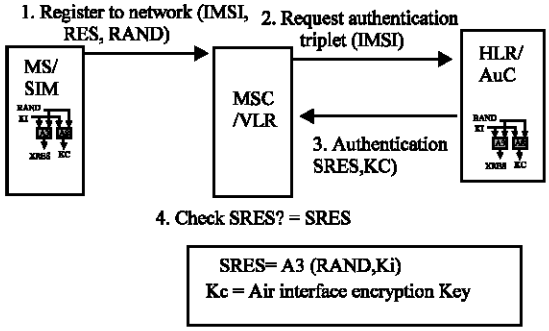


Fig. 3: Proposed authentication for GSM

Each mobile when switched on will generate RAND and then compute signed response RES = A3 (RAND, $K_i$), MS send authentication request IMSI, SRES and RAND to VLR which pass IMSI and RAND to AuC, which compute SRES and then send SRES to VLR which will compare it with the RES. If equal, then authentication is successful and else is fail. Here the numbers of messages is minimized from five to three. This will enhance the performance. Figure 3 describes the proposed authentication for GSM.

The challenge response message and all signalls transmitted between GSM components are protected by ciphering theses traffic by $K_c$ which is generated in MS, then eavesdropping is prevented.

For proposed authentication mechanisms the authentication delay can be computed as:

$$Td_{auth} = DT_{MS\ to\ VLR} + 2 * {}_{DTVLR\ to\ AuC}$$

## UMTS AUTHENTICATION MECHANISM

This mechanism using secret key K that is shared between MS and the HLR/AuC, this is known as authentication and key agreement (AKA). We will describe UMTS authentication mechanism by Fig. 4 as follow:

- MS sends IMSI with authentication request to VLR/SGSN (Visitor Location Register/Serving GPRS Support Node).
- VLR passes this authentication request to HLR.
- HLR Generates authentication vectors AV(1..n) and sends authentication data response AV(1..n) to VLR/SGSN. This AV consists of RAND, XRES (Expected Response), CK (Cipher Key), IK (Integrity Key) and AUTN (Authentication Token). The authentication vectors are ordered by the sequence number.

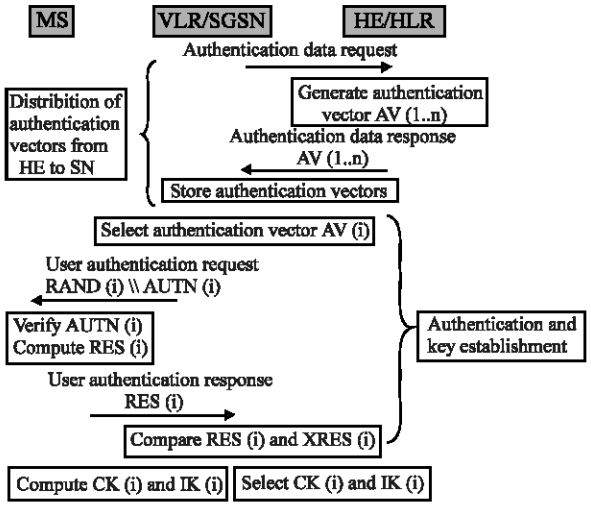


Fig. 4: Authentication and key agrement

- 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 AuC is not needed for every authentication events.
- MS computes the anonymity Key AK = F5 (Rand, K), retrieve Sequence number SQN = (SQN⊕AK) ⊕AK, computes expected message authentication code XMAC = $F_1$ (SQN, Rand, AMF authentication message field) and compares XMAC with MAC which is included in AUTN, If XMAC not equal to MAC then MS sends failure message to the VLR/SGSN, else if XMAC equal MAC then MS check that received SQN is in the correct rang. 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 Response RES = $F_2$ (K, Rand) and CK = $F_3$ (K, Rand), after that it sends RES to VLR/SGSN.
- VLR compares the received RES with XRES. If they match then authentication is successfully completed.
- Figure 4-6 describes authentication and key agreement AKA in UMTS Network (http://www.ets.org).

