AENSI Journals

**Australian Journal of Basic and Applied Sciences**

ISSN:1991-8178

Journal home page: www.ajbasweb.com

# An Approach to Reduce Authentication Delay after Abrupt Termination of Mobile Node

[1]K. Regin bose and [2]V. Sankaranarayanan

[1]*Department of Computer Science and Engineering B.S.Abdur Rahman University, Chennai,600048, Tamil Nadu India*
[2]*Professor, Department of Information Technology B.S.Abdur Rahman University, Chennai,600048, Tamil Nadu India*

**ARTICLE INFO**

***Article history:***
*Received 2 March 2014*
*Received in revised form*
*13 May 2014*
*Accepted 28 May 2014*
*Available online 23 June 2014*

***Keywords:***
*abrupt termination, inter MSC handover, authentication delay.*

**ABSTRACT**

In mobile communication the mobile node (MN) can be abruptly disconnected from the network even when the connection is in established state. Then the mobile node is again required to re-establish the connection to be in the network. This is same as establishing a new connection. To avoid the process of connection establishment again, we have introduced an agent called Mobile Information Centre (MIC) along with an MIC Re-Registration Algorithm (MICRRA) for the re - establishment of connection. This MIC is placed within the Mobile Switching Centre (MSC). The algorithm authenticates the mobile node directly from MIC bypassing the home network during the abrupt termination. This re-establishment process reduces the communication overhead by utilizing the previous call-establishment parameters. The data packets received after re-establishment by the old MIC are rerouted to MN through new MIC, and thus avoids the retransmission delays. Security aspects are addressed by dual authentication procedures for the verification of a mobile node. Also mobile identity privacy is preserved without violating the security aspects. The keys used by the algorithm for the re - establishment process are longer in size, which reduces the possibilities of security attacks. Our algorithm saves time by 11%, compared to the existing algorithms. This mechanism reduces network traffic and the packet drops.



**To Cite This Article:** K. Regin bose, V. Sankaranarayanan., An Approach to Reduce Authentication Delay after Abrupt Termination of Mobile Node. ***Aust. J. Basic & Appl. Sci.,*** *8(9): 7-12, 2014*

## INTRODUCTION

Handover is an important process that occurs in mobile devices. Users are required to keep their communication active while travelling. The handover process between the boundaries of base stations (BS) should be graceful to keep their communication alive. This is the major challenging task in the call handover process. But BS services become inoperable for various reasons. They are inclement weather, imbalance of traffic between the two cell sites area of coverage, the network configuration not being set up properly, Co-channel and Adjacent channel interference, neighbour cells with the same frequencies interfere with each other, deteriorating the quality of service, software glitch, transmission problems, faulty transceiver inside the base station, mobile node call loss, sunspots and solar flares, increased cell capacity, momentary overload of signals to switch, tall buildings, mountains and thick foliage. Hence the connection is terminated abruptly. To continue communication, the MN has to register with new BS as a new user and also it has to go through the entire authentication process as a new connection. To ensure reliability in communication under the above said circumstances, a new MIC is introduced within the MSC. Now the MIC authenticates MN to new BS which reduces the re-establishment process and re-establishment time for the MN. Also a dual authentication algorithm (MICRRA) with longer key size is proposed to enhance security aspects.

### *Literature Review:*

The authentication process (Chin-Chen Chang, Jung-San Lee, 2005; Wilayat Khan, Habib Ullah, 2010; Alberto Peinado, 2004) involves various sequences of operations. The detailed studies about the authentication process are carried out and discussed as follows. We have learnt from the work of Hwang *et al*.'s (2003) authentication protocol, for the GSM architecture that it has reduced considerable amount of bandwidth between home location register (HLR) and visitor's location register (VLR). He used key Ki and Random number (RAND) at HLR to generate a temporary key, using A3 algorithm. Further he shared that key with MN and visiting VLR. Ki is the secret key with MN and HLR, and the Random number is generated by HLR. He has

