International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Enhanced Security Encryption Scheme for Lower Bit Error Rates for Use in Noisy Transmission Media

K. Charan Kumar
M. Tech. Student
CVSR College of Engineering
charan467@gmail.com

P. Ramakrishna
Associate Professor, ECE Department
CVSR College of Engineering
prk.cvsr@gmail.com

Abstract **- In this paper, we propose a modification to the existing Data Encryption Standard (DES) to make it secure and prone to the bit errors caused by the transmission channel. Channels are an open medium to intruders and their attacks; encryption is a vital process to assure security over these channels. However, using well-known encryption algorithms to encrypt data in communication will result in a catastrophic error due to the avalanche effect, which is implemented in these algorithms to assure security. Although this effect is desirable to assure security, these algorithms do not take into account the bit error characteristics of the wireless channel. So the need for a new secure encryption algorithm that takes into account the bit error characteristics of channels becomes necessary. The goal is to compare the bit error rate (BER) of different algorithms. Finally, we observe that using the modified algorithm in transmission channels, improves the bit error rate (BER) performance as well as security compared to DES.**

Keywords **- Avalanche Effect, Bit Error Rate, Cryptography, Encryption, Security.**

I. INTRODUCTION

Encryption is an essential process to assure confidentiality over transmission channels, because channels are an open medium to intruders in which they can intercept and alter the contents of any transmitted information. Well known standardized encryption algorithms such as DES and AES were designed to achieve security against intruders. Hence, DES and AES were designed in such a way to satisfy the avalanche effect criteria. The avalanche effect of an algorithm requires that changing a single bit of the key or the plaintext (i.e., the data before encryption) to change half the bits of the ciphertext (i.e., the data after encryption) on average [1]. This effect also requires that a single bit change of the ciphertext or the key will result in some significant and random looking changes at the plaintext. On average half the bits will be in error. Any algorithm that has this property does not exhibit any statistical correlation between input and output that an adversary might use in attack, thus the algorithm will multiply bit errors, that is if there is one error at the received ciphertext, there will be many errors at the decrypted plaintext. However, this effect becomes catastrophic in wireless channels, because wireless channels tend to add noise to the signal. So the wrong reception of a single bit in a certain block at the receiver will result in half the bits of the decrypted block on average to be in error. So it is clearly noticed that an algorithm that satisfies the avalanche effect is very sensitive to bit errors. If one bit of the ciphertext is received in error, then each bit of the plaintext will have 0.5 probability of error. This means that there is a tradeoff between the security and the bit error rate. So encrypting the information with traditional encryption approaches will significantly degrade the performance of wireless networks, especially when the SNR is too bad. Some researchers had noticed this problem and tried to solve it in two main approaches. In [1] the authors introduced what is called opportunistic encryption, in which they encrypt the data with longer keys which implies more security whenever the SNR of the channel is higher so that the probability of error at the received ciphertext will be lower than for lower SNR values and hence higher security can be used. They also used forward error correction (FEC) codes to protect encrypted packets from bit errors. They also assumed perfect knowledge about the channel in order to use opportunistic encryption. Using their new encryption technique, the authors showed that the throughput of the system was more utilized than for that of using fixed encryption of AES. In [2] the author introduced a new mode of operation in which the data is transmitted, the design goal of the author work was to design a mode of operation for encryption algorithms that has substantially less error propagation than other modes. The Author called the new mode ECFB; the new mode has a lower bit error rate than other modes. However, the BER was not significantly improved. Another way of thinking about a solution for this problem was to design new algorithms which are specific for wireless applications. Some encryption algorithms such as MISTY1, KASUMI and KASUMI-R were specifically designed for wireless applications such as the Universal Mobile Telecommunications System (UMTS) [3]. However, these algorithms were only designed with security in mind. In [4], the authors show that these algorithms satisfy the avalanche effect as in other traditional encryption algorithms. These algorithms are also shown to be vulnerable to different types of attacks as shown in [5]. Now it becomes clear that a new algorithm which takes into consideration the error nature of wireless channels is critically needed. In this paper, we propose a new algorithm to be used in wireless communication.

