International Journal of Computer Theory and Engineering, Vol. 1, No. 3, August 2009
1793-8201

A Novel Approach for Authentication Technique in Mobile Communications

C. Koner, *Member, IACSIT*, P. K. Bhattacharjee, *Member, IACSIT*, C. T. Bhunia, *Sr. Member, IEEE* and U Maulik *Sr. Member, IEEE*

***Abstract*—Authentication of mobile subscriber is a challenge of future researchers due to increasing security threats and attacks with the enhanced population of wireless traffic. 3G mobile communication system has been developed to speed up the data communication. In general the authentication technique in 2G mobile communication is solely dependent on checking the authenticity of MS (Mobile Station or Subscriber) by challenge/response mechanism. Here authenticity is one-way for which MSC (Mobile or Main Switching Center) checks the validity of MS. 3G mobile communication works on two different switching techniques. One is circuit switching for voice and low speed data communications. The other one is 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 is established by packet switching process through PDSN (Packet Data Serving Node) servers. In circuit switching (3G 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, we enlighten different new approaches that can be effectively used as an authentication tool in 3G mobile communications.**

***Index Terms*—Authenticity of Mobile Station or Subscriber, Challenge/Response Mechanism, Circuit Switching, Identifier, Packet Switching, PDSN, Password.**

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 [6]-[9]. 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]. The packet switched can be enhanced 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. There are different control channels e.g. MAC channel, Reverse Traffic Channel, Access Channel etc which are associated to and fro MS to MSC or PDSN to set up the communication path implemented by proper authentication scheme.

Chandan Koner is an Assistant Professor in the Department of Computer Science and Engineering, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He is pursuing PhD course. He is member of IACSIT and IAENG (phone: +91-9434535556).

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. (phone: +91-33-25954148, +91-9432166768; fax: +91-3463-271354;).

Chandan Tilak Bhunia is a Director, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He is a Senior Member of IEEE, FIE (I) and FIETE.(phone: +91-9434033157).

Ujjwal Maulik is currently a Professor in the Department of Computer Science and Technology, Jadavpur University, Kolkata, India. He is a Senior Member of IEEE and FIE(I). (phone: +91-33-24131766).

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 [6]-[9]. In 2000 A.D, TIA (Telecommunication Industry Association) publishes 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.

