DOI: 10.21917/ijct.2010.0018

DATA SECURITY IN LOCAL AREA NETWORK BASED ON FAST ENCRYPTION ALGORITHM

G. Ramesh[1] and R. Umarani[2]
[1]*Department of MCA, Thiruvalluvar College of Engineering and Technology, Tamil Nadu, India*
Email: mgrameshmca@yahoo.com
[2]*Department of Computer Science, Sri Sarada College for Women, Salem, Tamil Nadu, India*
Email: umainweb@gmail.com

Abstract
Hacking is one of the greatest problems in the wireless local area networks. Many algorithms have been used to prevent the outside attacks to eavesdrop or prevent the data to be transferred to the end-user safely and correctly. In this paper, a new symmetrical encryption algorithm is proposed that prevents the outside attacks. The new algorithm avoids key exchange between users and reduces the time taken for the encryption and decryption. It operates at high data rate in comparison with The Data Encryption Standard (DES), Triple DES (TDES), Advanced Encryption Standard (AES-256), and RC6 algorithms. The new algorithm is applied successfully on both text file and voice message.

Keywords:
Plaintext; Encryption, Decryption, S-Box, Key-updating, Outside attack

1. INTRODUCTION

Wireless Local Area Network (WLAN) is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. WLAN is found in the office buildings, and in many other public areas [1]. The security in WLAN is based on cryptography, the science and art of transforming messages to make them secure and immune to attacks by authenticating the sender to receiver within the WLAN.

The cryptography algorithms are divided into two groups: symmetric-encryption algorithms and asymmetric-encryption algorithms. There are a lot of symmetric-encryption algorithms used in WLAN, such as DES [2], TDES [3], AES [4], and RC6 [5]. In all these algorithms, both sender and receiver have used the same key for encryption and decryption processes respectively. The outside attackers use the fixed plaintext (such as: the company-title which is sent in the first packets of the message) and encrypted text to obtain the key used in the WLAN.

A new symmetrical encryption algorithm is proposed in this paper. The new algorithm avoids fixed-key exchange between sender and receiver with each authentication process in WLAN. The paper is organized as follows. Section 2 gives a short review of the symmetrical-encryption algorithms. Section 3 presents the proposed algorithm. Section 4 shows the results. Finally, Conclusion are presented in Section 5.

2. REVIEW ON THE SYMMETRICAL-ENCRYPTION ALGORITHMS

There is a lot of the symmetrical-encryption algorithms used in WLAN. DES [2], known as Data Encryption Algorithm (DEA) by the ANSI [6] and the DEA-1 by the ISO [6] remained a worldwide standard for very long time and was replaced by AES on October 2000. DES provides a basis for the comparison of new algorithms. It is a block cipher symmetric algorithm that uses the same key for both encryption and decryption. The basic building block (a substitution followed by a permutation) is called a round and is repeated for 16 times [2]. The substitutions process depends on the S-Box. S-Box is a matrix of 4 rows and 16 columns. DES has 8 different S-Boxes in each round. S-Box is used to map the input code to another code to the output. The input code specifies the output code position in this S-Box. The first and last bits specify the row number, and the rest bits specify the column number. The permutation tables are used for changing the bit-orders in the packet. For each DES round, a sub-key is derived from the original key using an algorithm called key schedule which is the same for encryption and decryption except for the minor difference in the order (reverse) of the sub-keys for decryption. In the encryption process, DES encrypts the data in 64-bit blocks using a 64-bit key (although its effective key length in reality is only 56-bit).

TDES is a block cipher formed from the DES cipher by using it three times. When it was found that a 56-bit key of DES is not enough to guard against brute force attacks, TDES was chosen as a simple way to enlarge the key space without the need to switch to a new algorithm. The simplest variant of TDES encryption operates as follows: DES(k3;DES-1(k2;DES(k1;M))), where M is the message block to be encrypted , k1, k2, and k3 are DES keys, and DES and DES-1 refer to the encryption and decryption modes respectively. While the TDES decryption operates as follows: DES-1(k1; DES (k2; DES-1(k3; C))), where C is the cipher text block.

AES algorithm is a symmetric block. It is used to encrypt and decrypt the plaintext and cipher text of 128-bits respectively by using cryptographic keys of 128-bits (AES-128), 192-bits (AES-192), or 256-bits (AES-256). The number of rounds in the encryption or decryption processes depends on the key size.

RC6 is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a nonnegative number of rounds r, and b denotes the length of the encryption key in bytes. Since the AES submission is targeted at w = 32 and r = 20, RC6 shall be used as shorthand to refer to such versions. When any other value of w or r is intended in the text, the parameter values are specified as RC6-w/r. Of particular relevance to the AES effort is the versions of RC6 with 16-, 24-, and 32-byte keys.

The complexity of the algorithm and the key size enhance the data security in WLAN, and they increase the difficulty to the attackers to discover the original message.

The new algorithm adds some difficulties to the attackers to discover the key. These difficulties are

- The longer key size, 512-bits, compared with DES, TDES, AES-256, and RC6.

- The key-updating with each packet.

The new symmetrical algorithm is applied on a text message and voice message. The comparison between the plain text and the decrypted text is easier than voice message. The two approaches used for measuring speech quality are the subjective and the objective approaches [8]. Subjective measures assess speech quality based on the perceptual ratings by a group of listeners [9]. Objective measures assess speech quality using the physical parameters [10]. The physical parameters are calculated from equations (1, 2, 3, and 4).

$$SNR = 10Log_{10}\frac{\sum_{i=1}^{N} x^2(i)}{\sum_{i=1}^{N}(x(i)-y(i))^2} \quad (1)$$

$$SNRseg = \frac{10}{M}\sum_{m=0}^{M-1} Log_{10}\sum_{i=Nm}^{Nm+N-1}\left(\frac{x^2(i)}{(x(i)-y(i))}\right)^2 \quad (2)$$

$$LLR = \left|Log\left(\frac{\overrightarrow{ax}\overrightarrow{Ry}\overrightarrow{ax}^T}{\overrightarrow{ay}\overrightarrow{Ry}\overrightarrow{ay}^T}\right)\right| \quad (3)$$

$$SD = \frac{1}{M}\sum_{m=0}^{M-1}\sum_{i=Nm}^{Nm+N-1}\left|Vx(i)-Vy(i)\right| \quad (4)$$

where: SNR is the signal-to-noise ratio [10], x(i) and y(i) are the original and decrypted speech respectively, N is the total number of samples in both encrypted and decrypted speech signals, M is the number of segments in the speech signals, LLR is the Likelihood Ratio [10], $\overrightarrow{ax}$ and $\overrightarrow{ay}$ are the Linear Predictive Coding (LPC) for the original and decrypted speech signals respectively, $\overrightarrow{Ry}$ is the autocorrelation matrix for the decrypted speech signal, SD [10] is Spectral Distortion, and Vx(i) and Vy(i) are the spectrum of the original and the decrypted speech signals respectively in dB for a certain segment in time domain.

