Mutual Authentication Technique Applying Three Entities in 4-G Mobile Communications

Pijush Kanti Bhattacharjee, *Member, IACSIT* and Rajat Kumar Pal

***Abstract*—Fourth Generation (4-G) mobile communications system has an evolution of high speedy data communications with connectivity all sorts of the networks, like 2-G and 3-G mobile networks, Internet, PSTN (Public Switched Telephone Network), PDN (Public Data Network), ISDN (Integrated Services Digital Network), WLAN (Wireless Local Area Network), WPAN (Wireless Personal Area Network), WCAN (Wireless Corporate Area Network), WHAN (Wireless Home Area Network), Wi-Fi, WiMAX (Worldwide Interoperability for Microwave Access), MANET (Mobile Ad Hoc Network), VANET (Vehicular Ad Hoc Network), etc. In 4-G Mobile communications ubiquitous access to applications over the most efficient combination of wireless systems in heterogeneous manner is available. Authentication of mobile subscriber and network is an important criterion due to increasing security threats and attacks in mobile communications. In circuit switching (3-G network), authentication is mutual where both MS and MSC or network authenticate each other, despite in packet switching - only network (servers in PDSN) verifies the authenticity of MS. In this paper, we propose a mutual authentication technique for circuit and packet switching both that examines the authenticity of the subscriber as well as the network by subscriber's password, SIM (expressed as identifier) and biometric property of the subscriber, called as mutual authentication technique using three entities in 4-G mobile communications.**

***Index Terms*—Authenticity of mobile station or subscriber, biometric scheme, challenge/Response mechanism, circuit switching, Packet switching, PDSN, AAA, SGSN, GGSN, identifier, password.**

I. Introduction

Mobile communications are upgraded to 3-G (3rd Generation) network. The distinction between 2-G [1], [2] and 3-G mobile communications is to increase data communication speed.

For effecting packet data services off the RAN (Radio Access Network) in UMTS (Universal Mobile Telecommunication System in USA) and overlooking the MSC is the first step for separating the circuit based world of the PSTN and the packet based world of PDNs (Public Data Networks) and the Internet [3], [4]. The European counterpart of UMTS is WCDMA (Wideband Code Division Multiple Access), generally commercialized as 3GSM. The WCDMA scheme has been ventured 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 adores an innovation for wideband CDMA, compatible with IS-95, which has given name as 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 [1]-[5]. Thus 3-G mobile communications system is able to afford high speed data communications in addition to the normal voice communications. The packet switched may be utilized in different speeds such as 38.4 kbps, 76.8 kbps, 153.6 kbps, 307.2 kbps, 614.4 kbps, 921.6 kbps, 1228.8 kbps, 1843.2 kbps, 2457.6 kbps etc.

Now the authentication technique is explored for identifying correct mobile subscribers as well as the mobile network. For implementing this, three entity like SIM, Password and Biometric property such as caller's fingerprint, image, voice print, retinal scan, clapping and flipping sound etc. are collected and cross interchanged between MS, SIM and the network. Subscriber biometric authentication is a technique to examine a valid subscriber with the help of subscriber's physical characteristics like one's fingerprint, image, voice print, retinal scan, ear's otoacoustic emission, flipping or clapping sound [2] etc.

Proposed three-entity (3-E) subscriber and network authentication technique [2] is an algorithm to authenticate for communicating subscriber according to what you know (password), what you have (SIM) and what you are (biometric entity). Hence the subscriber and the network authenticity are verified by applying password, SIM and biometric entities of a subscriber simultaneously. Thus we propose an efficient and reliable three entity subscriber authentication technique that verifies the authenticity of subscribers as well as MSC or server like PDSN (network) in 4-G mobile communications.

II. Architecture of 3-G Packet Switching Mobile Network

In 3-G mobile communication, voice communication is committed by MSC and its accessories. In packet switching, authentication is checked separately by PDSN servers.

Architecture of a 3rd Generation packet switched wireless network is illustrated below in Fig. 1. Packet switched service able to provide high speed with large volume multimedia and business written message communications.

This 3-G network has circuit switched voice service, circuit switched data service like 2-G (CDMA One or GSM), in addition to this, packet switched data and multimedia service. In 2000 A.D, TIA (Telecommunication Industry

Manuscript received July 16, 2011; revised September 30, 2011.

