ATLANTIS PRESS
Advances in Engineering Research (AER), volume 142
International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018)

An Approach to Reduce Authentication Delay In Inter MSC Handover

[1] K.Regin Bose , [2] V.Sankaranarayanan, [3]Belwin J Brearley
[1] Associate Professor, Department of Computer Science and Engineering, SMIT, Chennai
[2] Former Director (University Project), B.S.A Crescent Institute of Science & Technology, Chennai
[3] Assistant Professor (SG), Department of EEE, B.S.A Crescent Institute of Science & Technology
reginbose1@yahoo.co.in, sankarammu@yahoo.com, belwin@bsauniv.ac.in

***Abstract*—In Global System for Mobile (GSM) communication based wireless networks, authentication delay is an important factor during handover. In present system, mobile nodes are authenticated by its home Authentication Centre (AuC). In this paper a Mobile Information Centre (MIC) is introduced within a Mobile Switching Centre (MSC) and a Mobile Information Centre Authentication Algorithm (MICAuA) is written to authenticate the Mobile Node (MN) directly from MIC. This method reduces authentication delay, network traffic and the packet drops in Inter Mobile Switching Centre (Inter-MSC) handover. A dual authentication procedure is also used for the verification of a mobile node (MN). The proposed algorithm saves the processing time by 16% compared to the existing algorithm.**

Keywords: inter-MSC handover, authentication delay, security, efficiency

I. INTRODUCTION

Mobile users expect to keep their contact active during travelling. Hence the major challenging task in the contact-continuation process is to maintain their contact alive even during handover. In handover authentication is necessary in order to prevent unauthorized users requesting for the service thereby provides privacy to MNs [1]. This process includes some challenging procedures since access control is normally based on the identity of the user who requests for a resource. The authentication protocol plays a major role in mobile communication architecture. However there are certain drawbacks such as bandwidth consumption between Visitor's Location Register (VLR) and Home Location Register (HLR), storage overhead in VLR etc.,

In the proposed system the HLR transaction of the MN is reduced by introducing the MIC. It also reduces the communication overhead between HLR and visiting VLR. Dual authentication is used to enhance the security. Also a MICAuA algorithm is formulated to reduce the authentication delay during inter MSC handover.

II. LITERATURE REVIEW

The authentication process [2][3][4] involves various sequences of operations. The detailed studies about the authentication process are carried out and discussed as follows. Hwang et al.'s [5] formulated an authentication protocol for the GSM architecture which reduces considerable amount of bandwidth between HLR and VLR. In this protocol a secret key (Ki) and random number (RAND) are used to generate a temporary key based on A3 algorithm which is shared with MN and visiting VLR. Ki is the secret key with MN and HLR, and the Random number is generated by HLR. A certificate CERT_VLRZ for A3 (Timestamp of MN, Ki) at HLR is used to verify the visiting VLR of MN. The author Chin-Chen Chang [2] in his paper has used Temporary Mobile Subscriber Identity (TMSI) and (Location Area Identifier) LAI to recognize International Mobile Subscriber Identity (IMSI) between MN and VLR during authentication request. Further VLR forwards IMSI along with time stamp to HLR for calculating Signed Response (SRES). Though the IMSI transmission between MN and VLR are avoided, it has to be forwarded to HLR for SRES calculation. For mutual authentication Chun-I Fan [6] has proposed time and nonce based protocols between MN, VLR and HLR. A clock synchronization among the system is also suggested. Further stable transmission is a prerequisite in this system which leads to hardware speculations. In the authentication protocol between user and system, the final verification of authentication is done at the MN. For mutual authentication during roaming services Yixin Jiang [7] suggested self certified scheme. This requires the transmission of the shared key through the secured channel. A temporary identity for authentication between VLR, HLR and MN is being used for the purpose of combining certificated-based and identity-based key systems.

In Caimu Tang's [8] work a trust model is framed to bypass the VLR and HLR for the purpose of mutual authentication between MN and AuC. An offline authentication between HLR and MN within the same network is being used. Ming-Chin Chuang [9] implemented authentication mechanism as a seamless handover process in Proxy Mobile IP version 6. In this architecture, a set of MSCs are connected with local mobility anchor and authentication-authorization-accounting server. Yuh-Ren Tsai[10] proposed subscriber identity module based authentication mechanism. WLAN concept is used for authentication purpose, which involves DHCP, Authentication server and gateway. This authentication mechanism has temporary IP address acquisition phase and subscriber identity verification Phase. In Subscriber Identity Verification Phase MN sends a registration request along with IMSI number. The authentication server identifies MN's HLR then forwards the message to the HLR. HLR generates triplet based on A3 and A8 algorithms. Qiang Tang [11] in his Cryptanalysis of hybrid authentication protocol for large mobile network suggested not burdening the MN for extensive computations for the purpose of authentication. The hybrid authentication protocol has to authenticate every message through Kerberos V4 and V5.