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,

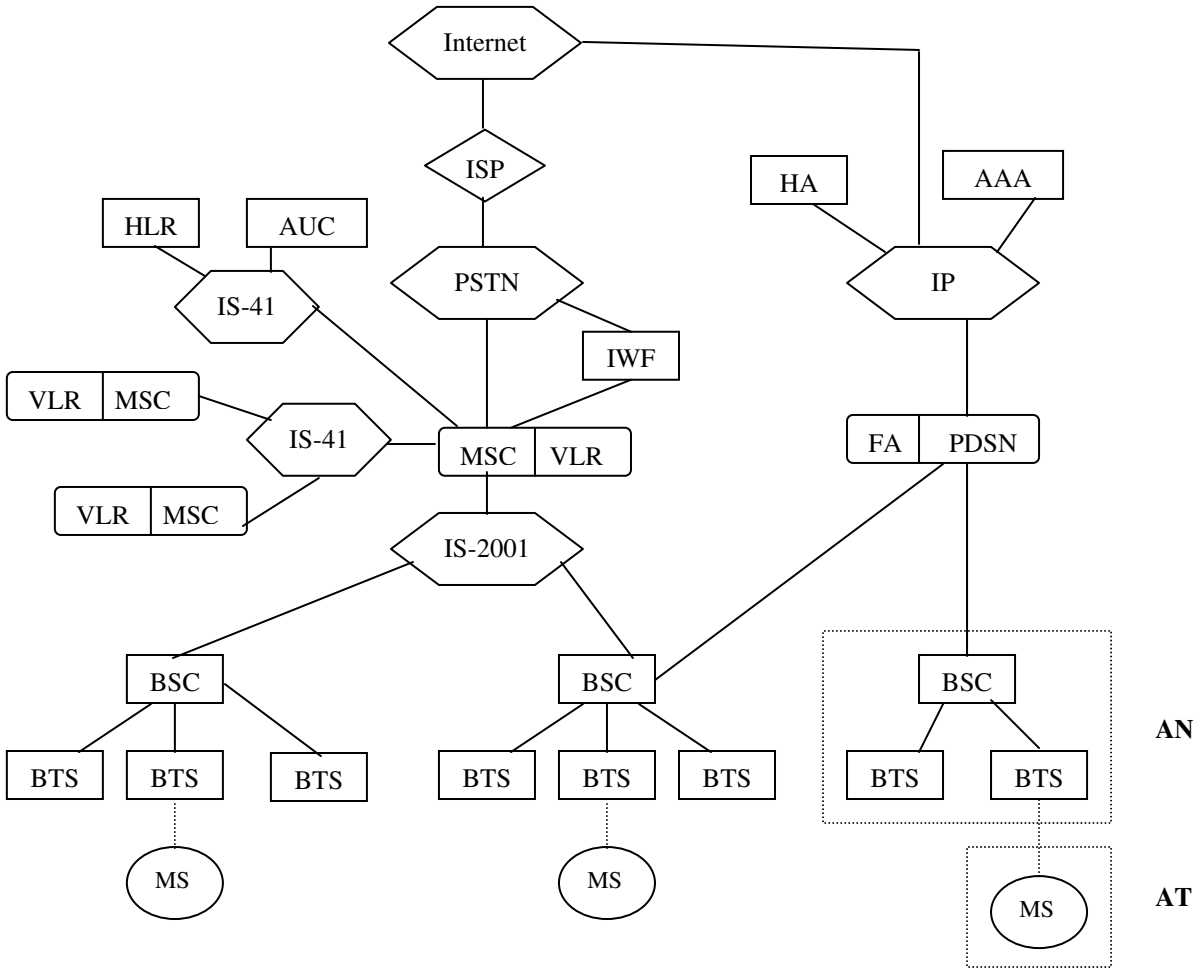

Fig.1. A typical 3G wireless network architecture with high speed data network

contains TRXs i.e. transceivers or radio units.

BSS – Base Station Sub Sys-BSCs & BTSs.

Submit your manuscript electronically for review.

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 or servers, specially for voice and low speed data communications.

HLR – Home Location Register occupies identities of mobile subscriber as IMSI [International Mobile Subs Identity], service parameters, location information 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 Ki 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 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 [2], [6], [7]. Thus AN acts as an interface between AT and PDSN. AT and AN are connected by IS-856 network.

For increasing data rate in 2-G, the first step begins with deploying 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 could be provided as an extended feature to the circuit gateway or the PDSN for 3-G mobile communications. The VoIP gateway will hold 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 [7]-[9].

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]-[2], [6]-[9] 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 [6]-[9]. 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 is existing 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

III. AUTHENTICATION IN MOBILE

GSM (2-G) networks utilize authentication for verifying authenticity of subscriber [3]-[5]. Each subscriber is identified with a unique IMSI (International Mobile Subscriber Identity) number. He has a unique subscriber authentication key (Ki).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, Ki 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 Ki 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.

IV. AUTHENTICATION FOR MOBILE COMMUNICATIONS 3-G NETWORK

In 3-G mobile communication, voice communication is held by MSC and its accessories. In packet switching, authentication is done separately by PDSN servers [6]-[9].

In circuit switching, the authentication for establishing voice path is done by the following procedure,

1. Mutual authentication where MS and MSC are confirmed identity individually.
2. Assure that the authentication information and keys are not being re-used (key freshness).

Additional parameters and cryptographic checks are introduced in 3-G network to provide mutual entity authentication between the USIM at the user side and the AUC at the network side. This technique uses symmetric key or code using a secret subscriber authentication key K which is shared between and available only to the USIM and the AUC in the user's HE (Home Environment). In addition, the AUC entrusts with track of a counter SQNHE and at the same time USIM controls track of a counter SQNMS. It also stores additional data to support network authentication providing the user with assurance by key freshness.