Authors are with Assam University, Silchar, Pin 788011, Assam, India. (phone: +91-33-25954148, email-pijushbhatta_6@hotmail.com; phone: +91-33-25954148, email-rajat.kp@gmail.com).

Association) standardizes IS-856 (Interim Standard-856) network. It is known 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.

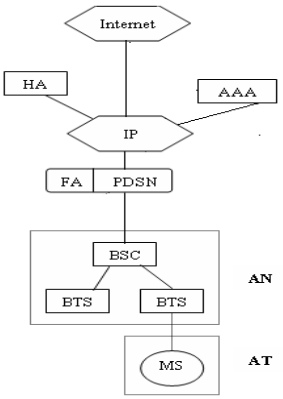

Fig. 1. A typical 3-G wireless data network architecture.

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 TRXs, i.e., transceivers or radio units.

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

In data network [1], [4], 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 cares data and further transmits to PDSN through IS-2001 (Interim Standard-2001) network specified by ITU. Therefore, AN acts as an interface between AT and PDSN. Both AT and AN are connected by IS-856 network.

For enhancing data rate in 2-G, the first thing is to organize GPRS or the PSDN (Public Switched Data Network) for enabling packet data services in GSM and CDMA-One networks. The VoIP (Voice-over-IP) gateway function can be afforded as an extended feature to the circuit gateway or the PDSN for 3-G mobile communications. The VoIP gateway will cling to the vocoding algorithms converting between a voice call encapsulated in an air interface frame and an IP end point that may be an IP-enabled phone, IP based PBX or PC etc [3], [4]. This packet switched data network is having two parts.

(a) Packet Data Serving Node (PDSN): The PDSN is a circuit that offers 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 such as Internet or Intranet etc.

(b) 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 is given guarantee packet data network connectivity services to the mobile users.

Authentication indicates the user to forward 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 function of AAA is accounting. It collects information about the using of packet data services 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 having with the foreign agent (FA). This router resides in the MS home IP network. It acts as a point for communications with the mobile network.

(b) Foreign Agent (FA): This is another router residing in other PDSN. When MS travels to 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 achieved 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 offers 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 providing mainly by two systems like WCDMA and CDMA-2000 [1], [2]. 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 mixture 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).

III. Architecture of 4-G Mobile System

Architecture of a fourth generation (4-G) wireless network is shown in Fig. 2. In essence, 4-G aims to transfer communications architectures from traditional vertical stovepipe to horizontal integrated systems [9]. Personal Networks like WPAN, WCAN, WLAN, Wi-Fi, WiMAX, MANET, VANET, etc. are a dynamic network building on the above mentioned wireless networking technologies, which facilitate personalized communications with any number of subscribers anywhere at any time. Fig. 2 shows the network architecture established by 4-G mobile communications. Thus all the subscriber's networks connected to 4-G as personal network can be expanded or shrunk depending on the availability of users, their demands and environment. A WPAN is a network of devices that consist of a mobile phone, a PDA, a notebook PC, a digital camera, etc. The WPAN expansion can physically be made via interconnecting structures, e.g., GSM and CDMA 2-G, 2.5-G GPRS (General Packet Radio Service), EDGE (Enhanced Data Rates for GSM Evolution), 3-G mobile communications (WCDMA, CDMA-2000, UMTS, etc.) and the Internet, to remote networks such as home area networks, corporate area networks or vehicular area networks, etc. in 4-G mobile communications.

This 4-G network can provide circuit switched voice service, circuit switched data service like 2-G (CDMA-One or GSM), 3-G (WCDMA, CDMA-2000, UMTS), in addition to this packet switched data and multimedia service at a very high data rate [6], [4]. Data rate dimensioning targets for 4-G is 50 to 500 bit/s/Hz/Km^2, whereas in 3-G it is around 10 bit/s/Hz/Km^2 using HSDPA (High Speed Downlink Packet Access) technology.

Now we mention some abbreviations and briefly describe them that are used in mobile communications technology.

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

BTS—Base Transceiver Station serves mobile connection to one or more cells and sectors in the cellular network, and contains TRXs, i.e., transceivers or different radio units.

