Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCED SECURITY FRAMEWORK FOR AUTHENTICATION AND INTEGRITY (ESFAI) IN CDMA NETWORKS

[1]V.VIJAYA KUMAR, [2]Dr.R.SAMSON RAVINDRAN
[1]Assistant Professor AVS Engineering College, Salem
[2]Executive Director, Mahendra Engineering College
E-mail: [1]vijayakumarv0281@gmail.com

ABSTRACT

Universal Mobile Telecommunications System is the third generation mobile communications system. It was built on the concepts of GSM and it is the starting point in the development of the fourth generation network. This paper proposes enhancements for the initial identification and for the Authentication and Key Agreement (AKA) protocols that solve two known vulnerabilities of UMTS security: identity catching and secret key exposure. It protects the messages exchanged during the Authentication and Key Agreement protocol. Considering the CDMA communications drawback, this paper proposes a two phased solution. The first phase of the solution consists of a secure key generation. The secure key generation phase is called AKA (Authentication and Key Agreement) -phase. The second phase of the solution is able to solve the problem of redirection attacks, man-in-the-middle attack, sequence number depletion attack, and roaming attack. This phase includes a User Confidentiality for UMTS (EMSUCU) protocol. This proposed solution is able to solve the problems, vulnerabilities through eliminating it and the solution is able to improve the security and efficiency. The enhanced SHAI technique proposed is able to solve redirection attacks, man-in-the-middle attack, sequence number depletion attack, and roaming attack.

Keywords: *Master Server (MS), AKA (Authentication And Key Agreement), User Confidentiality For UMTS (EMSUCU) Protocol*

1. INTRODUCTION

1.1 CDMA Networks

Code division multiple access (CDMA) is a channel access method used by various radio communication technologies. CDMA is an example of multiple accesses, where several transmitters can send information simultaneously over a single communication channel. This allows several users to share a band of frequencies. To permit this to be achieved without undue interference between the users CDMA employs spread-spectrum technology and a special coding scheme where each transmitter is assigned to a code.

Code Division Multiple Access (CDMA) mobile communication system starts from IS-95, called 2nd generation system, to CDMA2000 1x, which is the 3rd generation system. And now, CDMA2000 1x EV-DO system for high speed packet data is served in many countries. CDMA 2000 1xRTT technology makes eavesdropping very complex. It uses 42-bit PN (Pseudo-Random Noise) Sequence called "Long Code" to scramble voice and data [1]. The existing CDMA systems use Cellular Authentication and Voice Encryption (CAVE) algorithm. It provides only unilateral authentication, which leads to false base station attacks, and it is also prone to cryptographic attacks. The unattended nature of sensor networks and the limited resources of their nodes make them susceptible to attacks. These are the major challenges in the existing CDMA systems [1].

ideband Code Division multiple Access (WCDMA) is being used by Universal Mobile Telecommunication System (UMTS) as platform of the 3rd generation cellular communication system. W-CDMA uses noise-like broadband frequency spectrum where it has high resistance to multipath fading whereas this was not present in a conventional narrowband signal of the 2nd generation (2G) communication system.

1.2 applications

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The 3rd Generation Partnership Project (3GPP), a consortium formed by various telecommunication associations from various parts of the world. High data rate signal transmission can be transmitted over the air by using the W - CDMA system, thus enabling of multimedia rich applications such as video streams and high resolution pictures to end users. Thus, this paper need suitable modulation technique and error correction mechanism to be used in the W - CDMA system. Technique presents various advantages such as high fidelity and high resistance to signal perturbations, secured communications and low power consumption. Therefore, Multi-Carriers CDMA (MCDMA) and transmit several user signals simultaneously through one wireless system, such as the 4G mobile system. There are a number of multiple access techniques to improve signal quality, especially for the next - generation channel. In general, what are used are three-dimensional will provide higher data rates of up to 200Mbps [1]. On the other carriers with the CDMA system (MBC CDMA). In the next hand, the use of different time slots in one frame with the sections, further details on the proposed multiple access same frequency is referred to as time division multiple technique is d), WiMAX, and Digital TV transmission [3]. The technical issues in MC CDMA are time dispersion, synchronization, Doppler spreading, frequency and phase offset subcarrier selection and high PAPR. Multicarrier modulation system applications are Digital data Transmission over the Telephone system, Digital audio broadcasting, Digital Television, and Wireless Local Area Networks

1.3 Issues in CDMA Networks

Errors can be easily produced as the number of users is increased and the mobile terminal is subjected to mobility. Although employing security code, sensor nodes are still vulnerable to information forgery and DoS attacks. In addition, the binary CDMA sensor networks can easily be exposed to adversaries using an RF jamming attack on radio interface. To protect against these attacks, the security mechanism against them is required [2]. Some of the attacks on CDMA are as follows

