Securing Text Messages using Elliptic Curve Cryptography and Orthogonal Frequency Division Multiplexing.

O. Shoewu[1] and Segun O. Olatinwo[2*]

[1] Department of Electronics and computer Engineering, Lagos State University, Epe Campus, Nigeria.
[2] Department of Computer Engineering, Moshood Abiola Polytechnic, Abeokuta, Nigeria.

E-mail: segunolatinwo@yahoo.co.uk*

ABSTRACT

This paper focuses on encryption, decryption, transmission, modulation, and demodulation in a wireless environment to secure messages sent on GSM. This paper employs the use of Elliptic Curve Cryptography (ECC) for encryption and decryption of text messages in order to preserve the quality, integrity, and security of text messages as well as the use of Orthogonal Frequency Division Multiplexing (OFDM) for good signal reception in order to transmit the encrypted message over Rayleigh fading environment.

This paper is based on improving the reliability of SMS sent in wireless networks and it is aimed at the use of ECC encryption and decryption algorithms to identify/verify its use as a reliable method base on key considerations (speed, key length, strength).

(Keywords: elliptic curve cryptography, ECC, encryption, orthogonal frequency division multiplexing, OFDM, quadrature amplitude modulation)

INTRODUCTION

Mobile communication devices have become common place during the past few years, integrating multiple wireless networking technologies to support additional functionality and services. They have become popular tools for gathering and disseminating information and data. One of the most important developments that have emerged from communication technology is Short Message Service (SMS). It was designed as part of Global Communication System for Mobile Communication (GSM) [1].

The SMS is a text message that enables users to send short messages to other users on the GSM network. It was originally meant to notify users of their voice mail messages but it has now become a popular means of communication by individuals and businesses. Banks worldwide are using SMS to conduct some of their banking services. For example, clients are able to query their bank balances via SMS or conduct mobile payments. Also, people sometimes exchange confidential information such as passwords or sensitive data among each other. SMS can be sent and received simultaneously with GSM voice, data and fax calls.

With the advent of mobile communication technology, there is unavoidable use of wireless connectivity and because of the challenges of integrity and security of signals or messages to be transmitted; it becomes essential to identify and make use of the best and suitable cryptosystem for messages from sending end to receiving end.

Although the network connections between the Short Message Service Center (SMSC) and nodes in a GSM network are usually protected by Virtual Private Network (VPN) tunnels, the SMS message are stored unencrypted at the SMSC. Many SMSC also retain a copy of SMS messages for audit, billing and dispute resolution purposes. Therefore, SMS travels as plain text and privacy of the SMS contents cannot be guaranteed, not only over the air but also when such massages are stored on the handset. The contents of messages are visible to network operator's system and personnel. The demand for active SMS based services can only be satisfied when a solution that addresses end to end security issues of SMS technology is available, where primary security parameters of authentication, confidentiality, integrity and non-repudiation are satisfied. This is because wireless circuits are easier to tap than their wired

counterparts. Therefore, an end to end key based encryption and decryption technology for SMS plugs the gaps in transit security of SMS [1].

Encryption is the conversion of data into a form called Cipher text that cannot be easily understood by unauthorized people or the art of achieving security by encoding messages to make them non-readable while decryption is the process is the process of converting encrypted data back to its original form so it can be understood. In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key i.e. the stronger the cipher, the harder it is for unauthorized people to break it.

With the fast growth of wireless and mobile networks, many new applications have been designed and developed for user needs. With the use of wireless networks, information could be transmitted in a more convenient fashion. Wireless network include many popular techniques such as Wireless Local Area Networks (WLAN), World Wide Interoperability for Microwave Access (WMAX), Wireless Metropolitan Area Networks (WMAN), General Packet Radio Service (GPRS), Personal Area Network (PAN), 3G\4G, Bluetooth and Wireless Sensor Networks (WSN) [2]. The wireless connectivity is used in GSM technology, because of the mobility in its technology. With wireless networks, Radio Frequency (RF) and light signals is used to carry information invisibly through the air, compared to the wired network which uses cablings to transfer electrical currents that represents information.