**Corresponding Author:** K.Regin bose, Department of Computer Science and Engineering B.S.Abdur Rahman University, Chennai,600048, Tamil Nadu India
E-mail: regin01bose@gmail.com

created a certificate CERT_VLRZ for A3 (Timestamp of MN, Ki) at HLR. He has used this certificate to verify the visiting VLR of MN. The author Chin-Chen Chang (2005) 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 he has avoided the IMSI transmission between MN and VLR, he has to forward IMSI to HLR for SRES calculation. For mutual authentication Chun-I Fan (2010) has proposed time and nonce based protocols between MN, VLR and HLR. He also suggested clock synchronization among the system. Further stable transmission is a prerequisite in his proposed system. This may lead 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 (2006) suggested self certified scheme. This requires the transmission of the shared key through the secured channel. Also he has used the temporary identity for authentication between VLR, HLR and MN. He has used this temporary identity for the purpose of combining certificated-based and identity-based key systems. In Caimu Tang's (2008) work we have observed a trust model is framed to bypass the VLR and HLR for the purpose of mutual authentication between MN and AuC. He has also used offline authentication between HLR and MN within the same network. We have used the similar concept for the purpose of inter MSC authentication. Ming-Chin Chuang (2013) implemented authentication mechanism as a seamless handover process in Proxy Mobile IP version 6. In his architecture, a set of MSCs are connected with local mobility anchor and authentication-authorization-accounting server. He adopted 3 procedures. They are initial registration, authentication, and password change procedure. There are 12 steps to complete these authentication procedures. Yuh-Ren Tsai (2006) proposed subscriber identity module based authentication mechanism. He has used WLAN concept 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 a temporary IP address the Acquisition Phase MN finds out DHCP server and also gets a temporary IP address of authentication servers. 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 and returns to the authentication server. Further he has utilized the existing A3 and A8 algorithms. Qiang Tang (2006) in his Cryptanalysis of hybrid authentication protocol for large mobile network suggested not burdening the MN for extensive computations for the purpose of authentication. As 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 (2011) in his 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. Also in the existing works the re-establishment of the communication after abrupt termination is being done as new communication. 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. We have used the three parameters SRES, RAND, and Kc from these existing works for the process of authentication in our proposed system.

***Proposed Method:***

In the proposed work a new agent called Mobile Information Centre is introduced, to take care of Inter MSC handover processes exclusively (Fig 1). MIC has a database to participate in the authentication process of a MN during the abrupt termination. Instead of Authentication Centre, MIC is the proxy authorized one to authenticate the MN.

Each BS has a Location Area Identifier (LAI). To avoid the misuse of identity information, a Temporary Mobile Subscriber Identity (TMSI) is provided to the MN, by the foreign network. Visitors Location Register (VLR) manages the TMSI number.

***MIC Re-Registration Algorithm (MICRRA):***

When MN is in the abruptly terminated state during inter MSC handover, MN needs to establish the connection with the new network.