A mathematical function is called one-way function, which is to compute and generate authentication vector.

The main problem in UMTS is that authentication data response (i.e., uthentication vectors) is transmitted

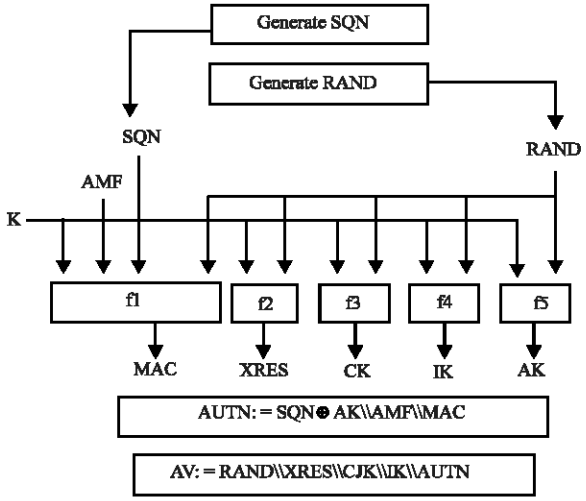


Fig. 5: Generation of athentication vector

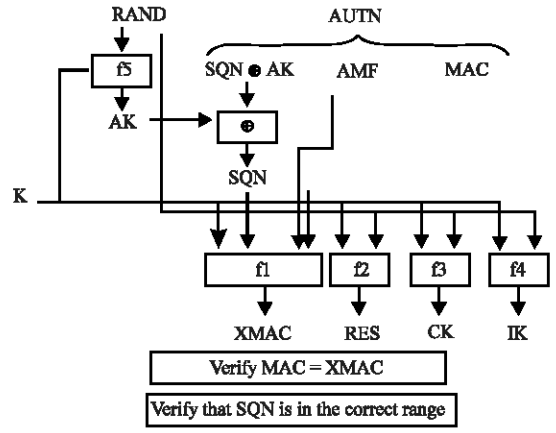


Fig. 6: User authentication function in the USIM

transmitted unprotected via the signalling network to a visited network (i.e., from HLR to VLR) that needs to check the authenticity of a mobile station. The above technique assumes trust between all network operators and the IMSI is still revealed to the visited network and can still be demanded by an attacker that impersonates a base station, as there is no network authentication in this process.

## PROPOSED AUTHENTICATION MECHANISMS FOR UMTS NETWORKS

The new UMTS authentication mechanism solves the main problem in UMTS authentication which is listed above and to enhanced security. The proposed authentication mechanism will prevent replay attacks and Guessing attacks by the key refreshment method which is supported by new authentication mechanism. This technique provides TMSI refreshment, key refreshment and authentication of MS to the VLR and VLR to the HLR and authentication of the MS to HLR.

In new this technique the MS and HLR share a secret key K, the VLR and HLR share another secret key K'. The new mechanisms work as follow

**Step 1:** MS generate random number ($R_{Mobile}$) and send TMSI and $R_{Mobile}$ to the VLR.

$$MS \xrightarrow{(TMSI \,||\, R_{Mobile})} \Rightarrow\Rightarrow VLR$$

**Step 2:** VLR receives the request from the MS and passes it to the HLR and VLR generates random number ($R_{VLR}$), then VLR sends the identification of VLR $ID_{VLR}$ and random number ($R_{VLR}$) to the HLR.

$$VLR \xrightarrow{(TMSI \,||\, R_{Mobile} \,||\, R_{VLR} \,||\, ID_{VLR})} \Rightarrow\Rightarrow HLR$$