According to Rana et al. (2011), information transmitted can be of different modulation schemes like Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK) and M-Quadrature Amplitude Modulation (M-QAM) technique which can be either single carrier systems; signal representing each bit of information uses all of the available spectrum or multi carrier system.

Single carrier system modulates information on to one carrier using frequency, phase or amplitude adjustment of the carrier. For digital signals, the information is in form of bits or collection of bits called symbols that are modulated on to the carrier (Litwin and Pugel, 2001). As higher bandwidths (data rates) are used, the duration of one bit or symbol of information becomes smaller. The system becomes more susceptible to loss of information from impulse noise, signal reflections and other impairments such as interference from other continuous signal sources. These impairments can impede the ability to recover information sent.

In order to solve this problem of single carrier modulation, its concept is extended by using multiple sub carriers within the same single channel (data transmission in parallel). This type of modulation system is called Multi Carrier Modulation System. In a single carrier system, a single fade or interferer can cause the entire link to fail, but in multicarrier system, only a small percentage a small percentage of the subcarriers will be affected. There are various multiple carrier systems such as Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) and Orthogonal Frequency Division Multiplexing (OFDM) (Chin-Feng, et al., 2009).

According to Rana et al. (2011), OFDM is used as a modulation scheme of wireless communications over others because of its high immunity for multipath fading and high spectra efficiency. It is a combination of schemes like modulation and multiplexing in which a high data stream is divided into different low data streams that are subsequently modulated into various carriers (orthogonal). Orthogonality of the sub carriers prevents inter-symbol interference (ISI). OFDM provides various advantages such as immunity for frequency selective fading and narrow band interference. Also, it provides improved spectral efficiency than Frequency Division Multiplexing (FDM) and it maintains orthogonal relationship between carriers (Parker and Tellambura, 2002).

METHODS AND MATERIALS

This paper employs single carrier and Orthogonal Frequency Division Multiplex as a modulation technique for the transmission of the encrypted data. The encryption method employed is Elliptic Curve Cryptography (ECC). The system simulation was carried out in the use of MATLAB programming.

System Model

Figure 1 shows the system model. From the diagram, the text message is first encrypted using the encryption algorithm of Elliptic Curve Cryptography to hide its content and make it impossible to read. The algorithm is as shown below:

Key Generation:

Generate Point of a curve:

Algorithm gen_ points (a, b, p)
{x=0 while(x<p) {find res= $(x^3 + ax + b)$}

Find different values of y^2whose mod with p is equal to res

Find square root of y;

Finally, all values of (x, y) gives different points on elliptic curve.}}

Generate Keys of a user:

Suppose there are two users A and B.

Following algorithm is used for generating keys.

Algorithm Generate_ keys( )
{ User A will select any random number kA as a private key.

Select generator point G(point having small x and y coordinates) from the curve points.

To generate public key kA_p multiply kA with G using point_ mult() algorithm.

Follow above steps to generate keys (kB, kB_p) for user B.}

Point Multiplication in ECC:

To multiply any number K with point p(x, y) we repetitively apply point doubling and addition operations.

Algorithm Point_ mult()

For doubling a point(2p) use following formulae:

$$s = [\frac{3x^2 + a}{2yp}] \text{mod} p$$

Then $2p$ has coordinates (XR, YR) given by:
$XR = (S^2 - 2x) \text{mod} p$
$YR = [S(x - XR) - y] \text{mod} p$

To determine 3P, we use P + 2P, treating 2P=Q. Here P has coordinates (x, y), Q (=2P) has coordinates (XQ, yQ).

$$s = \frac{\left[\frac{yQ - y}{XQ - x}\right]}{mod\ p}$$
$P + Q = -R$
$XR = (s^2 - x - XQ)\ mod\ p$
$YR = (s(x - XR) - y)\ mod\ p$

Encrypting Text:

Algorithm Encrypt_ Text()
{ Convert character in a text into its ASCII format, select any point pm from generated points of a elliptic curve multiply ASCII value with pm to get another point pm1 using Point_ mult algorithm Cipher text will be $\{kG, pm1 + k^* kA_p\}$}

The encrypted text is then converted into bits and then modulated using Orthogonal Frequency Division Multiplexing as the modulating technique. This involves passing them through serial to parallel converter to inverse fast Fourier transform. Guard interval is inserted between adjacent symbols to suppress Adjacent Symbol Interference (ASI). Cyclic prefix is then inserted in the guard interval to suppress Adjacent Channel Interference (ACI). The N bits data streams are then transmitted using N subcarriers which is mutually orthogonal. Multipath Rayleigh Fading and Additive White Gaussian Noise channel is added to the transmission medium to reduce the noise and improve the overall performance.

