Security Enhancement Using Mutual Authentication in Existing CDMA Systems

L. Krishna Bharathi[1],
Department of ECE,
Pondicherry Engineering College,
Pondicherry, India.

Gnanou Florence Sudha[2],
Department of ECE,
Pondicherry Engineering College,
Pondicherry, India.

***Abstract*— Even though CDMA2000 wireless networks are being widely deployed as a cellular digital standard around the world, it has some hidden vulnerabilities concerned with security issues. The existing CDMA systems use authentication mechanism by CAVE (Cellular Authentication and Voice Encryption) algorithm. This authentication method has several disadvantages. Only one way authentication is provided, that is, only a base station authenticates a subscriber. And, CAVE algorithm is prone to cryptographic attacks. This work proposes to implement 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 autocorrelation, 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.**

Keywords—ESA, AKA, CAVE, CDMA, authentication

I. INTRODUCTION

As wireless services become increasingly prevalent, new possibilities and challenges continue to emerge. Security becomes vital to delivering solutions that meet today's demand for mobility.

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 uses 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. These are the major challenges in the existing CDMA systems.

This work proposes to apply ESA instead of CAVE in the authentication process of CDMA mobile communication systems. If ESA can be applied in the existing systems, demerits of CAVE algorithm can be improved. The rest of the paper is designed as follows. Section II discusses about the CAVE algorithm and its drawbacks. Section III and IV discuss about the proposed scheme in detail. Section V discusses the simulation results and section VI concludes the proposed work. Finally, section VII discuss about the future work.

II. SECURITY IN EXISTING CDMA2000 NETWORKS

Security has been a major concern for both service providers and subscribers, since the birth of the cellular industry. Service providers are primarily concerned with security to prevent fraudulent operations such as cloning, while subscribers are mainly concerned with privacy issues. CDMA2000 1xRTT network security protocols rely on a 64-bit Authentication Key (A-Key) and the ESN of the mobile. A random binary number called RANDSSD, which is generated at the Authentication Center (AC), is been used for authentication procedure. This section discusses about the generation of Shared Secret Data (SSD) and Authentication signature using CAVE algorithm and the drawbacks of CAVE algorithm.

A. Cellular Authentication and Voice Encryption Algorithm

Cellular Authentication and Voice Encryption (CAVE) is a set of cryptographic algorithms collectively referred to as the CAVE algorithm which is used during the authentication process. Based on the

inputs used, the CAVE algorithm enables calculation of SSD and authentication signature during challenge/response procedure.

1) Authentication key: The Authentication Key (A-key) also known as "master key", is the cornerstone of CAVE-based authentication. The A-key is provisioned in the home Authentication Center and the mobile station (MS).The purpose of the A-key in authentication is to generate Shared Secret Data.

2) Shared secret data: Shared Secret Data is a 128-bit value that is calculated using the CAVE algorithm. The SSD has two parts: SSD_A (64 bit) and SSD_B (64 bit) [2]. The mobile uses the SSD_A and the broadcast RAND as inputs to the CAVE algorithm to generate an 18-bit authentication signature and sends it to the base station. Figure 1 illustrates the generation of shared secret data in existing CDMA 2000 networks. This signature is then used by the base station to check that the subscriber is legitimate.

The mobile uses the SSD_B and the CAVE algorithm to generate a Public Long Code Mask (PLCM), a Cellular Message Encryption Algorithm (CMEA) key (64 bits), and a data key (32 bits). The PLCM is utilized in both the mobile and the network to change the characteristics of a Long code. This modified Long code is used for voice encryption.

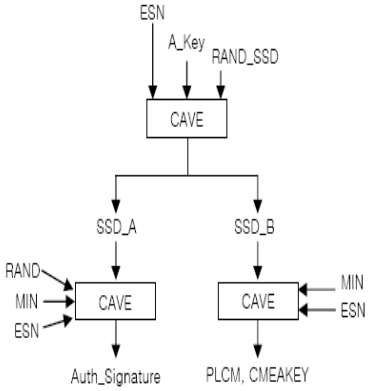

Figure 1. Generation of shared secret data

B. Drawbacks of CAVE Algorithm

The CAVE algorithm is intended to authenticate a legitimate subscriber to the wireless network and protect the network and customers of mobile phones from the cloning fraud. The different attacks on CAVE algorithm namely false base station attacks and cryptographic attacks are described as follows.