- Replay attacks
- Bogus routing information
- Sybil attacks
- Sinkhole attacks
- RF jamming attacks

1.4 Security for CDMA Networks

Direct sequence spread-spectrum system, also known as code-division multiple access (CDMA), was historically developed for secure communication and military use. In CDMA systems, each user is assigned a specific spreading sequence to modulate its message signal. The spreading process increases the bandwidth of the message signal by a factor N, known as a spreading factor or the processing gain. In the meanwhile it reduces the power-spectrum density of the signal also by a factor of N. With large bandwidth and low power spectrum density. CDMA signals are resistant to malicious narrowband jamming and can easily be concealed within the noise floor and preventing from being detected by an unauthorized person.

Moreover, the message signal cannot be recovered unless the spreading sequence is known, this makes it difficult for unauthorized person to intercept the signal. Due to high spectrum efficiency and simplicity in system planning, CDMA is now finding widespread civilian and commercial applications such as cellular phones, personal communications, and position location. However, the security features provided by these systems are far from being adequate and being acceptable when used for data communications. Wireless security is generally considered from MAC layer and the network layer.

The security services of a network have four fundamental objectives designed to protect the data and the network's resources. Confidentiality, Availability, Integrity and Usage are the main objectives of the network system. So the system with security enhancement must be provided by considering those objectives [3] [4] [5] [7].

Considering the CDMA communications drawback, this paper proposes a two phased solution. The first phase of the solution consists of a secure key generation. The secure key generation phase is called AKA (Authentication and Key Agreement) -phase. The second phase of the solution is able to solve the problem of redirection attacks, man-in-the-middle attack, sequence number depletion attack, and roaming attack. This phase includes a SHAI algorithm.

For a flow contained development, this paper first gives an introduction related to CDMA network in the section one. The second section is a literature study of some previous related works. A well-structured and modularized proposal is given

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in section three followed by a simulation result in section four. At last an overall conclusion is given.

2. LITERATURE REVIEW

L. Krishna Bharathi and Gnanou Florence Sudha [1] have proposed to implement an authentication method using ESA (Enhanced Subscriber Authentication) algorithm instead of CAVE algorithm in the existing CDMA systems. Authentication mechanism using ESA algorithm uses AKA (Authentication and Key Agreement) to enhance security strength and to provide mutual authentication between a base station and a mobile terminal. AKA with 128-bit key adopts the SHA1 hash algorithm to generate authentication value and message encryption keys. Performance analysis of the proposed work is done by calculating the auto correlation, cross correlation of the transmitted voice signal and also the BER (Bit Error Rate) of the system. Thus the proposed work enhances the security strength of the system with increased key strength and bilateral authentication. The proposed scheme can readily be applied to the existing CDMA systems because only the algorithm is replaced, but the input parameters remain the same. However the SHA1 algorithm is prone to collision attack.

Jae Hoon Roh et al [2] has proposed security functionalities of the Binary CDMA technology which can be used for wireless personal area network, and classifies many of attack types, then defines the security requirements for binary CDMA sensor networks. With the security requirements, they have designed an efficient cryptographic protocol corresponding to defensive countermeasures from adversaries. Their cryptographic protocol model has been designed to be a practical use by utilizing the binary CDMA security code in sensor networks. However, since CDMA security code list can easily be opened to eavesdroppers at an early session establishment phase, eavesdropping is still a major concern on binary CDMA sensor networks.

Tahereh Shojaeezand et al [3] have proposed and studied LDPC coded CDMA receiver system. This system has a built-in security enhancement by the reason of using AES scrambling as a secure scrambling method along with the usage of LDPC codes for increasing the secrecy in addition to better performance. The purpose of the paper was to use LDPC codes and secure scrambling in the CDMA system simultaneously to have security enhancement and at the end observe the system performance to verify the usefulness of the system. The receiver system was an iterative multiuser detection system and a bank of LDPC decoder block for the next stage. However, there is computational complexity.

Tongtong Li et al [4] have proposed an encryption-based secure scrambling process. First, instead of using the long-code sequences generated by the LFSR directly, the scrambling sequences are generated through AES operations. As a result, the physical layer built-in security of the CDMA system significantly increases with very limited complexity load. Second, it is shown that by scrambling the training sequence and the message sequence separately with two independent scrambling sequences, both information privacy and system performance can be further improved. Finally, error-tolerant decryption can be achieved through secure scrambling. The proposed scheme is very feasible and can readily be implemented for security enhancement in wireless networks. However, non-spread spectrum system may not have the same ant jamming features as the spread-spectrum systems, since the frequency domain diversity is not available anymore.