At the receiver, the text is demodulated by removing the guard interval inserted between the adjacent symbols and the cyclic prefix and pass through parallel to serial converter before it is finally decrypted to view its content. The decryption algorithm as shown below:

Decrypting Text:

Algorithm Decrypt_ text()
{ Take Cipher text will be $\{kG, pm1 + k^* kA_p\}$ calculate $pm = pm1 + k^* kA_p - kbkG$ }

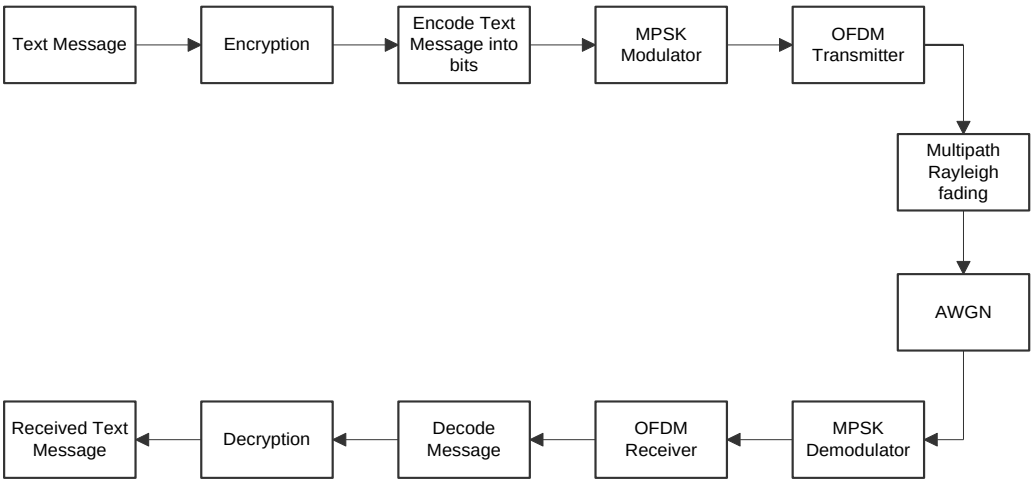

Figure 1: Encrypted and Decrypted Text Message with OFDM System Model.

Method of Simulation

We attempted to evaluate the performance of Orthogonal Frequency Division Multiplexing and single carrier, thereby some mathematical modeling and numerical simulations would be performed and graphs plotted. Collection of data would be done by generating sufficient numbers of independent random realizations of the system parameter.

The development of the data needed for the performance evaluations of the system are as stated:

i. Defining the mathematical equations that represents the systems parameters

ii. Determining the constraints and conditions needed for the simulation

iii. Writing the pseudo-code or algorithm

iv. Selecting and organizing the right data structure and functions

v. Writing the main code in steps

vi. Debugging the code for errors and making modifications in steps

vii. Testing the final program

Simulation Parameters

Table 1: Simulation Parameters for the Coding System.

Parameters	Values
Ifft/fft size	64
OFDM transmitted frame size	4
Number of bits per OFDM symbol	fft_ size+(fft_ size/4)
Samples per frame	10
Number of data subcarriers	16
SNR	0dB-20dB
Modulation order	4
Number of iteration	10

System Simulation

MATLAB was employed to perform the analysis of the system model and flow-chat. The MATLAB high performance language for technical computing integrates computation, visualization and programming in an easy-to-read environment where problems and solutions are expressed in familiar mathematical notation.