1) False base station attacks: Authentication mechanism by CAVE algorithm provides only one way authentication, i.e. only a base station authenticates a subscriber and subscriber cannot authenticate the base station. This leads to base station impersonation or false base station attacks [3]. False base station attacks leads to eavesdropping of private identity information of the subscriber.

2) Cryptographic attacks: A hash function must be able to withstand all known types of cryptographic attacks. As a minimum, it must have the following properties:

a) Pre-image resistance: Given a hash h, it should be difficult to find any message m such that h = hash(m). Functions which don't satisfy this property are vulnerable to pre-image attacks.

b) Second pre-image resistance: Given an input message m1, it should be hard to find another input message m2 (not equal to m1) such that hash(m1) = hash(m2). Functions which don't satisfy this property are vulnerable to second pre-image attacks.

c) Collison resistance: It should be difficult to find two different messages m1 and m2, such that hash(m1) = hash(m2). Functions which don't satisfy this property are vulnerable to collision attacks.

d) Reconstruction attack : The reconstruction attack on CAVE shows that the security offered by CAVE- 4 is less than 12 bits as it computes a pre-image for a given hash value in around 2^11 hashing operations of the algorithm (around 2^13 for CAVE-8). This attack clearly reveals that, 4-round CAVE can be broken in average time equivalent to 1.3*2 ^10 and 8-round CAVE can be broken in 1.25*2^12 executions of the algorithm [4, 5]. Increasing number of rounds from 4 to 8 increases only the workload by 8 times. Hence, increasing the number of rounds of CAVE is not an effective way to increase security.

e) List attack: The second approach to attack CAVE is List attack. In this attack, precomputation is done to establish look-up-tables that define the operation of a segment in CAVE [4, 5]. These experiments reveal that the resulting data sets can specify about half of the unknown LFSR (Linear Feedback Shift Register) bits.

III. ENHANCED SUBSCRIBER AUTHENTICATION ALGORITHM

Enhanced Subscriber Authentication refers to the 3rd generation authentication, this new form of authentication is based on 3GPP Authentication and Key Agreement (AKA). Authentication mechanism by CAVE algorithm uses a symmetry key cryptosystem

with Challenge-Response protocol between a base station and a mobile station. This authentication mechanism has several disadvantages. Only one way authentication is provided, that is, only a base station authenticates a subscriber and CAVE algorithm is also prone to cryptographic attacks. But, Authentication mechanism using ESA algorithm uses AKA to enhance security strength and to provide mutual authentication between a base station and a mobile terminal. This section discusses about the implementation of the ESA algorithm to the existing CDMA systems and also the generation of shared secret data, authentication signature value, voice privacy code and signaling message encryption key using ESA algorithm.

A. *Implementation of the ESA Algorithm to the Existing CDMA Systems*

Implementation of the ESA algorithm to the existing CDMA systems involves the following three phases – Generation of SSD from A_Key, Generation of Auth_Signature from SSD_A and Generation of PLCM from SSD_B. Figure 2 illustrates the ESA algorithm implementation in the existing CDMA systems. To reduce the simulation runtime the Long Code has been replaced by Short code in this proposed work.

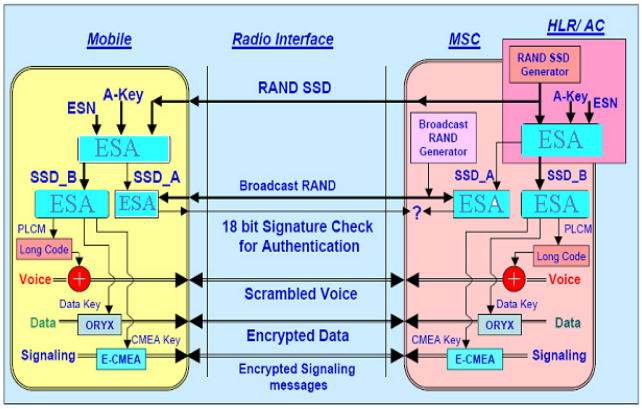

Figure 2. ESA algorithm implementation in the existing CDMA systems

B. *Generation of SSD from A_Key*

Generation of SSD from A_Key, involves the generation of shared secret data for authentication, SSD_A and shared secret data for encryption, SSD_B, using ESA algorithm and subscriber's secret key A_key. As a preceding work to do this, construction of inputs of ESA algorithm is done.

