International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, 2010
1793-8201

Mutual Authentication Tracking Loop Technique for 3-G Mobile Communications

Pijush Kanti Bhattacharjee, *Member, IACSIT*

***Abstract*—Hacking and threats are increasing day by day. Authentication of mobile subscribers and network is an important criterion to the researchers. Now mobile communication system (3-G or advanced) has been developed to speed up the data communication. 3-G mobile communication uses two different switching techniques: circuit switching for voice and low speed data communications, and packet switching mainly for data communication, but can afford 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 circuit switching (3-G network), authentication is mutual where both MS and MSC or network authenticate each other, but in packet switching only network (servers in PDSN) examines the authenticity of MS. In this paper, I propose a mutual authentication tracking loop technique that verifies the authenticity of the subscriber as well as the network by subscriber's password, SIM and biometric property of the subscriber. Two biometric parameters are used in which one biometric parameter is stored in SIM. The other biometric parameter, taken as voice frequency for the common words spoken by a subscriber, called certified document (CD), is stored at the server (PDSN or MSC). An algorithm is developed by these four entities to check this authentication process at the starting time of a call as well as a regular time intervals (say 10~20 secs) while the call is progressing, named mutual authentication tracking loop technique for 3-G mobile communications.**

***Index Terms*—Biometric property, Certified Document, Voice frequency, Clapping sound, Flipping sound, Mutual Authentication tracking, Packet Switching, Password, SIM.**

I. Introduction

The influence of the Internet and IP technology has extended to enlighten the cellular area in high speed data transmission [1]–[5]. 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 [3]-[6].

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 [1], [5]-[6]. Now four entity mutual authentication tracking loop technique is proposed for identifying correct mobile subscriber as well as mobile network always.

The mutual authentication [8] tracking loop technique is a scheme where authenticity of a subscriber is verified after each fixed time interval (may be 10~20 secs) by the mobile station during conversation or progress of a call. When the subscriber is attempting to make a call connection, the authenticity of subscriber is checked, according to what you know (Password), what you have (SIM), what you are (Biometric entity) and what you posses (Certified Document). This mutual authenticity is verified by applying identifier, password, biometric entities of the subscriber, one in SIM and the other in server or switch as certified document (CD). Here voice frequency for the common words spoken by the subscriber like Hello, Well, OK, Achha, Right, Carry on, Take Care, Bi etc are taken as certified document. The authenticity of a subscriber at the starting time of talking as well as in course of talking in regular intervals (say 10~20 secs) is checked by the mobile station by certified document only. Thus mutual authentication tracking loop ensures the system more secure and safe. This is also identifying that proper or authenticated subscriber is taking part during whole conversations in a call, eliminating unauthorized subscribers to intervene.

II. Architecture of 3-G 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) [3]-[5], in addition to this packet switched data and multimedia service [4]-[6]. In 2000 A.D, TIA (Telecommunication Industry Association) publishes IS-856 (Interim Standard-856) network. It is known CDMA 2000

Pijush Kanti Bhattacharjee is an Assistant Professor in the Department of Electronics and Communication Engineering, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He was an Ex Asssitant Director in the Department of Telecommunications (DoT), Government of India, India. He has possessed vast working experience in the field of Telecommunications including Mobile Communications, Image Processing, VLSI etc during last 29 years.

He is a member of IACSIT, Singapore; CSTA, USA; IAEng, Hongkong. (phone: +91-33-25954148; email: pijushbhatta_6@hotmail.com)

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 information etc.

