International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 6 (June 2014), PP.42-48

A Study Report on Authentication Protocols in GSM, GPRS and UMTS

P. Ravi Kiran[1], Y. K. Sundara Krishna[2]
[1]*Research Scholar, Dept of Computer Science, Krishna University, Machilipatnam, AP*
[2]*Professor, Department of Computer Science, Krishna University, Machilipatnam, AP*

Abstract:- Masquerading and eavesdropping are major threats in mobile Communications. To provide protection in communication we require enciphering of voice message and authentication for subscriber with the communication network. This paper presents a complete study report on authentication protocols and its application on mobile communication systems like GSM, GPRS and UMTS. In addition, we describe the Encryption and authentication algorithms that are used in these architectures.

Keywords:- Authentication protocols, Telecommunication systems, GSM, GPRS, UMTS

I. INTRODUCTION

Wireless and Mobile Communications are having great features and is attractive among users as well as service providers. Unlike wired, Wireless networks provide anytime, anywhere access to the users. The *Global System for Mobile Communications* (GSM) has witnessed marvelous growth of almost 70% in wireless market of users and is used by 2 billion subscribers in the world [1]. Wireless communications include GSM, GPRS and UMTS. The increase in their usage leads to security problems like authentication and privacy are also increasing. The authentication makes no unauthorized user be able to get required services of an authorized user from the home system. The privacy refers to the communication messages will not be intercepted by eavesdroppers. The mechanism to solve these problems is done by authentication protocol and ciphering of voice messages using symmetric key encryption.

The rest of the paper is organized as follows: Section 2 briefly introduces the architectures of the GSM, GPRS and UMTS mobile communication systems. Section 3 describes the algorithms that are used for authentication and encryption in these networks. Section 4 narrates the authentication attacks that are most commonly encounter in the communication systems. In section 5 we discuss about the authentication and ciphering in GSM. Section 6 and Section 7 explains about the authentication protocol in GSM and UMTS respectively. Section 8 discusses and concludes with the improvements that are made in GSM and UMTS Authentication Protocols.

II. TELECOMMUNICATION SYSTEMS

A. GSM Architecture

GSM, the Groupe special mobile was developed and named as Global System for Mobile Communications that provides voice services that compatible to Integrated Services Digital Network (ISDN) and Public Switch Telephone Network (PSTN) systems. A GSM system consists of three subsystems, Radio Subsystem (RSS), Network and Switching Subsystem (NSS), and Operation Subsystem (OSS). The Mobile Station (MS) in RSS contains Subscriber Identity Module (SIM) consists the services like Authentication key Ki, International Mobile Subscriber Identity Module (IMSI) and other user related information.

The Base Station Subsystem (BSS) performs necessary functions like encoding/decoding of voice, rate adaption to maintain radio connections with an MS. The Base Station Controller (BSC) controls several base stations by managing their radio resources. Many BSCs are connected to Mobile Services Switching Center (MSC) in NSS. Along with MSC, NSS also called Core Network (CN) consists of several databases like Visitor Location Register (VLR) and Home Location Register (HLR). Gateway MSC (GMSC) which connects the GSM Network to PSTN and ISDN. MSC provides several functions like registration, authentication, location updating, handovers and call routing using HLR and VLR. HLR is the major database and stores all user-specific information elements.VLR is a dynamic database, responsible for copies of all relevant information for the user from HLR. It also stores the dynamic information about subscriber location. The Equipment Identity Register (EIR) and Authentication Center (AuC) in the third subsystem, OSS contains device information and algorithms for authentication, encryption/decryption and generation of session keys respectively.

B. GPRS Architecture

A new packet oriented service of GSM, powerful and flexible data transmission is General Packet Radio Service (GPRS). It provides a packet mode transfer for applications and allow broadcast, multicast and unicast services. The GPRS architecture introduces three new network elements GPRS Support Node (GSN), Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN). GSN integrated into GSM network, SGSN takes the response of performing several security functions and GGSN internetworking unit that connects GPRS to Packet Data Networks (PDN). SGSN users the HLR and EIR along with an additional database for GPRS called GPRS Register (GR) stores user addresses.