Correlation [11] is a measure of the relationship between two variables. If the two variables are

- In perfect correlation, then the correlation coefficient (C.C) equals one.
- Highly dependent (identical), In this case the encrypted data is the same as the original data and the encryption process failed in hiding the details of the original data.
- If the C.C equals zero, then the original data and its encryption are totally different, i.e., the encrypted data has no features and highly independent on the original data.
- If C.C equals (-1), this means the encrypted data is the negative of the original data.

So, the success of the encryption process means smaller values of the C.C. The C.C is measured by the following equation:

$$C.C = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \quad (5)$$

where: $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, and x and y are values of the original and encrypted data.

3. THE NEW SYMMETRICAL ALGORITHM

The new algorithm uses a key size of 512-bits to encrypt a plaintext of 512-bits during the 16-rounds. In this Algorithm, a series of transformations have been used depending on S-BOX, different shift processes, XOR-Gate, and AND-Gate. The S-Box is used to map the input code to another code at the output. It is a matrix of 16 x 16 x 16. The S-Box consists of 16-slides, and each slide having 2-D of 16 x 16. The numbers from 0 to 255 are arranged in random positions in each slide. The S-Box is generated according to the flowchart of Fig.1. Each slide in the S-Box is described by the following equation:

$$S^i|_{X\times Y} = S|_{X\times Y\times i} \quad (6)$$

where i=1,2,…,16, and i is defined as the round number used in the key-generation, encryption, and the decryption processes. So, the first round operates on the first slide, $S^1|_{X\times Y} = S|_{X\times Y\times 1}$, and the second round operates on the second slide, $S^2|_{X\times Y} = S|_{X\times Y\times 2}$, and so on. For example, if the input 5A, in the hexadecimal form, is applied on the S-Box in round number 12, then $S^i|_{X\times Y} = S^{12}|_{X\times Y} = S|_{X\times Y\times 12}$. Let $S|_{X\times Y\times 12}$ have the contents of Table.1. The output code takes the row number 5 and column number A, or the output code is ED.

3.1. KEY GENERATION

The key generation generates 16-keys during 16-rounds. One key of them is used in one round of the encryption or decryption process. In the first time, the initial key is divided into four parts a, b, c, and d, 128-bits each. In each round of the key generation, there are series of the transformation used to generate the round-key. The round-key consists of four parts a*, b*, c*, and d*, and it is used in the same round –order to encrypt to the data, see Fig.2.

The procedures of the key-generation are as the following:

Step 1: Divide the initial key into four parts a, b, c, and d, 128-bits each.

For example, Let the initial key be,

BC107FE3F95071555D8DB639D0782BD62F5D35EBCE
A7627C7334D3A0341F0D61CEEDB8AB2A8DE37195F3
50F5B4DF06BC54DB4585EE4538A3318792CFCF4E112
F

Thus,

a= BC107FE3F95071555D8DB639D0782BD6
b= 2F5D35EBCEA7627C7334D3A0341F0D61
c= CEEDB8AB2A8DE37195F350F5B4DF06BC
d= 54DB4585EE4538A3318792CFCF4E112F

Step 2: $a^* = a \oplus b$

a*=934D4A0837F713292EB96599E46726B7

Step 3: Horizontal Left-Shift (Circular Shift)

The c-part is rearranged to a matrix form of 4*4, and each element of the matrix appears as two hexadecimal numbers. No shift in the first row. The second, third, and forth row is left-shifted by one, two, three elements (circular shift) respectively.

c=

CE	2A	95	B4
8D	F3	DF	ED
50	06	B8	E3
BC	AB	71	F5

→h=

CE	2A	95	B4
ED	8D	F3	DF
B8	E3	50	06
AB	71	F5	BC

Step 4: b*=m= $S^i|_{X\times Y}\ (h)$

h, is mapped into another code by applying S-Box on h to have m at the output. Each round uses one slide from S-Box according to the round number i, where i=1,2,…,16, as discussed later. Let $S|_{X\times Y\times 12}$ have contents of Table.1, thus b* is obtained as the following:

57	F2	E9	94
82	42	02	D1
85	C8	3C	6A
25	91	8A	15

b*=57828525F242C891E9023C8A94D16A15

Step 5: Vertical Upper-Shift (Circular Shift)

The d-part is rearranged to a matrix form of 4*4, and each element of the matrix appears as two hexadecimal numbers. No shift in the first column. The second, third, and forth column is upper-shifted by one, two, three elements (circular shift) respectively.

d=

54	EE	31	CF
DB	45	87	4E
45	38	92	11
85	A3	CF	2F

→w=

54	45	92	2F
DB	38	CF	CF
45	A3	31	4E
85	EE	87	11

Step 6: $c^* = m \oplus w$

c*=359C0A0B77A6B7F7BCD0D0DBB1E2404

Step 7: d*=a

d*=BC107FE3F95071555D8DB639D0782BD6

Thus, the round key consists of four parts a*, b*, c*, and d*, or

Ki=934D4A0837F713292EB96599E46726B757828525F242C891E9023C8A94D16A15359C0A0B77A6B7F7BCD0D0DBB1E2404BC107FE3F95071555D8DB639D0782BD6.

Step 8: Repeat the previous steps 15-times to obtain the 16-keys used to encrypt or decrypt the data.

3.2 ENCRYPTION

The Encryption process in the new algorithm is used to encrypt the plaintext of size of 512-bits by a key of size of 512-bits in each round during 16-rounds. Series of transformations are applied on the plaintext in each round as shown in Fig.3 to obtain a cipher text finally.

The encryption procedures are as the following:

Step 1: $Kp = Kv \oplus Ki$

where:

- Ki is the round-key that generated by the key-generation process.
- i is the round number, and i=1,2,…,16.
- Kv is the value of the feedback, as shown in the Fig.3, and its value in the first time is zeroes in all its 512-bits.