Initial authentication has to be re-hashed by the MN. Guangsong Li [12] suggested a concept of Proactive Key Distribution - Ticket-based Re-authentication Scheme for fast Handover method, used the authentication server to provide the handover ticket to MN. Each ticket corresponds to the neighboring access point of MN. The ticket contains encrypted pairwise master key neighbor access point, generated by the authentication server. With this ticket the MN can re-authenticate with neighbor access point.

In the existing methods the probability for attacks is found to be high due to the usage of permanent key Ki, IMSI number for authentication purposes. In Kerberos versions, in order to initiate the authentication process it requires permission from key distribution center (KDC) and ticket granting center (TGC) which increases the network traffic and congestion. In general, the authentication process is verified for each MN by its home network which consume more time and also increases the traffic. In the proposed work the dual authentication is done by MIC using the local parameters LMSI and ciphering key (Kc) which reduces the congestion, traffic and enhances the security. In this proposal three parameters SRES, RAND, and Kc are used from these existing works for the process of authentication in our proposed system.

III. PROPOSED WORK

In the proposed work a new agent called MIC is introduced, to take care of Inter MSC handover processes exclusively (Figure 1). MIC has a database to participate in the authentication process of a MN during the inter MSC handover. Instead of Authentication Centre, MIC is the proxy authorized one to authenticate the MN. Hence in the proposed system the burden of the home network and the network traffic due to authentication request is reduced. The security level is also higher than the existing methods. After authentication, if existing MIC receives any data packet which should be redirected to the new MIC, it avoids the retransmission of the data packet. Each BS has a Location Area Identifier (LAI). To avoid the misuse of identity information, a TMSI is provided to the MN, by the foreign network. VLR manages the TMSI number.

A. MIC Authentication Algorithm (MICAuA):

The MN measures the signal strength of its traffic channel while data transmission takes place. When the signal strength is below the threshold value, MN measures the signal strength of the neighbouring cells and sends the report to the existing base station controller (BSC). The BSC checks up the type of handover involved in the particular case (whether it's an intra BSC, intra MSC or inter MSC handover). If it's an inter MSC then the request is forwarded to the existing MSC's MIC. This MIC further identifies the new MSC from the received signal strength (RSS) report. This initializes new authentication process (Figure 2).