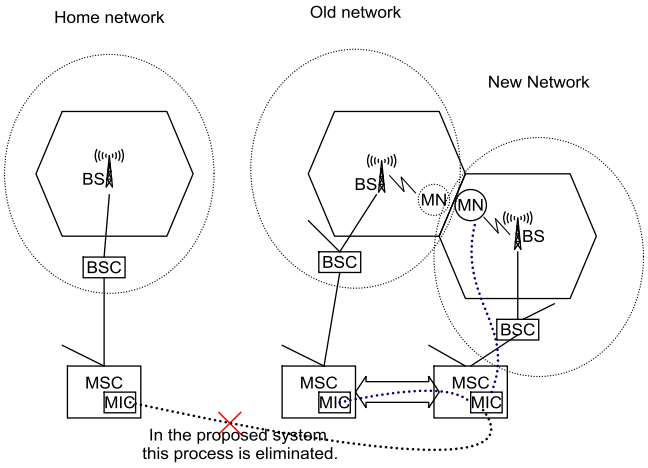


**Fig.1**: Authentication Architecture.

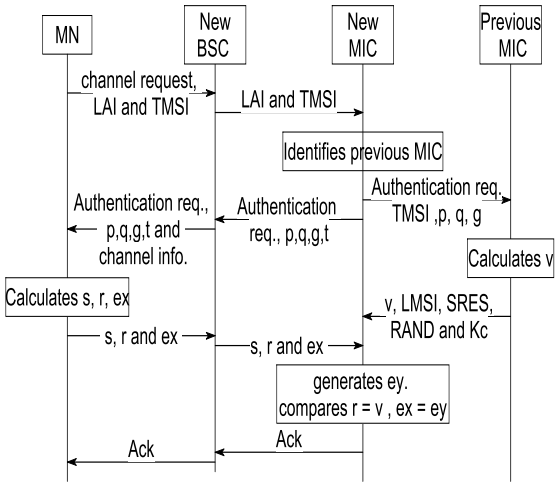


**Fig. 2:** micrra process.

MN sends the channel request along with the LAI and TMSI information of the previous MSC to new MIC as shown in Fig. 2. MIC of the new MSC identifies the previous MSC from the LAI.

***Authentication Process in New MIC: After receiving request from MN:***

New MIC forwards the TMSI number and *p* (a 512 bit prime number), *q* (a 160 bit prime factor of p-1) , *g* [$g= h^{(p-1)/q} \bmod p$] values from its database to the previous MIC along with the authentication request (Fig. 2). It also forwards authentication request with *p*, *q*, *g* and *t* (a 160 bit random number generated by new MIC ) value to MN. The total size of these parameters is 1344 bits.

***Authentication Process in Previous MIC:***

The Previous MIC receives the authentication request from the new MIC and identifies the MN's previous Triplet (random number (RAND), signed response (SRES) and ciphering key (Kc)) from the VLR database. The size of triplet is 364 bits. Using the triplet, *p*, *q* and *g* values, the algorithm generates *v* [$v=((g)^{u1}(y)^{u2}) \bmod p) \bmod q$, $y= g^{LMSI} \bmod p$] value of 160 bits. Then it forwards *v*, Local Mobile Subscriber Identity (LMSI) and triplet values to new MIC. This algorithm takes 0.01771709 seconds to compute *v* value.

***Authentication Process in MN:***

After receiving the authentication request as a reply from the new MIC, the algorithm gets *p*, *q*, *g*, and *t* values. MN has LMSI, SRES and RAND values. Using these values *s* [$s= RAND^{-1}(SRES + (LMSI * r)$

*mod q*], r [$r=z \bmod q$, $z= g^{RAND} \bmod p$] and ex [$ex= g^{es} \bmod p$, $es = e*SRES+t*er \bmod q$] values are calculated. Intruder will not be in a position to analyze these parameters, due to the 512 bit key size. The probability of guessing the correct value is almost zero. The time taken for this process is 0.03603858 seconds. MN forwards *s, r* and *ex* values to the new MIC for further verification.

***Authentication Process in New MIC: After receiving reply from MN:***

New MIC checks the *v* value of previous MIC with *r* value of MN. If it matches then our algorithm calculates *ey* [$ey=y^{(yz^z)}er^{er} \bmod p$, $er= g^t \bmod p$ ] value from LMSI, RAND, SRES, *p, q, g, t* and *s* values. Further the values of *ey* and *ex* are compared. If it is same then the mobile user is an authorized user and permits to communicate further. This process takes 0.021175635 seconds to calculate and compare the values.

***Discussion and Comparison:***

MIC Re-Registration Algorithm (MICRRA) introduces an agent MIC which is connected with the neighbouring MICs. This enforces a strong mechanism over the data security. This algorithm initiates the *p, q, g, t* values and protects their security by the above mechanism.

***Securing the Identity of a Mobile Node:***

Privacy of the International Mobile Subscriber Identity (IMSI) number is an important part in the MN security as it is the unique identifier of it. The key Ki is also the unique identity for every MN. In the existing (COMP-128) system IMSI is sent along with authentication request. The ciphering key Kc is used for encryption and decryption process in the data transmission. In MICRRA system, the IMSI and Ki are not used for the authentication of the MN. Local Mobile Station Identity (LMSI), SRES, and RAND numbers are used for authentication. Hence this algorithm avoids the retransmission of IMSI and Ki during handoff. So this method provides a means to secure the identity of the MN quicker than the existing algorithms.

