IJSRCSEIT

International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Encryption of Voice in GSM Network Using RC4 Algorithm

Nuha Hussain Abd Alrazig[1], Faisal Mohammed Abdullah[2]

[1]M.Sc. Student, College of Computer Science and Information Technology Sudan University of Science and Technology, Sudan

[2]Assistant Professor, College of Computer Science and Information Technology Karary University, Omdurman, Sudan

ABSTRACT

Mobile telecommunications such as Global System for Mobile Communication (GSM) are now well established globally and users rely heavily on the convenient communications it provides. The level of security provided by GSM is superior to its predecessors and is more than adequate for the majority of users. However, some users in the areas of government, defense or business require more security over and above that provided by the GSM standards and by standard GSM equipment. In a GSM network, only the radio channels between the mobile station (MS) and the base transceiver station (BTS) are encrypted. This paper presents methodology for implementation of end-to-end security over the available GSM infrastructure by adding encryption algorithm (RC4 algorithm) to standard GSM. The communications between parties is encrypted in GSM environments and simulation is carried using MATLAB software as simulation tool the results show that's the proposed method can be applied and without any modification to GSM standard and optimum result can be obtained.

Keywords: GSM Voice Encryption, GSM Speech Coding, GMSK, Voice Coefficients, Voice Encryption, RPE-LTP.

المستخلص: يقدم هذا البحث نظاما مقترحا لتطبيق تشفير الصوت من النهاية (موبايل) للنهاية (موبايل) على شبكة الهاتف الخليوي (GSM) . في معيار (GSM) يتم استخدام خوارزمية التشفير (A5) فقط ما بين الهاتف ومحطة الارسال والاستقبال اما في بقية مكونات الشكبة فلا يوجد تشفير ترسل البيانات كما هي ، لذا قمنا في هذا البحث باقتراح تطبيق التشفير من النهاية للنهاية باضافة خوارزمية (RC4) لضمان التشفير الكامل للبيانات على كل الشبكة . تم استخدام برمجية الماتلاب (MATLAB) كاداة محاكاة (GSM) وتم الحصول على أفضل النتائج في سياق امن الصوت والجودة.

I. INTRODUCTION

Wireless Networks share many common characteristics with traditional wire-line networks such as public switch telephone/data networks, and hence many security issues with the wire-line networks also apply to the wireless environment. The GSM system doesn't provide end-to-end security and lacks in provision of traffic confidentiality to its subscribers. Anonymity, authentication, and confidentiality are the security services which are offered by the world's largest mobile telephony system. Still this system is defenseless against many attacks and fails to ensure taut safety of the user's telephone conversations and data transfer sessions. Confidentiality of transmitted data is achieved by encrypting the information flow between the communicating parties. In GSM networks, only the radio link between the mobile terminal and the base station is encrypted whereas the rest of the network transmits data in clear-text. Radio link confidentiality in GSM is not sufficient for attaining end-to-end security. As a result, a need for investigating mechanisms for implementing absolute confidentiality of traffic arises.

In this paper, a new method for securing GSM mobile networks is proposed, using MATLAB software as simulator in GSM environments . MATLAB (Matrix Laboratory) becomes the de facto tool in digital signal processing. MATLAB is a well-known tool for numerical calculations, this paper employs its features as simulation of GSM environment.

1. GSM SECURITY :

GSM is still the most widely used cellular system in the world, even the fourth and fifth generations are now operated in some countries. However, GSM bears numerous security vulnerabilities and for that reason it has seriously considered security threats. Although GSMs architecture is designed in such a way to provide various security features like authentication, data and signaling confidentiality, and the user secrecy, the GSM channel is yet susceptible to replaying, interleaving and man-in-the-middle attacks. The GSM voice calls are encrypting a family of algorithms collectively called A5[8][9]. this algorithm exposed to number of attacks on A5/1 have been published, and the American National Security Agency is able to routinely decrypt A5/1 messages according to released internal documents.

Some attacks require an expensive preprocessing stage after which the cipher can be broken in minutes or seconds. Until recently, the weaknesses have been passive attacks using the known plaintext assumption [10].

2. GSM SECURITY ATTACK :

1. Replay Attack:

The attacker can misuse the previously exchanged messages between the subscriber and network in order to perform the replay attacks [2][9].

2. Attacks on A5/1 algorithm:

guess-and-determine attack on the A5/1 stream cipher, by analyzing the clocking mechanism of the cipher and guessing both some bits and some clocking states, the complexity brute-force attack.