C. UMTS Architecture

A worldwide communication system that allows for terminal and user mobility prepared by ETSI is called Universal Mobile Telecommunications System (UMTS) and for radio interface is UMTS Terrestrial Radio Access Network (UTRAN) which handles cell level mobility. The Radio Network Subsystem (RNS) handles handovers, ciphering and deciphering and radio resource management. User Equipment (UE) connects to UTRAN and CN via U_u and I_u interfaces respectively.

III. ALGORITHMS

This section describes the authentication and encryption algorithms that can be used in mobile communication systems. Three different algorithms namely: A3 – authentication, A8 – generating session keys and A5 – ciphering and deciphering.

A. A3 and A8

A3 and A8 are one–way algorithms that can be used for authentication and generating session keys K_c. A3 can be implemented on the client SIM card and on the HLR of CN. It uses challenge response mechanism to authenticate the client with the network using authentication key K_i (128bit). The random number RAND (128bit) and the key K_i are used in A3 algorithm to Generate Signal Request SRES (32bit). A8 uses the same in generating session key K_c (64bit). This SRES/Kc is generated by using COMP128 in A3/A8. Over-the-air-attacks might leads to problem in networks [3] propelled to replace COMP128 by COMP128-2 after exploiting the weakness in the present algorithm.

B. A5 and GEA

A5 is a standardized pseudo-random-key stream cipher consists of three clocked linear feedback shift registers (LFSR). The register inputs are shifted in a linear function of its current content. A5/1 and A5/2 are very similar stream ciphers. The A5/2 is a modified weaker version of the earlier.

In initialization phase the registers are kept zero and fed with 64bit key K_c. In the operation phase the clocking starts to work, which scrambles timing of the shifting of registers adding a non-linear-part to the algorithm. A5/2 is a strong cipher, works like A3, except that small change in allocation of bits in register. A5/1 and A5/2 are known to be weak and security is obscurity won't work. A5/3 is a public cipher also known as KASUMI supports the session key K_c of size 84bit used in 3rd generation mobile services such as UMTS. A5/4 is identical to A5/3 except that it has 128bit key K_c. to implement A5/4 one must also use a UICC/USIM and execute the UMTS AKA protocol.

GPRS Encryption Algorithm (GEA) used for traffic and signaling encryption in packet oriented GSM i.e. GPRS. It uses session key K_c to generate key stream of range 5 – 1600byte. The original GEA uses K_c of 54bit whereas GEA2 and GEA3 are using K_c which is of 64bit. GEA3 is effectively same as A5/3 and GEA and GEA2 do not have any relation with A5/1 and A5/2.

IV. AUTHENTICATION ATTACKS

In this section we describe the possible attacks against GSM/GPRS protocols that feature in the proceeding discussion.

A. Passive Attacks

Passive attack is the fundamental attack on A5/2 uses onetime pre-computation and releases the decrypted voice by finding the key. It intercepts 4 frames of A5/2 encrypted voice just in milliseconds, look up the key from the known linear relationships from the encrypted frames.

B. Replay Attacks

Replay Attacks is a type of active attack, on A3 and A8 as both are one-way algorithms uses challenge-response mechanism. The opponent simply copies the message preserves and replay the message when the original message is suppressed.

C. Masquerading

Masquerading is also a type of active attack, when a real base station and the mobile would both prefer to use a stronger encryption algorithm than A5/2 like A5/3, the false base station can convince the mobile to use A5/2 long enough to break it, recover the key, and respond to the real base station with correctly encrypted voice using the stronger algorithm. This works because the same key is used for both the weak and the stronger algorithms.

D. Time-space tradeoff

A Time-space tradeoff can be achieved by pre-computing the list of hashes of Dictionary words and storing them in databases with hash as key. The attacker takes four consecutive encrypted frames, runs a processing phase on them, and checks if the output is in their database. If they are lucky, it is, and they can then very quickly determine the input key.