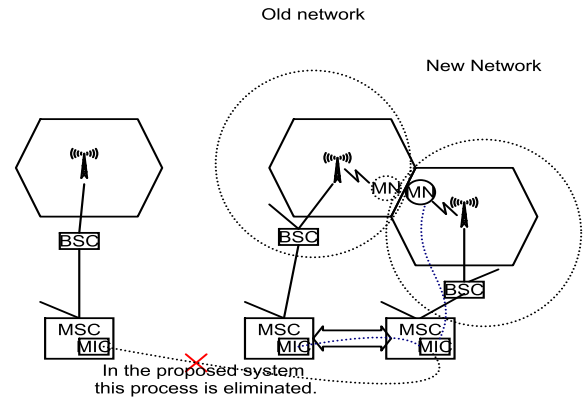

Figure 1. Handover between MIC's

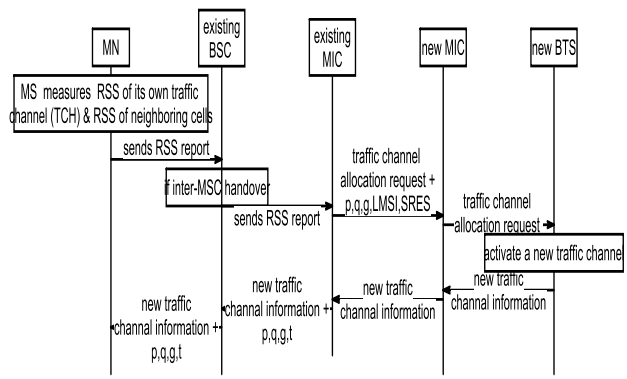

Figure 2. Data flow in authentication initialization process

From the MIC's database it chooses p(a 512 bit prime number), q(a 160 bit prime factor of p-1) and g [$g= h^{(p-1)/q}$ *mod p*] values. It receives the LMSI, RAND, SRES values from its VLR. MIC sends a handover request message along with p, q, g, LMSI and SRES values to the new MIC. The new MIC receives the message from that it separates p, q, g, LMSI, SRES and then it forwards the handover request to the new Base Station (BS). The new BS activates a Traffic Channel (TCH) and this TCH information is given to new MIC. The TCH information is being forwarded to existing MIC. Existing MIC forwards the TCH information along with p, q, g, t(a 160 bit random number generated by new MIC) value to MN.

A1. Authentication Process in MN

The MN tunes to new TCH to connect with new BS and also it computes *s* [$s= RAND^{-1}(SRES + (LMSI * r)$ *mod q*], *r* [$r=z$ *mod q*, $z= g^{RAND}$ *mod p*], *ex*[$ex= g^{es}$ *mod p*, $es = e*SRES+t*er$ *mod q*] values (Figure 3). If the MN is genuine then it can generate correct value. Since 512 bit size key is used the probability of getting the correct value for the intruder is very less. MN generates the results and it sends handover access burst message along with *s*, *r* and *ex* (104 bytes). The time taken to process the result is 0.3603858 seconds.

A2. Authentication Process in New MIC

When the handover access burst message along with s, r and

ex are received by new BS, it forwards the message to new BSC. It checks the message and if it finds it to be inter-MSC handover then it forwards the message to new MIC. New MIC has already received p, q, g, LMSI, SRES values along with traffic channel allocation message from old MIC. Now the new MIC calculates y value (y= g^{LMSI} mod p). When new MIC receives the s value it starts the verification process. For verification it generates the v [$v=((g)^{u1}(y)^{u2})$ *mod p)mod q*, u1= $s^{-1}LMSI$ (mod q), u2= $s^{-1}r$ (mod q)] value (Figure 4). If both *v* and *r* values are same, then the MN is the authorized one, otherwise the MN is an intruder. If new MIC completes its authentication, it sends *ex* value to old MIC for second authentication. To compute first authentication the time taken is 0.1771709 seconds.

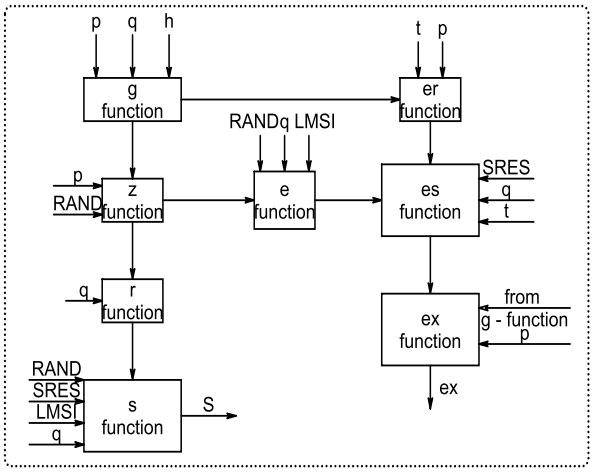

Figure 3. Detailed design of MICAuA in MN

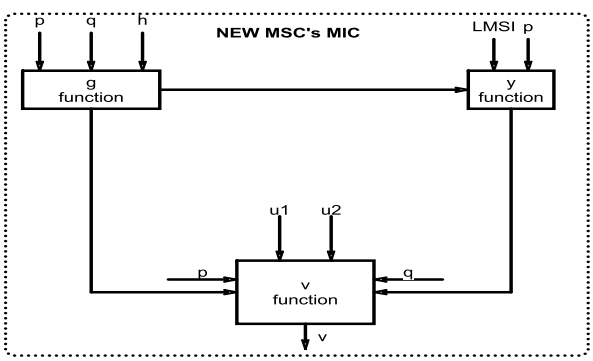

Figure 4. Design of MICAuA in new MSC's MIC

A3. Authentication Process in Old MIC

When it receives the *ex* value from new MIC it authenticates once again. Already this MIC has generated the *ey* [$ey=y^{(yz^z)}er^{er}$ *mod p,* $er=g^t$ *mod p*] (Figure 5) value because it has all the parameters. If both *ex* and *ey* are same then the MN is the authorized one. If MN is authorized node then it sends acknowledgement to the new MIC. The time taken to compare these two is negligible because *ey* was already calculated. If both new MIC and old MIC are authenticated then MN is the authorized node. Figure 6 shows the authentication process of both new and old MIC. Total time taken for MICAuA authentication is 0.3603858 + 0.1771709 = 0.5375567 seconds.