Step 2: $Kpi = S^i|_{X\times Y}\ (Kp)$

Kp is rearranged into a matrix format of 8×8, and each element has two hexadecimal numbers, as descript in the key-generation procedures. Then, Kp is applied on one slide of the S-Box according to the round number to produce Kpi. Kpi is a 512-bits key. It is used to update the total key used to encrypt the data with each packet depending on the feedback as shown in Fig.3. Kpi value is backed to AND with Rv to obtain Kv, see equation (7).

$$Kv = Kpi \bullet Rv \qquad (7)$$

where, Rv is a 512-bits key, and all bits are one. It is used to reset the system if the synchronization is lost during the encryption and decryption processes due to the total key-updating with each packet in each round.

Step 3: $Mn = S^i|_{X\times Y}\ (M)$

Step 4: $Ms = R(Mn)$

R(Mn) is a series of different shifting direction followed by XOR with Ki, see Fig.4. The steps of R(Mn) as the following:

First, Horizontal Left-Shift (circular shift), as descript in key-generation process. But, the matrix becomes 8 x 8 instead of 4 x 4.

Second, Vertical Upper-Shift (circular shift), as descript in key-generation process. But, the matrix becomes 8 x 8 instead of 4 x 4.

Third, the result of shift processes is XORed with ki.

Step 5: $Mp = Ms \oplus Kpi$

Step 6: $M^* = S^i|_{X\times Y}\ (Mp)$

Step 7: Repeat the previous steps 15-times to obtain the cipher text of size of 512-bits.

Table.1. The contents of S-Box at round 12, $S^{12}|_{X*Y}$

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*A*	*B*	*C*	*D*	*E*	*F*
0	6E	C7	0B	F8	FF	75	C8	B9	07	49	5C	72	67	FC	0F	C3
1	DF	5B	2D	45	E3	FD	58	D2	CC	FE	AE	6F	A8	B4	70	80
2	42	B0	13	BC	5D	7B	F6	5A	65	2F	F2	44	73	EB	D6	CF
3	D0	3F	2B	A7	04	EC	18	B2	39	EA	8B	76	EA	D8	DA	90
4	D3	8E	3B	D1	F4	F9	33	3A	C2	DC	9A	4D	9D	9C	DE	4B
5	85	35	42	B5	F1	23	D4	81	14	79	*ED*	32	A6	EF	63	7E
6	8D	0A	17	7C	6C	1D	4A	21	E6	E8	B6	2C	88	9E	E5	B1
7	E7	8A	36	69	22	A5	87	E1	26	0D	89	29	A9	55	1B	97
8	95	F3	74	C6	EE	D5	68	4F	40	CE	30	6B	43	82	78	37
9	B3	64	E4	F7	1E	E9	1F	D9	28	52	48	F5	19	A4	10	1C
A	5F	A3	A0	15	C9	92	56	C1	0E	AC	F0	91	A2	7F	60	84
B	CD	A1	77	CA	94	53	09	0C	3C	8F	3D	93	25	50	31	71
C	E2	DB	41	AB	AA	24	1A	00	54	08	66	E0	06	9B	57	AD
D	C5	16	FA	7A	3E	CB	BE	BB	C0	D7	8C	61	6D	4E	27	02
E	FB	11	9F	6A	51	B7	86	20	2A	47	BA	01	12	D1	4F	26
F	AC	E5	72	42	C0	15	43	D0	95	56	7B	00	01	76	EF	D1

3.3 DECRYPTION

The decryption of the new algorithm is the same as the encryption except:

- The direction of the encryption process is reversed, see Fig.5.
- The direction of R (Mn) is reversed, see Fig.6.
- The shift direction is reversed
  - Horizontal right-shift instead of left-shift
  - Vertical down-shift instead of upper-shift.

3.4 APPLICATIONS

Text and voice messages are used as applications to prove the success of the new encryption algorithm to encrypt and decrypt the different messages. The application is run inside the WLAN environment, see Fig.7. The voice message is also applied inside the Wired LAN environment using the point-to-point connection, see Fig.8. The proposed algorithm uses the following:

i. Software

- Microsoft Visual C# dot net program.
- MATLAB v7.

ii. Hardware

- Desktop: Intel® Pentium® 4 CPU 2.8GHz 1GB of RAM
- LAPTOP Acer: Intel® Atom™ CPU N270 @ 1.60GHz 1GB of RAM
- A 54M Wireless Access Point of TP-Link (TL-WA501G)
- A 54M Wireless USB Adapter of TP-Link (TL-WN322G).
- 1.5 m Ethernet cable.

Fig.9.a gives a plain text, and its decrypted version and the encrypted version are shown in Fig.9.b and 9.c. Fig.9.d shows the other encrypted version for the same plain text. The difference between the two encrypted texts is cleared in Fig.9.c and 9.d. which proves the principle of the key-updating.

The voice encryption and decryption processes are applied between two computers using wired or wireless connection. The voice transmission is applied using a microphone at one side, and a speaker at the other computer. The distance between them is about 1.5m to minimize the errors and the noise even if using the wired or wireless connection. In the wireless connection, the original voice and the decrypted voice are shown in Fig.10.a and their spectrograms are shown in Fig.10.b and the encrypted voice and its spectrogram are shown in Fig.10.c. In the wired connection, the original voice and the decrypted voice are shown in Fig.11.a and their spectrogram are shown in Fig.11.b and the encrypted voice and its spectrogram are shown in Fig.11.c.

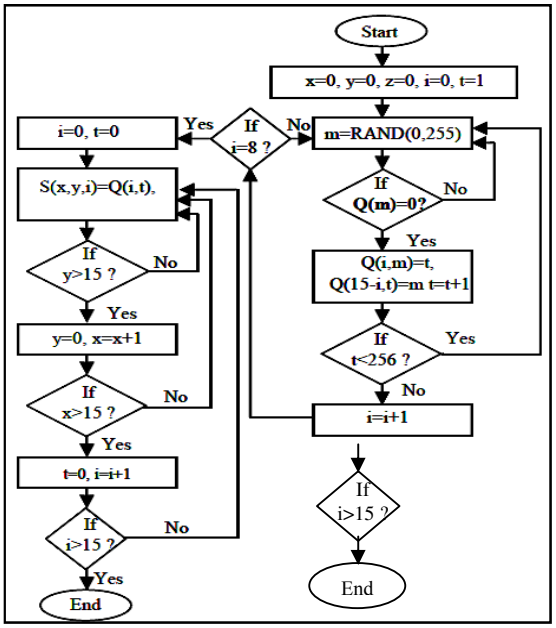

Fig.1. Flowchart of the S-Box Generation $S|_{X\,x\,Y\,x\,i}$ (16x16x16)