A. A. Ortega et al [6] have proposed an enhanced time-hopping CDMA network architecture capable of supporting both point-to-point and point-to-multipoint communication of up to 128 end users. By using a Hamming-weight minimization algorithm together with an encrypted Bloom filter algorithm they provide confidentiality, reliability, and integrity between two or more end users in an optical channel using a simple error correction stage. Also, there is increased level of bandwidth utilization. However, in an optical star-topology, there are locations where little or no interference among users is present, for instance, next to the transmitter output of an end user the signal power is high and can be singled out from the background noise.

Yu-Lun Huang et al [8] proposed a new Secure Authentication Key Agreement Protocol (S-AKA) scheme to enhance the security to resist the attacks. To improve the efficiency and redundancy of UMTS AKA, S-AKA reduces both the authentication messages and bandwidth consumption of UMTS AKA. The formal proof of S-AKA is also given to ensure the security strength of S-AKA. However the bandwidth consumption is only up to 45%.

Daniel Caragata et al [9] have proposed enhancements for the initial identification and for the Authentication and Key Agreement (AKA)

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

protocols that solve two known vulnerabilities of UMTS security: identity catching and secret key exposure. The solution, inspired from Al Saraireh identification protocol, realizes the encryption of the permanent identity of the subscriber and protects the messages exchanged during the Authentication and Key Agreement protocol. The solution proposed enhances the identification protocol EMSUCU: the exchanged messages have their integrity protected, the size of Kc, is increased as to respect NIST and ECRYPT security recommendations and the key Kmh is replaced with the key K. Also, the messages exchanged during the AKA procedure are protected. However, there is no guaranteed security.

3. PROBLEM IDENTIFICATION AND PROPOSED METHODOLOGY

3.1 Problem definition

CDMA systems in comparison with other communication systems, are resistant against unauthorized information detection attacks, yet have some weakness with respect to some eavesdropping techniques. Increasing the physical layer built-in security through secure methods is an advantageous way.

To enhance the security and to provide mutual authentication between a base station and mobile terminal an authentication method using ESA (Enhanced Subscriber Authentication) algorithm employing AKA (Authentication and Key Agreement) is proposed [1]. The AKA enhances the security strength of the system with increased key strength and bilateral authentication. Also the generation of shared secret data, authentication signature value, voice privacy code and signaling message encryption key is done by using ESA algorithm.

The SHA1 algorithm used here is prone to collision attacks in this scheme. Moreover AKA is still vulnerable to some attacks, including redirection attacks, man-in-the-middle attack, sequence number depletion attack, and roaming attack.

The proposed method starts with an architectural diagram of our proposed method with a description. Then in the next section the AKA phase is clearly described. This phase is modulated with modular diagram, a brief description and well defined algorithm. The next phase consists of User Confidentiality for UMTS (EMSUCU) protocol. This phase is empowered by modular diagram, a brief description and an algorithm. At last an overall procedure is given.

3.2 Proposed Solution

In order to solve the above issues, this paper proposes an enhanced security framework for Authentication and integrity in CDMA networks.

In our solution to eliminate the vulnerabilities and to improve the security and efficiency we apply Secure Authentication Key Agreement Protocol (S-AKA) [8].

- Here Location Area Identity (LAI) send from the MS is verified by the SGSN to resolve the re-direction attack.
- It uses Payload Encryption Key (PLK) to encrypt the payload to handle the man-in-the-middle attack.
- And it uses a ticket-based authentication scheme for bandwidth reduction.

In addition to these, for ensuring the integrity, this paper can use Enhancement Mobile Security and User Confidentiality for UMTS (EMSUCU) protocol [9]. This can be applied in our solution for encrypting the IMSI whenever the TMSI cannot be used. The integrity of the control messages is also ensured. On the whole this paper can achieve the system with enhanced security, which is vulnerable to several attacks.

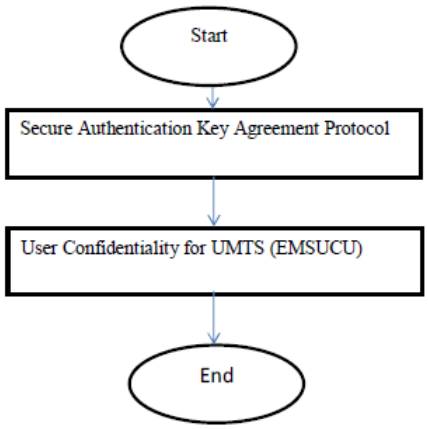

Fig 1: shows the architectural diagram

3.2.1 Secure Authentication Key Agreement Protocol

To cope with the aforementioned problems, a new secure AKA scheme (S-AKA) is proposed. Before elaborating the proposed scheme, this paper first states the assumptions about the environment, which is consistent with 3GPP. The assumptions