MS to BTS path—It is a reverse path that is used for up linking.

BTS to MS path—It is a forward path that is used for down linking.

BSC—Base Switching Center that controls one or more BTSs and performs inter-BTS and intra-BTS switching and handovers.

BSS—Base Station Subsystem, like BSCs and BTSs.

RNC—Radio Network Controller in UMTS (Universal Mobile Telecommunication Service) in 3-G, 4-G, like BSC in GSM or CDMA in 2-G and 3-G.

MSC—Mobile Switching Center or Main Switching Center, which is a basic digital electronic exchange, e.g., 5ESS means the fifth version of electronics switching system.

MSC controls all the functions of a mobile network via different registers or servers, especially for voice and low speed data communications.

Access controller provides connection to user's network with server or switch.

Service adaptation or gateway – It extends connection to other worldwide network or Internet.

PSTN—Public Switched Telephone Network, i.e., land or wire line telephone network.

PDN—Public Data Network.

ISDN—Integrated Services Digital Network.

Server—AAA server, or PDSN server, or any other server for high speed data communications, in general, but in special conditions it can also provide voice communications. Switch – It is used to give circuit connectivity like circuit or packet or both switching system for voice and data communications.

Workstation—It is used for connecting data network or any other network consisting of computers (PCs, Laptop, etc.), mobile phones, etc.

In 4-G mobile communications, the voice and data services are arranged in same pattern as in GSM and CDMA-One (in 2-G) or WCDMA, CDMA-2000, UMTS, etc. (in 3-G or 4-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 or RNC carries out mobility management, i.e., controlling hand over or hand off. Additional networks are provided in 3-G, 4-G for providing packet switched data service usually higher speed than that of circuit switched data service in 2-G.

In UMTS (Universal Mobile Telecommunications System), 3-G and 4-G, the core network, i.e., server or switch consists of SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node), which are interconnected via IP network. The SGSN keeps track the location of individual mobile stations, and performs security functions and access control. The GGSN encapsulates packets received from external IP networks and routes them towards the SGSN. GGSN directs outside data to SGSN. SGSN is connected to the RNC (Radio Network Controller), which is further attached to BTS via asynchronous transfer mode; both RNC and BTS stay in UTRAN (UMTS Terrestrial Radio Access Network) unit. RNC is in charge of the overall control of the logical resources provided by UTRAN. Mobile communications are made through a radio interface based on WCDMA technology.

In 4-G mobile communications, additional network is provided that Access Controller or Gateway for the network

is connected from the switch or server in between the switch or server to user's equipment or Internet or other networks. It works seamlessly on the basis of Internet protocol IPv4 or IPv6. There are lot of sub-networks like 2-G and 3-G mobile networks, WPAN, WLAN, WCAN, WHAN, Wi-Fi, WiMAX, MANET, VANET, etc. are connected to the main 4-G mobile network, at the same time with all other outside networks such as Internet, PSTN, ISDN, etc. through respective gateways or access controllers. Thus the gateways and access controllers are taken key part in 4-G mobile communications for imparting local network or MS to afford world wide connectivity.

In 4-G, mobility management is responsible for tracking the dynamics of the personal network and users. Several types of mobility are identified within personal networks, viz. terminal mobility, network mobility, and session mobility. QoS (Quality of Service) is defined as a set of service characteristics that the network is requested to meet when transporting a sequence of data packets. The service characteristics can be expressed in terms of throughput, delay, loss, bit error rate, or as a relative priority of access to the network. End-to-end QoS in personal network is calculated in different domains: WPAN, UMTS, and IP QoS-enabled interconnecting structures such as the future Internet. In this heterogeneous environment, the end-to-end QoS would rely on the coordination of QoS mechanisms in different domains along the end-to-end communication path. Each of these domains (Bluetooth, WLAN, WCAN, MANET, IEEE 802.15.3 or UMTS, etc.) has its own QoS provisioning mechanisms and separately QoS for each domain is computed.

IV. Mobile Authentication Technique Using Three Entities for 4-G Mobile Network

The proposed mobile authentication technique using three entities (3-E) is a set of four different phases, called as, Subscriber Enrollment Phase, Subscriber Authentication Phase, Network Authentication Phase and Subscriber Password Change Phase.