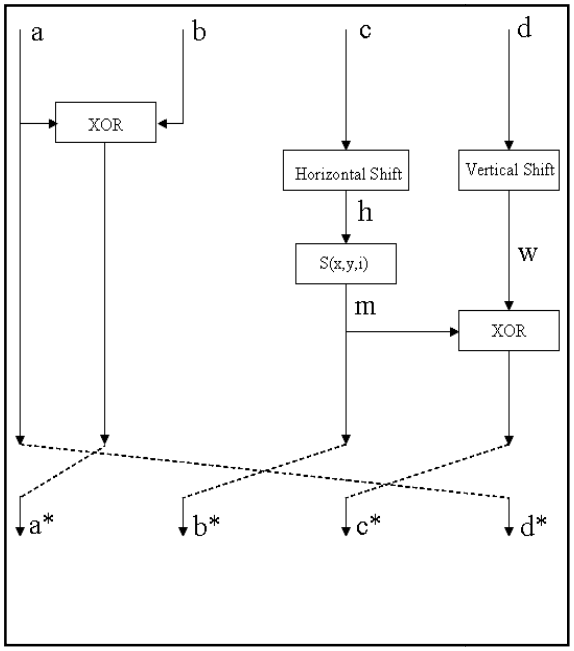

Fig.2. Key-Generation procedures in one round

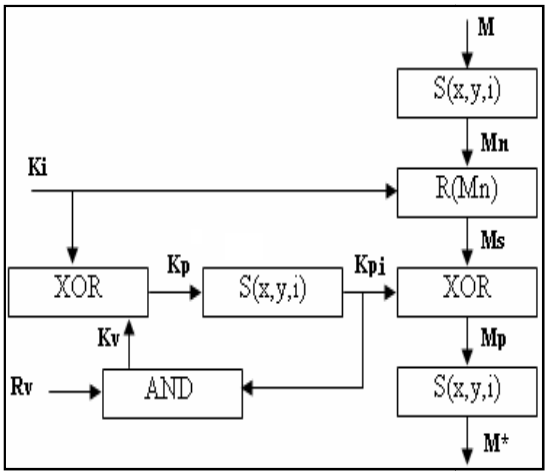

Fig.3. Encryption Process in each round

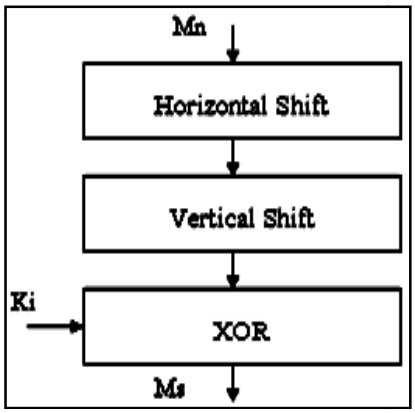

Fig.4. R(Mn) Steps

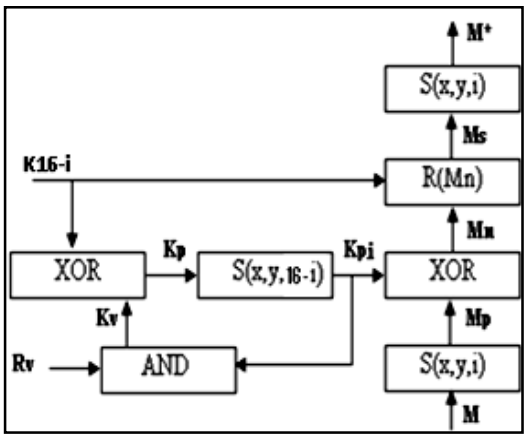

Fig.5. Decryption Process in each round

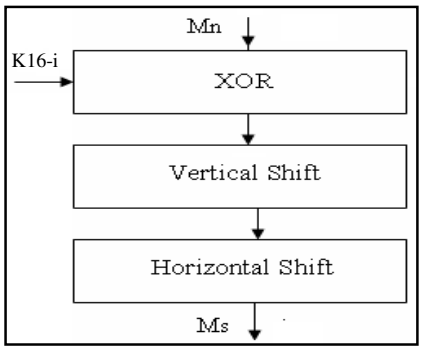

Fig.6. Inverse Process of R(Mn)

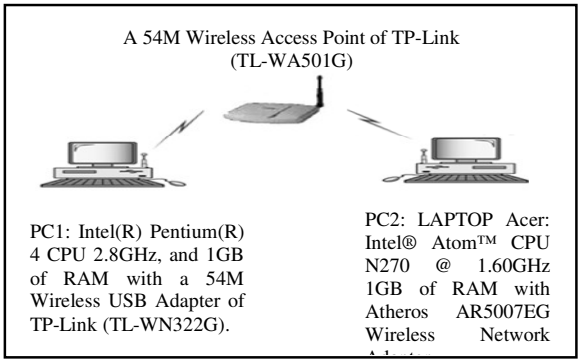

Fig.7. Wireless LAN (Infrastructure mode)

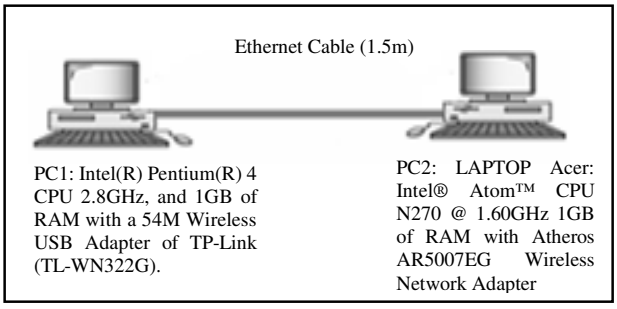

Fig.8. Wired LAN (Point-to-Point Connection)

Wireless local area network (WLAN) is one of the fastest-growing technologies. The demand for connecting devices without use of cables is increasing everywhere. WLAN can be found on collage campus, in office buildings, and in many public areas [1]. The security in WLAN is based on cryptography, the science and art of transforming messages to make them secure and immune to attack. Cryptography can be used to authenticate the sender and receiver of the message to each other within WLAN. The cryptography algorithms can be divided into two groups: symmetric-encryption algorithms and asymmetric-encryption algorithms.

Fig.9.a. Plain Text

Wireless local area network (WLAN) is one of the fastest-growing technologies. The demand for connecting devices without use of cables is increasing everywhere. WLAN can be found on collage campus, in office buildings, and in many public areas [1]. The security in WLAN is based on cryptography, the science and art of transforming messages to make them secure and immune to attack. Cryptography can be used to authenticate the sender and receiver of the message to each other within WLAN. The cryptography algorithms can be divided into two groups: symmetric-encryption algorithms and asymmetric-encryption algorithms.