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

are: 1) The VLR/SGSN is trusted by the user's home network to handle the authentication information securely, 2) The links between the VLR/SGSN and the HLR/AuC are adequately secure, and 3) the user trusts the HLR/AuC. The goals of our proposed scheme include the following:

1) defeats the redirection attack, 2) defeats the man-in-the-middle attack, 3) achieve mutual authentication between MS and HLR/AuC, 4) accomplish mutual authentication between MS and SGSN, 5) negotiate a cipher key CK and an integrity key IK, 6) freshness assurance to the user of the established keys, and 7) reduce the bandwidth consumption. With these goals, our proposed scheme has the capability to provide more secure and efficient services.

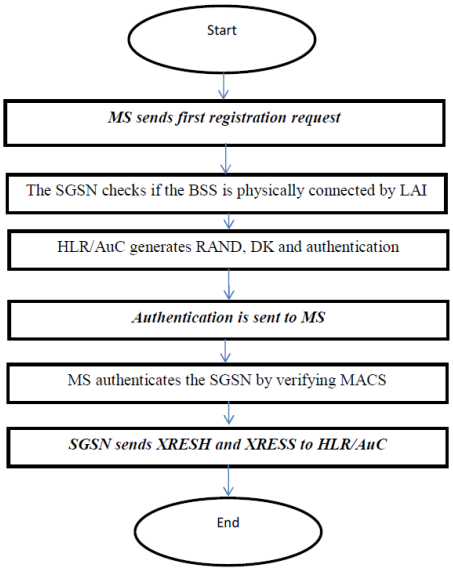

Fig 2: Shows A Modular Diagram Of ***(EMSUCU) Protocol***

S-AKA resolves the redirection attack with the assistance of the MS itself and the SGSN. In S-SKA, the MS rejects illegal base station connection. The SGSN verifies the LAI sent from the MS. For LAI is illegal, the SGSN drops the connection. The LAI in UMTS AKA is not encrypted. The LAI altered by the adversary for the redirection attack. In S-AKA, this paper use MAC to protect the integrity of LAI. On the adversary attempt ion to modify LAI, the illegal modification is detected immediately. S-AKS copes with the man-in-the-middle attack. S-AKA introduces a key, PLK, to encrypt the payload. Connecting to a GSM BSS, the MS and SGSN generate a PLK to encrypt and decrypt the messages transmitted between them. PLK prevents an adversary to eavesdrop as well as to modify the communication. This paper introduces a new key generation function f7 for PLK. The proposed S-AKA scheme uses a ticket-based authentication scheme for bandwidth reduction. This ticket-based authentication scheme allows the HLR/AuC to authorize the SGSN for subsequent mutual authentication between SGSN and MS. After the HLR/AuC authenticates the MS for the first time, it sends delegation key DK to SGSN. The SGSN then uses DK for subsequent authentication. The ticket-based authentication scheme benefits from the traffic reduction between the HLR/AuC and SGSN, and thus greatly reduces the number of messages and the bandwidth consumption. Because there is no DK generation function in UMTS AKA, this paper use a new key generation function f6 to generate DK. As shown in Figure 1, S-AKA can be divided into two protocols. The first protocol, called S-AKA-I, is the authentication procedure taking place for the first time when the MS and the SGSN authenticate each other. The second protocol, S-AKA-II, is the authentication procedure executed for the sequent authentication between the MS and the SGSN. In the initial authentication using the S-AKA-I protocol, the SGSN will communicate with the HLR/AuC to obtain the authorization and delegation information for the sequent authentication to be used in the S-AKA-II protocol. In the S-AKA-II protocol, the MS and SGSN can authenticate each other without data transmission between SGSN and HLR/AuC, which drastically reduces the bandwidth consumption in the course of the authentication procedure.

MS sends first registration request

First, MS computes DK = f6K (FRESH) with the pre-shared key K. MS sends a registration request to the (Serving GPRS Support Node) SGSN through a BSS (base station services). This message is comprised of IMSI, FRESH, LAI and MACMS. IMSI (International Mobile Subscriber Identity) is used herein which is the permanent identifier of a user. By 3G convention, IMSI can be also replaced by the temporary user identifier TMSI (Temporary Mobile Subscriber Identity) to protect user privacy. For simplicity, this paper will only show the use of IMSI herein. FRESH is a random number generated by MS and is served as a random challenge for authentication in the protocol. LAI is the location area identifier used to defeat the redirection attack.