Also some of their version designed to Middle East and countries has no security.

3. Interleaving Attack:

A masquerade which involves use of information derived from one or more ongoing or previous authentication exchanges. The interleaving attack is usually applied to two parallel sessions of a protocol. Attacker collects information from different executions of a security protocol and might be able to break the protocol.

4. Man-in-middle Attack:

This is the network that authenticates users but user does not authenticate network. So, the attacker can use a false BTS with the same mobile network code as the subscriber's legitimate network to impersonate himself and perform a man-in-the-middle attack.

3. RELATED STUDIES :

a. Khaled Merit and Abdelazziz Ouamri [4] in their paper used Data Encryption Standard algorithm (DES with random permutation and Inverse) proposed method to solve the problem of adjustable of that traditional encryption algorithms with RPE-LTP vocoder requirements and constrains in GSM system.

b. Himanshu Gupta and Dr. Vinod Kumar Sharma [5] in their paper explore the role of multiple encryptions in secure voice communication over the insecure network.

4. Methodology:

This paper present methodology for implementation of end-to-end security over the available GSM infrastructure by adding encryption algorithm (RC4 algorithm) to standard GSM handset (see figure 1).

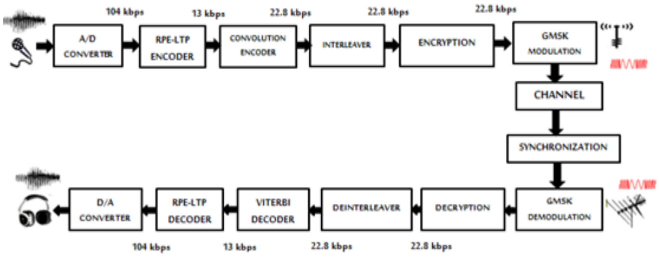


Figure 1. Proposed system

In this paper summaries the transmitted operation and received operation as :

4.1. RPE-LTP Encoder/Decoder: Regular Pulse Excitation Long Term Prediction (RPE-LTP) codec the data. ADC (Analog to Digital Converter) samples data at sampling frequency of 8K with 13 bit resolution to achieve output data rate of 104kbps fed them to RPE-LTP after split up into frames with 160 samples/frame/20 ms then fed it to RPE-LTP. It extract the coefficient (76 parameters) from speech data their output data rate 260 bits/20 ms =13kbps [3][4].

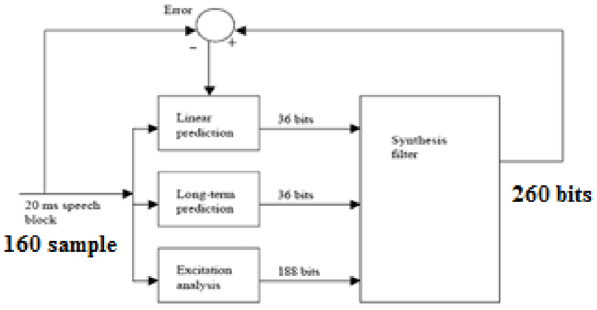


Figure 2. RPE-LTP Encoder

At receiver the RPE_LTP Encoder will retrieve the data from their parameter see figure 3

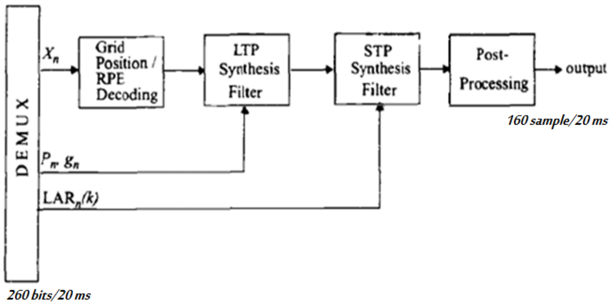


Figure 3. RPE-LTP Decoder

4.2. Channel Coding/Decoding : In GSM the Channel Coding used is a combination of :

Error Detection Coding: employed are Cyclic Redundancy Check (CRC) or polynomial codes.

Error Correction Coding (Convolution Encoder): Convolution code is a very powerful type of error-correcting code used in channel coding to counter the random errors that occur during the signal transmission. The idea of channel coding is to improve the capacity of a channel by adding some carefully designed redundant information to the data being transmitted through the channel. In the process the data can be recovered with more certainty at the receiver[4][5].