Fig.9.b. Decrypted Text

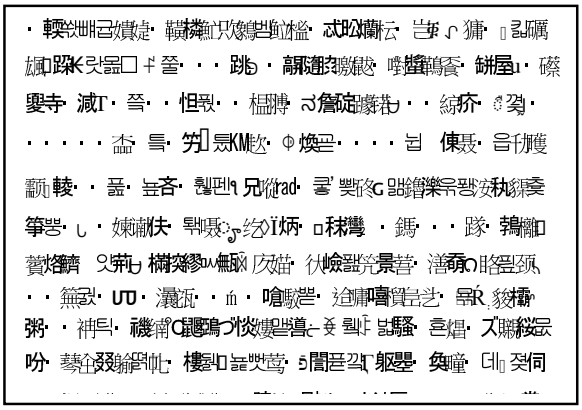

Fig.9.c. Cipher Text

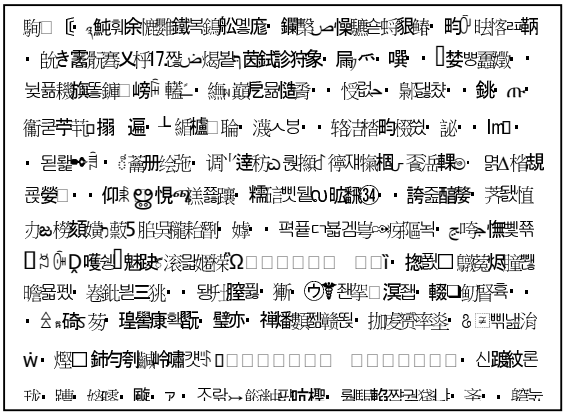

Fig.9.d. The other Cipher Text for the same Plain Text

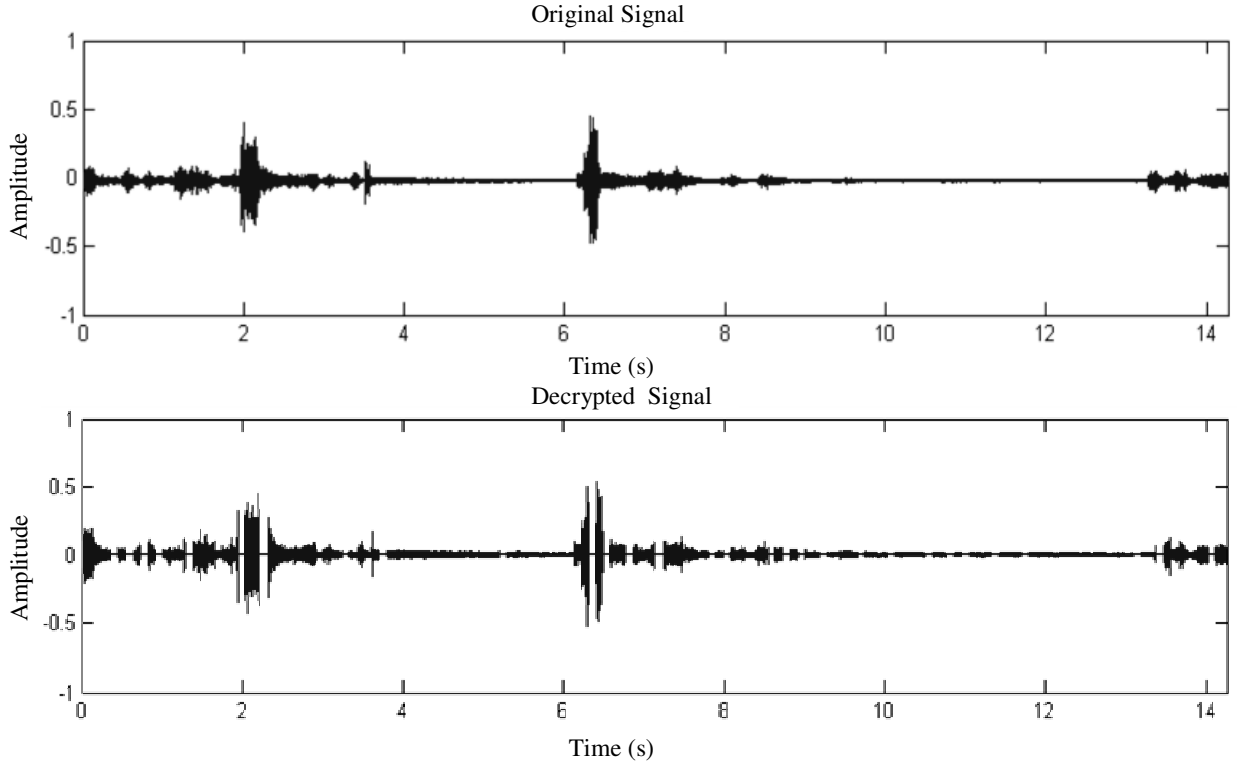

Fig.10.a. The original and decrypted voice (wireless connection)

