A NOVEL PASSWORD BASED MUTUAL AUTHENTICATION TECHNIQUE FOR 4-G MOBILE COMMUNICATIONS

Tamal Dhar[1], Chandan Koner[2]

[1, 2]*Computer Science & Engineering, Dr. B. C. Roy Engineering College, West Bengal, India*
td.tamal@gmail.com, chandan_durgapur@yahoo.com

Abstract

Subscriber and network mutual authentication in mobile systems is a process by which mobile network gains confidence about the identity of the communicating subscriber and subscriber verified that he is communicating with correct network. Authentication in mobile systems is a challenge issue due to swift growth of wireless traffic with increasing security threats and attacks in mobile systems. 4G mobile communications system has brought for the high speedy data communications network by packet switching technology for networking transmission through SGSN servers. In this paper, we propose a mutual authentication technique that verifies the authenticity of the subscriber as well as the network by subscriber password in 4G mobile system. We focus on the advantages of our proposed technique, termed as password based mutual authentication technique.

Keywords: *Identifier, Mutual Authentication, Packet Switching, Password, SIM.*

----------***----------

1. INTRODUCTION

The cellular area in high speed data transmission [1-5] is introduced due to the demand of speedy data network and Internet technology. As a result the mobile communications is enhanced to 4th Generation (4G). 4G mobile systems [6-7] is an initiative to move beyond the limitations and problems of 3G (including 2.5G, sub3G). Data rates reach up to 20 Mbps to 100 Mbps in mobile node for 4G mobile communications, opening opportunities for high performance applications like extensive wireless multimedia services, full-motion video applications and wireless teleconferencing. In 3G, the data rate is only 384 Kbps to 2Mbps and performance is not sufficient for high performance applications. 4G operates in higher bandwidth (100 MHz or more) than 3G. Roaming and Interoperating across networks is difficult in 3G due to multiple standards of voice traffic but 4G provides global mobility and service portability by its digital packet network. Due to those disabilities and disadvantages of 3G, researchers motivate to work with 4G before 3G has not been deployed.

4G is facing to enclose a multitude of cellular and wireless networking technologies which include Satellite Radio Network, Wireless Local Area Network (Wi-Fi, Bluetooth), 2G and 3G cellular network. These wireless networking technologies are seamlessly interconnected by the Internet Protocol (IP) backbone network. Fourth Generation mobile service is assured mainly all digital with packetized voice switching that utilizes IP in its fullest form with converged voice and data capability. Password Authentication technique [8] was the most popular and basis for authentication of user in remote network. But there is no scheme in mobile system, where the authenticity of subscriber as well as network will be verified by subscriber password. This motivates to construct a password based authentication scheme for 4-G mobile system that provides subscriber and network authentication. In this paper, we propose an efficient and secure password based authentication technique that verifies the authenticity of subscriber as well as MSC or the network of 4-G mobile system. Subscriber authenticity is verified by applying password of subscriber. For this, subscriber password is collected and cross interchanged between MS, SIM and the network.

2. ARCHITECTURE OF 4-G MOBILE SYSTEM

Architecture of a 4th Generation wireless network is described below in Fig. 1. Generally, 4G mobile system [6-7] is a hybrid network which envisaged encompassing a multitude of wireless networking technologies which include Ad-hoc network, Mobile (3G and 2G systems) network, Wireless Local Area Network (Wi-Fi, Bluetooth) and Satellite radio networks. These wireless networks are interconnected by IP backbone network. So 4G mobile network is moving towards for adopting packet switching technology to meet its promised performance and throughput.