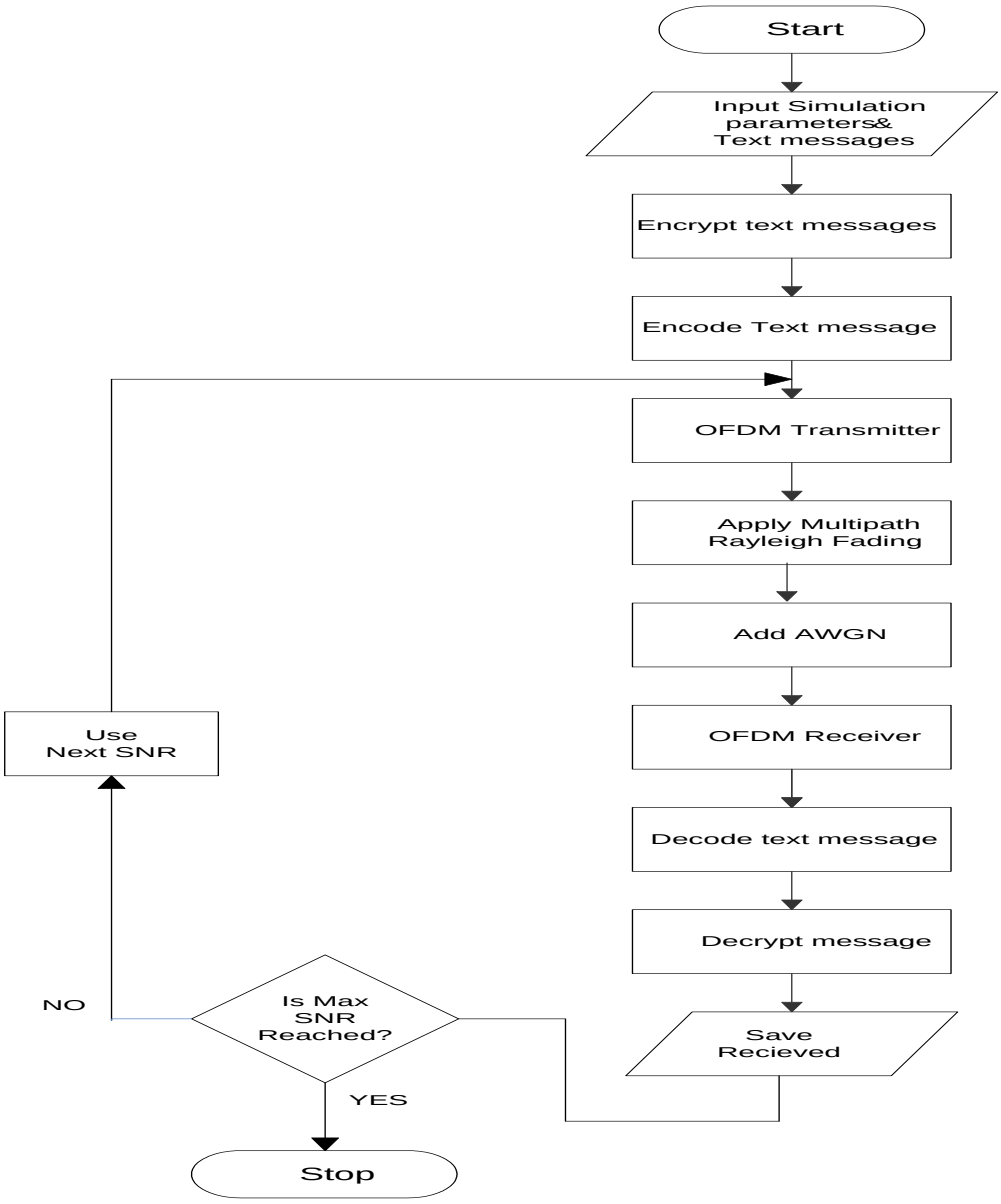

Figure 2: System Simulation Flow-Chart.

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. It allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non-interactive language such as C# or Fortran.

RESULTS AND DISCUSSION

Simulation Results

In this section, a simulation was performed to show the performance of multicarrier system over Single carrier channel using Elliptic Curve Cryptography cryptosystem to encrypt the text transmitted.