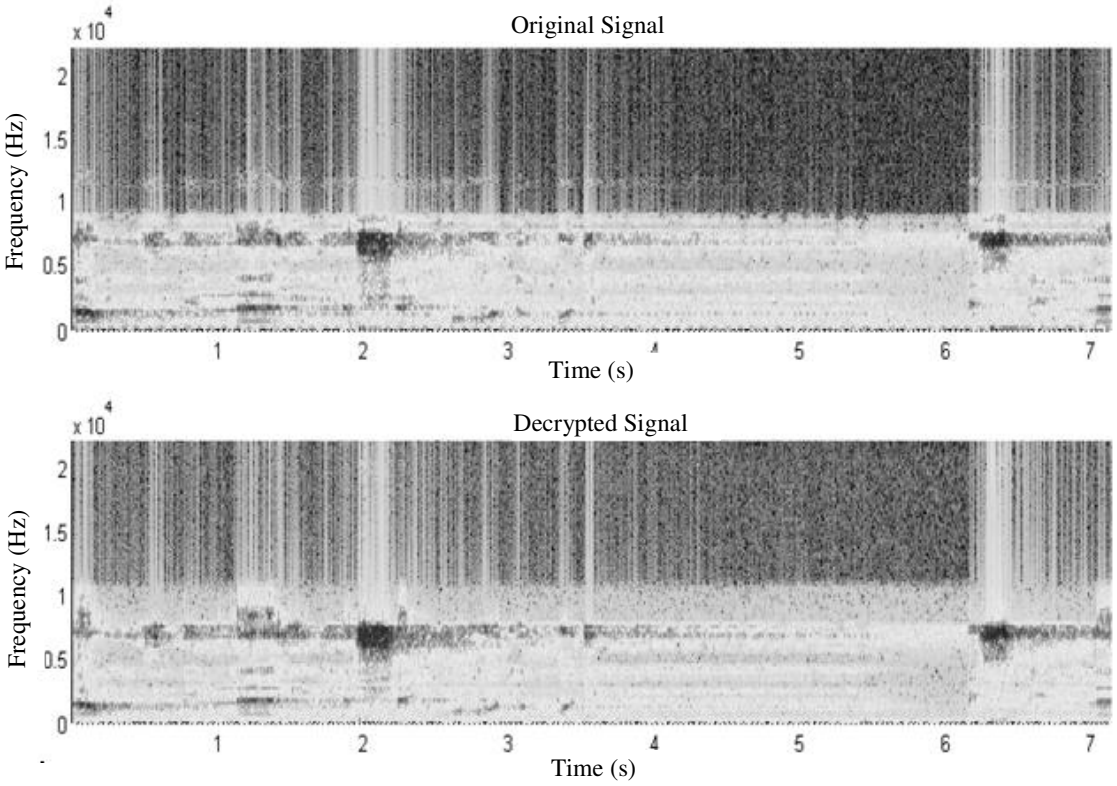

Fig.10.b. The spectrogram of the original and decrypted voice

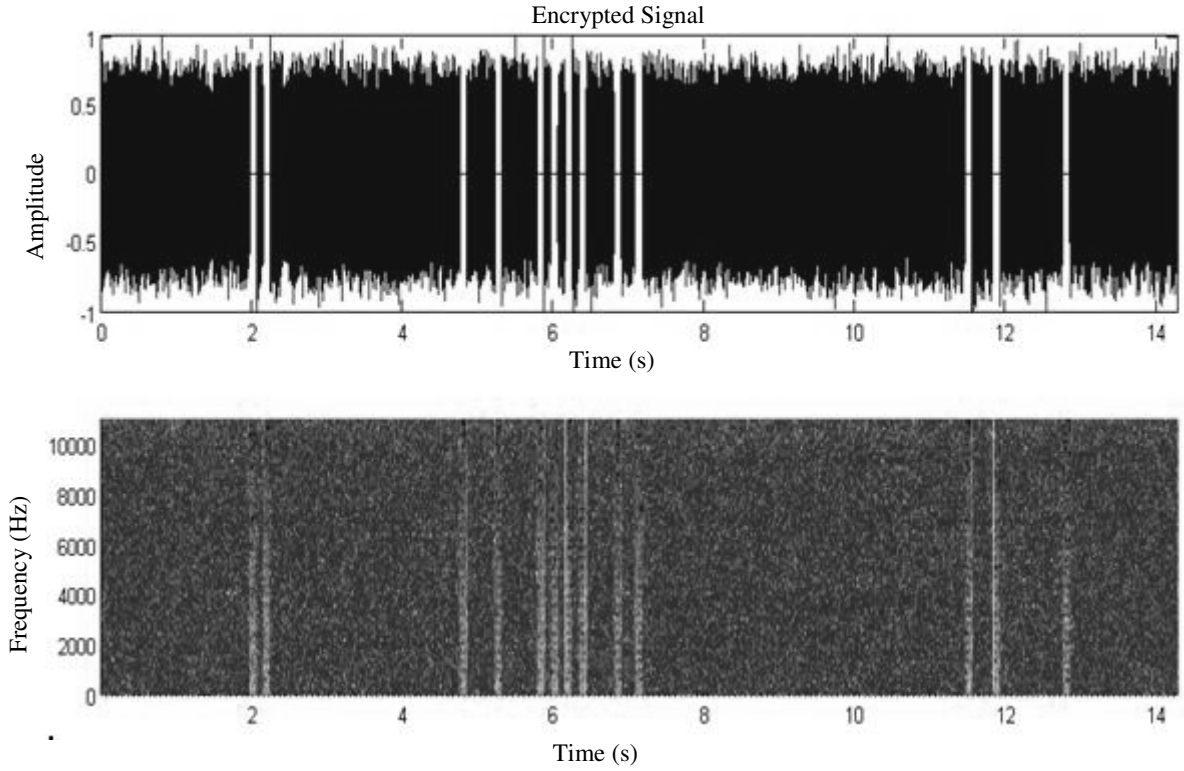

Fig.10.c. The encrypted voice and its spectrogram (wireless connection)

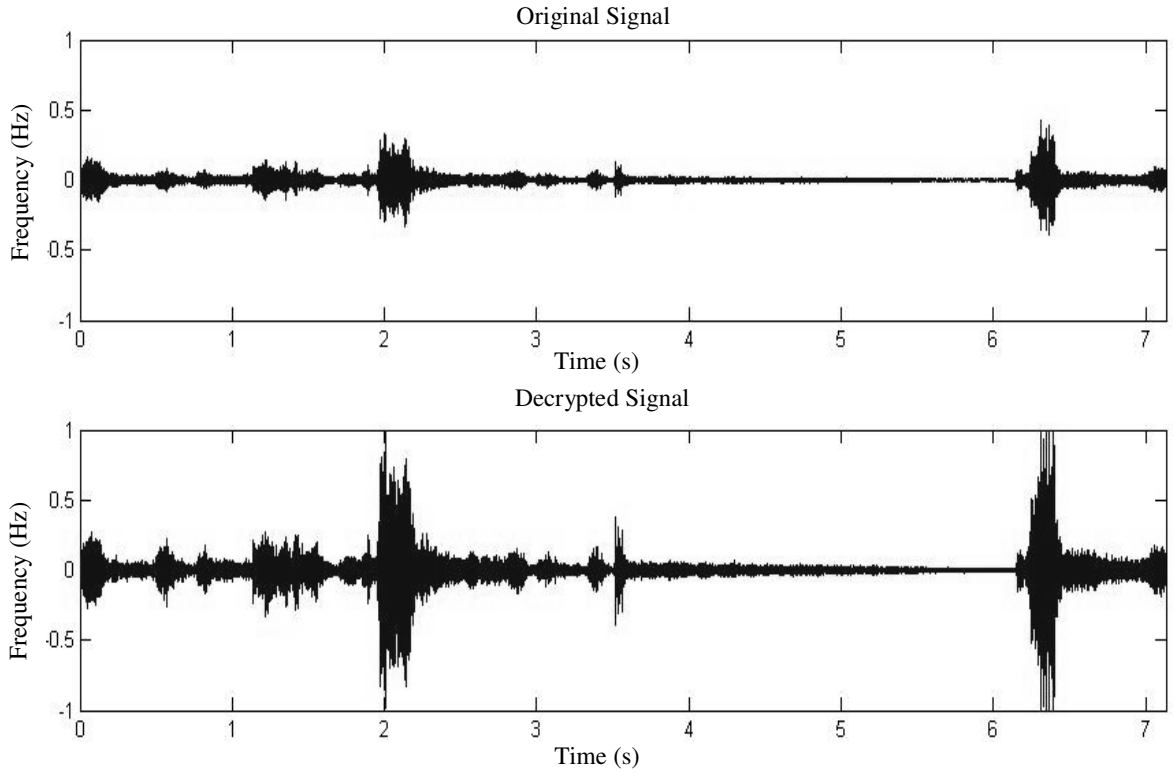

Fig.11.a. The original and decrypted voice (wired connection)