V. GSM AUTHENTICATION & CIPHERING

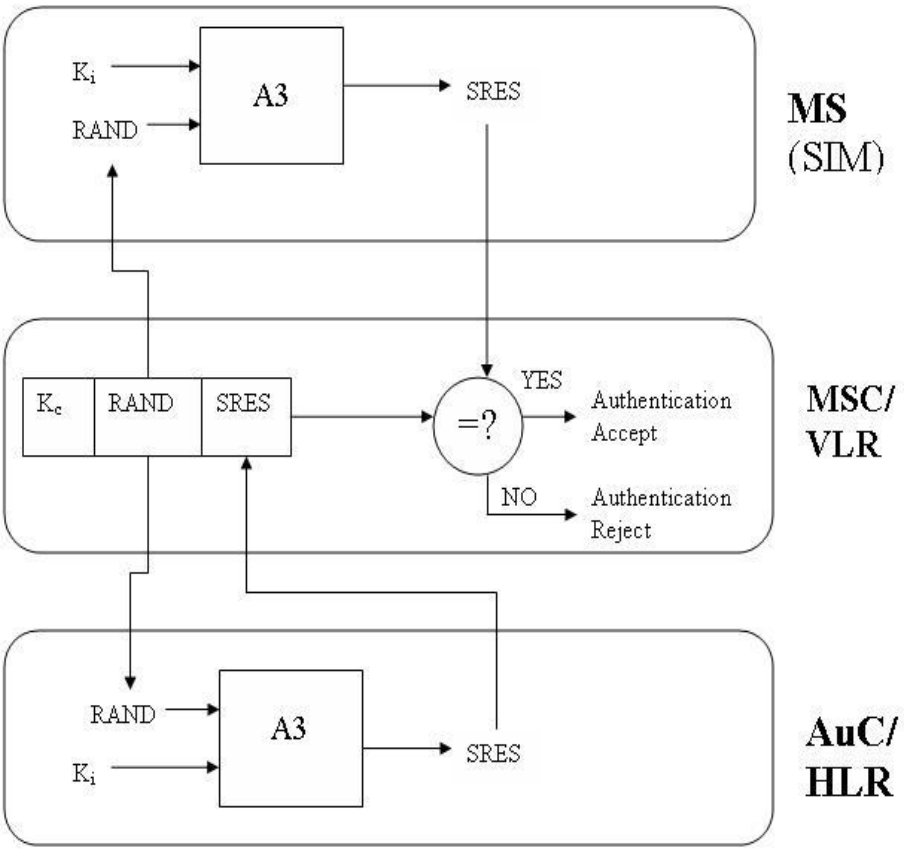

Fig. 1: GSM Authentication Architecture

In the entire authentication process, the three main actors are the MS, MSC/VLR, HLR/AuC as given in the Figure 1. The VLR sends the RAND to both mobile station HLR/AuC. The HLR/AuC and Mobile Station uses Authentication algorithm (A3) to generate Signal RESponse (SRES) from authentication key K_i and RAND. The SRES generated by HLR/AuC is stored in VLR database. The MS sends the SRES' to the VLR for checking, if they match, the authentication succeeds otherwise it fails.

Similarly for encryption the session keys K_c are to be generated by both HLR and MS as similar to authentication uses the algorithm (A8) as shown in the figure 2. The stored K_c is used for encryption at MS and at BTS.