The proposed algorithm is a modification to DES encryption algorithm by which we are achieving a very high security compared to that of DES. The proposed algorithm is modified to have much lower bit error rates than that of DES. We studied the effect of each S-Box in DES on the BER. We redesigned the S-Boxes so that the error is reduced. We also introduced a new round to the sixteen rounds of DES, to increase the security of the

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

algorithm to an unbreakable level and to reduce the bit error rate significantly. In this paper, the new algorithm is still a 64-bit input algorithm as DES, but with 128-bit ciphertext and 136-bit key. The rest of the paper is organized as follows: Section II describes the architecture of the proposed algorithm (M-DES) and Triple M-DES. In Section III the performance of the proposed algorithm is evaluated. Simulation results are presented in Section IV. Finally, some conclusions are drawn in Section V.

II. Proposed Modified Algorithm Architecture

In this paper, we introduce two main modifications to the standard DES in order to improve the BER performance of the received data, and to enhance its security. Fig. 1 shows the general architecture for the proposed modified- DES (M-DES). As shown in the figure, the first sixteen rounds in the proposed algorithm have the same structure as the standard DES rounds [6], except that in the MDES we propose using different S-Box mapping tables than that of standard DES. All of the first four S-boxes in the M-DES will have the same mapping table as the mapping table in the first S-Box of original standard DES, while the rest of the S-Boxes (number five through eight) will have the same mapping table as the mapping table of the second S-Box of standard DES. The S-Box is a mapping table that maps a 4-bit input to 6-bit output. In standard DES, each of the eight S-Boxes has a distinct mapping table. The S-Boxes were initially designed in such a way to meet the avalanche effect criteria [7].

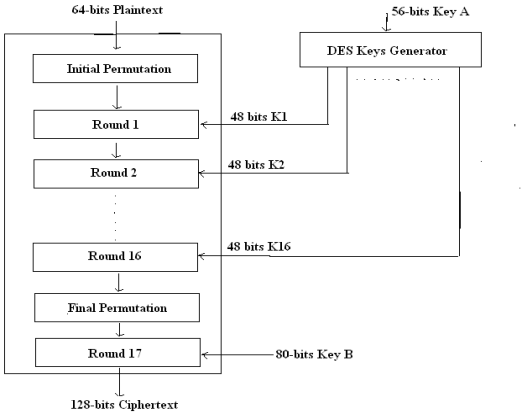

Fig.1. M-DES General Architecture with the addition of Round17, which has two inputs and one output. Inputs are 64-bit output of final permutation and 80-bit key, the output is a 128-bit ciphertext

In the MDES, we are still having eight S-Boxes in each round, but with only two distinct mapping tables rather than the eight distinct mapping tables in standard DES. This in fact will improve the BER performance, however, at the price of reducing security. In our proposed algorithm, we will also propose another modification not only to compensate for this reduction in security but also to improve security as compared to standard DES. This will be described in the rest of this section.

Our motive for the second modification is in fact coming from the work in [8], where the authors showed that DES can be cracked using the differential cryptanalysis attack if the attacker has 2^{47} pairs of plaintext and ciphertext. The authors also show that each distinct S-Box mapping table requires around $2^{6.5}$ pairs to be cracked. Therefore, in our proposed M-DES, while using only two distinct mapping tables (rather than the eight distinct mapping tables in the standard DES), the number of pairs needed to crack the algorithm reduces to 2^{13} pairs. To overcome with this security reduction, we introduce round 17 in the M-DES as shown in Fig. 1. By introducing round 17, the algorithm becomes infact secure to both brute force and differential cryptanalysis attacks as will show later in this section. Round 17 has two inputs and one output, the two inputs are the 64-bit output of the final permutation and an 80-bit key, the output is the 128-bit cipher. The 80-bit key is used to map the 64-bit input of Round 17 to a 128-bit output. This mapping procedure is shown in Fig. 2 where the 64- bit input of round 17 is divided into sixteen sub-frames of four bits each. While the output 128-bit consists of 32 sub-frames of four bits each. Each five bits of the 80-bit key is used to map one of the 4-bit input sub-frames to one 4-bit output sub-frame. So the input sub-frames will be scrambled in 16 out of the 32 output sub-frames. The remaining 16 sub-frames of the output are randomly filled with zeros and ones.

