Assam University Journal of Science & Technology :
Physical Sciences and Technology
Vol. 7 Number II
36-43, 2011
ISSN 0975-2773

A Novel Subscriber Message Authentication Technique in 3-G Mobile Communications Using Digital Signature

***Pijush Kanti Bhattacharjee*[1] *and Chandan Koner*[2]**
[1]Department of Electronics & Telecommunication Engg., Assam University, Silchar-788011, India.
[2]Department of Computer Science Engineering, Bengal Institute of Technology & Management, Santiniketan-731236, India.
Correspondence; email : [1]pijushbhatta_6@hotmail.com, [2]chandan_durgapur@yahoo.com,

Abstract

Hacking and threats are the common problems in wireless traffic. Authentication of mobile subscribers and network are an important issue to the researchers. Now mobile communication systems 3-G (or advanced Generation) have been invented to make speedy data communications. 3-G mobile communications use two different switching techniques: circuit switching for voice and low speed data communications, and packet switching mainly for data communication, but can extend voice communication like VoIP (Voice Over Internet Protocol), video telephony, multimedia service etc. Generally high speed data communication uses packet switching process through PDSN (Packet Data Serving Node) servers. In this paper, we propose a subscribe message authentication technique by using digital signature cryptography that examines authenticity of the subscriber and the network by subscriber's message only.

Keywords : Message Authentication, Digital Signature, Packet Switching, Password, SIM.

Introduction

Uses of the Internet and IP technology have enlightened the cellular area in high speed data transmission (Lee, 2008; Rappaport, 2006; Bhattacharjee 2007, 2008; Forouzan, 2006). Data rates reach upto 2 Mbps or more for 3-G mobile communications, opening opportunities for extensive wireless multimedia services. Enabling packet data services off the RAN (Radio Access Network) in UMTS (Universal Mobile Telecommunication System in USA) and by passing the MSC is the beginning step for separating the circuit based world of the PSTN and the packet based world of PDNs (Public Data Networks) and the Internet (Goodman, 1990; Ramjee *et al.*, 1998; Koner *et al.,* 2009; Bhattacharjee *et al.,* 2009; Kim *et al.,* 2003).

The European counterpart of UMTS is WCDMA (Wideband Code Division Multiple Access), generally marketed as 3GSM. The WCDMA scheme has been developed as a joint effort between ETSI and ARIB (Japanese) during the second half of 1997, whereas, in March 1998, the TIA (Telecommunications Industry Association) TR45.5 committee adopted an innovation for wideband CDMA, compatible with IS-95, which is called CDMA-2000. This 3-G network can provide circuit switched voice service, circuit switched data service like 2-G (CDMA One or GSM), in addition to this, packet switched data service (Lee, 2008; Goodman, 1990).

We propose message authentication technique that authenticates proper subscriber and the network by applying digital signature cryptography on subscriber's message. Here simultaneously messages in packet form with their corresponding digital signature are transmitted and at the receiving end, this digital signature is cross checked to verify the authenticity of the subscriber as well as the network.

Architecture of 3G Mobile System

Architecture of a 3rd Generation wireless network CDMA-2000 or WCDMA is described below in Fig. 1. This 3-G network can provide circuit switched voice service, circuit switched data service like 2-G (CDMA One or GSM) (Bhattacharjee, 2007, 2008; Forouzan, 2006) in addition to this packet switched data and multimedia service (Goodman, 1990; Ramjee *et al.,* 1998; Koner *et al.,* 2009; Bhattacharjee *et al.,* 2009). In 2000 A.D, TIA (Telecommunication Industry Association) publishes IS-856 (Interim Standard-856) network. It is known as CDMA 2000 1X EV-DO (Evolution Data Optimized). CDMA-2000 1X is having chip rate 1.2288 Mcps, While WCDMA chip rate is 3.84 Mcps, but CDMA-2000 3X chip rate is 3.6864 Mcps.

MS - Mobile Station or Mobile Subscriber for transmitting and receiving signals in air interface. It consists of USIM (Universal Subscriber Identity Module) or SIM which contains user identity i.e. subscriber's number, data bases, call charging etc.

MS to BTS path - Reverse or Up link,

BTS to MS path - Forward or Down link.

BTS – Base Transceiver Station serves mobile connection to one or more cells and sectors in the cellular network,

BSS – Base Station Sub Sys-BSCs & BTSs

BSC – Base Switching Center controls one or more BTSs and perform inter BTS and intra BTS switching and handovers.