1) Construction of ESA input to produce SSD: Construction of ESA input to produce SSD involves the construction of Input 1 and Input 2. Figure 3 shows the construction of Input 1. 512-bit length Input 1 is comprised of 16 words and size of each word is 32 bits. First word is the value XORed Index into standard SHA1 constant value [6]. SHA1 constant value can be any value with 32-bit length. Second word is the value XORed ESN into SHA1 constant value. And, third and fourth words are each XORed first and second word of RANDSSD into SHA1 constant value.

W[0]	W[1]	W[2]	W[3]	W[4]		W[15]
Index xor Constant	ESN xor Constant	RANDSSD[0] xor Constant	RANDSSD[1] xor Constant	Constant	.....	Constant

Figure 3. Construction of Input 1

Next is to construct 160-bit Input 2. Input 2 consists of 5 words. Figure 4 shows the construction of Input 2. First and second words are each XORed A_Key into first and second words of standard SHA1 Initial Vector.

W[0]	W[1]	W[2]	W[3]	W[4]
A_Key[0] xor IV[0]	A_Key[1] xor IV [1]	IV[2]	IV[3]	IV[4]

Figure 4. Construction of Input 2

2) Generation of SSD_A and SSD_B: Input 1 and Input 2 are used for the generation of SSD_A and SSD_B. Figure 5 shows the Generation of SSD_A and SSD_B by ESA algorithm. Input 1 and Input 2 are loaded into SHA1. Run SHA1 to produce 160-bit output [7]. And then, polynomial AX+BmodG is computed, where A and B are predetermined 160-bit random numbers and treated as polynomials with binary coefficients in the variable T. X is a 160-bits output from SHA1 operation.

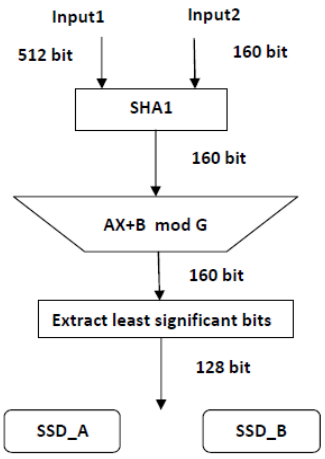

Figure 5. Generation of SSD_A and SSD_B by ESA algorithm

C. *Generation of Auth_Signature from SSD_A*

The generation of authentication signature value Auth_Signature, using ESA algorithm can be discussed as follows:

1) Construction of ESA input to produce auth_signature :

Construction of ESA input to produce AUTH_SIGNATURE is almost similar to the construction of Input 1 and Input 2 besides some parameters are changed as follows. Figure 6 shows the construction of Input 3. Referring to the construction of Input 1, first word of Input 3 is filled with SHA1 constant value which is the same value used in Input1. Second word is the value XORed ESN into SHA1 constant value. The construction of Input 4 is identical with the construction of Input 2 besides A_key is replaced with SSD_A.

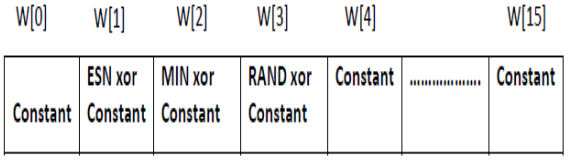

Figure 6. Construction of Input 3

2) Generation of auth_signature: Input 3 and Input 4 are used for the generation of Auth_Signature. Most steps are similar to Figure 5, however, only least significant 18 bits of final 160 bits is extracted as Auth_Signature.

D. *Generation of PLCM from SSD_B*

The generation of voice privacy code, PLCM, CMEAKEY, using ESA algorithm can be discussed as follows:

1) Construction of ESA Input to Produce PLCM :

Construction of ESA input to produce PLCM is almost similar to the construction of Input 3 and Input 4. Besides, first word of Input 3 is the value XORed Index into SHA1 constant value to produce Input 5. And, SSD_A in Input 4 is replaced by SSD_B to produce Input 6.