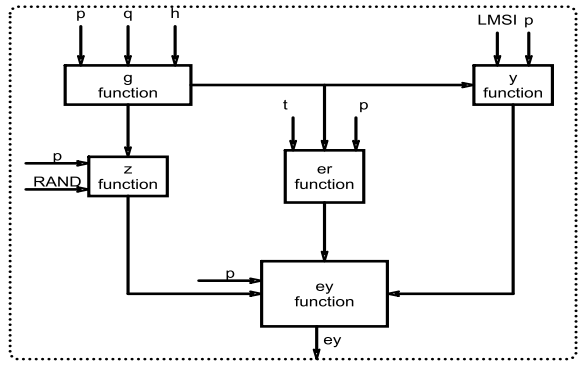

Figure 5. Detailed design of MICAuA in old MSC's MIC

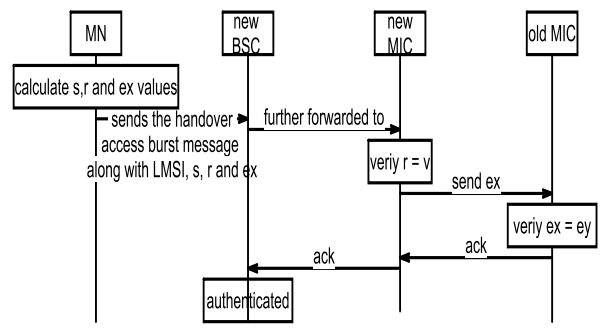

Figure 6. Data flow in MIC authentication process

IV. DISCUSSION AND COMPARISON

In MICAuA, MIC is a dedicated agent for inter MSC and MIC is trustworthy. Also it is an initiator as well as it protects the p, q, g, t values.

A. Mobile Node Identity Privacy

In existing (COMP-128 algorithm) algorithm MN transmits IMSI number (unique number) along with authentication request for identification of genuine MN. Also the security key (Ki) used for authentication is unique. Hence the probability of attacks is high. In MICAuA the authentication is carried out using LMSI, SRES, and RAND numbers (varing in nature) which reduces the attacks. It also avoids the retransmission of IMSI and Ki during handover. Hence the proposed method provides stronger user identity privacy than other existing algorithms.

B. Mutual Authentication between MN, Old MIC and New MIC

Here MN is authenticated by both old and new MIC. Hence our system provides dual authentication, where as in existing algorithm MN is authenticated by HLR alone.

C. Communication in authentication process

In COMP-128 algorithm, 8 steps require to complete authentication process.

Step 1: MN sends registration request to HLR via VLR

Step 2: Verify the International Mobile Equipment Identity (IMEI) number with

Equipment Identity Register (EIR)

Step 3: Authentication centre generates RAND number

Step 4: HLR generates SRES value

Step 5: Send Triplet values: RAND, SRES and Kc to VLR

Step 6: VLR sends RAND number to MN

Step 7: MN generates SRES value and sends to VLR

Step 8: Compare the SRES of step 4 and step 7. If both are equal, MN is a authenticated user.

In the proposed system, 4 steps are required to complete the MICAuA process (Figure 7).

Step 1: Old MIC sends p, q, g, LMSI and SRES values to new MIC also p, q, g and t values to MN

Step 2: MN generates r, s and ex values then sends to new MIC

Step 3: New MIC generates v value and compare it with r value. If it matches then send *ex* value to old MIC

Step 4: In old MIC compare ex value with ey value. If it matches sends acknowledgement to new MIC.

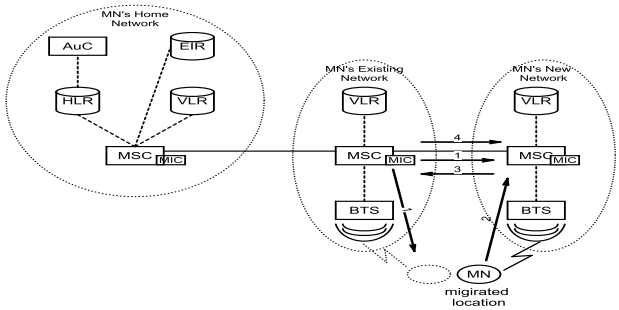

Figure 7. Implementation of MICAuA

Since the authentication process is being carried out among the neighbouring MSCs the transmission time for MICAuA is very low.