MSC – Mobile Switching Center or Main Switching Center which is a basic digital electronics exchange, e.g., 5ESS means 5th version of Electronics Switching System. MSC controls all the functions of a mobile network via different registers.

HLR – Home Location Register occupies identities of mobile subscriber as IMSI service parameters, location etc.

VLR – Visitor Location Register contains permanent and temporary (roaming) mobile subscriber's identity as TMSI, ISDN directory number, routing etc.

EIR – Equipment Identity Register contains identity of mobile equipment called IMEI [International Mobile Equipment Identity], connected with MSC or PDSN. It may be valid, suspect or prohibited.

AUC – Authentication Center contains authentication data called K_i in 2-G and in 3-G several keys or encryption codes with algorithm for encrypting user speech and data due to security purpose.

Billing Center – It provides all sorts of charging or commercial information. One billing center can handle the calls from several MSCs. In case of data transfer, this billing function is done by AAA server associated with PDSN in data communication network.

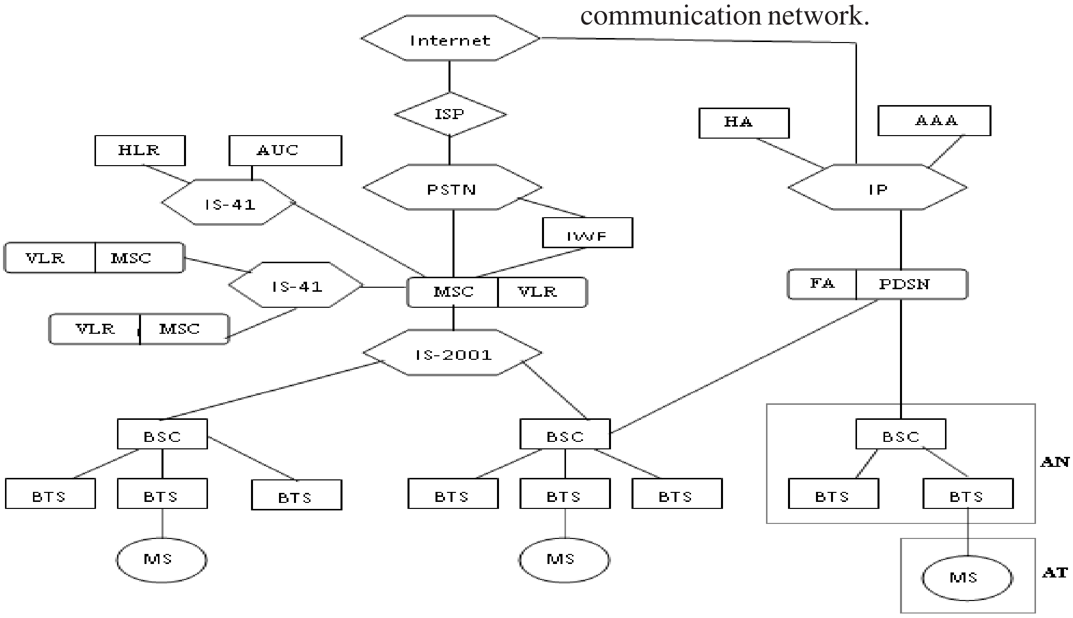

Fig.1. A typical 3-G mobile network architecture with high speed data network

In data network, MS is called AT (Access Terminal) where data or messages in written form is originated or terminated, where as BTS with BSC are called AN (Access Network) which handles data and further transports to PDSN through IS-2001 (Interim Standard-2001) network specified by ITU (Rappaport, 2006; Goodman, 1990; Ramjee *et al.,* 1998; Koner *et al.,* 2009; Bhattacharjee *et al.,* 2009; Kim *et al.,* 2003).

Thus AN acts as an interface between AT and PDSN. AT and AN are connected by IS-856 network.

The circuit switched voice and data services are arranged in same pattern as CDMA-One (2-G) by MS, BTS, BSC, MSC, HLR, VLR, AUC and IWF. An IWF (Inter-Working Function) is configured for converting a signal into a form compatible with a destination network receiving the data. While IWF enables circuit switched data service and BSC carries out mobility management i.e. controlling hand over or hand off. Additional networks are provided in 3-G for providing packet switched data service usually higher speed than that of circuit switched data service in 2-G.