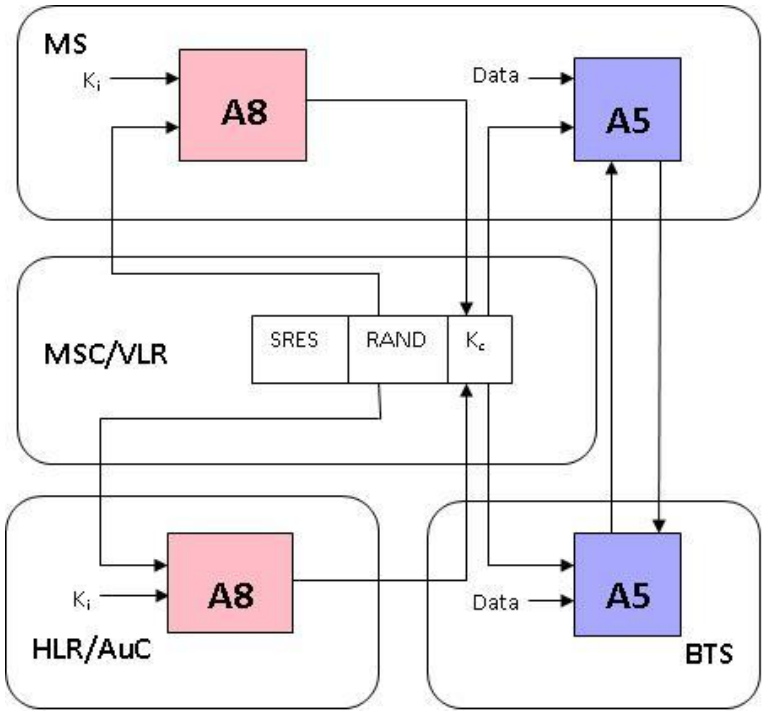

Fig. 2: GSM Encryption Architecture

VI. GSM AUTHENTICATION PROTOCOL

In GSM, the most important part is the authentication protocol. In the following section we discuss the notations used throughout this section, the existing GSM authentication protocol and Hwang et al.'s authentication protocol shown in sub-sections A, B and C respectively.

A. Notations

Before demonstrating these authentication protocols, we first list the notations used throughout this paper in the following.

HLR	Home Location Register
VLR	Visitor Location Register
TMSI	The temporary mobile subscriber identity
IMSI	The international mobile subscriber module
LAI	The location area identity
ID_V	The identification of VLR
K_i	The secret key shared between MS and HLR
T	The timestamp generated by MS
R	The random number generated by HLR
R'	Random number generated for the first time
SRES'	The signal response computed for the first time of the authentication
SRES	Signal response stored in VLR
CERT_VLR'	The certificate of the visiting VLR computed for the first time of the authentication
CERT_VLR	Certificate VLR stored in MS
K_T	Temporary secret key generated by HLR

B. Existing GSM authentication protocol

In this subsection, an overview of the current GSM authentication protocol is shown in Figure 3. And the details are described as follows:

Step1: While MS joins into a new visiting area and asks for new communication service, an authentication request is sent to VLR first, where the request includes TMSI and LAI.

Step2: After receiving the request, the new VLR uses the received TMSI to get the IMSI from the old VLR and then sends IMSI to HLR.

Step3: Then, HLR generates n distinct sets of authenticating parameters $\{SRES, R, K_C\}_h$, where h=1,2,..n, and sends them to VLR.

Step4: After receiving those sets of authenticating parameters, VLR keeps them in its own database and selects one set of them to authenticate the mobile station for each call. Next, VLR sends the selected R to MS.

Step5: Once MS receives R from VLR, it computes SRES'=A3(R, K_i) and the temporary session key K'c=A8(R, K_i), respectively, where K'= is kept secret for communication. Then the SRES' is sent back to VLR.

Step6: Upon receiving SRES' from MS, VLR compares it with the selected SRES kept in its own database. If they are not the same, the authentication is failure; otherwise, VLR can make sure that MS is legal.