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$MACMS = f1K(FRESH \| LAI)$ is used to protect the integrity of FRESH and LAI.

Algorithm
1. Combine {IMSI/TMSI, Request, LAI, MACMS}->message.
2. MS instants BSS -> sends message->SSGN

The SGSN checks if the BSS is physically connected by LAI

In the second step, The SGSN checks if the BSS is physically connected by LAI. If not, the SGSN rejects the request. Otherwise, the SGSN stores the FRESH. Then it forwards IMSI, FRESH, LAI, and MACMS to HLR/AuC Home Location Register/Authentication Center.

Algorithm-
1. @SGSN-
If (! connection to LAI)
Reject;
Else
Send to HLR/AuC Home Location Register/Authentication Center.

HLR/AuC generates RAND, DK and authentication

In the third step, upon receipt of the request, HLR/AuC generates RAND, DK and computes $f1K(RAND \| AMF)$.

After that, HLR/AuC generates $AUTN = (MACH \| RAND \| AMF)$ for verifying the legality of the MS. HLR/AuC sends DK and AUTN to the SGSN. In this way, HLR/AuC can successfully delegate SGSN to authenticate the MS for the subsequent authentication in the S-AKA-II protocol.

Algorithm-
1. @ reception (request)
@GENERATOR(=HLR/AuC)
{
$AUTN = (MACH \| RAND \| AMF)$;
SENDS to SSGN;
}

Authentication is sent to MS

In the fourth step-.
@ SGSN (generates RANDS),
{
$MACS = f1DK(MACH \| RANDS \| RAND \| FRESH)$,
$AUTNS = (MACS \| RANDS \| RAND \| AMF \| FRESH)$
]
Sends to MS;
}

MS authenticates the SGSN by verifying MACS

In the step five, MS authenticates the SGSN by verifying MACS. The MS checks if the received authenticated response FRESH is equal to his earlier challenge FRESH. To authenticate a response FRESH in AUTNs,

$f1DK(MACH \| RANDS \| RAND \| FRESH)$

is verified. In response to MI-4, MS computes

$XMACH = f1K(RAND \| AMF)$

An $XMACS = f1DK(XMACH \| RANDS \| RAND \| FRESH)$ to authenticate both HLR/AuC and SGSN. For authentication of HLR/AuC, the equality of MACH and XMACH is verified. MS can also authenticate SGSN by checking if XMACS is equal to MACS. Either HLR/AuC or SGSN is invalid, and MS drops the connection. When both are valid, the MS computes

$XRES_H = f2K(RAND)$, $XRES = f2DK(RANDS)$, $IK = f4DK(RANDS)$, and

$CK = f3DK(RANDS)$.

To withstand false GSM BSS attacks, MS checks if a GSM BSS is connected. If so, $PLK = f7DK(RANDS)$ is used to encrypt payloads before CK and IK to protect the session. After that, the SGSN checks the legitimacy of MS by verifying XRES. The SGSN computes IK, CK and PLK if it detects a GSM BSS involved in the session.

Algorithm-
1. Verification (input 1, input 2)
{
If (input 1==input2)
Return verified;
Else
Return false;
}
2. @ MS

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

{

$$XMACH = f1K(RAND \,||\, AMF);$$

XRESH= f2K(RAND), XRES= f2DK(RANDS), IK= f4DK(RANDS),;

$$CK = f3DK(RANDS);$$

Verification (earliest 1, latest 1);

}

3. @MS

{

If (Check connection==ok)

$$PLK = f7DK(RANDS);$$

Calculate CK,PLK,IK;

}

SGSN sends XRESH and XRESS to HLR/AuC

At last (optional). The sixth message is an optional message. SGSN computes $XRESS = f2DK(RAND)$, and sends it back to HLR/AuC together with XRESH received from MS. Then, HLR/AuC can mutually authenticate the legitimacy of MS and SGSN by verifying $XRESH = f2K(RAND)$ and $XRESS = f2DK(RAND)$ respectively. Receipt of the two responses from MS and SGSN ensures HLR/AuC that both participants have successfully completed the S-AKA, and acquire all the secrets needed for subsequent authentications. To achieve the mutual authentication only between MS and SGSN, the sixth message is not needed. However, this message serves as a response to HLR/AuC, and provides S-AKA additional security features where HLR/Auc can authenticate the MS and ensure that SGSN receives the security information he sent earlier.