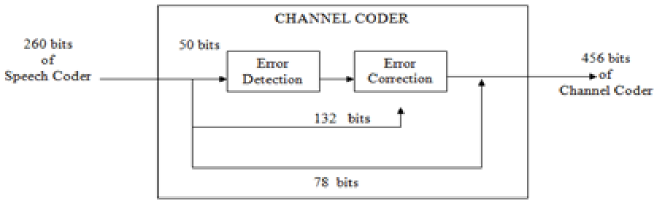


Figure 4. Channel Coding

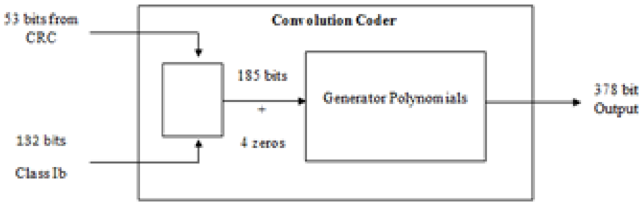


Figure 4. Error Correction- Convolution Coder

At receiver side the inverse operation called **Viterbi decoder :** logically explores in parallel every possible user data in sequence. It encodes and compare each one against the received sequence and picks up the closest match: it is a maximum likelihood decoder. To reduce the complexity the number of possible data sequence double with each additional data bit, the decoder recognizes at each point that certain sequences cannot belong to the maximum likelihood path and it discards them

4.3.Interleaver/De-Interleaver: convolutional codes are best suited to randomly distributed errors and do not perform well if burst errors occur. Therefore Interleaving is used to spread over eight time slots in sub-blocks of 57 bit each (to avoid the risk of losing consecutive data bits) figure 5 explain how the interleaving done.

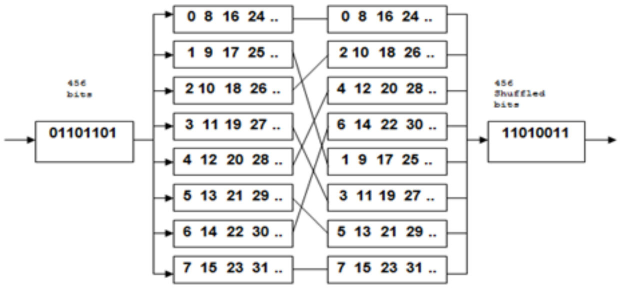


Figure 5. Interleaving

The De-Interleaving is taken more time because it wait to receive all blocks and rearrange it per bit from each column.

4.4. Encryption/Decryption (RC4 Algorithm) :

A protection has been introduced in GSM by means of ciphering the transmission. Ciphering is achieved by performing an exclusive or" operation between a pseudo-random bit sequence produced by RC4 algorithm and a 456 bit received from Interleave function then it divided it to blocks each one has 8 bits. after encryption process completed data is sent to Modulation function . the pseudo-random sequence is derived from the pseudo-random generation algorithm (PRGA) and a key established previously. Deciphering follows exactly the same operation of encryption

4.5. Modulation/Demodulation:

GSM uses Gaussian Minimum Shift Keying (GMSK) as its modulation scheme. In digital communication, GMSK is a Continuous-Phase Frequency-Shift Keying modulation (CPFSK) scheme . In GMSK modulation the incoming sequence of bits is converted to NRZ sequence with 4 samples per symbol corresponding to four 1's for bit '1' and four -1's for '0'. Then this NRZ sequence is filtered with a Gaussian filter which provides spectral efficiency figure 7. The filtered NRZ sequence is integrated to produce the phase information that is the inherent characteristic of a FM modulation. The phase is scaled for pi/2 change for every bit. The sine and cosine of this phase are taken to produce I and Q channel information. The GMSK complex signal consists of I as the real part and Q as the imaginary part.

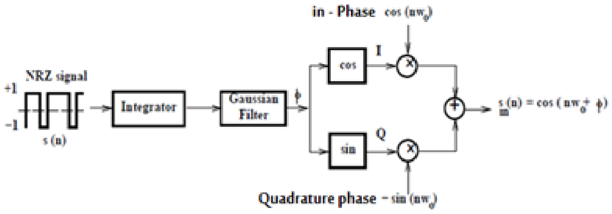


Figure 7. GMSK Modulator

We have employed one bit differential detector which delays the incoming sequence of GMSK complex signal by one bit that is 4 to 5 samples delay. The resulting complex signal is multiplied with the original GMSK signal to produce the phase information that is stored in the imaginary part of the complex signal figure 8