A. Subscriber Enrollment Phase

In subscriber enrollment phase, the subscriber has to enroll to a particular server may be AAA or PDSN server or switch (MSC) belonging to the network. This phase is executed only once for one subscriber.

SE1: The subscriber chooses his identifier I, password P and Biometric property B, i.e., the extracted template of biometric entity of the subscriber, e.g., caller's fingerprint, voiceprint, face image, clapping and flipping sound [2] etc. Thereafter the subscriber passes these information (*I, P, B*) secretly to the authority concerned (mobile service provider) for initialization of the SIM.

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

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

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

SE2.3: Stores the parameters {*B, 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.

B. Subscriber Authentication Phase

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

The subscriber enters his identifier *I* and password P' and imprints his biometric entity B' from the biometric device in the MS, e.g., caller's fingerprint, voiceprint, face image, clapping or flipping sound etc. are taken by the camera or the receiver and its associated electronics circuit installed in the MS, ultimately these template's array or matrix information represents the biometric entity B′.

SA1: The MS computes $L=h(s)\oplus G\oplus h(I\oplus P'\oplus B')$. Then checks whether L is equal to the $h(s)$ or not.

[$L=h(s)$ when $G\oplus h(I\oplus P'\oplus B')=0$, i.e., completely matching *G* and $h(I\oplus P'\oplus B')$]. If $L=h(s)$, MS performs the following tasks, otherwise terminates the communication.

SA1.2: Computes $O=(G\oplus h(T))$, where T is the current time while the subscriber initializing a call.

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

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

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

SA2.1: The server or switch checks the difference between *T** and *T* whether it is valid time interval or not, for measuring transmission delay, i.e., $T^*-T=\delta t_1$. If it (δt_1) is valid time interval, i.e., correct, the server or switch performs the next tasks.

SA2.2: The server or switch requests for e, s from SIM.

SA2.3: SIM sends e, s to the server or switch through paging or secured channel.

SA2.4: The server computes $N'=h(h(e)\oplus h(s)\oplus O)$.

SA2.5: The server or switch checks whether $N = N'$. If it holds good, i.e., matches, the server or switch accepts the communication request of the subscriber.

If $N \neq N'$, the server or switch cancels the communication request of the subscriber with a notice of failure subscriber's authentication phase.

C. Network Authentication Phase

The network (Server or Switch) is verified in this phase, this is executed when the subscriber is authentic.

NA1: The server or switch requests for *I, P, B* from SIM.

NA2: SIM sends *I, P, B* to the server or switch through secured channel.

NA3: The server or switch computes $Q=h(T^{**}\oplus h(T\oplus h(s)\oplus h(I\oplus P\oplus B))$, where T^{**} is current time.

NA4: The server or switch sends (Q, T^{**}) to the subscriber through a paging channel.

Suppose subscriber receives (Q, T^{**}) at time T^{***}.

NA5: MS checks the difference between T^{***} and T^{**} whether it is valid time interval for transmission delay or not, i.e., $T^{***}-T^{**}=\delta t_2$. If it ($\delta t_2$) is correct then the MS performs the next tasks.

NA5.1: MS computes, $Q'=h(T^{**}\oplus h(T\oplus K))$

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

If $Q \neq Q'$, call request is terminated, hence network (server or switch) authentication fails.

D. 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) and imprints his biometric entity (B) at the biometric device in MS. The MS verifies the entered I and P with the stored values of I and P in the SIM and the biometric entity of the subscriber with the stored values B. 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 $G' =h(I\oplus P'\oplus B)$ and $K'=(h(s)\oplus G')$

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

V. Advantages of the Proposed Authentication Technique

The proposed authentication system is working in two ways. In one hand it connects the authentic, i.e., desired subscribers to its home or appropriate network by checking mutually. With adoption of this mutual check up system, huge amount of data, messages, information etc. are interchanged between MS and network (MSC or server) smoothly in 4-G mobile communications. It is having lot of advantages which are mentioned below:

(a) Here subscriber authentication is verified by the physical characteristics of the user, i.e., biometric property.

(b) One way hash function and XOR operation are only used for authentication purpose which minimizes computation complexity and program execution time.

(c) 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.