This packet switched data network is consisting of two parts.

(1) Packet Data Serving Node (PDSN): The PDSN is the element that provides packet switched data service, like MSC for circuit switching. It is an internet protocol (IP) router that switches user data traffic to a public data network i.e. the internet. It deals with packet switched traffic (generally data) between the MS i.e. the user and packet switched network namely Internet or Intranet etc.

(2) Authentication, Authorization and Accounting (AAA): The AAA is a server that provides three main functions like authentication, authorization and accounting services for the packet data traffic connected with PDSN. It ultimately ensures packet data network connectivity services to the mobile users.

Authentication requires the user to provide an account number and password i.e. exchange of logical keys or certificates between the client and the server. If this authentication is correct, the MS is permitted for packet data service by Authorization. Last but not the least, function of AAA is accounting. It collects information on its usage of packet data service for billing or tariff calculation.

The CDMA-2000 network is supporting simple IP and mobile IP functions.

(i) Simple IP: An MS residing in home PDSN is given an IP address M and the server on the internet has an IP address S. Using these two addresses, IP packets containing data or information are exchanged between the MS and different servers in the same PDSN. A PDSN is consisting of several servers for routing packets in different directions. These servers are identified by the assigned address.

(ii) Mobile IP: Two additional network elements are provided for supporting Mobile IP.

(a) Home Agent (HA): This is a router together with the foreign agent (FA). This router resides on the MS home IP network. It serves as a point for communications with the mobile network.

(b) Foreign Agent (FA): This is another router residing in other PDSN. When MS travels a foreign IP network, the FA in the foreign network receives packet forwarded from the HA and delivers them to the MS. Thus it functions as the mobile node's point of attachment when it travels to the foreign network i.e. the network other than its home network.

Thus mobile IP uses a tunneling protocol to allow messages from the PDSN to be directed to the mobile node's IP address. This is accomplished by way of routing messages to the foreign node for delivery via tunneling the original IP address inside a packet destined for the temporary IP address assigned to the mobile node by the foreign node. This method allows for seamless communications between the mobile node and applications residing on the PDSN, always-on connectivity for mobile data applications and wireless computing.

Third Generation mobile service is assured mainly by two systems like WCDMA and CDMA-2000.

Some of the common feature between these two systems i.e. CDMA-2000 1X and WCDMA are the followings:

Direct sequence spread spectrum multiple access (CDMA-2000 1X uses 1.25 MHz bandwidth, WCDMA uses 5 MHz bandwidth), Orthogonal (Walsh) code division multiple access (mitigates interference), Random access, Fast uplink power control, Rake receivers, Soft handoff (between BTSs), Softer handoff (between BTS sectors), Soft hand off (SHO) active set (seamless service with increased spectral efficiency), Single frequency reuse, QPSK (Quadrature Phase Shift Keying) modulation, Downlink slotted paging, Blind rate detection, Down link reference channel (share common pilot), Downlink channel structure (separating channels with Walsh codes), Scrambling (for uniform interference and communication privacy), Speech regulated vocoder (increased system capacity) etc. In case of packet switching, variable length orthogonal codes are a mandatory feature for both CDMA-2000 and WCDMA for managing the mix of voice and non voice (data, multimedia) communications. Packet switching can afford different services like data, VoIP, Push to Talk, Video Telephony, Multimedia communications etc. These include enhanced downlink and uplink packet access techniques. High speed packet data communications is done in identical features like CDMA 2000 1X EV-DO (Evolution-Data Optimized) and WCDMA HSUPA (High Speed Uplink Packet Access), HSDPA (High Speed Downlink Packet Access).

At the same time there does exist some difference also between these two systems such as,

(i) Both WCDMA and CDMA-2000 use separate coding scheme.

(ii) Both use control channels to manage the network.

(iii) WCDMA and CDMA-2000 are not compatible from the perspective that they have different chip rates like 3.84 Mcps for WCDMA vs. 1.2888 Mcps for CDMA-2000. WCDMA uses a 5 MHz channel (bandwidth) initially, CDMA-2000 1X uses only a 1.25 MHz channel, but CDMA-2000 3X, three 1.25 MHz channels combine to form 5 MHz bandwidth. There are three modes of operation for WCDMA or CDMA-2000

• Direct sequence (DS) WCDMA in UMTS for frequency Division Duplex (FDD).