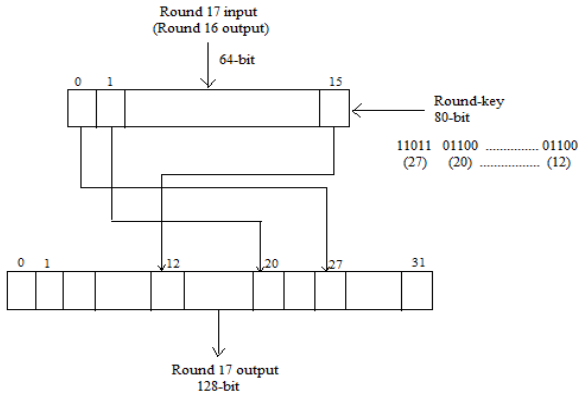

Fig.2. Round 17 Design, mapping the 16 input sub-frames into the 32 output sub-frames using the 80-bit key

For example, if the first 5 bits of the key are 00101. This means that the first 4-bit sub-frame of the input will be mapped to the fifth 4-bit sub-frame of the output. At the receiver side, the receiver will have the 80-bit key, so he will be able to recover the useful 64-bit ciphertext out of the total 128-bit received ciphertext.

So the proposed algorithm has a plaintext of 64 bits, a ciphertext of 128 bits and a key of 136 bits. So round 17 will scramble the useful 64-bit encrypted frame inside a 128-bit frame. In order for an intruder to crack the algorithm, 2^{13} useful pairs of plaintext and useful ciphertext are needed. Assuming that an intruder has the ability to encrypt 2^{13} plaintexts and get their corresponding 2^{13} ciphertexts. The intruder can't directly use those pairs to crack the algorithm, because he will need to guess the useful 64-bit out of each 128-bit cipher he obtains. So the intruder will need to try all the possible 64 bits

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

combinations out of the 128 bits for each of the 2^{13} ciphers. The probability of getting one correct pair (64-bit input and its corresponding 64-bit output out of the 128-bit cipher) is given by

$$P_1 = \frac{1}{\binom{32}{16}} = 1.6637 \times 10 - 9 \quad (1)$$

So the probability of getting 2^{13} correct pairs is

$$P_2 = \left(1.6637 \times 10^{-9}\right) 2^{13} \approx \quad (2)$$

This probability is very small, so the algorithm is considered immune to differential cryptanalysis. Round 17 also solves a very critical security problem in DES, by the new 80-bit key of round 17, M-DES will have a total of 136 bits as its key. Using the Brute force attack(testing all possible 256 keys), DES was shown to be cracked in less than 20 hours [6]. However, having a key size of 136 bits in M-DES, this problem was resolved, because it is impossible for an intruder to try all possible 2^{136} in a feasible amount of time. Assuming that the key of DES can be cracked in only one second, it will need more than 136 trillion years to crack M-DES. Therefore, M-DES is secure against brute force attack.

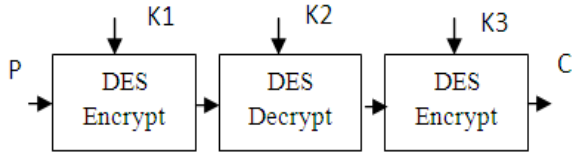

Fig.3. Triple DES architecture

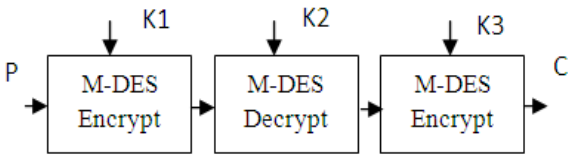

Fig.4. Triple M-DES architecture

Similarly we can implement this concept for Triple DES (Fig.3) also. Fig.4 shows architecture for Triple M-DES. We can observe an improvement in the BER performance along with much improved security in triple M-DES.