2) Generation of PLCM : Input 5 and Input 6 are used for the generation of PLCM and CMEAKEY. Most steps are similar to Figure 5, however, only least significant 15 bits is used for PLCM and 64 bits for CMEAKEY are extracted from the 160 bit output.

E. *Advantages of ESA over CAVE Algorithm*

ESA algorithm overcomes the false base station attacks using AKA mechanism. It also overcomes the cryptographic attacks. Table I shows the comparison of attacks in ESA and CAVE algorithm.

Table I: Comparison of attacks in ESA and CAVE

Types of attacks	CAVE algorithm	ESA algorithm
Pre-image attack	2^128 hashing operations	Nil
Second pre-image attack	2^128 hashing operations	Nil
Collision attack	2^16 hashing operations	2^52 hashing operations
Reconstruction attack	2^91 hashing operations	Nil
List attack	2^72 hashing operations	Nil

IV. AUTHENTICATION AND KEY AGREEMENT

Authentication and Key Agreement relies on an authentication key associated with the MS and available only to the MS and its home AC. AKA involves a challenge process that allows the network to authenticate the MS. However, in AKA the information provided during this challenge also enables the MS to authenticate the network, providing for bilateral authentication [8]. Following the bilateral authentication, AKA also allows for the generation of new Cipher Key (CK) and Integrity Key (IK). These 128-bit keys enable a security association between the MS and the serving MSC for supporting security

services such as data integrity and data encryption. This section discusses about the various phases involved in AKA process.

A. *Phases involved in AKA Process*

AKA process involves four major phases - Distribution of Authentication Vectors (AV), Authentication of the network by the MS, Authentication of the MS by the network, Establishment of security association between MS and MSC. Figure 7 illustrates the AKA mechanism.

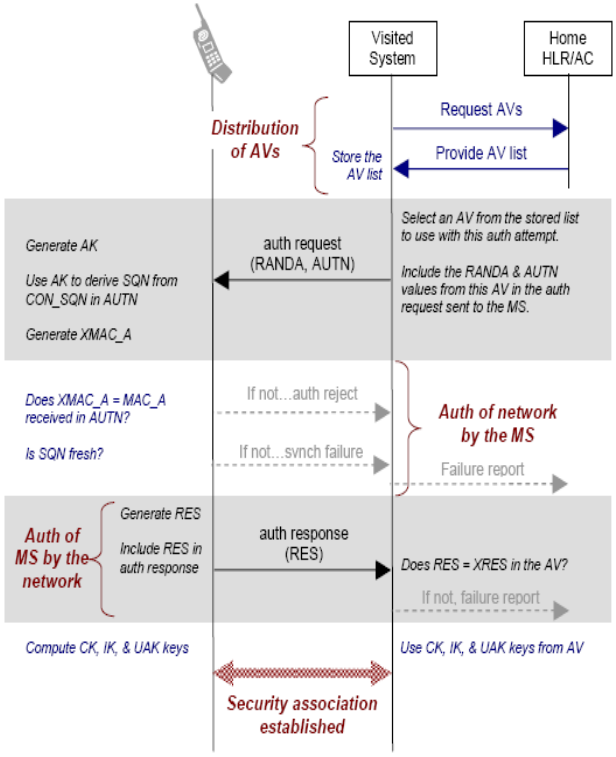

Figure 7. Authentication and key agreement mechanism

B. *Distribution of Authentication Vectors*

An Authentication Vector (AV) is essentially a group of information used for one AKA attempt. Figure 8 illustrates the information contained in an authentication vector. AVs are generated by the home AC and distributed to the visited network [8]. Each AV contains all information required by the visited network to locally perform AKA with an AKA-enabled mobile station. To thwart replay attempts, each AV must be used for only one AKA attempt.