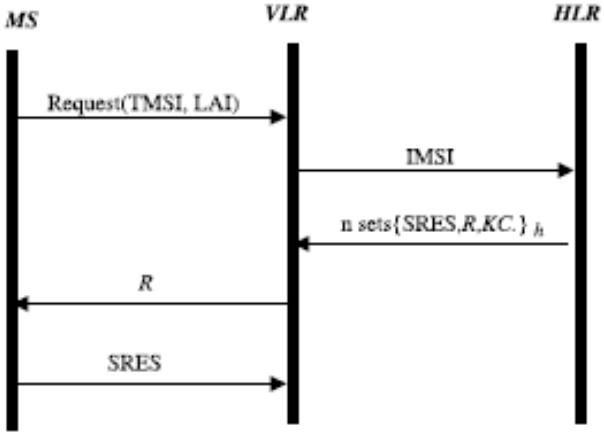

Fig. 3: Existing GSM Authentication Protocol

C. Hwang et al.'s GSM authentication protocol

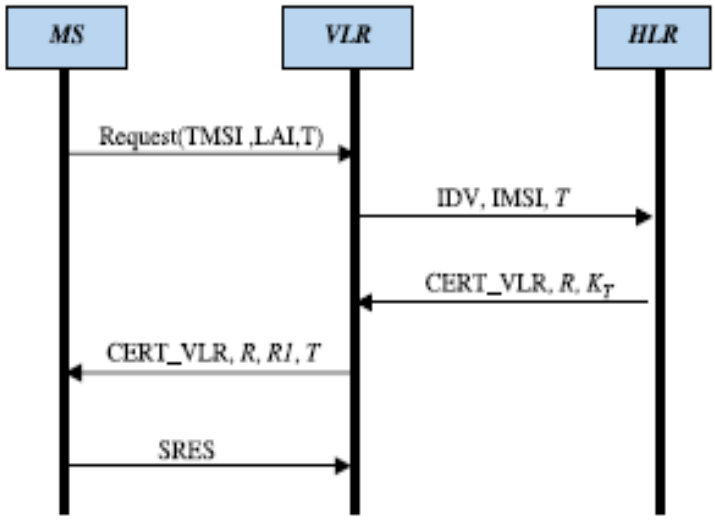

Fig. 4: Hwang et al's GSM Authentication Protocol [courtesy]

To solve the existing drawbacks of the current authentication protocol of the GSM architecture, Hwang et al. proposed a new authentication protocol. The flowchart of Hwang et al's authentication protocol is shown in Figure 4 and the details of the protocol are described as follows.

Step1: While MS enters a new visiting area and asks for new communication service, an authentication request including the TMSI, LAI and T is sent to VLR.

Step2: After receiving the request, the new VLR uses the received TMSI to get the IMSI from the old VLR and then sends the IMSI along with its identification IDV and T to HLR through a secure channel.

Step3: After receiving the information from VLR, HLR checks whether the timestamp T is extinct and the identity ID_V of the visiting VLR of MS is legitimate or not. If both T and ID_V are valid, HLR randomly chooses a number R and computes CERT_VLR=A3(T, K_i) and K=A3(R, K_i). Then HLR transmits the computation results and R to the visiting VLR. Otherwise, HLR will terminate the authentication protocol.

Step4: Once VLR receives the information, it computes SRES=A5(R', K_T) and stores it in its own database, where R1 is the random number generated by VLR for the present communication. Then, VLR passes R, R', T and CERT_VLR to MS.

Step5: While receiving the information from VLR, MS first checks whether T is valid or not. If it holds, MS computes CERT_VLR'=A3(T, K_i) of VLR. Next, MS compares CERT_VLR' with the received CERT_VLR. If they are not equivalent, the authenticating process is halted; otherwise, MS computes K=A3(R, K_i) and SRES=A5(R', K_T). Then MS sends SRES' back to VLR.

Step6: Upon receiving SRES' from MS, VLR compares it with the SRES kept in its own database. If it holds, the authentication is successful; otherwise, the request is rejected.

VII. 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). There are two phases in UMTS Authentication protocol: (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 5, UMTS authentication procedure works as follows.