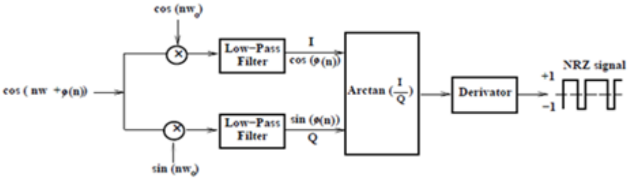


Figure 8. GMSK De Modulator

II. RESULTS

To evaluate the encryption performance of the proposed method, it is employed to encrypt the voice data. An original voice signal having 40,000 samples, sampled at rate of 8 KHz is encrypted using the keystream generated out of the RC4 algorithm. The voice signal is preprocessed, compressed and do some operation (mentioned in this chapter) on it to get the corresponding voice bit stream. The voice bit stream is then XORed with the keystream. The simulation result of voice encryption is shown in Figure(4-14) . As it can be seen that the encrypted voice signal shown in Figure(4-14)(b) is totally distinct from the original voice signal shown in Figure(4-14)(a) and it is randomly distributed like a noise signal. The signal distribution in Figure(4-14)(b) is completely flat/uniform at two extreme ends. This shows the effectiveness and suitability of the proposed scheme for voice data encryption.

Figure(4-14)(c) explain the recovered voice with considered that the delay is 1symbol (4 samples).

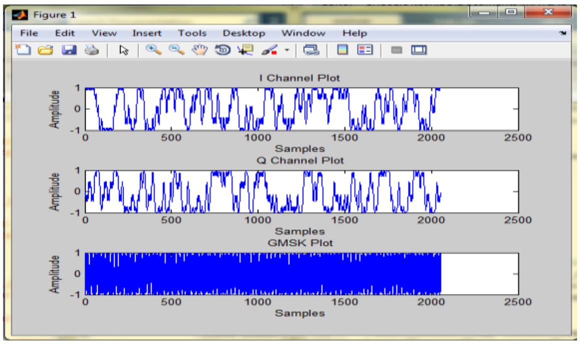


Figure 9. In phase, Quadrature phase and GMSK signal at Modulation

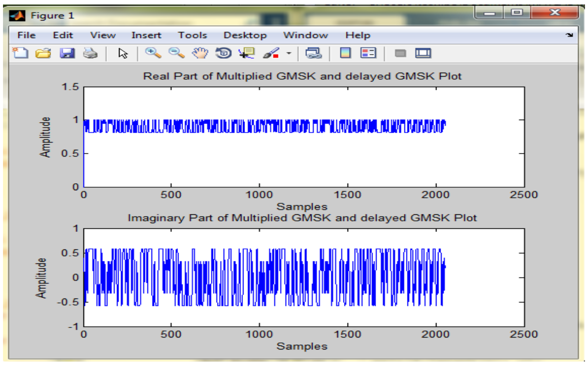
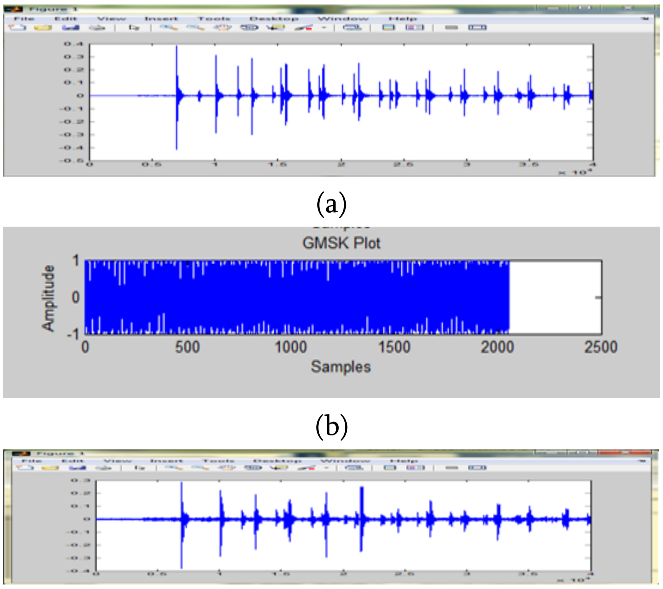


Figure 10. Real and Imaginary part of Multiplied GMSK Signal and Bit Delayed GMSK Signal at Demodulation



(a)

(b)

(c)

Figure (4-14). Voice Encryption (a) Original voice (b) Encrypted voice (c) Recovered voice

The experiment also show the closed values between original voice values in table (4-2) and their Corresponding recovered voice values in table(4-3).