In this simulation, Orthogonal Frequency Division Multiplexing was employed as multicarrier while Quadrature Amplitude Modulation (4QAM) was employed as single carrier. The output file was observed at Signal to Noise Ratio (SNR) of 10, 15, and 20 dB. A comparison between Bit Error Rate (BER) of the encrypted text transmitted using OFDM and QAM was made. Also, graph of Bit Error Rate versus Signal to Noise Ratio for both OFDM and QAM was compared. The results were obtained by computer based simulations of the developed algorithms using MATLAB application package.

Input Text File:

This is a text file for testing OFDM for the protection of secret information. OFDM will be seen to be capable of mitigating multipath fading much better than single carrier.

Encrypted Text File:
dSEaEa=fE7=I[=aEo$_lG!I[S=4[I=cEIoIa=
c[=EoI[+EIo_lG!E77=a==oI=c47=I+EE$E
o$+• 7E4SJEo$+• cS==[SoaEo$7=c[[E=[.

Output Text File for SNR of 10 dB

Table 2 shows the output text file with the use of OFDM compared to that of 4QAM,it is observed that the number of errors in the 4QAM is 28 words, while that of OFDM is 7 words hence not many errors were discovered in signal transmission through OFDM.

Table 2: Output Text File for Signal to Noise Ratio of 10 dB.

4QAM output	OFDM Output
Thiu iw a ext$fiìu ¯ testéng SVFÍ or he(prwection$³f segr informšti¿p. OFLM i¬l be seåît e cšpale óf mitginml©pavèfadiîg mcj båter t¨¡¢î§le"carrie	This is a text file for testing OÆDM for the protection of secret information. OFDM wéll!âe se%n to be capable of mitigating multipath fading mu#è better uhan single carrier.
No of errors: 28 words	No of errors: 7 words

Output text file for SNR of 15 dB

Table 3 shows the output text file with the use of OFDM compared to that of 4QAM,it is observed that the number of errors in the 4QAM is 23 words, while that of OFDM is 6 words hence not many errors were discovered in signal transmission through OFDM.

Table 3: Output Text File for Signal to Noise Ratio of 15 dB.

4QAM output	OFDM Output
Vh³Pis@q |8t fl- fot(teutig FLM@ for tÚe protctior ofsecreDn¦ormaon2 WFD• {lbe seen to @re(cpabe qh m{tioatpç mulŸ©patp fa¤mn§ much better tèan wing¬e carrier	This is a text file for tåsting OFDM for the psotection oæ secret information. OFDM wéll be seen to bå capable of mitigating oultipath fading much better than single carrier.
No of errors: 23 words	No of errors: 6 words

Output text file for SNR of 20 dB

Table4 shows the output text file with the use of OFDM compared to that of 4QAM,it is observed that the number of errors in the 4QAM is 25 words, while that of OFDM is 3 words hence not many errors were discovered in signal transmission through OFDM.

Table 4: Output Text File for Signal to Noise Ratio of 20 dB.

4QAM output	OFDM Output
Vhiw$• s a text file`for testing ON• f□r tle prqvcxo@of seevmiformai¯n. • FÄU wll be see® to(jg(eepible"oæ íqtigativg muìtpat afîowch"bi´teò than £ingne £crrkm´.	This is a text file for tåstin' OM for the protection oæ secret information. OFDM will be seen to be capable of mitigating multipath fading much better than single carrier.
No of errors: 25 words	No of errors: 3 words

Bit Error Rate of the Encrypted Message for OFDM and Single Carrier

The relationship between the bit error rates of the encrypted file when transmitted through OFDM and single carrier system is shown in Table 5 for signal to noise ratio of 0 dB-20 dB. It can be seen that for each of the SNR the BER of OFDM is much less compared to that of the single carrier system. This is also represented in the graph shown in Figure 3.