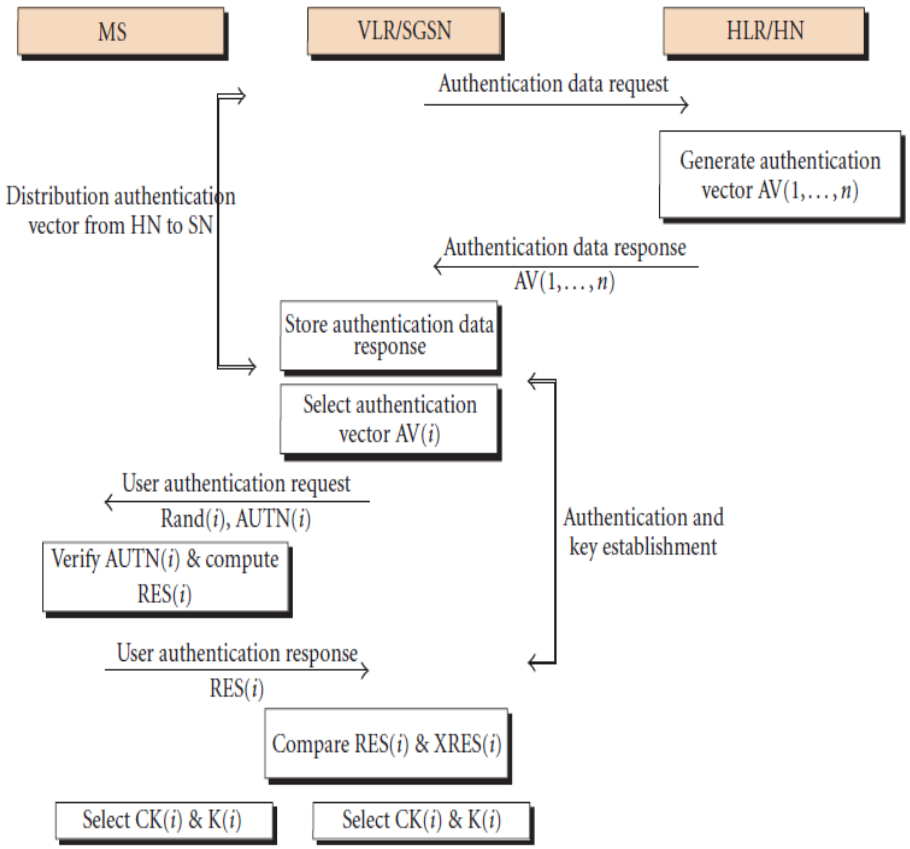

Fig. 5: UMTS Authentication Protocol

Step1: MS sends international mobile subscriber identity (IMSI) and authentication request to (VLR/SGSN)

Step2: VLR passes this authentication request to HLR.

Step3: HLR Generates authentication vectors AV(1, . . . , n) and sends the authentication data response AV(1, . . . , 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.

Step4: 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 signaling between VLR and HLR/AuC is not needed for every authentication event.

Step5: MS verifies the AUTN(i) and computes RES(i) authentication response and sends back to VLR/SGSN.

Step6: VLR compares the received RES with XRES. If they match, then authentication is successfully completed.

VIII. DISCUSSION AND CONCLUSIONS

This paper surveys the major security features that are included in the GSM and UMTS Standards. In GSM the authentication algorithm A3 and Generation of session key algorithm A8 are a one-way authentication, has be improved by implementing mutual authentication. When we apply mutual authentication, two schemes: MA1 and MA2 [2] are used for improving efficiency. These improvements reduce the problem of space overhead.

In A5 algorithms, the existing GSM used symmetric key encryption. This can be improved by substituting asymmetric key cryptography [3]. In UMTS, Authentication Key Agreement (AKA) protocol which gives more security by reducing the authentication time and signaling messages [9]. As Future work we suggest to implement mutual authentication on Timestamp based mechanisms in UMTS system.

REFERENCES

[1] Yong Li, Yin Chen, and Tie-Jun MA, "Security in GSM", Retrieved March 18, 2008, from http://www.gsmsecurity.net/gsm-security-papers.shtml

[2] Efficient authentication protocols of GSM Chin-Chen Chang*, Jung-San Lee, Ya-Fen Chang, Computer Communications 28 (2005) 921–928.

[3] Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography Wilayat Khan and Habib Ullah, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 9, May 2010.

[4] Authentication Protocols in Wireless Communications, Hung-Yu Lin, Lein Harn, and Vijay Kumar

[5] Authentication Protocols for Personal Communication Systems, Hung-Yu Lin and Lein Harn

[6] An Authentication Protocol for Mobile Cellular Network, L. A. Mohammed, Abdul Rahman Ramli, Mohamed Daud*, and V. Prakash, Malaysian Journal of Computer Science, Vol. 15 No. 1, June 2002, pp. 37-44.

[7] Extension of Authentication and Key Agreement Protocol (AKA) for Universal Mobile Telecommunication System (UMTS), Ja'afer AL-Saraireh & Sufian Yousef, International Journal of Theoretical and Applied Computer Sciences, Volume 1 Number 1 (2006) pp. 109–118.

[8] Designing Authentication Protocols for Third Generation Mobile Communication Systems, shu-min cheng, shiuhpyng shieh, wen-her yang, fu-yuan lee and jia-ning luo, Journal of Information Science and Engineering 21, 361-378 (2005).

[9] A New Authentication Protocol for UMTS Mobile Networks, Ja'afer Al-Saraireh and Sufian Yousef, EURASIP Journal on Wireless Communications and Networking Volume 2006, Article ID 98107, Pages 1–10.

[10] UMTS Security, K. Boman, G. Horn, P. Howard, and V. Niemi, For publication in the October 2002 issue of IEE Electronics & Communication Engineering Journal.