**Step 3:** HLR receives the request from VLR and then searches for the secret keys for MS (K) and VLR (K') in the HLR database depending on TMSI for MS and $ID_{VLR}$ for VLR. Also HLR generate the Random number $R_{HLR}$, AV and AUTN where

$$AV = XRES \,||\, CK \,||\, IK,$$
$$AUTN = SQN \quad AK \,||\, AMF \,||\, MAC$$

Also it generates to refreshment key K' and $K'_1$ to an encrypted authenticated message. Then generate authentication message from HLR to MS, where

$$AUTH_{HLR\ to\ MS} = Encrypt\ [R_{HLR}, (R_{Mobile} \,||\, AUTN)_{K'}]_{K}$$

And generate authentication message from HLR to VLR where

$$AUTH_{HLR\ to\ VLR} = Encrypt\ [R_{HLR}, (AV \,||\, R_{VLR})_{K1'}]_{K1}$$

$$HLR \xrightarrow{(AUTH_{HLRtoVLR} \,||\, AUTH_{HLRtoMS})} \Rightarrow\Rightarrow VLR$$

**Step 4:** The VLR receives the message from the HLR then VLR decrypts the message by the shared secret key $K_1$ to get $R_{HLR}$

$$R_{HLR} = Decrypt\ (AUTH_{HLR\ to\ VLR})_{K1}$$

Also based on $R_{HLR}$, the VLR calculate refreshed key $K'_1$ (i.e. a new secret key), where

$K'_1 = E\ [K_1, h\ (K\ R_{HLR})]$, where h is one way hash function

According to derived secret key $K'_1$ the VLR decrypt $AUTH_{HLR}$ to VLR to derive it from AV and $R_{VLR}$.

Then it retrieves integrity key (IK), cipher key (CK) form above AV and according to IK and CK, the VLR generates session key $K_{VM}$ to apply it between the MS and VLR. Where

$$K_{VM} = IK \oplus CK$$

And generates authentication message from VLR to MS where

$$AUTH_{VLR\ to\ MS} = (ID_{VLR} \| R_{Mobile} \| TMSI') K_{VM}$$

Then, VLR passes the $AUTH_{HLR\ to\ MS}$ to the MS and $AUTH_{VLR\ to\ MS}$ to the MS

**Step 5:** The MS receives the message from the VLR then MS decrypts the message by the shared secret key K to get $R_{HLR}$

$$R_{HLR} = Decrypt\ (AUTH_{HLR\ to\ MS})_K$$

Also based on $R_{HLR}$, the MS calculate refreshed key K' (i.e., a new secret key), where

$K' = E[K, h (K \oplus R_{HLR})]$, where h is one way hash function

And according to the derived secret key K' the MS decrypts $AUTH_{HLR\ to\ MS}$ to derive it from AUTN and $R_{Mobile}$.

Also MS generates CK and IK by using $R_{HLR}$ to get session key $K_{VM}$ to apply between MS and VLR. MS decrypting $AUTH_{VLR\ to\ MS}$ to retrieve $ID_{VLR}$, $R_{MS}$ and TMSI'.

According to $R_{HLR}$ the MS computes the RES value toward the VLR to compare RES and SRES. The authentication is successful if matching occurs between RES and SRES. Figure 7 describes the new authentication mechanism.

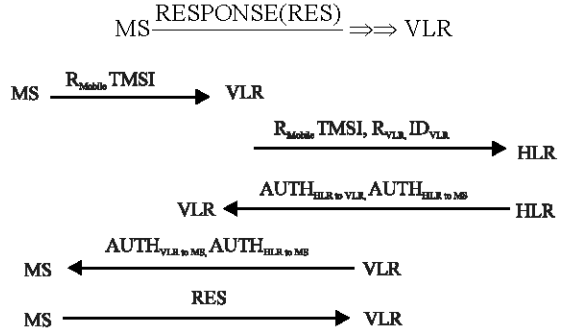


Fig. 7: The new authentication mechanisms

The proposed authentication mechanism provides high level of security as follows:

- Authentication of the MS to the VLR,

$$AUTH_{VLR\ to\ MS} = (ID_{VLR} \| R_{Mobile}) K_{VM},$$

  In step 4 the VLR generate session key $K_{VM}$ to apply between the MS and VLR, because VLR will only get the session key then MS knows that messages are coming from VLR.
- Authentication of the VLR to the HLR: by verifying the response message $AUTH_{HLR\ to\ VLR}$ which includes the challenge message $R_{VLR}$.
- Authentication of the MS to the HLR, by decrypting the $AUTH_{HLR\ to\ MS}$, the MS gets $R_{HLR}$ to compute the AK = F5 (K, RAND), then obtain the value of SQN, so it computes the XMAC to compare with MAC within AUTN. If they achieve matching to each other, it can verify that MS authenticates HLR.
- Establishment of new session key $K_{VM}$, the new shared key of the MS and VLR is assigned by them.
- Assurance to the MS and VLR that the secret key is fresh
- Prevent Reply attack: which it is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Hackers capture old messages and reply them at later times. By replying the message it becomes legal (Hwang *et al*., 2000). Suppose MS wants to prove his identity to HLR. HLR requests his IMSI as proof of identity, which MS dutifully provides (possibly after some transformation like a hash function); meanwhile, hacker is eavesdropping the conversation and keeps the IMSI. After the interchange is over, hacker connects to HLR posing as first MS; when asked for a proof of identity, hacker sends the first MS IMSI read from the last session, which HLR must accept.

A way to avoid replay attacks is that proposed authentication mechanism contains freshness property which is supported in this proposed mechanism.

## CONCLUSIONS

The proposed authentication for 2nd generation mobile Networks 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 enhanced security.

The proposed authentication for GSM has been generated while keeping the aim of not only keeping the complexity of this function as low as possible but keeping a high level of security and efficiency.

The proposed authentication for UMTS has five messages similar to the current authentication method, but provides authentication of the MS to VLR, VLR to HLR and MS to HLR. The aim is development is to prevent replay attacks by the freshness properties. The HLR refreshes the secret key K and $K_1$ to be K' and $K_1$', then distributes keys to the MS and VLR with its random number, respectively. The new keys of K' and $K_1$' are derived from old keys K and $K_1$ with random number from MS, VLR and HLR in each authentication process, respectively. The subscriber uses different key to request for registration and authentication, hence the replay attacks and guessing attack are infeasible while performance has been improved. Meanwhile, the performance is improved by reducing the communication times and data sizes during the process of authentication.

## REFERENCES

William, S., 2004. Cryptography and Network Security, Principles and Practice. 3rd Edn., USA: Prentice Hall.

Mark, J., 2002. Revenue Assurance, Fraud and Security in 3G Telecom Services. VP Business Development Visual Wireless AB, Journal of Econoic Management, Volume 1, Issue 2.

Ari, V., 2005. Cellular Telephone Network security. [Interned Accessed 22 Sept 2005] www.adela.karlin.mff. cuni.cz/l1/~ tuma/ nciphers /CELL_SEC_E.ppt

3G TS 33.102: "3G security; Security Architecture," http://www.ets.org

Lin, H.Y., 1999. Security and Authentication in PCS. Computers and Electrical Engineering, 25: 225-248.

Al-tawil, K., A. Akrami and H. Youssef, 1998. A new authentication protocol for GSM network, Proceedings of IEEE 23rd Annual Conference on Local Computer Networks, October 1998, Boston, pp: 21-30.

Min Shiang Hwang, Yuan Liang Tang and Cheng-chi Lee, 2000. An Efficient Authentication Protocol for GSM Network. EUROCOMM 2000.

Hwang, M.S., Y.L. Tang and C.C. Lee, 2000. An efficient authentication protocol for GSM networks. Proceedings of AFCEA/IEEE EuroComm'2000, May 2000, pp: 326-330.