ALGORITHM

@SSGN

{

$$XRESS = f2DK(RAND);$$

Verify (XRESS);

}

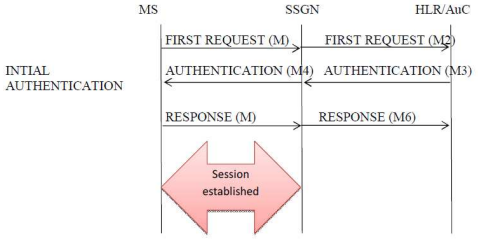

Fig 3: S-AKA algorithm

Algorithm for S-AKA phase

Step-1- initialize the procedure.
Step-2- MS sends first registration request.
Step-3- The SGSN checks if the BSS is physically connected by LAI
Step-4- HLR/AuC generates RAND, DK and authentication
Step-5- Authentication is sent to MS.
Step-6- MS authenticates the SGSN by verifying MACS
Step-7- *SGSN sends XRESH and XRESS to HLR/AuC.*
Step-8- forward the control to section 3.2.2.

3.2.2User Confidentiality for UMTS (EMSUCU)

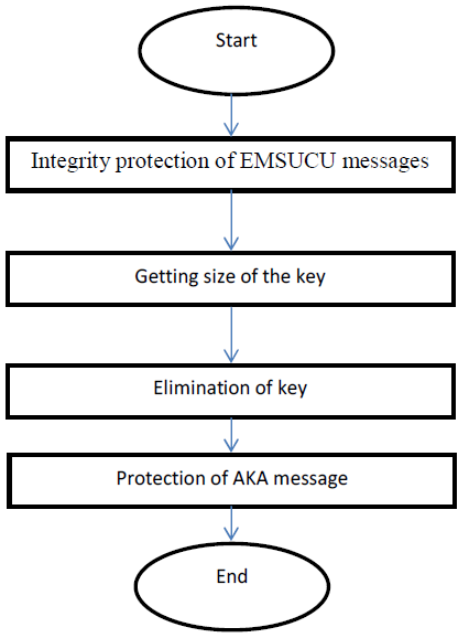

*Fig 4: Shows The Modular Diagram Of **EMSUCU** Phase*

This protocol, named Enhancement Mobile Security and User Confidentiality for UMTS (EMSUCU), offers a means of encrypting the IMSI whenever the TMSI cannot be used. The encryption is realized with a special security function.

This paper considers some changes and improvements to the UMTS security need to respect the general lines of UMTS security development philosophy. It is very important that new solutions do not bring about major changes in security protocols. UMTS security did not come with radical new protocols and procedures. It is developed as an enhancement of the existing GSM security. This paper proposes security protocols to counter the vulnerabilities described above. This paper either enhances already proposed solutions or

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

this paper imports useful principles from one part of UMTS security to another. The security protocols that this paper enhance are the EMSUCU identification as well as the AKA procedure, while and the security principles that this paper imports from other parts of UMTS security are the use of temporary values and the protection of message integrity and confidentiality.

Integrity protection of EMSUCU messages

UMTS security protocols are based on the integrity of the control messages. This paper proposes to respect this rule for the EMSUCU messages. The key *Kc* and a hash function, *f12*, is used to compute a MAC code that will ensure the integrity protection. The hash function is to be chosen in such a way as to be faster than the encryption function, because this will speed up the identification process.

Algorithm-
1. @generation (key)
{
K_c=new hash (f_{12});
}

Getting the size of the key

The function f9, which is used to generate *Kc* generates only 64 bits. A 64 bits key is not able offer a good level of security, according to NIST and ECRYPT. This paper proposes to use a new security function, *f11*, to compute *Kc*. For the UMTS networks that use UAI1 or UAI2, *f11* may be based on the KASUMI or SNOW 3G encryption algorithms.

Algorithm-
1.@ security()
{
Generate f11(KAUSMI/3G);
Generate key =key.hash (f11);
}

Elimination of key

Kmh key is necessary for the EMSUCU procedure. *Kmh* key is shared between the HLR and all of its clients and it allows the HLR to decipher all the messages received during the identification procedure. It is a weakness, a single point of failure, because an attacker that retrieves its value will be able to break the identification procedure of all the users of the HLR. This is why this paper proposes an identification protocol that does not use a key shared by all of the users. This paper proposes replacing *Kmh* with *K* when *KC* is computed by the user. In this case, the task of the HLR will be to find the key *K* that was used by the user. The HLR stores all the pairs (*Ki*, IMSIi). It also stores the state of each mobile phone: on or off. It uses all the *Ki* belongs to mobiles that are turned off to decipher the value of the encrypted IMSI. If that value is IMSIi, then the mobile has been identified.