• W-CDMA Time Division Duplex (TDD).

• CDMA 2000 Multicarrier FDD.

Authentication in Mobile Communications 2G Network

GSM (2-G) networks utilize authentication for verifying authenticity of subscriber (Rappaport, 2006; Bhattacharjee, 2007, 2008; Forouzan, 2006). Each subscriber is identified with a unique IMSI (International Mobile Subscriber Identity) number. He has a unique subscriber authentication key (K_i).The authentication algorithm used in the GSM system in 2-G is known as the A3 algorithm. The SIM (Subscribe Identity Module) contains the IMSI, K_i and A3 algorithm. The AUC (Authentication Center) contains the A3 algorithm as well as a database of authentication information about the subscriber. A3 actually generates 128 bits of output. The first 32 bits of those 128 bits form the Signed Response. The A3 algorithm is implemented in the SIM (Subscriber Identity Module).

Authentication in the GSM network utilizes following Challenge/Response mechanism,

1. The HLR (Home Location Register) generates a 128-bit RAND (Random Challenge).

2. The HLR sends RAND to the MSC (Mobile Switching Center).

3. The MSC sends it to the BTS (Base Transceiver Station).

4. The BTS sends it to the MS (Mobile Station).

5. The MS receives it and generates 32-bit SRES* (Signed Response) utilizing RAND and the 128-bit K_i from the SIM (Mobile Station's Subscriber Identity Module) utilizing the A3 algorithm.

6. The MS sends the SRES* to the BTS.

7. The BTS sends the SRES* to the MSC.

8. The MSC checks whether SRES = SRES* or not. If they are same, MS is authentic.

This process authenticates the MS (Mobile Station) to the GSM or CDMA-One network. One known security limitation of 2-G networks is that the network is never authenticated by the MS (Mobile Station). This one-way authentication makes it possible for an attacker to pretend to be a network provider. As 2-G mobile authentication mechanism is only one way, therefore the user is not given the assurance that they have established a connection with an authentic serving network.

Proposed message authentication technique for 3G Mobile Network

The proposed technique is divided into three phases which are Key generation phase, Data sending phase, Data receiving phase.

A. Key Generation Phase

This phase is executed at the time of registration of a subscriber by the mobile service provider. In this phase the authority of particular mobile service executes the following steps,

KG1: Generates Encryption Key (E) and Decryption Key (D) by RSA (Rivest, Shamir and Adleman) algorithm (Forouzan, 2006).

KG2: Personalizes SIM with the parameter E.

KG3: Sends the SIM to the subscriber in a secure channel.

B. Data Sending Phase

When subscriber wants to send a message, then MS performs the following operations.

Let the subscriber message M is continuous bit string. MS divides M into different blocks each size of 160 bits. Let the blocks are M_1, M_2............, M_i, where i is the number of block or packet. At first MS sends M_1 and the Digital Signature of M_1 i.e. DM_1. Digital Signature of a message (DM_i) is calculated by first taking the Hash of M_i i.e. HM_i, then encrypting HM_i by E i.e. encryption key which yields DM_i. Then it sends M_2 and Digital Signature of M_2. Next sends other left blocks and digital signature of them sequentially. During the sending time if MS receives any reject signal from message server for a particular block or packet then it resends that faulty block alongwith digital signature of it to the server or network without any delay.

C. Data Receiving Phase

After receiving the first message block M_1 and the Digital Signature of M_1, the message server executes the following steps:

DR1: Decrypts the Digital Signature of M_1 by D and calculate the hash of M_1.

DR2: Compares the two results. If they are same, confirms that M_1 is come from the authentic subscriber. If they are not same, rejects M_1 and sends a reject signal to the subscriber to send M_1 again.

Then message server receives the message blocks (M_2,............, M_i) one by one sequentially and repeat the above operations for each message block separately.

Results and Discussions

The following phases are computed step by step to ensure the authenticity of the subscriber and the server or network.

1. Key Generation Phase

Encryption and Decryption key is found out by RSA algorithm likewise,

Let, two large prime numbers P=13 and Q=19.

So, N = PQ =13×19=247. Now P-1 = 12, Q-1 = 18,

X = (P-1) (Q-1) = 12X18 = 216.

According to RSA Algorithm, if Encryption Key (E) and Decryption Key (D), (DXE) mod 216 = 1 i.e.