This scheme is assembled of a challenge/response protocol identical to the 2-G mobile subscriber authentication with an additional feature of network authentication. The HE, which manages both the AUC and the USIM, possesses some technique in the management of sequence numbers.

In 3-G mobile communication, voice communication is held by MSC and its accessories. In packet switching, authentication is done separately by PDSN servers [6]-[9].

In circuit switching, the authentication for establishing voice path is done by the following procedure,

1. Mutual authentication where MS and MSC are confirmed identity individually.
2. Assure that the authentication information and keys are not being re-used (key freshness).

Additional parameters and cryptographic checks are introduced in 3-G network to provide mutual entity authentication between the USIM at the user side and the AUC at the network side. This technique uses symmetric key or code using a secret subscriber authentication key K which is shared between and available only to the USIM and the AUC in the user's HE (Home Environment). In addition, the AUC entrusts with track of a counter SQNHE and at the same time USIM controls track of a counter SQNMS. It also stores additional data to support network authentication providing the user with assurance by key freshness.

This scheme is assembled of a challenge/response protocol identical to the 2-G mobile subscriber authentication with an additional feature of network authentication. The HE, which manages both the AUC and the USIM, possesses some technique in the management of sequence numbers.

This scheme is assembled of a challenge/response protocol identical to the 2-G mobile subscriber authentication with an additional feature of network authentication. The HE, which manages both the AUC and the USIM, possesses some technique in the management of sequence numbers.

2.4. Computes an expected response XRES = f2K (RAND), where f2 is a (possibly modified) message authentication function;

2.5. Computes a cipher key CK = f3K (RAND), integrity key IK = f4K (RAND) and anonymity key AK = f5K (RAND), where f3, f4, f5 are key generating functions.

2.6. Computes the concealed sequence number SQN ⊕ AK.

2.7. Assembles the authentication token AUTN = SQN [⊕ AK] || AMF || MAC-A and the quintet Q = (RAND, XRES, CK, IK, AUTN) and updates the counter SQNHE.

3. AUC sends that ordered array of n quintets to the VLR.

4. When the VLR initiates the authentication scheme it selects the next quintet from an array held in the VLR and

sends the parameters RAND and AUTN to the user.

5. After receiving of a (RAND, AUTN) from the VLR, USIM in MS computes the following procedure:

5.1 If the sequence number is concealed, the USIM computes the anonymity key AK = f5K (RAND) and retrieves from AUTN the unconcealed sequence number SQN = (SQN$\oplus$ AK).

5.2 The USIM then computes XMAC-A = f1K (SQN ‖ RAND ‖ AMF) and compares XMAC-A with MAC-A which is included in AUTN.

5.3 If they are not matching i.e. MAC-A ≠ XMAC-A, the USIM directs the MS to fail a user authentication response with indication of integrity failure to the VLR and cancels the further execution.

If they are matched i.e. MAC-A = XMAC-A, the USIM computes the following:

5.4 The USIM verifies that the received sequence number SQN is acceptable or not.

5.5 If the sequence number SQN is not acceptable, the USIM computes the re-synchronization token AUTS and directs the MS to fail a user authentication response, with an indication of synchronization failure, including the re-synchronization token AUTS and abandons the procedure.

If SQN is acceptable, the USIM progresses through the following procedures:

5.6 The USIM then computes the response RES = f2K(RAND) and directs the MS to send back a user authentication response back to the VLR, with an indication of successful receipt of the signed challenge and including the response RES.

6. The VLR compares the received RES with XRES. If they identical, the VLR confirms that the MS (USIM) is authentic and therefore authentication proceeding is successfully completed.

B. Authentication for Packet Switching in 3G network:

Authentication for packet switching is done by AAA (Authentication, Authorization and Accounting) server [2], [6]-[9]. Authentication requires the user to provide an account number or identifier and password i.e. exchange of logical keys or certificates between the client (MS) and the server in PDSN. If this authentication is correct, then MS is permitted for packet data service by Authorization.

An AAA server is a server program that handles user requests for access to network resources. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.