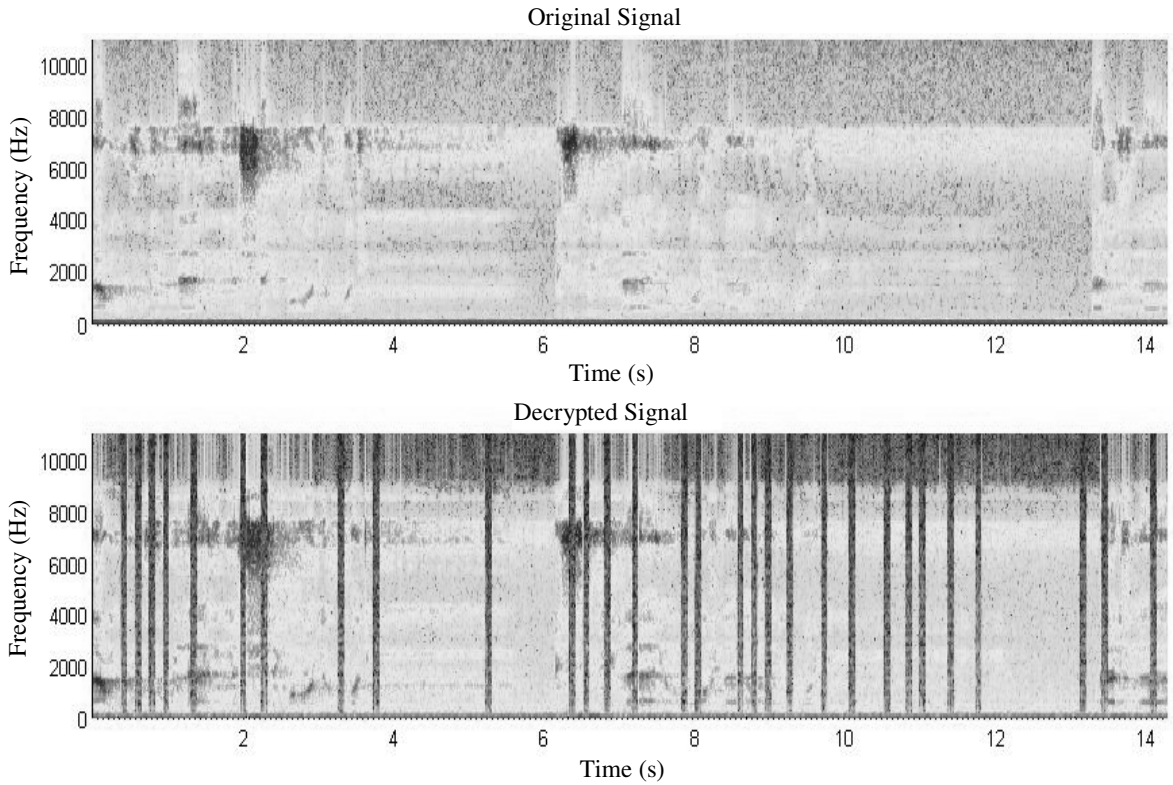

Fig.11.b. The spectrogram of the original and decrypted voice (wired connection)

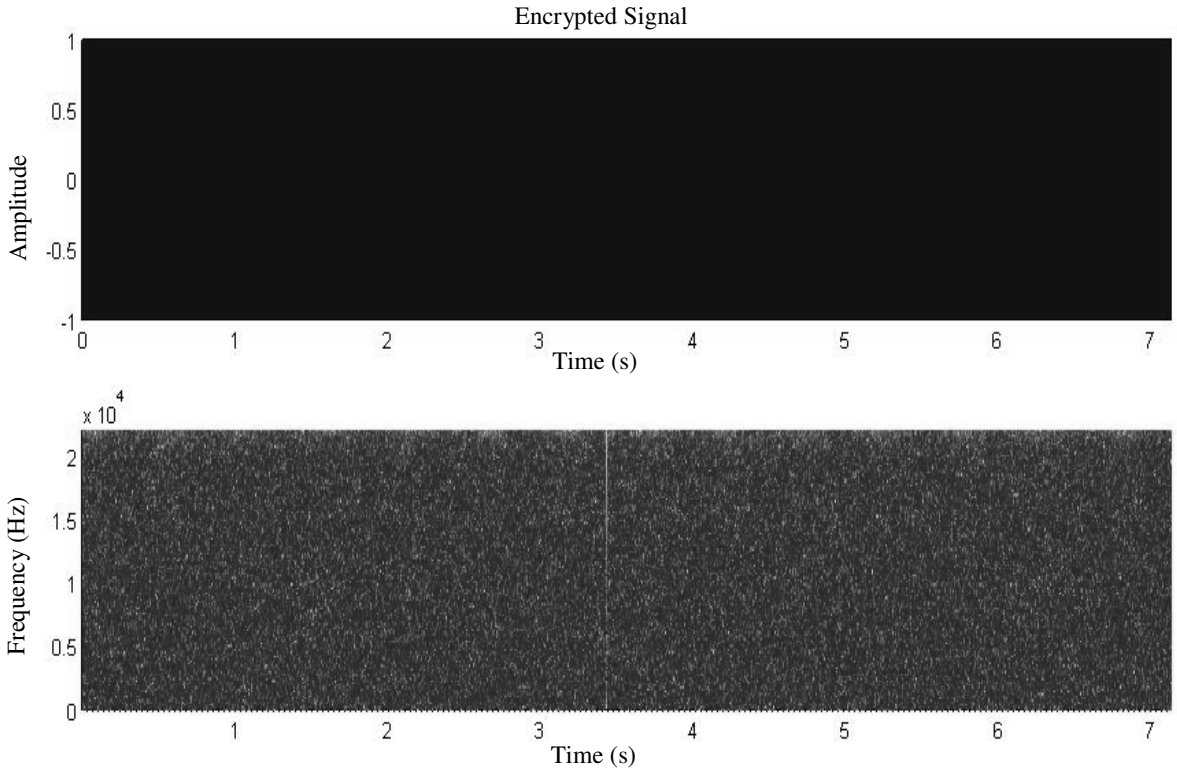

Fig.11.c. The encrypted voice and its spectrogram (wired connection)