DXE = 216 m + 1, where m is any positive integer, the smallest value of m is 1, then DXE = 217, Factorizing 217 ensures that Encryption Key (E) = 31 and

Decryption Key (D) = 7

2. Data Sending Phase

Suppose Subscriber sends a message of 2400 bits to the server, Subscriber's message: "Authentication in sending information is a great research challenge. Remote system authentication is a process by which a remote system gains confidence about the identity of the communicating partner. Subscriber message authentication can be done by applying digital signature on subscriber's message."

Subscriber sends a message block of 160 bits to the sever in one session. The blocks are $M_{1,}$ M_2, M_3, M_4, upto $M_{15.}$ Each of them is size of 160 bits because the total size of M is 2400 bits.

Using C programming language under Linux environment we have computed hash functions, encrypted digital signature and decrypted digital signature etc.

Message Set (M_i):

M_1 =41757468656e7469636174696f6e20696e 207365
M_2= 6e64696e6720696e666f726d6174696f6e206973
M_3= 2061206772656174207265736561726368296368
M_4= 616c6c616e67652e52656d6f7465207379737465
M_5= 6d2061757468656e7469636174696f6e20697320
M_6= 612070726f636573732062792077686963682061
M_7= 2072656d6f74652073797374656d2067696e73
M_8= 20636f6e666964656e63652061626f7574207468
M_9= 5206964656e74697479206f662074686520636f
M_{10}=6d6d756e69636174696e6720706172746e65722e
M_{11}= 5375627363726962657220 6d6573736167652061
M_{12}= 757468656e7469636174696f6e2063616e206265
M_{13}= 20646f6e6520627920617070c79696e67204469
M_{14}= 676974616c205369676e6174757265206f6e2073
M_{15}= 7562736372696265722773206d6573736167652e

MS applies Hash function on each message block M_i to obtain HM_i (Hash of M_i) in one session. HM_i is also size of 160 bits.

Hash Set (HM_i) of M_i:

HM_1= 42e743957f49558a4d6e6e36d840c4c828b50402
HM_2= a85f2c4bdc021e6f8b624812624e14eaa9fc7b31
HM_3= 41142e9c38c0a3017ec833b8d0dd3fd27e15071e
HM_4= 6ce258cf7eab54ebbd886744682f00b2dbaf561d
HM_5= 528fe2d161c85b6d5d9e8f71c5d03b4873c760ac
HM_6= 653f5061485490489238187a94e0f4fa73c9bc15
HM_7= 96b7acf35835acd82241df00efe2f3b2d0164380
HM_8= e0770291fa97e762e4d0fd7c3e5e49a8662e10b0
HM_9= 0e6bef8147b1f2f720613a1df368d41034a0f84b
HM_{10}= 4c3f17baad4ca60d96c31ac9aaa19a94da7bce85
HM_{11}= f45831d6e38a7376005f513a6a456b4930a23e52
HM_{12}= 6e708232116d299d1cbc377193704825e28d1582
HM_{13}= 62be34fbe9694752cc36778754d5274b647be485
HM_{14}= d85956a2a2e6578f9b974ea1b91b5ea0c59d3b71
HM_{15}= 1d7ef7cbd7b01f019420f3c05d34a7791069a3c8

MS encrypts HM_i by E (E = 31) to obtain DM_i (Digital Signature of M_i). DM_i is also size of 160 bits.

Digital Signature Set (DM_i) of M_i:

DM_1= c4a659b0cd0506e24d7c7c18534076cb4f33c7c1
DM_2= e95f634bdcc11ed63d47a29747753a9c8270d731

DM_3 = 413a546838e7c9017ecb81a7d0dd50737eae2d1e
DM_4 = ba4958a87e4c2eebe3216744ea2c00b2b8554692
DM_5 = 040d49d162cb8f15cee80d7166d088a2d252e5ac
DM_6 = 1750b462a22e90a2e0385d0856b91d3ed2a36fae
DM_7 = 95b7ac305869ac53c8419a007d4930b2d0cc5902
DM_8 = 1df5c132b912a64713d08920245e05e9c55451bc
DM_9 = 286b7db53bd587004862149230ea93514ea001ab
DM_{10} = ab50daeed4abc05b95a91aa3aab1295665d77785
DM_{11} = 3e583196bde2d242005f37140b456b05a5f12404
DM_{12} = 7cbbc391e11580833f6f1071adbba28449ecaec3
DM_{13} = 47394ec7cfde3b04e618f53c2e2f274b4ad71385
DM_{14} = 530f46f1f116570d5a1275b1d31b5ea066838871
DM_{15} = 927e0094afbca401564830e7ce4e437951dec9cb

3. Data Receiving Phase

After receiving the messages in packet form with the corresponding digital signatures, decrypts each digital signature (DM_i) of a message (M) by Decryption Key (D = 7), called TM_i and also calculate hash function of each message block i.e. HM_i.