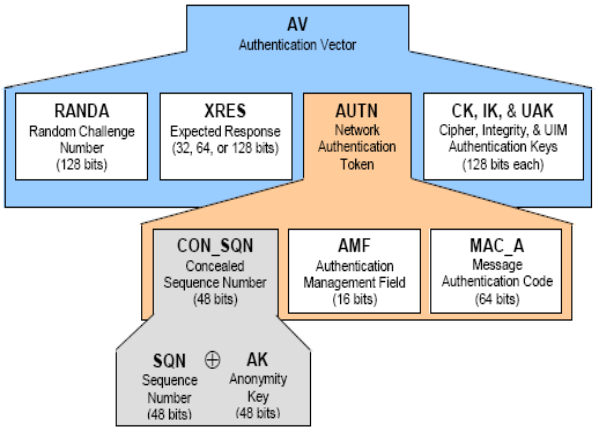

Figure 8. Information contained in an authentication vector

C. *Authentication of the Network by the MS*

To ensure synchronization between MS and network, a sequence number is provided by the network and compared against the sequence number maintained by the MS. To validate the authenticity of the message, a MAC_A (Message Authentication Code) is provided by the network and compared against an XMAC_A (Expected Message Authentication Code) computed by the MS.

D. *Authentication of the MS by the Network*

Authentication of the MS by the network in AKA is similar to a unique challenge without shared SSD in CAVE. The Authentication response (RES) received from the MS is verified against the Expected RES (XRES) received from the home system in the network authentication token (AUTN).

E. *Establishment of Security Association between MS and MSC*

The CK, IK and UIM authentication key (UAK) are generated by the MS in such a way that they are identical to the ones provided to the visited network in the AV. The security association between MS and MSC involves using these keys to support security services such as confidentiality and integrity. The last phase involves the establishment of a security association following bilateral authentication between MS and network.

V. PERFORMANCE METRICS

In this Section, the performance of the ESA algorithm has been evaluated by effective voice transmission and reception and also by calculating autocorrelation, cross-correlation and BER of the system in a CDMA environment.

A. Speech Signal

For the security analysis, the proposed method utilized speech signal of the type WAV (Waveform Audio File Format), which is sampled at 16 kHz. The generated short PN-sequence is been XORed with the given voice signal to generate scrambled voice. The Figure 9 shows the speech waveform and Figure 10 shows the autocorrelation of short PN-sequence. The short PN-sequence generated using the LFSR has been used to scramble the given voice signal. All simulations are done using Matlab 7.8.0 version software.

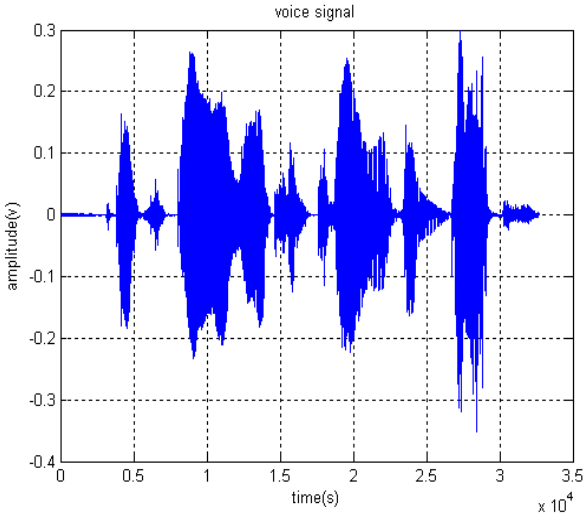

Figure 9. Speech signal waveform

1) Cross-correlation between voice and scrambled-voice: Cross-correlation compares two sequences from different sources rather than a shifted copy of a sequence with itself. The cross-correlation between voice and scrambled voice is shown in Figure 11. From this figure, it is observed that the correlation between the voice and scrambled voice is zero, i.e. both the sequences are dissimilar.