Algorithm
1. @(generate K_{mh})
K_{mh}=K+KC;
@HLR
@(generate k)
{
}
{
Store (*Ki*, IMSIi);
Store state (on/off);
}

Protection of AKA message is done

One easy way to protect against this type of attacks is to encrypt the values that are sent over the radio link:

RAND, AUTN = (SQNHE⊕AK ‖ AMF ‖ MAC) and RES.

At the time of encryption and integrity keys, CK and IK, need to be changed, the mobile equipment and the network drop them and the AKA procedure is run in order to establish a new set of keys. Our proposition is very simple and practical: instead of dropping CK and IK immediately after they expire.

Algorithm-
1.@ generate (authentication)
{
RAND, AUTN = (SQNHE⊕AK ‖ AMF ‖ MAC) and RES.;
CK=change (CK);
IK= change (IK);
}
2. finalize ()
{
CK.close();
IK.close ();
}

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

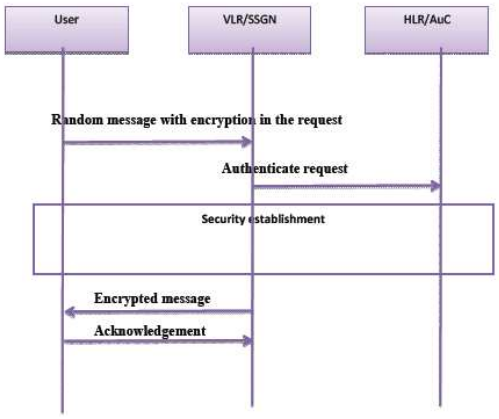

*Fig 5: **EMSUCU Identification***

Algorithm for User Confidentiality for UMTS phase

Step-1- get the input from phase one as described section 3.2.1.
Step-2- Integrity protection of EMSUCU messages.
Step-3- Getting the size of the key
Step-4- Elimination of key
Step-5- Protection of AKA message is done.
Step-6- end the procedure.

3.3 Overall algorithm

Step-1- initialize the network.
Step-2- go to the Secure Authentication Key Agreement Protocol phase as given in section 3.2.1.
Step-3- go for the User Confidentiality for UMTS (EMSUCU) protocol as given in section 3.2.2.
Step-4- finalize the procedure.

4. SIMULATION RESULTS

4.1 Simulation Model and Parameters

The Network Simulator (NS2) [10], is used to simulate the proposed architecture. In the simulation, 50 mobile nodes move in a 500 meter x 500 meter region for 50 seconds of simulation time. All nodes have the same transmission range of 40 meters. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in table.

Table.1 Simulation Settings

No. of Nodes	25
Area Size	500 X 500
Mac	IEEE 802.11
Transmission Range	40m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Requests	25,30,35,40,45 and 50
Attackers	2
Rate	50kb

4.2 Performance Metrics

The proposed Enhanced Security Framework for Authentication and Integrity (ESFAI) is compared with the S-AKA technique [8]. The performance is evaluated mainly, according to the following metrics.

- **Packet Delivery Ratio:** It is the ratio between the number of packets received and the number of packets sent.
- **Packet Drop**: It refers the average number of packets dropped during the transmission
- **Delay**: It is the amount of time taken by the nodes to transmit the data packets.

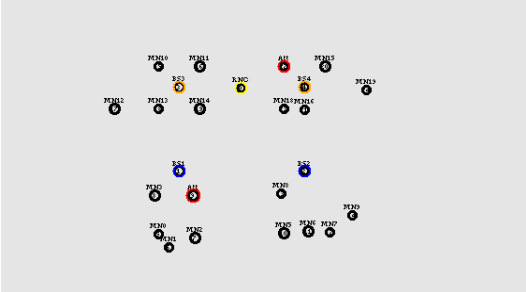

Fig 6: Simulation Topology

4.3 Results

1) Based on Requests

In our experiment we vary the number of requests as 25, 30,35,40,45 and 50.