(d) Any subscriber's identifier (I), password (P), database (B) etc. are not require to store in the server (may be AAA or PDSN) or switch, hence these information cannot be hacked from the network (server or MSC or switch).

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

VI. Experimental Results from the Proposed Algorithm in 4-G Mobile Communications

The proposed algorithm is tested by using C-language program under Linux environment. We obtain very good and reliable results which can be easily implemented in the 4-G mobile network for the authentication purpose. We are mentioning the experimental results below. The following parameters are considered for executing the program. In case of the biometric entity, for simplicity we have taken twenty numbers of alphabetic characters as mentioned below.

Subscriber or user Password (P) is taken "User's Authentication".

Subscriber or user Identifier (I) is taken "IdentityofSubscriber".

Subscriber or user Biometric Entity (B) is "Biometric Fingerprint".

Secret key (s) of the SIM allotted by AAA server is "71".

Secret number (e) of the SIM allotted by AAA server is "255".

Timestamps are considered like followings

T - 14-02-2010, 10:10

T^* - 14-02-2010, 10:11

T^{**} - 14-02-2010, 10:12

T^{***} - 14-02-2010, 10:13

Timestamps are within valid time intervals.

A. Subscriber Enrollment Phase

The subscriber chooses identifier (I), password (P), biometric property (B) as mentioned above and submits this information to the server or switch (MSC). The server or switch 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:

Subscriber Password (P) = User's Authentication =
5573657227734175746865 6e7469636174696f6e

$G =h(I\oplus P\oplus B)=$
1a5facec6b6e3a17d38d03421a42c3135f7118c5

$K=h(s)\oplus G=$
09b27cd2330845dc5cb643ec945f072c0a44324b

B. Subscriber Authentication Phase

At the start up of communication, firstly the MS checks the subscriber password (P) and biometric property (B) with current time 14-02-2010, 10:10 (T). Then MS computes O and N and sends to the server or switch. Results of Subscriber Authentication Phase are mention below:

$O =G\oplus h(T)=$
10255d21d796b502646abd236c4cd66b2c90781c

$N =h(h(e)\oplus K\oplus h(T))=$
6f8124d9de0a2750bf61acab3a40a4520e78587c

After receiving those at server or switch on 14-02-2010, 10:11 (T^*), comparing $T^*-T\leq 1$ m (δt_1), is a valid time interval, the server or switch computes N' by receiving e and s from SIM and compare it with N.

$N' =h(h(e)\oplus h(s)\oplus O)=$
6f8124d9de0a2750bf61acab3a40a4520e78587c

As $N=N'$, the server or switch certifies that the subscriber is authentic. So the network (server or switch) accepts the communication request of the subscriber.

C. Network Authentication Phase

The Network's genuineness is ascertained by the following steps. First the server or switch computes Q by ascertaining I, P, B, 14-02-2010, 10:12 (T^{**}) from MS. Thereafter the server or switch sends Q to MS. After receiving Q at the MS on 14-02-2010, 10:13 (T^{***}), comparing $T^{***}-T^{**}\leq 1$ m (δt_2), which is a valid time interval, then the MS computes Q' and compare it with Q. Results of Network Authentication Phase is described below:

$Q= h(T^{**}\oplus h(T\oplus h(s)\oplus h(I\oplus P\oplus B))=$

12570a0b41bab78a37c1f3c8f329d755b8e7f37a
$Q' = h\,(T^{**} \oplus h\,(T \oplus K)) =$
12570a0b41bab78a37c1f3c8f329d755b8e7f37a

As $Q = Q'$, the MS certifies that the network (server or switch) is authentic.

VII. Conclusions

In this paper we have elaborately discussed the proposed three entity subscriber and network (server or switch) authentication technique in 4-G mobile communications. By applying this technique, 4-G mobile communications are completely restricted within the proper authentic subscriber and the network. This technique is very fast operating, since our proposed algorithm written in C-language program is tested and found absolutely correct. Therefore, this authentication method is adopted in real time basis for all sorts of 4-G mobile network.

References

[1] T. S. Rappaport, *Wireless Communication: Principles and Practice*, 2nd ed, India: Prentice Hall Pub Ltd, 2006.