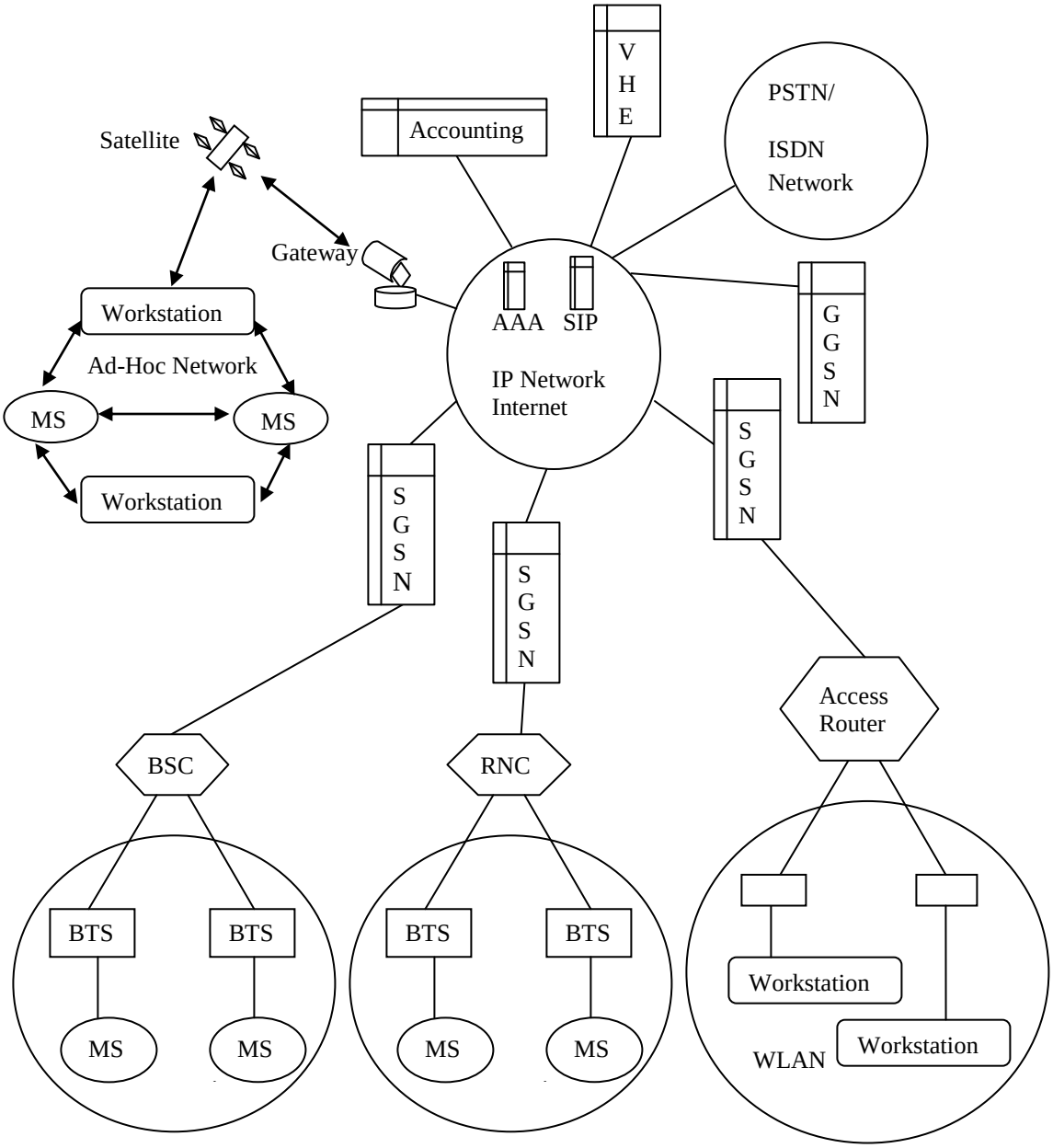

Figure 1: Probable architecture of 4G Mobile system

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, contains transceivers or radio units.

BSC – Base Switching Center controls one or more BTSs and perform inter BTS and intra BTS switching and handovers.
RNC – Radio Network Controller which is in charge of the overall control of the logical resources provided by BSCs.
RNC controls (attach/detach and location management), logical link management, and authentication and charging functions. The location register of the SGSN stores location

information (e.g., current cell, current VLR) and user profiles (e.g., IMSI, address (es) used in the packet data network) of all users registered with this SGSN.

Accounting – It provides all sorts of charging or commercial information. One billing center can handle the calls from several networks.