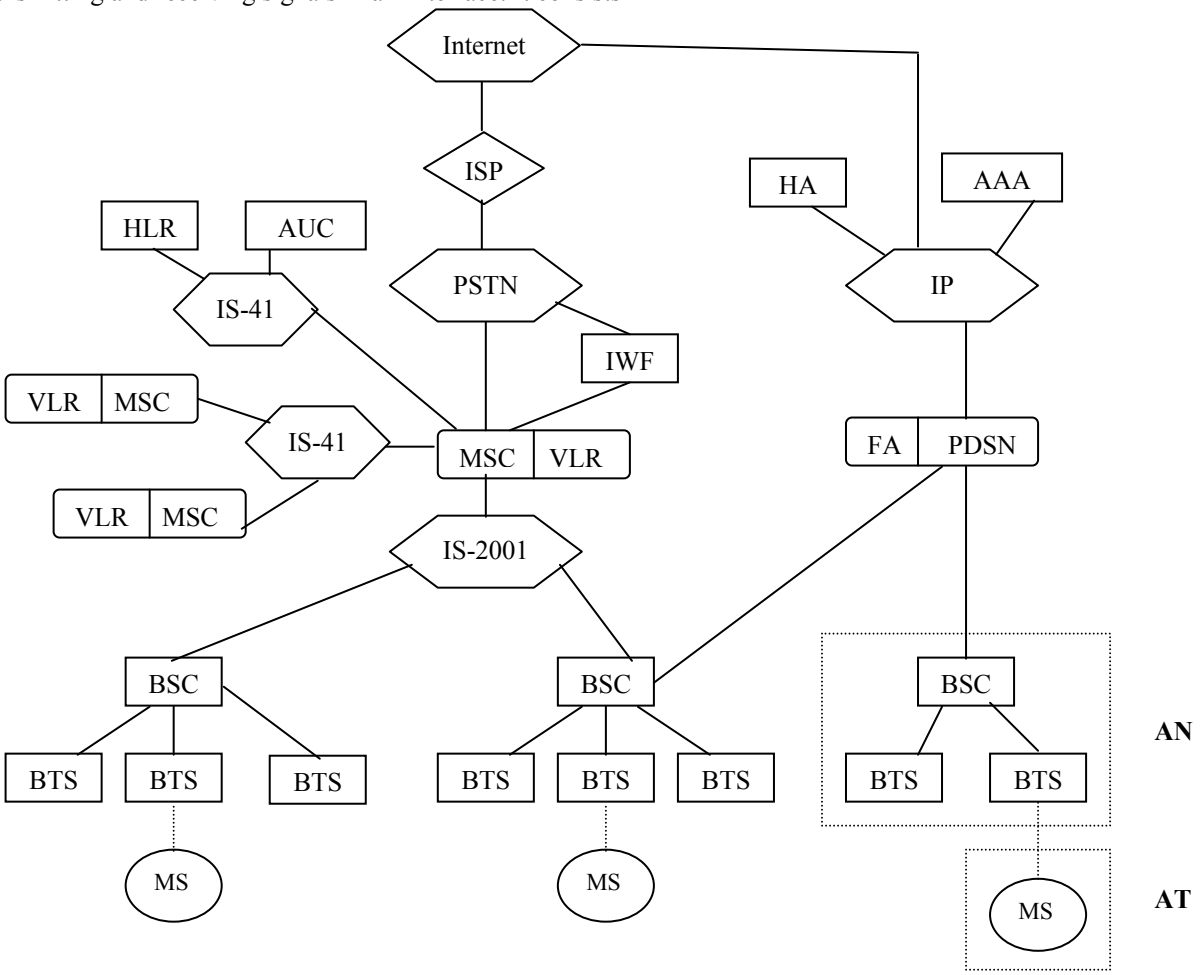

Fig.1. A typical 3G wireless network architecture with high speed data network

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.
BSS – Base Station Sub Systems include BSCs & BTSs
BSC – Base Switching Center controls one or more BTSs and perform inter BTS and intra BTS switching and handovers or handoffs.
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 or servers, especially for voice and low speed data communications.
HLR – Home Location Register occupies identities of mobile subscriber as IMSI [International Mobile Subscriber's Identity], service parameters, location information etc.
VLR – Visitor Location Register contains permanent and temporary mobile subscriber's identity as TMSI, ISDN directory number, routing etc, especially while a subscriber is roaming outside from home cell area or parent BTSs.
EIR – Equipment Identity Register contains identity of mobile equipment i.e. instrument number, called International Mobile Equipment Identity [IMEI], connected with MSC or PDSN. It may be converted to valid, suspect or prohibited type subscriber using proper software.
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.