Table (4-2). first 24 values of original speech

1	0.0000000000	2	0.0000305176	3	0.0000305176	4	0.0000000000
5	0.0000305176	6	0.0000000000	7	0.0000000000	8	0.0000000000
9	0.0000000000	10	0.0000000000	11	0.0000000000	12	0.0000305176
13	0.0000000000	14	0.0000000000	15	0.0000000000	16	0.0000000000
17	0.0000000000	18	-0.0000305176	19	0.0000000000	20	0.0000000000
21	0.0000305176	22	0.0000305176	23	0.0000000000	24	0.0000000000

Table (4-3). first 24 values of recovered speech

1	0.0015563965	2	0.0048522949	3	0.0047607422	4	0.0002136230
5	0.0000000000	6	-0.0000305176	7	0.0000000000	8	0.0000305176
9	0.0001525879	10	0.0005493164	11	0.0001831055	12	-0.0000610352
13	0.0016479492	14	-0.0043334961	15	-0.0015869141	16	0.0014648438
17	0.0000000000	18	0.0000915527	19	0.0000000000	20	0.0000000000
21	0.0002441406	22	-0.0000305176	23	0.0001525879	24	0.0001525879

table (4-4) show that no change appears on two signals before encryption and after decryption this result prove that RC4 algorithm add more confidentiality and protect speech/data without any modification in GSM modules.

Table (4-4). compare encrypt/decrypt data

Data before pass to RC4 algorithm
10111111101110000101101110101110101011111100000110111101110010010111001100010010110110100111000110011000110111100110001100000010011011101110110101101010100000110011010100111011110110101011010000111100011100010110011010100101010011010001100011101100011100001110110010101001111110001000011101111100010010110010000000011001101111011000001010110101010001101000101110110110110010010010010110111000011010101101010011111110000010101001000110001101101001101110101100000000000000000000000000000000000000000000000000000000
Encrypted Data
0101101001011101101111100100101101001010001001000101100000101100100101101111011100111111100101000111110100111011100001101110011110001011000010001000111101100110110100001101111000111111010100011101100110010100100000110100000010101000111111010000100110010101000010010100110000011101011000101001100110101110110001011111110001011000011001110101000010100011011011100101001100101100110000000101110110001111001100010001101111101111011101000110100001000011000011101110010111100101111001011110010111100101111001011110010111100101
decrypted Data
10111111101110000101101110101110101011111100000110111101110010010111001100010010110110100111000110011000110111100110001100000010011011101110110101101010100000110011010100111011110110101011010000111100011100010110011010100101010011010001100011101100011100001110110010101001111110001000011101111100010010110010000000011001101111011000001010110101010001101000101110110110110010010010010110111000011010101101010011111110000010101001000110001101101001101110101100000000000000000000000000000000000000000000000000000000

III. CONCLUSION

In this research we proposed encryption method to fulfill the end–to-end secured communication in the GSM voice. We use RC4 algorithm to add more confidentiality to GSM conversation and data. The proposed method was implemented without any modification on GSM standard .

The advantage of this method it was depended on GSM specification and without any adjustment in current GSM signaling system . the simulation is carried up using MATLAB software and the results obtained show that RC4 algorithm in GSM add more confidentiality and protect speech without any modification to GSM modules with reasonable speed compared with other ciphers such as DES, AES .

IV. REFERENCES

[1]. Data Communication and Networking By Behrouz A.Forouzan 4th Edition.

[2]. Mobile-Communications 4th Edition by Dr-Jochen-Schiller .

[3]. Securing Speech in GSM Networks using DES with Random Permutation and Inversion Algorithm (International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012)

[4]. Role of Multiple Encryption in Secure Voice Communication (International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 2 (2013) ISSN 2320–4028 (Online)

[5]. GSM and Personal Communications Handbook (Mobile Communications Library) by Siegmund Redl , Matthias Weber , Malcolm W. Oliphant .

[6]. Brand/GSM_vokoder.pdf

[7]. Security in the GSM Network Ammar Yasir Korkusuz Bogazici University, Electrical-Electronics Engineering Department, MSc. Student.

[8]. Wireless Communication by V. S. Bagad .

[9]. An Investigation Into Authentication Security of GSM Algorithm for Mobile banking By Ali Raheem .

[10]. Proceedings of the International Conference on Information Systems Design and Intelligent Application 2012 edited by Suresh Chandra Satapathy, P S Avadhani, Ajith Abraham.