Decrypted Digital Signature Set (TM_i) of M_i:

TM_1 = 42e743957f49558a4d6e6e36d840c4c828b50402
TM_2 = a85f2c4bdc021e6f8b624812624e14eaa9fc7b31
TM_3 = 41142e9c38c0a3017ec833b8d0dd3fd27e15071e
TM_4 = 6ce258cf7eab54ebbd886744682f00b2dbaf561d
TM_5 = 528fe2d161c85b6d5d9e8f71c5d03b4873c760ac
TM_6 = 653f5061485490489238187a94e0f4fa73c9bc15
TM_7 = 96b7acf35835acd82241df00efe2f3b2d0164380
TM_8 = e0770291fa97e762e4d0fd7c3e5e49a8662e10b0
TM_9 = 0e6bef8147b1f2f720613a1df368d41034a0f84b
TM_{10} = 4c3f17baad4ca60d96c31ac9aaa19a94da7bce85
TM_{11} = f45831d6e38a7376005f513a6a456b4930a23e52
TM_{12} = 6e708232116d299d1cbc377193704825e28d1582
TM_{13} = 62be34fbe9694752cc36778754d5274b647be485
TM_{14} = d85956a2a2e6578f9b974ea1b91b5ea0c59d3b71
TM_{15} = 1d7ef7cbd7b01f019420f3c05d34a7791069a3c8

Since this decrypted digital signature of each message block (TM_i) is equal to the hash function (HM_i) of the corresponding message block or packet, therefore the subscriber as well as the network is authenticated correctly.

Conclusion

In this paper we have elaborately discussed the proposed message authentication technique with the help of popular RSA Algorithm. By utilizing this technique, the mobile communications are completely restricted within the proper authentic subscriber and the network. This technique is very fast operating since our proposed algorithm tested in C-language programming under Linux environment. Therefore, this authentication technique can be applied in real time basis for all sorts of 3-G or any advanced generation mobile networks.

References

Lee, William C. Y. (2008), *Wireless and Cellular Communications*, 3rd Edition McGraw Hill Publishers.

Rappaport,T. S. (2006), *Wireless Communication: Principles and Practice*, Prentice Hall Pub Ltd, 2nd Ed.

Bhattacharjee, P. K. (2007), A New Era in Mobile Communications- GSM and CDMA *National Conference on Wireless and Optical Communications (WOC-07)* at Punjab Engg College (D.U), India, pp 118-126, on 13th- 14th Dec.

Forouzan, B. A. (2006), *Data Communications and Networking*, Tata McGraw Hill Publishing Company Ltd, 4th Edition.

Bhattacharjee, P. K. (2008), Hybrid GSM And CDMA Mobile Communication Systems Enhancing Channel Capacity *National Conference on Wireless and Optical Communications (WOC-08) with IEEE*, India, pp 1-8, from 18-19th Dec.

Goodman, D. (1990), Cellular Packet Communication, *IEEE Trans on Comm.*, vol. 38, no. 8, pp. 1272-1280, August.

Ramjee, P. and Tero, O. (1998), An Overview of CDMA Evolution towards Wideband CDMA, *IEEE Communications Survey*.

Koner, C; Bhunia, C. T. and Maulik, U. (2009), An Efficient and Reliable Three-Entity Remote User and Server Authentication Technique *International Journal of Engineering and Technology*, Singapore, Vol. 1 No.2 pp195-200, June.

Koner, C; Bhattacharjee, P. K.; Bhunia, C. T.; Maulik, U. (2009), A Novel Approach for Authentication Technique in Mobile Communications, *International Journal of Computer Theory and Engineering*, Singapore, vol. 1, no. 3, pp. 225-229, August.

Kim, H.; Afifi, H. (2003), Improving Mobile Authentication With New AAA Protocols, *IEEE International Conference on Communication (ICC 2003)* vol 1, pp 497-501, May.