In data network, MS is called Access Terminal (AT) where data or messages in written form is originated or terminated, where as BTS with BSC are called Access Network (AN) which handles data and further transports to PDSN through Interim Standard-2001 (IS-2001) network specified by ITU [1], [3]-[8]. 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 [1]-[6], [8] 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 [1]-[6]. 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).

III. Proposed Mutual Authentication Tracking Loop Technique for 3-G Mobile Network

The proposed mutual authentication tracking loop technique is a collection of five different phases, namely, Subscriber Enrollment Phase, Subscriber Login Authentication phase, Network Authentication Phase, Subscriber Authentication Tracking Loop Phase and Subscriber Password Change Phase. Out of these five phases, Password Change Phase is operated to change the password only.

A. Subscriber Enrollment Phase

In subscriber enrollment phase, the subscriber is enrolled to particular switch (MSC) or AAA server 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. Now subscriber average voice frequency (V) for the common words at the time of talking (like Hello, Ok, Bi etc) is measured by sophisticated electronic instrument in Hz. Thereafter the subscriber passes these information (I, P, B) secretly to the authority concerned (mobile service provider) for initialization the SIM and V for storing in the server or switch.

SE2: The AAA server or switch has received the

enrollment request from subscriber with I, P, B, V data and executes the following tasks.

SE2.1: Stores V into the AAA server or switch.

SE2.2: Computes G = h (I ⊕ P ⊕ B), h (.) is a one-way hash function and ⊕ is a bitwise XOR operation.

SE2.2: Computes K= (h (V) ⊕ G)

SE2.3: Stores the parameters {B, G, I, K, P} into a SIM.

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

B. Subscriber Login Authentication Phase

This phase is executed every time when the subscriber is attempting to make a call connection.

The subscriber enters his identifier I, password P′ and imprints his biometric entity B′ from the biometric device in the MS e.g. caller's fingerprint, clapping sound, flipping sound, face image etc are taken by its associated electronics circuit installed in MS, ultimately these template's array or matrix information represents biometric entity B′. The subscriber voice frequency (V′) for the common words is computed by highly sophisticated electronics instrument lying in MS which can analyze exact frequency range in Hz.

SA1: SIM requests for V from AAA server or switch.

SA2: AAA server or switch sends V to SIM through paging or secured channel.

SA3: MS checks that |V ~ V'| is tolerable (within certain range) or not. If tolerable then performs the following tasks, otherwise sends authentication failure message to subscriber.

SA3.1: The MS computes L= h (V) ⊕ G ⊕ h (I⊕ P′⊕ B′). Then checks whether L is equal to the h (V) or not. [L = h (V) when G ⊕ h (I ⊕ P′ ⊕ B′) = 0 i.e. completely matching G and h (I ⊕ P′ ⊕ B′)]. If L = h (V), MS performs the following tasks, otherwise terminates the communication.

SA3.2: Computes O = (G ⊕ h (T)), where T is the current time while the subscriber initializing the call.

SA3.3: Computes N = h (K⊕ h (T)).

SA3.4: Sends the communication request {O, N, T} to the AAA server or switch.

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 i.e. whether [T* ~ T] is valid time interval for measuring transmission delay or not. If it is correct (valid) then the AAA server performs the next tasks, otherwise terminates communication.

SA2.4: Computes N′ = h (h (V) ⊕ O).

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

If N ≠ N′, the AAA server or switch cancels the communication request of the subscriber due to failure of subscriber authentication phase.

C. Network Authentication Phase

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

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

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

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

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

Suppose subscriber receives (M, T**) at time T***.

NA5: MS checks the difference between T*** and T** i.e. whether [T*** ~ T**] 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**⊕ h (T ⊕ K))

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

If M ≠ M′, call request is terminated, hence network authentication fails.