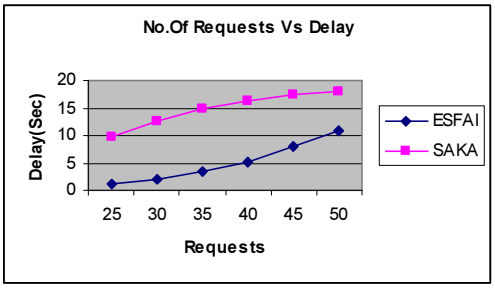

Fig 7: No. Of Requests Vs Delay

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

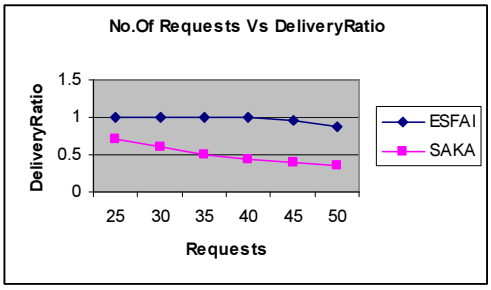

Fig 8: No. Of Requests Vs Delivery Ratio

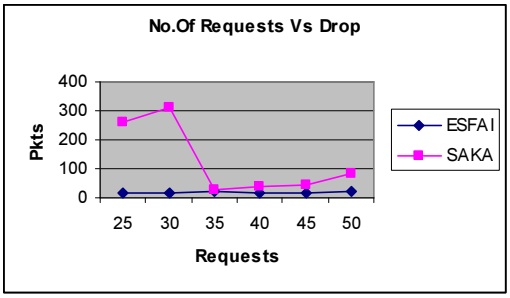

Fig 9: No. Of Requests Vs Drop

Figure 7 shows the delay of ESFAI and SAKA techniques for different number of requests scenario. We can conclude that the delay of our proposed ESFAI approach has 68% of less than SAKA approach.

Figure 8 shows the delivery ratio of ESFAI and SAKA techniques for different number of requests scenario. We can conclude that the delay of our proposed ESFAI approach has 49% of higher than SAKA approach.

Figure 9 shows the drop of ESFAI and SAKA techniques for different number of requests scenario. We can conclude that the drop of our proposed ESFAI approach has 67% of less than SAKA approach.

5. CONCLUSION

Considering the CDMA communications drawback, this paper proposes a two phased solution. The first phase of the solution consists of a secure key generation. The secure keys generation phase is called AKA (Authentication and Key Agreement)-phase. The second phase of the solution is able to solve the problem of redirection attacks, man-in-the-middle attack, sequence number depletion attack, and roaming attack. This phase includes a User Confidentiality for UMTS (EMSUCU) protocol. For a flow contained development, this paper first gives an introduction related to CDMA network in the section one. The second section is a literature study of some previous related works.

This proposed solution is able to solve the problems, vulnerabilities through eliminating it and the solution is able to improve the security and efficiency. The enhanced SHAI technique proposed is able to solve redirection attacks, man-in-the-middle attack, sequence number depletion attack, and roaming attack.

REFERENCE

[1] L.Krishna Bharathi and Gnanou Florence Sudha, "Security Enhancement Using Mutual Authentication in Existing CDMA Systems", *(IJCSE) International Journal on Computer Science and Engineering*, Vol. 02, 2010.

[2] Jae Hoon Roh, Mi-Yeon Kim and Ho Kun Moon, "An Approach to Designing Lightweight Security Protocol on Binary CDMA Sensor Networks", *Ultra Modern Telecommunications & Workshops*, ICUMT'09. International Conference, IEEE, 2009.

[3] Tahereh Shojaeezand, Dr. Paeiz Azmi and AmirMansour Yadegari, "Performance Analysis of a LDPC Coded CDMA System with Physical Layer Security Enhancement", *Wireless Communications Networking and Mobile Computing (WiCOM)*, 2010 6th International Conference, IEEE 2010.

[4] Tongtong Li, Qi Ling, and Jian Ren, "Physical Layer Built-In Security Analysis and Enhancement Algorithms for CDMA Systems", *Hindawi Publishing Corporation EURASIP Journal onWireless Communications and Networking* Volume 2007.

[5] Muhammad Zohaib Mushtaq, Muhammad Ahsan, Muhammad Inam Ur Rehman and Muhammad, "Improving Quality of Security for CDMA using Orthogonal Coding Method", *2011 International Conference on Computer Science and Network Technology*.

[6] A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin and D. F. Grosz, "Hamming-weight Minimisation Coding for CDMA Optical Access Networks with Enhanced Security", *Future Generation Communication Technology (FGCT),* 2012 International Conference, IEEE 2012.

[7] Mohammed A. Mahdi, Mohamed M. Abd-Eldayem, Salwa S. Elgamal and Tat-Chee Wan, "Security Analysis and Enhancement of Authentication in CDMA Based on Elliptic

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Curve Cryptography", *Research Journal of Information Technology,* 2012.

[8] Yu-Lun Huang, C. Y. Shen, Shiuhpyng Shieh, Hung-Jui Wang and Cheng-Chun Lin, "Provable Secure AKA Scheme with Reliable Key Delegation in UMTS", *2009 Third IEEE International Conference on Secure Software Integration and Reliability Improvement*

[9] Daniel Caragata, Safwan El Assad, Charles Shoniregun and Galyna Akmayeva, "UMTS Security: Enhancement of Identification, Authentication and Key Agreement Protocols", *6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates.*

[10] Network Simulator: http:///www.isi.edu/nsnam/ns