VHE (Virtual Home Environment) – This system is for personalized service portability across network boundaries and between terminals. The concept of the VHE is such that UMTS users are consistently presented with the same personalized features, user interface capabilities and services in whatever network and whatever terminal, where ever the user may be located. The exact configuration available to the user at any instant will be dependent upon the capabilities of the USIM, terminal equipment and network currently being used or on the subscription restriction.

SIP (Session Initiation Protocol)– It is a signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over IP. The protocol can be used for creating, modifying and terminating unicast or multicast sessions consisting of one or several media streams.

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. It ultimately ensures packet data network connectivity services to the mobile users.

Several tools and techniques are employed to make 4G as IP-based cellular system. Wireless access technologies such as full duplex OFDMA (orthogonal frequency-division multiple access), FH-OFDMA/CDM (frequency hopping-OFDMA/Code Division Multiplexing) and MC-CDMA (multiple carrier code-division multiple access) are adopted. AMC (Adaptive modulations and coding), SDR (Software defined radio) are installed to optimize the modulation and coding power control. The high-order modulation, turbo coding, and LDPC (low-density parity-check codes) tools are used for easy implementation. Multiple antennas with advanced coding techniques are combined to form MIMO (Multiple input multiple output) systems. The WPAN expansion can physically be made via interconnecting structures, e.g. Universal Mobile Telecommunications System (UMTS) [3-4] and the Internet, to remote networks such as home area networks, corporate area networks or vehicular area networks. A WPAN is a network of devices which could consist of a mobile phone, a PDA, a notebook PC, a digital camera, etc. All or a parts of these devices are carried around by a person in everyday life for both work and pleasure.
SGSN – Serving GPRS (General Packet Radio Service) Support Node (SGSN) is responsible for the delivery of data packets from and to the mobile stations within its geographical service area. Its tasks include packet routing and transfer, mobility management all the functions of a mobile network via different registers or servers, especially for voice and low speed data communications.

3. PROPOSED PASSWORD BASED MUTUAL AUTHENTICATION TECHNIQUE FOR 4-G MOBILE NETWORK

The proposed password based authentication technique is a collection of four different phases, namely, Subscriber Enrollment Phase, Subscriber Authentication phase, Network Authentication Phase and Subscriber Password Change Phase.

3.1 Subscriber Enrollment Phase

In subscriber enrollment phase, the subscriber is enrolled to particular AAA server belonging to the network. This phase is executed only once for one subscriber.

SE1: The subscriber chooses his identifier I, password P. Thereafter the subscriber passes these information (I, P) secretly to the authority concerned (mobile service provider) for initialization of the SIM.

SE2: The AAA server has received the enrollment request from subscriber with I, P data and executes the following tasks.

SE2.1: Computes $G = h \oplus (I \oplus P)$, h (.) is a one-way hash function and $\oplus$ is a bitwise XOR operation.

SE2.2: Computes $K= (h \oplus (s) \oplus G)$, where s is a secret key allotted by the AAA server for a particular SIM and it is assigned in different code for different SIMs.

SE2.3: Stores the parameters { e, G, I, K, P, s } into a SIM, where e is assigned a secret number and stored in each enrolled subscriber's SIM.

SE2.4: Sends the SIM to the subscriber for use.

3.2 Subscriber Authentication Phase

This phase is executed every time when the subscriber starts communication by setting up a call connection.

The subscriber enters his identifier I and password P′.
SA1: The MS computes $L= h (s) \oplus G \oplus h (I \oplus P')$. Then checks whether L is equal to the h(s) or not. [$L = h(s)$ when $G \oplus h (I \oplus P') = 0$ i.e. completely matching]. If $L = h(s)$, MS performs the following tasks, otherwise terminates the communication.
SA1.2: Computes $O = (G \oplus h(T) \oplus h (e))$, where T is the current time while the subscriber initializing the call.

SA1.3: Computes $N = h (K \oplus h (T) \oplus h (e))$.

SA1.4: Sends the communication request {O, N, T} to the AAA server.

SA2: The AAA server has received the communication request {O, N, T} at time T* and executes the following tasks.