D. Subscriber Authentication Tracking Loop Phase

This phase is executed to check authenticity of a subscriber (both calling and called subscribers) when the call is continuing i.e. the conversation is going on. This phase is executed at a regular interval say 10~20 secs (ΔT) during the time of talking by a calling subscriber with the called subscriber.

The MS checks its current voice frequency for the common words (V′) with that of the stored voice frequency (V) at the server or switch.

The MS checks that |V ~ V'| is tolerable (within certain range) or not after every ΔT interval.

If it is tolerable, MS does not perform any task.

If it is not tolerable then MS sends the authentication failure message to the subscriber cutting or terminating communication link with the server i.e. communication is not further permitted or allowed.

E. 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), password (P′), imprints his biometric entity (B′) and voice frequency (V′) at the biometric device in MS.

SP1: MS requests for V from AAA server or switch.

SP2: AAA server or switch sends V to MS through paging or secured channel.

The MS checks that |V ~ V'| is tolerable (within certain range) or not.

If it is tolerable, MS performs the following tasks, otherwise repeat the above procedure.

SP3: 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 B′ with the stored values B. If all the verifications are matched correctly, then MS executes the following tasks.

SP4: Asks the subscriber to enter a new password and he chooses a new password P* and enters it.

SP5: Computes G* = h (I ⊕ P* ⊕ B) and
K* = (h (V) ⊕ G*)

SP6: The P*, G* and K* are stored in the place of P, G and K respectively.

IV. 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. By adopting this mutual check up system, huge amount of data, messages, information etc are interchanged between MS and network (MSC or PDSN) smoothly in 3-G mobile communications. At the same time this authentication technique keeps an eye to the authentic subscriber using the call (whole duration) under regular intervals. It has lot of advantages which are specifically listed below:

1) Subscriber authentication is checked after every fixed time interval by the MS (say 10~20 secs).
2) Subscriber authentication is checked by the physical characteristics of the user i.e. biometric property.
3) One way hash function and XOR operation are only used which minimizes computation complexity and time.
4) Many SIMs with the same identifier can not be allocated for service i.e. the same login (identifier) from different SIM can not make connection to the network.
5) Any subscriber's identifier (I), password (P), biometric property (B) are not require to store in the AAA server or switch, hence these information can not be hacked from the server or switch.
6) The user can freely choose his password and change the password as and when necessary.
7) I, P, B can be reset or changed with user's request by the authority (service provider) without concerning the server or switch, but certified document i.e. voice frequency (V) is only changed by consulting the server or switch.

V. Experimental Results from The Proposed Algorithm

The proposed algorithm is tested by exploring in C-language programming under Linux environment. Very fairly results are obtained, which can be easily implemented in the mobile network for this authentication purpose. I describe the experimental result below. The following parameters are considered for executing the program. In case of the biometric entity, for simplicity I have taken twenty numbers of alphabetic characters as mentioned below.

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

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

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

Subscriber or user Average voice frequency (V) for the common word (say Hello) is "2653" Hz.

Timestamps are considered like followings

T - 14-01-2010, 11:12
T* - 14-01-2010, 11:13
T** - 14-01-2010, 11:14
T*** - 14-01-2010, 11:15

Timestamps are within valid time intervals.

A. Subscriber Enrollment Phase

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

Subscriber Password (P) =
5573657227734175746865 6e7469636174696f6e
G = h (I⊕ P⊕ B) =
1a5facec6b6e3a17d38d03421a42c3135f7118c5
K= (h (V) ⊕ G) =
954b44b8e6429c814d3a20e5851bd25e0f5099fe

B. Subscriber Authentication Phase

At the starting time of communication, firstly the MS checks or matches the subscriber identifier (I), password (P), biometric property (B) and Voice frequency (V) by verifying whether L = h (V). Then MS computes O and N and sends to the AAA server or switch. Results of Subscriber Authentication Phase are mentioned below:

O = G ⊕ h (T) =
e17622f46d3761b6760b3b621a76e0348c3433bc
N = h (K⊕ h (T)) =
501189a7d4608a6ec5bbc09cdf3f28879a5fbd69

After receiving those, the AAA server or switch computes N′ and compares it with N.