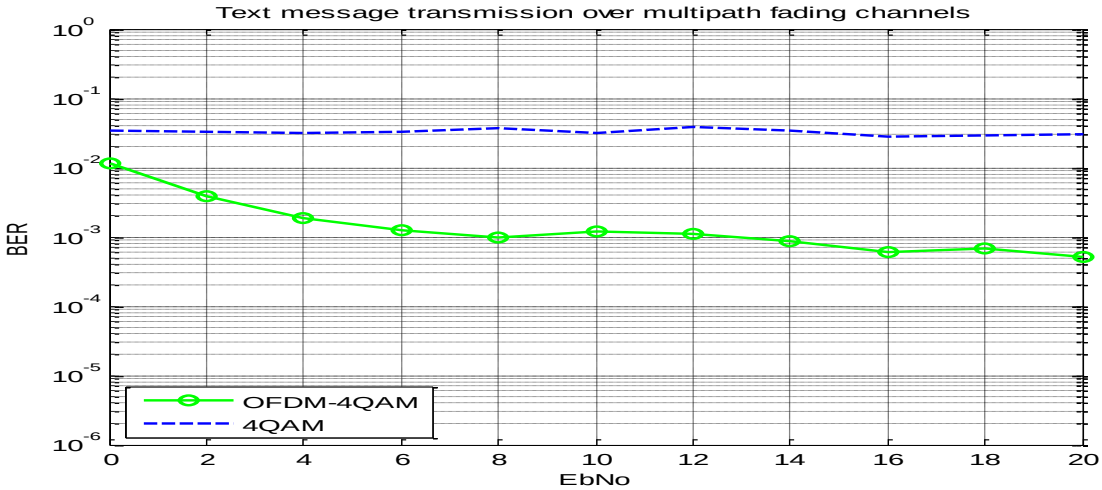

Figure 3: Graph of BER against SNR.

Table 5: Bit Error Rate of the Encrypted Message for OFDM and Single Carrier.

SNR [dB]	Average BER OFDM-4QAM	Average BER 4QAM
0	0.0116	0.0336
2	0.0039	0.0332
4	0.0019	0.0311
6	0.0012	0.0329
8	0.0010	0.0368
10	0.0012	0.0314
12	0.0011	0.0387
14	0.0009	0.0340
16	0.0006	0.0275
18	0.0007	0.0296
20	0.0005	0.0300

CONCLUSION

The performance of information transmitted using orthogonal Frequency Division Multiplexing and Quadrature Amplitude Modulation (4QAM) was obtained at different signal to noise ratio. The model for the system has been developed and simulated using MATLAB programming language. The results shows that the use of OFDM allows signal allows the sub-carrier spectra to overlap thus, increasing the spectral efficiency. As long as the orthogonality is maintained, it is possible to recover the individual subcarrier signal despite their overlapping spectrums. This gives better advantage compare to 4QAM.

The average Bit Error Rate for OFDM and 4QAM were obtained. It is shown from the results that as the signal to noise ratio increases the bit error rate for OFDM.

RECOMMENDATIONS

Based on the results obtained in this research work, the following are recommended:

- In this research work, correlated Rayleigh fading channel was used. Other fading channel such as Ricean, Nakagami, etc. can also be used. However, this is dependent on the conditions of propagation environment that is being considered.

- The performance metric used in the research work was Average BER. Other performance metrics like Outage Probability, Level Crossing Rate, Average Output SNR and Average Fade Duration may be considered.

REFERENCES

1. http://www.cscjournals.org/csc/manuscript/Journals/IJCSS?volume 3/Issue6/IJCSS-169.pdf. Accessed July 2012.

2. Shieh, S. 2011. “Wireless and Mobile Security - Principles and Practice”. National Chiao Tung University. 7-8.

3. Nasri, A. and R. Schober. 2009. “Adaptive Lp-Norm Metric for Secondary BICM-OFDM Systems”. In: *Proceedings of the Global Telecommunications Conference (GLOBECOM’09)*. 1–3.

4. Huemer, M., C. Hofbauer, and J. Huber. 2010. “The Potential of Unique Words in OFDM”. In: *Proceedings of the 15th International OFDM Workshop (InOWo’10)*. 142–144.

5. Meyer, R., W. Gerstacker, R. Schober, and J.B. Huber. 2006. “A Single Antenna Interference Cancellation Algorithm for Increased GSM Capacity”. *IEEE Trans. on Wireless Communications*. 5(7):1616–18.

SUGGESTED CITATION

Shoewu, O. and S.O. Olatinwo. 2013. “Securing Text Messages using Elliptic Curve Cryptography Orthogonal Frequency Division Multiplexing”. *Pacific Journal of Science and Technology*. 14(2):220-227.