V. PROPOSED AUTHENTICATION SCHEME FOR PACKET SWITCHED NETWORK

The entire packet switched mobile network authentication and improvements provide only one-way authentication i.e. only Servers in PDSN can check the authenticity of a user. The user can not check whether he is communicating with a correct server in PDSN or not. It is a vital gap where a potential adversary can spoof the servers in PDSN and get valuable user information. This motivates to construct an authentication scheme for packet switched mobile network that provides user and server authentication and the user gets access to the network resource only if <user, server>'s authenticity is passed correctly. The authenticity of user can be checked by different entities as in following procedures:

(i) Using log identifier with password for authentication of mobile subscriber.

(ii) Certified authority server checks the authenticity of subscriber (MS).

(iii) Different biometric authentication is a technique to check a valid user by user physical characteristic. Human physical characteristics are called Biometric property such as Fingerprint, Voiceprint, Retinal scan and Face recognition etc. Out of these biometric characteristics, we emphasis on following areas:

(A) Acoustic Recognition: In this process, sound detecting from ear of the mobile subscriber (MS) is done by biometric authentication method. Ear not only senses sound but also makes signals of its own called OAEs (Otoacoustic Emission). These OAEs are produced by the motion of hair cells within the outer part of the spiral shaped cochlea lying in the inner ear. Hearing is an active process where the ear actually puts energy into the incoming sound waves to replace energy lost as sound which is absorbed by the ear's function. Due to this process some of the energy added by the hair cells escape as OAEs. These OAE signals are detectable by supersensitive (ultra low noise) microphone. These signals prove unique to each individual including male, female etc. Thus this can be used as an authenticity marker for a caller or set of callers using MS to the network either in circuit or packet switching cases. Hence the use of stolen mobile can be automatically disabled in case of the users are not legitimate owner by simply matching the stored specimen of OAEs.

(B) Face recognition: Face images of the mobile equipment (MS) users are stored either in AUC or PDSN server. The MS (mobile caller) is authenticated by matching the face image of actual user with that of the notified users in MSC or PDSN database. If these two images are completely matched, the call will be progressed, otherwise not.

Authenticity of the network or server (MSC or PDSN) is identified by MS through the following procedure:

(i) Response and throughput time of the server.

(ii) Shared secret key pairs between the user and the server.

(iii) Received power level from the server.

VI. CONCLUSION

3-G mobile network is completely described above with the present authentication scheme. It is seen that wireless communication is enhanced in packet switching technology, as a result high speed secured data as well as voice transmission-reception is possible. Our future work is to invent new efficient mutual authentication technique using entities like Password, Identifier, Certified Authority, Biometric Property etc. of the subscriber in both circuit

switching and packet switching mobile communications.

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] P. K. Bhattacharjee, "A New Era in Mobile Communications- GSM and CDMA" in National Conference on Wireless and Optical Communications (WOC-07) at Punjab Engg College (D.U), pp 118-126, on 13th- 14th Dec, 2007.
[4] T. S. Rappaport, Wireless Communication: Principles and Practice, Prentice Hall Pub Ltd, 2nd Ed, 2006.
[5] P. K. Bhattacharjee, "Hybrid GSM And CDMA Mobile Communication Systems Enhancing Channel Capacity" National Conference on Wireless and Optical Communications (WOC-08), Punjab Engineering College (Deemed University), Chandigarh with IEEE, pp 1-8, from 18-19th Dec, 2008.
[6] D. Goodman, "Cellular Packet Communication", IEEETransactions on Communications, vol. 38, no. 8, pp. 1272-1280, August1990.
[7] S. N. Diggavi, N. Al-Dhahir, A. Stamoulis, R. Calderbank, "Great Expectations: The Value of Spatial Diversity in Wireless Networks, " Proceedings of the IEEE, Volume 92, Issue 2, pp. 219–270, Feb 2004.
[8] P. Ramjee, O. Tero, "An Overview of CDMA Evolution towards Wideband CDMA", IEEE Communications Survey, 1998.
[9] F. Adachi, M. Sawahashi, H. Suda, "Wideband DS-CDMA for Next Generation Mobile Communications System", IEEE Communication Magazine, pp 56-69, Sept, 1998.