SA2.1: Checks the difference between T* and T is valid time interval for measuring transmission delay. If it is correct then the AAA server performs the next tasks.

SA2.2: AAA server requests for s from SIM.

SA2.3: SIM sends s to AAA server through paging or secured channel.

SA2.4: Computes $N' = h(h(s) \oplus O)$.

SA2.5: The AAA server checks whether $N = N'$. If it holds good, the AAA server accepts the communication request of the subscriber.

If $N \neq N'$, the AAA server cancels the communication request of the subscriber due to failure of subscriber authentication phase.

3.3 Network Authentication Phase

The network or server is verified in this phase, this is executed when the subscriber is authentic.

NA1: AAA server requests for I, P from SIM.

NA2: SIM sends I, P to AAA server through paging or secured channel.

NA3: AAA server computes M = h (T**⊕ h (T⊕ h (s⊕ h (⊕ P))), where T** is current time.

NA4: AAA server sends (M, T**) to the subscriber through a paging channel.

Suppose subscriber receives (M, T**) at time T***.
NA5: MS checks the difference between T*** and T** whether it is valid time interval for transmission delay or not. If it is correct then the MS performs the next tasks.
NA5.1: MS computes, $M' = h(T^{**} \oplus h(T \oplus K))$

NA5.2: The MS checks whether $M = M'$. If it holds, then subscriber is connected to the desired network.

If $M \neq M'$, call request is terminated, hence network authentication fails.

3.4 Subscriber Password Change Phase

This phase is executed when the subscriber wants to change his password P by the new password P*.The subscriber enters his identifier (I) and password (P′). The MS verifies the entered I and P′ with the stored values of I and P in the SIM. If all the verifications are matched correctly, then MS executes the following tasks.

SP1: Asks the subscriber to enter a new password and he chooses a new password P* and enters it.

SP2: Computes $G^* = h(I \oplus P^*)$ and $K^* = (h(s) \oplus G^*)$

SP3: The P*, G* and K* are stored in the place of P, G and K respectively.

4. ADVANTAGES OF THE PROPOSED AUTHENTICATION TECHNIQUE

The proposed authentication system is working in two ways i.e. it connects the authentic (desired) subscribers to its home or appropriate network by verifying mutually. It has lot of advantages which are specifically listed below:

(a) One way hash function and XOR operation are only used which minimizes computation complexity and time.

(b) Many SIMs with the same identifier cannot be allocated for service i.e. the same login (identifier) from different SIM cannot make connection to the network.

(c) Any subscriber's identifier (I), password (P) etc are not require to store in the AAA server, hence these information cannot be hacked from the server.

(d) The user can freely choose his password and change the password as and when necessary without any involvement of the server.

5. EXPERIMENTAL RESULTS FROM THE PROPOSED ALGORITHM

The proposed algorithm is tested by exploring in C-program under Linux environment. We obtain very fairly result which can be easily implemented in the mobile network for authentication purpose. We describe the experimental result below. The following parameters are considered for executing the program.

Subscriber or user Identifier (I) is taken "Identity of Subscriber".
Subscriber or user Password (P) is taken "User's Authentication".

Secret Key (s) of AAA server is "71".

Secret number (e) of AAA server is "255".

Timestamps are considered like followings-

T - 13-03-2013, 10:10
T* - 13-03-2013, 10:11
T** - 13-03-2013, 10:12
T*** - 13-03-2013, 10:13

Timestamps are valid time interval.

5.1 Subscriber Enrollment Phase

The subscriber chooses identifier (I), password (P) as mentioned above and submits this information to the AAA server. AAA server computes G, K and personalizes a SIM. This is done only first time for enrolling the subscriber in a network. Results of Subscriber Enrollment Phase are given below:

SubscriberPassword(P)=
5573657227734175746865 6e7469636174696f6e

G=h(I⊕P) = 635f95978ec2c82742aa425d214088228b0c7354

K=h(s)⊕G = 70b245a9d6a4b7eccd9102f3af5d4c1dde3959da

5.2 Subscriber Authentication Phase

At the start up of communication, firstly the MS checks the subscriber password (P). Then MS computes O and N and sends to the AAA server. Results of Subscriber Authentication Phase are mention below:

O=Gh(T⊕)h(e)=⊕e4bd2e7d8e3bc920f2779f6a50f1baca4e34e52

N=h(Kh(T⊕)h(e))=⊕8e4a461c117deb3e968029fe30de7f1e4342c
b03

After receiving those, the AAA server computes N′ by receiving s from SIM and compares it with N.