***Authentication Process: MN, Previous MIC, New MIC:***

In MICRRA, previous MIC generates v value, MN generates *r* and *ex* values, new MIC generates *ey* value. New MIC compares *r* and *v* values as a first part of dual authentication. If both are equal then it checks *ex* and *ey* values as a second part of dual authentication. If it matches then MN is an authenticated user else MN is an unauthorized user. Here MN is authenticated by the values of both previous and new MIC. Hence the proposed system provides a dual authentication. In the existing algorithm MN is authenticated by HLR alone.

***Communication Steps in Authentication Process:***

The existing algorithm which computes the authentication parameters are given below.

*Step 1*: MN sends registration request to HLR via VLR
*Step 2*: Verify the IMEI (International Mobile Equipment Identity) number with Equipment Identity Register (EIR)
*Step 3*: Authentication centre generates RAND number
*Step 4*: HLR generates SRES value
*Step 5*: Home network sends 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 an authenticated user.

In the proposed system the above parameters are reduced to 5 steps to complete the authentication process.

*Step 1*: MN sends LAI and TMSI to new MIC
*Step 2*: New MIC forwards TMSI along with *p, q, g* values to previous MIC. Also it sends authentication request to MN along with *p, q, g* and *t* values.
*Step 3*: Previous MIC computes *v* value and forwards to new MIC along with triplet and LMSI.
*Step 4*: MN computes *r, s* and *ex* values then forwards to new MIC
*Step 5*: New MIC compares *r* and *v* values. If it is equal then computes *ey* value and compares it with *ex* value. If it is same then the MN is an authenticated user.

***Performance:***

The algorithms are coded in the python programming language. The experimental results are obtained by executing in the open source environment

***Space Complexity:***

In the existing system there are five compression tables. They have 512, 256, 128, 64 and 32 values respectively. It occupies 992 bytes space. In our MICRRA model there is no need of tables, hence this saves the storage space required for it.In the existing algorithm the space required by the parameters are 44 bytes. They

are RAND (128 bit), Ki (128 bit), SRES (32 bit) and Kc (64 bit). Our system parameters require 312 bytes. They are *p, ex, g, q*, LMSI, RAND, *r, s* and SRES. The first three parameters occupy 512 bits each and the rest of the parameters occupy 160 bits each. The total bit size amounts to 2496. Despite the increase in the parameter space requirement the table space is avoided in our algorithm. Though the parameter space required is more, the advanced hardware technologies in memory resources provide viable solutions. As in general multimedia SIM has minimum of 24 Kbyte RAM, 160 Kbytes ROM, 1 Mbytes electrically erasable programmable ROM (EEPROM). Therefore the 312 bytes of memory space can be easily accommodated.

***Time Evaluation:***

To compute *v* value at previous MIC, our algorithm executes in 0.01771709 seconds. To compute *s, r* and *ex* values, time taken by MN is 0.03603858 seconds. To compute *ey* and then to compare *r, v* and *ex, ey* values by New MIC, our process takes 0.021175635 seconds. Here the time taken at previous MIC is not to be included in the calculations, since the computation process happens in parallel along with the MN. The total time taken by the existing algorithm is 0.0640214 seconds and the time required for the proposed system is 0.057214215 seconds. Our algorithm saves the time by 11%.

***Avoiding delay in Equipment Identity Register:***

The validity of the mobile equipment is tested at EIR (Equipment Identity Register) by the MSCs. Here we have considered the abrupt termination of MN before Inter-MSC handoff process. Hence MN is required to register again with the new MIC. As it was in the connected state with previous MIC, our algorithm takes care of the re-registration process by avoiding the checking of Equipment's registration with the EIR. That is the verification of IMEI information with EIR. To confirm the identity of MN, the dual authentication process is included at new MIC, which itself gets the values from the previous MIC's VLR. Hence the identity is proved by the new MIC without visiting the EIR. This avoids the delay in EIR verification process. Hence the proposed algorithm saves processing time.