D. Storage Capacity

COMP-128 algorithm the compression set-1 has 512 values, set-2 has 256 values, set-3 has 128 values, set-4 has 64 values and set-5 has 32 values. In the MICAuA model there is no need of a compression set table to compute the algorithm. This saves the storage space required for these set of table values. The storage space required for the parameters of existing algorithm is 44 bytes. In our system the space required for the parameters are 312 bytes. Due to advanced technologies 312 bytes can easily be accommodated.

E. Performance

E1. Algorithm processing time

The algorithms are coded in the python programming language. The experimental results are obtained by executing in the open source environment. The total time taken by COMP-128 algorithm is 0.640214 seconds and time taken by the proposed system is 0.5375567 seconds. This time amounts to 84% of the existing algorithm, thus saves time by 16%

E2. Authentication Latency Estimation

In GSM network authentication Latency depends on the propagation time, transmission time and processing time. In propagation time measurement we need to calculate mobile node distance and received signal strength. We have estimated the authentication latency [13] using the following steps:

Step 1

Input frequency: A set of frequency $F=\{f_1,f_2,f_3.....f_n\}$, where f is in mega hertz and $f_1<=F<=f_n$

Input power: Transmission power $P_T=\{W_1,W_2,W_3.....W_n\}$, where W is in watts and $W_1<=W<=W_n$

Receiver Signal strength range: Un acceptable coverage = -101 dbm or less

Low Coverage = -100 dbm to -91 dbm

Medium coverage = -90 dbm to -81 dbm

Full coverage = -80 dbm or greater

Step 2

Path loss free space (L_{fs}):

$$L_{fs} = 10\log\left(\frac{Transmission\,Power}{\mathrm{Re}cieved\,Power}\right)$$

Distance in kilometres (d_{Km}): $L_{fs} = 32.45 + 20Log_{10}(d_{Km}) + 20Log_{10}(f_{MHZ})$

$d_{Km} = antiLog_{10}[\{L_{fs} - 32.45 - 20Log_{10}(f_{MHZ})\}/20]$

Propagation time: Propagation time=distance/speed, where speed= 3×10^8 m/s (light speed)

Transmission time: Transmission time=Message size/Data Rate

Step 3

Output: Latency=Propagation time+ Transmission time+ Processing time

The simulated output (matlab) for propagation time is given in Table 1 and for transmission time is given in Table 2. The received signal strength versus distance for various frequency ranges are plotted in Figure 8 and with propagation time are plotted in Figure 9. From the authentication latency simulation and also from the plotted graphs we found that the various relationships between signal strength, propagation time and distances are common to both existing as well as proposed method.

Frequency (MHZ)	Transmission Power		Receiver Power (dbm)	Distance (km)	Propagation time (µs)
	(Watts)	(dbm)			
880	2	33	-100	3.8	12
880	2	33	-50	0.012	.04
900	3.5	35	-95	2.8	9.3
915	5	37	-90	1.8	6.0
925	7	38	-85	1.2	4.0
950	8.5	39	-80	0.73	2.4
960	9.5	40	-75	0.43	1.4

Table 1: Propagation time for various frequency ranges

Data rate (Mbps)	Message size (bytes)	Transmission time(µs)
2	5	20
2.5	5	16
3.1	2	5.1
4	3	6
7.2	20	22