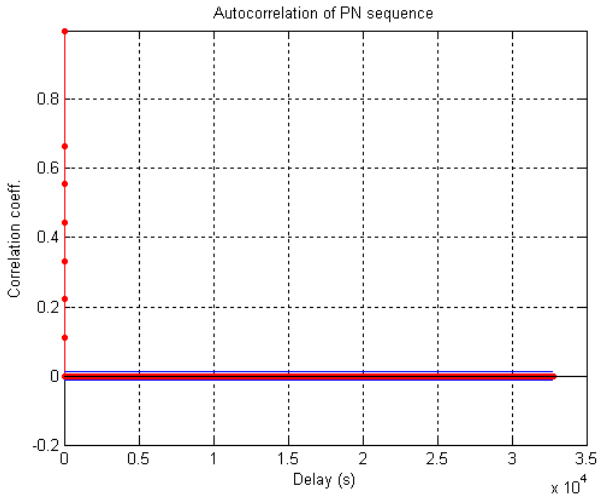

Figure 10. Autocorrelation for short PN-sequence

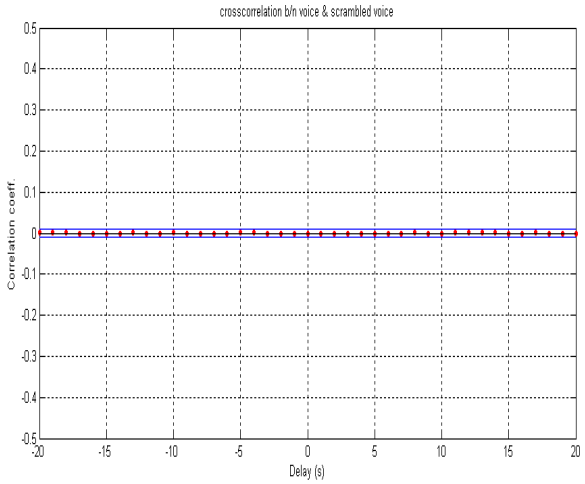

Figure 11. Cross-correlation between voice and scrambled-voice

B. Authentication and Key Agreement Process

Implementation of the ESA algorithm to the existing CDMA system is followed by the authentication and key agreement process. In AKA, the MS authenticates the network, similarly, the network authenticates the MS and finally security association is established between MS and MSC.

1) Establishment of Bilateral Authentication between MS and Network: The establishment of security association between MS and the network leads to bilateral authentication between the MS and the network. The bilateral authentication between MS and network is shown in Figure 12. From this figure, it is observed that successful completion of AKA process

leads to bilateral authentication between MS and network.