[2] P. K. Bhattacharjee, and R. K. Pal, "A novel approach on mutual authentication techniques in 4-G mobile communications," *International Journal of Computer Engineering and Computer Applications*, India, vol. 1, no. 1, June 2011.

[3] M. L. Roberts, M. A. Temple, R. F. Mills, and R. A. Raines, "Evolution of the air interface of cellular communications systems toward 4G realization," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 1, pp. 2-23, Mar. 2006.

[4] F. Adachi, M. Sawahashi, and H. Suda, "Wideband DS-CDMA for next generation mobile communications system," *IEEE Communication Magazine,* vol. 36, no. 9, pp. 56-69, 1998.

[5] P. K. Bhattacharjee, "Hybrid GSM and CDMA mobile communication systems enhancing channel capacity," in *Proc. of National Conference on Wireless and Optical Communications (NCWOC-08)*, Chandigarh, 2008, pp 1-8.

[6] S. N. Diggavi, N. Al-Dhahir, A. Stamoulis, R. Calderbank, "Great expectations: the value of spatial diversity in wireless networks," *Proceedings of the IEEE*, vol. 92, no. 2, pp. 219-270, Feb. 2004.

[7] P. Ramjee and O. Tero, "An overview of CDMA evolution towards wideband CDMA," *IEEE Communications Surveys*, vol. 1, no. 1, 1998.

[8] William C. Y. Lee, *Wireless and Cellular Communications*, 3rd ed., McGraw Hill Publishers, 2008.

[9] P. K. Bhattacharjee, "A new era in mobile communications- GSM and CDMA," in *Proc. of National Conference on Wireless and Optical Communications (NCWOC-07)*, Punjab Engg College, 2007, pp 118-126.

[10] D. Goodman, "Cellular packet communication," *IEEE Trans. on Communications,* vol. 38, no. 8, pp. 1272-1280, August 1990.

Pijush Kanti Bhattacharjee is associated with the study in Engineering, Management, Law, Indo-Allopathy, Herbal, Homeopathic & Yogic medicines. He is having qualifications ME, MBA, MDCTech, AMIE (BE or BTech), BSc(D), BIASM, CMS, PET, EDT, FWT, DATHRY, BA, LLB, KOVID, DH, ACE, FDCI etc. He had started service in Government of India, Department of Telecommunications (DoT) since 1981 as a Telecom Engineer,where he worked upto January 2007 (26 Years), lastly holding Assistant Director post at Telecom Engineering Centre, DoT, Kolkata, India. Thereafter, he worked at IMPS College of Engineering and Technology, Malda, WB, India as an Assistant Professor in the Department of Electronics and Communication Engineering from January 2007 to February 2008, from Feb 2008 to Dec 2008 at Haldia Institute of Technology, Haldia, WB, India, from Dec 2008 to June 2010 at Bengal Institute of Technology and Management, Santiniketan, WB, India and June 2010 to Aug 2010 at Camellia Institute of Technology, Kolkata, India. He joined in Assam University (A Central University), Silchar, Assam, India in Sept 2010 at the same post and department. He has written two books "Telecommunication India" & "Computer". He is a member of IACSIT, Singapore; CSTA, USA; IAENG, Hongkong; and IE, ISTE, IAPQR, IIM, ARP, India. His research interests are in Mobile Communications, Image Processing, VLSI, Nanotechnology, Management and Environmental Pollution.

Rajat Kumar Pal is a Professor of the Department of Information Technology under Triguna Sen School of Technology of Assam University, Silchar. He received his B.E. and M.Tech. degree from B. E. College (CU) and Calcutta University, respectively in 1985 and 1988, and awarded Ph.D. degree from IIT, Kharagpur in 1996. He was serving the University of Calcutta as a faculty in the Department of Computer Science and Engineering since 1994,and worked as the Head of the Department during 2005-2007. Dr. Pal has published more than 100 research articles and authored a book entitled "Multi-Layer Channel Routing: Complexity and Algorithms" that has jointly been published from *NAROSA Publishing House*, New Delhi, *CRC Press*, Boca Raton, USA, and *Alpha Science International Ltd*, UK, in September 2000. A second book co-authored by Dr. Pal on *Control System Theory* is in press now that will be published shortly. His major research interests include VLSI design, Graph theory and its applications, Perfect graphs, Logic synthesis.