***Avoiding Retransmission of Packets:***

In the existing system during the handoff process, the packets that were sent by the Corresponding Node (CN) are required to be retransmitted, since the ciphering key Kc is unique to that handover process alone. Our algorithm uses the Kc of previous MIC. So that the data packets received there after by the old MIC is rerouted to MN through new MIC. This avoids the retransmission of data packets.

***Security Complexity:***

Our algorithm uses 512 bit key against the 128 bit of the existing system. Hence the complexity of our algorithm is higher. Also in the authentication process of MN, the system has dual parts. In the first part previous MIC and MN parameters are verified by the new MIC. If it is valid then the second part of the authentication takes place. Hence the algorithm provides a dual authentication against the single authentication of the existing system. So the security is stronger.

***Conclusion:***

When the connection is in established state and before inter MSC handoff process, mobile node can be disconnected abruptly from the network. In this situation, there occurs a re-registration process between Mobile Switching Centres. An agent called Mobile Information Centre is placed within a Mobile Switching Centre. As the mobile node was in the connected state with previous MIC, MICRRA takes care of the re-registration processes. To confirm the identity of MN, the dual authentication process is included at new MIC. This method avoids unwanted traffic and congestion that occurs between new MSC and HLR. This algorithm at new MIC uses the same ciphering key of previous MIC. So that the data packets received there after by the old MIC is rerouted to MN through new MIC, avoiding the retransmission of data packets. Also a 512 bit key against the 128 bit of the existing system, makes the complexity of our algorithm is higher. Total time taken by the existing algorithm is 0.0640214 seconds and time taken by the proposed system is 0.057214215 seconds. This is of 89% of the existing algorithm, saving time by 11%.

## REFERENCES

Chin-Chen Chang, Jung-San Lee, Ya-Fen Chang, 2005. Efficient authentication protocols of GSM, Computer Communications, 28: 921-928.

Wilayat Khan, Habib Ullah, 2010. Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography, IJCSI International Journal of Computer Science, 7(3-9): 10-16.

Alberto Peinado, 2004. Privacy and authentication protocol providing anonymous channels in GSM. Computer Communications, 27.

Hwang, K.F. and C.C. Chang, 2003. A self-encryption mechanism for authentication of roaming and teleconference services, IEEE Transaction on Wireless Communication, 2(2): 400-407.

Chin-Chen Chang, Jung-San Lee, Ya-Fen Chang, 2005. Efficient authentication protocols of GSM, Computer Communications, 28: 921-928.

Chun-I Fan, Pei-Hsiu Ho and Ruei-Hau Hsu, 2010. Provably Secure Nested One-Time Secret Mechanisms for Fast Mutual Authentication and Key Exchange in Mobile Communications, IEEE/ACM Transactions on Networking, 18(3): 996-1009.

Yixin Jiang, Chuang Lin, Xuemin (Sherman) Shen and Minghui Shi, 2006. Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks, IEEE Transactions on Wireless Communications, 5(9): 2569-2577.

Caimu Tang and Dapeng Oliver Wu, 2008. An Efficient Mobile Authentication Scheme for Wireless Networks, IEEE Transactions on Wireless Communications, 7(4): 1408-1416.

Ming-Chin Chuang, Jeng-Farn Lee and Meng-Chang Chen, SPAM, 2013. A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks, IEEE Systems Journal, 7(1): 102-113.

Yuh-Ren Tsai, Cheng-Ju Chang, 2006. SIM-based subscriber authentication mechanism for wireless local area networks, Computer communications, 9: 1744-1753.

Qiang Tang , Chris, J. Mitchell, 2006. Cryptanalysis of a hybrid authentication protocol for large mobile networks, The Journal of Systems and Software, 79: 496-501.

Guangsong Li, Jianfeng Ma, Qi Jiang, Xi Chen, 2011. A novel re-authentication scheme based on tickets in wireless local area networks, J. Parallel Distrib. Comput, 71: 906-914.