N′=h(h(s)⊕O)
=8e4a461c117deb3e968029fe30de7f1e4342cb03

As N = N′, the AAA server certifies that the subscriber is authentic. So the AAA server accepts the communication request of the subscriber.

5.3 Network Authentication Phase

The Network's genuineness is ascertained by the following steps. First the AAA server computes M by ascertaining I, P from MS. Thereafter AAA server sends M to MS. After receiving M, the MS computes M′ and compare it with M. Results of Network Authentication Phase is described below:

M=h(T**h(⊕h(s)h⊕(IP)))=⊕ ⊕
576ce1adbdbb1af03010224d4a0002e2794fcc7c

M′=h(T**h(⊕K))=⊕
576ce1adbdbb1af03010224d4a0002e2794fcc7c

As M = M′, the MS certifies that the network is authentic.

CONCLUSIONS

4G mobile communications network is completely described above. It is observed that wireless communication is employed packet switching technology in 4G and somewhere in 3G, as a result high speed secured data as well as voice transmission-reception is possible.

In this paper we have described the proposed password based subscriber and network authentication technique. By adopting 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 under C-programming. Therefore, this authentication method can be applied in real time basis for all sort of 4-G Mobile network. In future, we are exposing to minimize computation cost by selective using of hash functions and logical operators.

REFERENCES

[1] C. T. Bhunia, Information Technology Network and Internet, New Age International Publishers, India, 5th Edition (Reprint), 2006.
[2] William C. Y. Lee, Wireless and Cellular Communications, 3rd Edition, McGraw Hill Publishers, 2008.
[3] D. Goodman, "Cellular Packet Communication", IEEE Transactions on Communications, vol. 38, no. 8, pp. 1272-1280, August 1990.
[4] P. Ramjee, O. Tero, "An Overview of CDMA Evolution towards Wideband CDMA", IEEE Communications Survey, 1998.
[5] F. Adachi, M. Sawahashi, H. Suda, "Wideband DS-CDMA for Next Generation Mobile Communications System", IEEE Communication Magazine, pp 56-69, Sept, 1998.
[6] M. L. Roberts et al, "Evolution of the Air interface of Cellular Communications Systems toward 4G Realization", IEEE Communications Surveys and Tutorials, 8(1), 2006.
[7] J. Pereira, "Fourth generation- Beyond the hype, a new paradigm", IEE 3G Mobile Communication Technologies, London, UK, March' 2001.
[8] L. Lamport. "Password authentication with insecure communication", Communication. ACM, Vol. 24, No. 11, pp. 770-772, 1981.

BIOGRAPHIES:

Tamal Dhar did his B.Tech in 2011 in Information Technology. He is pursuing M.Tech in Computer Sc & Engineering from Dr. B. C. Roy Engineering College, Durgapur-713206, West Bengal, India. His research interests include Mobile Communications, Network Security and Sensor Networks etc.

Chandan Koner did his B.Tech and M.Tech in Computer Sc & Engineering in 2005 and 2007, and Ph.D (Engineering) in 2012 from Jadavpur University. He is currently Associate Professor of Department of Computer Sc & Engineering, Dr. B. C. Roy Engineering College, Durgapur-713206.Dr. Koner is a Member of the Institution of Electronics and Telecommunication Engineers (IETE) and Computer Society of India (CSI), Indian Society for Technical Education (ISTE), Indian Science Congress Association, IACSIT, Singapure, CSTA, USA etc and Associate member of Institute of Engineers (IE), India. His research interests include Mobile Communications, Network Security, Computer Networks etc.