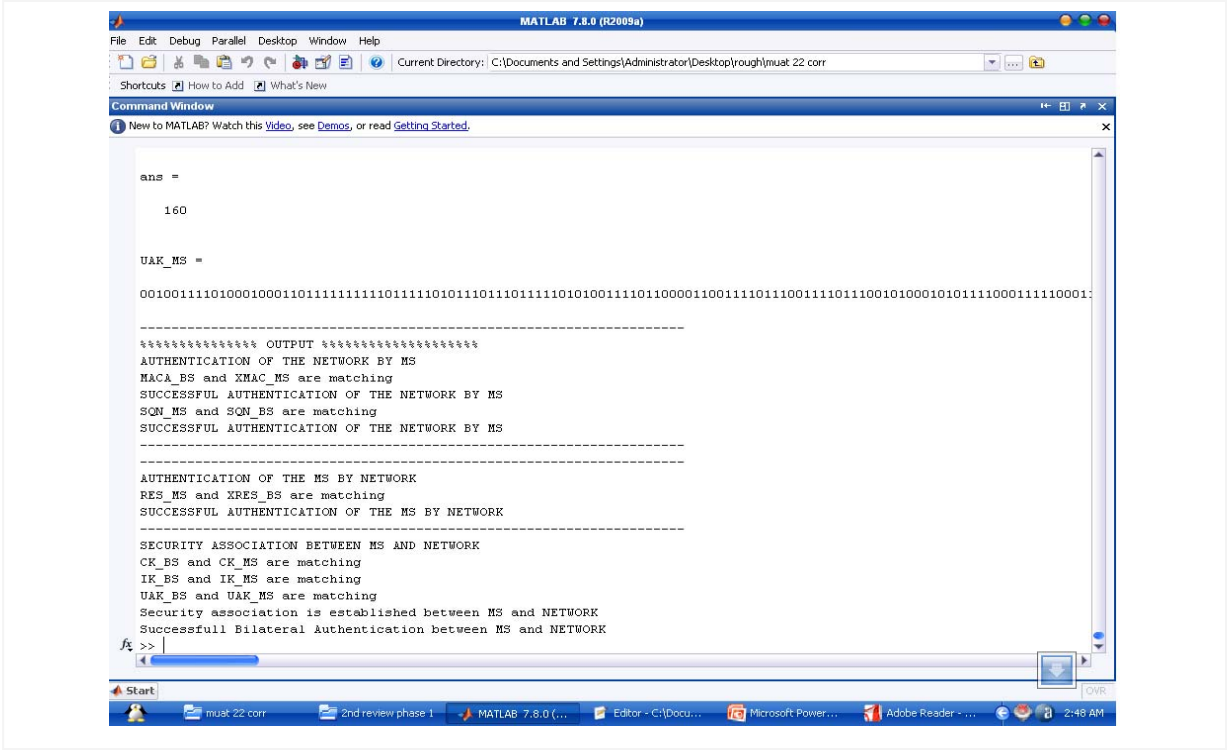

Figure 12. Establishment of bilateral authentication between MS and network

C. *Descrambling Process*

The scrambled voice which has been generated at the MS, after successful mutual authentication is transmitted to the MSC where the descrambling process takes place. If the mutual authentication fails, the descrambling of the voice signal does not takes place.

1) Cross-correlation between voice and descrambled-voice: Cross-correlation compares two sequences from different sources rather than a shifted copy of a sequence with itself. The cross-correlation between voice and descrambled voice is shown in Figure 13. From this figure, it is observed that the correlation between the original voice and descrambled voice is one, i.e. both the sequences are similar.

D. *Performance Analysis of ESA in CDMA Environment*

Performance analysis of the ESA algorithm is done after implementing the ESA algorithm in a CDMA. Using ESA, PLCM has been generated which is used for generation of short code, the generated short code is in turn used for voice encryption. The performance analysis is done by calculating the BER of the system.

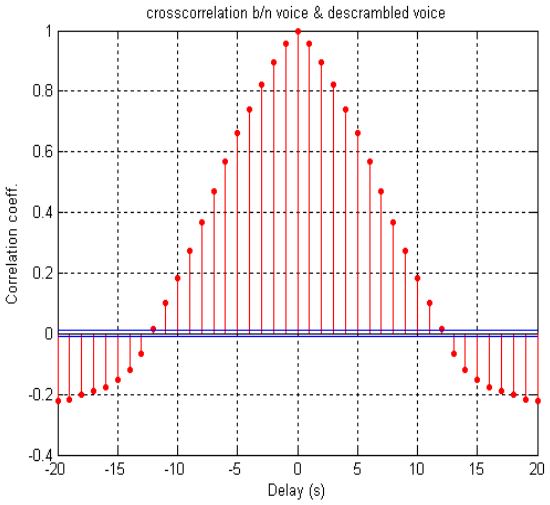

Figure 13. Cross-correlation between original voice and descrambled-voice

1) BER comparison for ESA PLCM and RAND PLCM: The BER comparison for ESA PLCM and RAND PLCM is shown in Figure 14. Here, RAND PLCM is nothing but the PLCM which has been randomly generated without using ESA algorithm. From this figure, it is observed that the proposed

algorithm shows better performance starts at low power. Consider the BER of 1/10000, the power utilized by the proposed algorithm is about 13db, while the power utilized by RAND PLCM is about 15db and the error rate is also less. This clearly implies that the performance of ESA algorithm is better than existing algorithm.