N′ = h (h (V) ⊕ O) =
501189a7d4608a6ec5bbc09cdf3f28879a5fbd69

As N = N′, the AAA server or switch certifies that the subscriber is authentic. So the AAA 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 AAA server or switch computes M by ascertaining I, P, B 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 (T⊕ h (V) ⊕ h (I⊕ P⊕ B))) =
C35411969b3a4729b5545cd3003128c2f80228b
M′= h (T**⊕ h (T⊕ K)) =
C35411969b3a4729b5545cd3003128c2f80228b

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

D. Subscriber Authentication Tracking Loop Phase

While a call is continuing, MS (both calling and called subscribers) measures its current voice frequency for the common words (V') and requests for stored voice frequency (V) from the server or switch, If |V ~ V'| is tolerable, then only the communication or call is continuing, otherwise the call is terminated with an authentication tracking loop failure message.

VI. Conclusion

In this paper mutual authentication tracking loop technique for subscriber and server authentication system in a continuous way is explored. By adopting this technique, the mobile communications are completely restricted within the proper authentic subscriber and the network (Server or

Switch). This technique is very fast operating since the proposed algorithm tested under C-language programming. Therefore, this authentication technique can be applied in real time basis for all sorts of 3-G Mobile networks, even advanced generation mobile network also.

REFERENCES

[1] William C. Y. Lee, Wireless and Cellular Communications, 3rd Edition McGraw Hill Publishers, 2008.
[2] T. S. Rappaport, Wireless Communication: Principles and Practice, Prentice Hall Pub Ltd, 2nd Ed, 2006.
[3] P. K. Bhattacharjee, "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, 2007.
[4] D. Goodman, "Cellular Packet Communication", IEEE Trans on Comm., vol. 38, no. 8, pp. 1272-1280, August 1990.
[5] P. K. Bhattacharjee, "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, 2008.
[6] P. Ramjee, O. Tero, "An Overview of CDMA Evolution towards Wideband CDMA", IEEE Communications Survey, 1998.
[7] H. Kim, H. Afifi, "Improving Mobile Authentication With New AAA Protocols", IEEE International Conference on Communication (ICC 2003) vol 1, pp 497-501, May, 2003.
[8] C. Koner, P. K. Bhattacharjee, C. T. Bhunia, U Maulik, "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, 2009.

Dr. Pijush Kanti Bhattacharjee is a pioneer in Engineering, Management, Law, Indo-Allopathy, Herbal, Homeopathic and Yogic medicines. He is having qualifications M.E, MBA, MDCTech, A.M.I.E, B.Sc, B.A, LLB, BIASM, CMS, PET, EDT, FWT, DATHRY, B.Mus, KOVID, DH, ACE, FDCI etc. He worked as an Engineer in Department of Telecommunications (DoT), Govt. of India from June 1981 to Jan 2007 (26 years), lastly holding Assistant Director post at RTEC [ER], DoT, Kolkata, India. Thereafter, he started working at IMPS College of Engineering and Technology, Malda, WB, India as an Assistant Professor in Electronics and Communication Engineering Department from Jan,2007 to Feb,2008 and Feb, 2008 to Dec, 2008 at Haldia Institute of Technology, Haldia, WB, India. In Dec, 2008 he joined at Bengal Institute of Technology and Management, Santiniketan, WB, India in the same post and department. He has written two books "Telecommunications India" & "Computer". He is a Member of IE, ISTE, IAPQR, ARP, IIM, India; CSTA, USA; IACSIT, Singapore and IAENG, Hongkong. His research interests are in Mobile Communications, Image Processing, VLSI, Network Security, Nanotechnology etc.