4. THE RESULTS

The data rate of the new algorithm is compared with DES, TDES, AES-256, and RC6 using different messages with different sizes, from 50KB until 3MB, see Fig.12. The delay time taken for encryption process of the different algorithms is measured inside their programs by using the DESKTOP device for the comparison purpose, see Fig.12. The Average data rate of the different algorithms is calculated from equation (8), and the measured values of the average data rate for different algorithms are shown in Table.2.

$$Bravg = \frac{1}{Nb}\sum_{i=1}^{Nb}\frac{Mi}{ti} \text{ (KB/s)} \qquad (8)$$

where:

- Bravg is the average data rate (KB/s)
- Nb is Number of messages with different sizes, from 50KB until 3MB
- M_i is the message size (KB)
- t_i is the time taken to encrypt the message M_i

Table.2 shows that, the new algorithm has higher average data rate than DES, TDES, and AES-256, but the RC6 has the higher value than the proposed algorithm. In addition, the new algorithm adds some difficulties to the attackers to discover the key. These difficulties are

- The longer key size, 512-bits, compared with DES, TDES, AES-256, and RC6
- The key-updating with each packet

Table.2. Average data rates comparison

	AES-256	TDES	***New***	**RC6**	DES
Average Data Rate (kb/s)	120.73	31.32	***146.73***	**271.56**	93.98

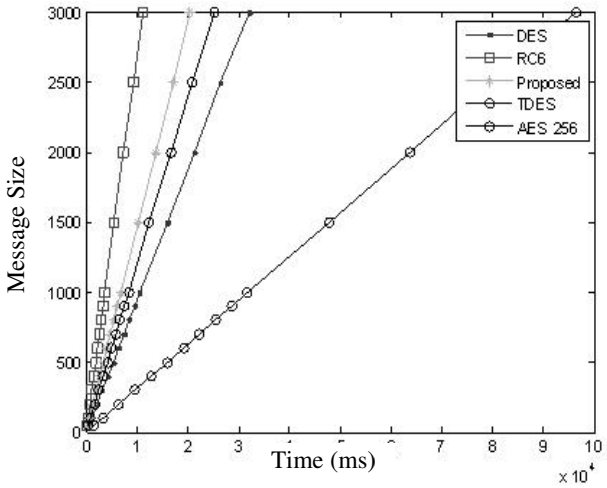

Fig.12. The Encryption delay time for the proposed, DES, TDES, AES-256, and RC6 algorithms

Table.3 shows the calculated correlation factor of the speech signal between the plain wave and the encrypted wave in the case of wired and wireless connection.

Table.3. The Correlation factor in the case of the wired and wireless connection (Speech Signal)

	Plain and Encrypted Waves
Wired Connection	0.0013
Wireless Connection	-0.0021

The success of the encryption process means smaller values of the correlation coefficient, and if the correlation coefficient equals zero, then the original data and its encryption are totally different, i.e., the encrypted data has no features and highly independent on the original data. The parameters of equations (1, 2, 3, and 4) are measured for new algorithm environment in the case of wireless connection and wired connection, see Table.4.

Thus, the system is more secure because of the following reasons,

1. The new algorithm adds some difficulties to the attackers to discover the key. These difficulties are

- The longer key size, 512-bits, compared with DES, TDES, AES-256, and RC6
- The key-updating with each packet

2. The outside attacks cannot obtain the key or any information about the algorithm even if he had the plaintext, the company title, S-Box, and the encrypted message because they lose the synchronization or the initial key of each round where they are independent.

In addition, the proposed algorithm has the following advantages:

- The delay time taken for the encryption and the decryption processes by the proposed algorithm is less than the time taken DES, TDES, and AES-256 algorithms
- Higher data rate than DES, 3DES, AES, and AES-256 algorithms
- The updating of the round-key with each packet
- The updating of the round-key prevents any change in the transmitted message because it is known to the sender and the receiver because of losing the synchronization between the encryption and the decryption. So it prevents the attackers such as, man-in-the middle attacks to analysis the traffic or to decrypt the encrypted message.

Table.4. The measured parameters in the case of wireless connection and wired connection

	Wireless Connection	Wired Connection
SNR	-3.5779	-3.5093
SNRseg	-3.6484	-3.5134
LLR	0.555	0.4667
SD	14.5672	14.1494

5. CONCLUSION

The key-updating is a new approach to increase the difficulty to discover the key. The text and speech signals are used to prove the success of the proposed algorithm. The proposed algorithm has higher data rate than DES, TDES, and AES-256 algorithms. The voice encryption and decryption is applied using wired and wireless connection. It is efficient and useable for the security in the WLAN systems.

REFERENCES

[1] William Stallings, "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] Paul. A.J, Varghese Paul, P. Mythili, "A FAST AND SECURE ENCRYPTION ALGORITHM FOR MESSAGE COMMUNICATION", IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007), Dr. M.G.R. University, Chennai, Tamil Nadu, India. December, 20-22, 2007. pp. 629-634.

[3] Jose J. Amador, Robert W.Green, "Symmetric-Key Block Ciphers for Image and Text Cryptography", International Journal of Imaging System Technology, 2005.

[4] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[5] Nawal A. El-Fishawy, Talat E. El-Danaf, and Osama M. Abou Zaid, "A MODIFICATION OF RC6 BLOCK CIPHER ALGORITHM FOR DATA SECURITY (MRC6)", International Journal of Network Security (IJNS), 2007.

[6] ANSI3.106, "American National Standard for Information Systems—Data Encryption Algorithm—Modes of Operation," American National Standards Institute, 1983.

[7] Bruce Schneider, John Wiley & Sons, Inc., "Applied Cryptography, Second Edition," New York, NYaq 1996.

[8] D. O'Shaughnessy, "Speech Communication: human and machine," New York NY. The Institute of Electrical and Electronics Engineers, Inc., 2000.

[9] ITU, "Methods for Subjective Determination of Transmission Quality," ITU-T. pp. 800. 1996.

[10] T. Falk and W.-Y. Chan,"Single Ended Method for Objective Speech Quality Assessment in Narrowband Telephony Applications," ITU-T, pp. 563, 2004.

[11] Nawal El-Fishawy and Osama M. Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security (IJNS), 2007.