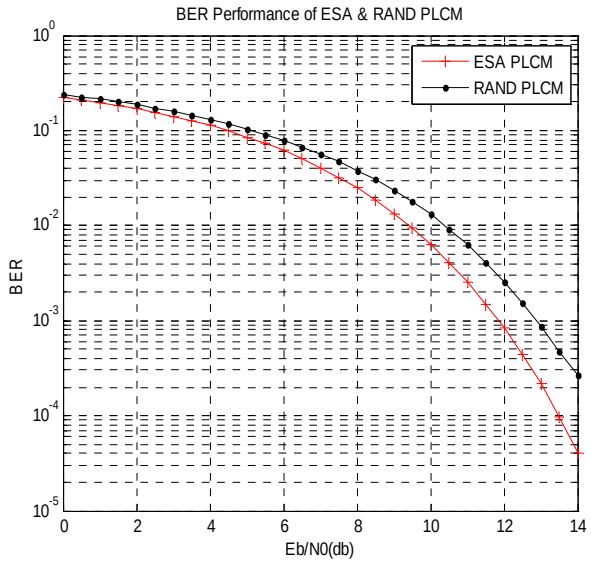

Figure 14. BER performance of ESA and RAND PLCM

VI. CONCLUSION

Thus the proposed work enhances the built-in security of CDMA systems by applying the ESA algorithm instead of CAVE algorithm in the authentication process of existing CDMA mobile communication systems. The proposed method is also compatible to the existing CDMA systems because only the algorithm is replaced but the input parameters remain the same.

This method utilizes the Authentication and Key Agreement which provides mutual authentication between a base station and mobile terminal with increased key size. Mutual authentication overcomes the problem of false base station attacks, thereby preventing the voice privacy or private identity information of the subscribers from being compromised. The ESA algorithm also dismantles the cryptographic attacks such as reconstruction attack and list attack, thereby enhancing the security of existing CDMA systems. The simulation results also clearly indicates that ESA based systems consumes less power and the error rate is also less when compared with CAVE based system. Thus, the Enhanced Subscriber Authentication algorithm enhances the security of the CDMA systems.

VII. SCOPE FOR FUTURE WORK

Though the proposed method enhances the security of CDMA systems, it can be further enhanced by employing AES in the scrambling process, instead of pseudo-random scrambling. It enhances the physical layer built-in security of CDMA systems through secure scrambling. AES consumes less memory and also ease of implementation and flexibility. CDMA systems with secure scrambling improve the system performance and information privacy.

Since, SHA1 algorithm is prone to collision attack, it can be overcome by using SHA2 algorithm instead of SHA1. In addition to that, the short PN-sequence can also be replaced by Gold codes to yield better system performance.

ACKNOWLEDGMENT

The authors would like to express their cordial thanks to Dr. E. Srinivasan for his valuable advice.

REFERENCES

[1] M.Naidu and C.Wingert, “CDMA 1xRTT Security Overview”, *Qualcomm Inc.*, August 2002.

[2] K.Chung, D.Hong and K.Kim, “Application of ESA in the CAVE Mode Authentication”, *World Academy of Science, Engineering and Technology*, Vol.18, pp.92-96, June 2006.

[3] Bellcore and S.Patel, “Weakness of North American Wireless Authentication Protocol”, *IEEE Personal Communications Magazine*, Vol.4, pp.40-44, June 1997.

[4] P.Gauravaram and W.Millan, “Cryptanalysis of the Cellular Authentication and Voice Encryption Algorithm”, *IEICE Electronics Express*, Vol.1, No.15, pp.453-459, November 2004.

[5] P.Gauravaram and W.Millan, “Improved Attack on the Cellular Authentication and Voice Encryption Algorithm”, *Proceedings of International workshop on Cryptographic Algorithms and their Uses*, Australia, pp.1-13, July 2004.

[6] FIPS 180-2, “Secure Hash Standard”, NIST, August 2002.

[7] 3GPP2 S.S0055, “Enhanced Cryptographic Algorithms”, January 2005.

[8] 3GPP AKA: http://www.cdg.org/

BIOGRAPHY

Krishna Bharathi received the B.E degree in Electronics & Communication Engineering in 2007 from Anna University, Chennai, India. He is currently pursuing M.Tech in the Department of Electronics & Communication Engineering at Pondicherry Engineering College in the field of Wireless

communication. His fields of interests include mobile and wireless network security.

Gnanou Florence Sudha completed B.Tech in Electronics & Communication Engineering from Pondicherry Engineering College affiliated to Pondicherry University in 1992. Obtained M.Tech in Electronics & Communication Engineering from Pondicherry Engineering College in 1994. Completed PhD in Electronics & Communication Engg in 2005. She joined the Dept. of Electronics & Communication Engg, Pondicherry Engineering College as Lecturer in 1995. She worked as Senior Lecturer in the same institute from 2000 to 2005. Currently, she is Associate Professor in the same department. She has published more than 36 journals and conference papers and her fields of research interests are in Signal Processing and Bio-Medical engineering.