Table 2: Transmission time for various message sizes

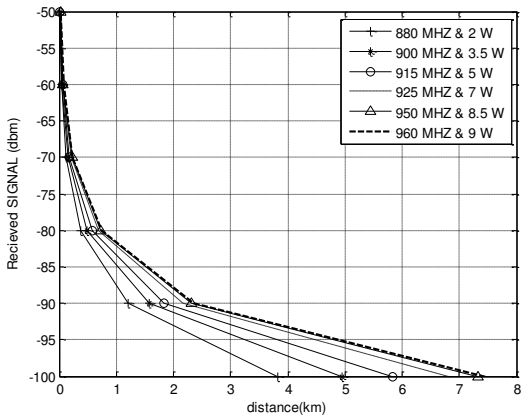

Figure 8. Distance Vs Received Signal

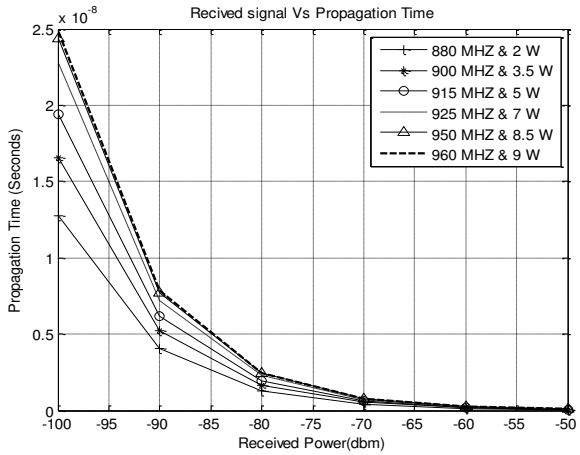

Figure 9. Received Signal vs Propagation Time

V. CONCLUSION

The proposed new Mobile Information Centre Authentication Algorithm requires less process time and it is more secure due to dual authentication. The mobile information centre reduces the burden of HLR, VLR, MSC and also avoids unwanted traffic. The process of verifying the International Mobile Subscriber's Identity with the Equipment Identity Register during the handover is taken care of by the MIC, thus saving substantial amount of time. Also the process of generating the random number has been avoided in our authentication algorithm. Total time taken by the existing algorithm is 0.640214 seconds and time taken by the proposed system is 0.5375567 seconds. This is of 84% of the existing algorithm, saving time by 16%. The key size is extended to 512 bits therefore the complexity of our method is quite greater which increases the security.

REFERENCES

[1] D aojing He, Chun Chen, Sammy Chan and Jiajun Bu,"*Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions*", *IEEE Transactions on Wireless Communications*; Vol. 11, No. 1, 2012, pp. 48-53.

[2] Chin-Chen Chang, Jung-San Lee, Ya-Fen Chang "*Efficient authentication protocols of GSM*". *Computer Communications Elsevier Journal*, Vol.28, Feb 2005 pp. 921–928.

[3] Wilayat Khan, Habib Ullah "*Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography*" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 9, May 2010.

[4] Alberto Peinado "*Privacy and authentication protocol providing anonymous channels in GSM*" Computer Communications Elsevier Journal 27 (2004).

[5] K. F. Hwang and C. C. Chang, "*A self-encryption mechanism for authentication of roaming and teleconference services*", *IEEE Transaction on Wireless Communication,* Vol. 2, No. 2, 2003, pp. 400–407.

[6] Chun-I Fan, Pei-Hsiu Ho, and Ruei-Hau Hsu, "*Provably Secure Nested One-Time Secret Mechanisms for Fast Mutual Authentication and Key Exchange in Mobile Communications*", *IEEE/ACM Transactions on Networking*, Vol. 18, No. 3, 2010, pp.996-1009.

[7] Yixin Jiang, Chuang Lin, Xuemin (Sherman) Shen, and Minghui Shi, *"Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks", IEEE Transactions on Wireless Communications, Vol. 5, No. 9, 2006, pp: 2569-2577.*

[8] Caimu Tang and Dapeng Oliver Wu, *"An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE Transactions on Wireless Communications, Vol. 7, No. 4, 2008, pp.1408-1416.*

[9] Ming-Chin Chuang, Jeng-Farn Lee, and Meng-Chang Chen. SPAM, "*A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks*", *IEEE Systems Journal,* Vol.7, No. 1, 2013, pp-102-113.

[10] Yuh-Ren Tsai , Cheng-Ju Chang, "*SIM-based subscriber authentication mechanism for wireless local area networks*". *Elsevier Journal on computer communications;* Vol. 9, 2006, pp- 1744–1753.

[11] Qiang Tang, Chris J. Mitchell, "*Cryptanalysis of a hybrid authentication protocol for large mobile networks*", *Elsevier Journal on The Journal of Systems and Software,* Vol. 79, 2006, pp- 496–501.

[12] Guangsong Li,, Jianfeng Ma, Qi Jiang , Xi Chen, *"A novel re-authentication scheme based on tickets in wireless local area networks", Elsevier Journal on J. Parallel Distrib. Comput, Vol. 71, 2011, pp- 906–914.*

[13] *Theodore Rappaport S. Wireless communication principles and practice Prentice* second edition Hall communications Engineering and technologies pp 102-108