III. Performance Evaluation

A. System Model

In this paper, we simulated the performance of the proposed algorithm in ModelSim using verilog. A large sequence of bits was generated randomly at the sender. The generated bits were then divided into 64-bit blocks; each block was then encrypted to a 128-bit block using M-DES. The encrypted blocks were then assumed to be transmitted over the wireless channel. The encrypted blocks received in error are then decrypted block by block. Then, the resulted sequence of bits at the receiver after decryption is compared with the sequence of bits at the sender before encryption, and the error is calculated. The same procedure is done using DES, Triple DES and Triple M-DES.

B. BER Analysis

Using simulation we show that the performance of M-DES in terms of BER is much better than DES. Initially, we studied the BER of DES, assuming one bit error only. We studied the effect of the error analytically up to the end of round three. Then it became harder to complete the sixteen rounds analytically, so we used simulations to evaluate the BER of DES, and we found that on average there was 32 bits in error out of the 64 bits. Simulations also show that in M-DES, having one or more errors at the received ciphertext block will not result in half the decrypted bits to be in error, while for DES if any bit is received in error, this will result in half the bits to be in error.

C. Security

We showed in details in the previous section how the algorithm is considered secure against brute force and differential cryptanalysis attacks. The addition of the new 80-bit key, make it impossible to crack the algorithm using brute force attack. While the addition of the new round reduces the probability of cracking the algorithm using differential cryptanalysis to almost zero.

D. Key Management

An efficient way to share the new key is to add the new 80-bit key to the old 56-bit key and deal with them as one key at the transmitter. Both the sender and the receiver will need to divide it into two keys when encryption or decryption is done.

E. Complexity

The proposed algorithm is less complex than DES in terms of the number of distinct S-Box mapping tables. However, the number of rounds and the key size of M-DES is more than DES, which might increase the complexity compared to DES.

IV. Simulation Results

This section provides the simulation results of the BER obtained for M-DES and Triple M-DES compared to DES. Here encrypted text is the output of encryption algorithm and encipher text is the input to the decryption algorithm after transmission. Here we have considered a random error bit is the changed bit while transmission. Here i and j are the iteration variables used for the 64 bits and 100 iterations respectively. The average ber is calculated which is observed as 31.62 for an standard DES algorithm, as shown below(Fig.5):

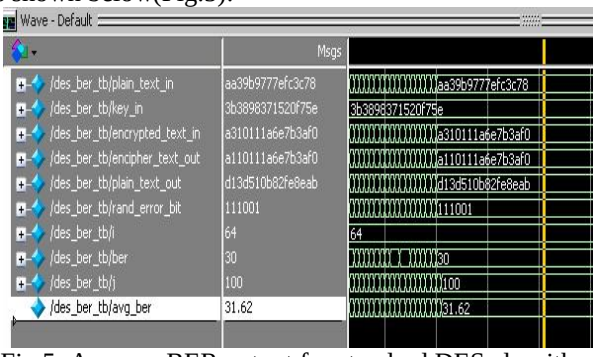

Fig.5. Average BER output for standard DES algorithm

Similarly, for M-DES algorithm requires the same 64-bit plaintext as for standard DES, but it takes a136-bit key and produces a 128-bit ciphertext. Here, the second key is the 80-bit key which is given to the Round 17. Here, we are assuming that the encrypted text differ from the encipher text by one random bit. So, here the average ber output is 18.16,which is comparatively much less than standard DES algorithm. Thus the ber performance is improved. (Fig.6)

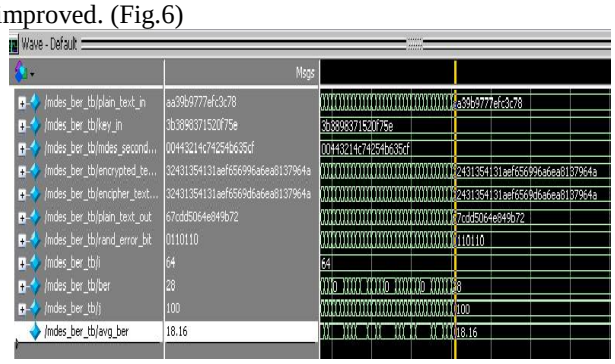

Fig.6. Average BER output for M-DES algorithm

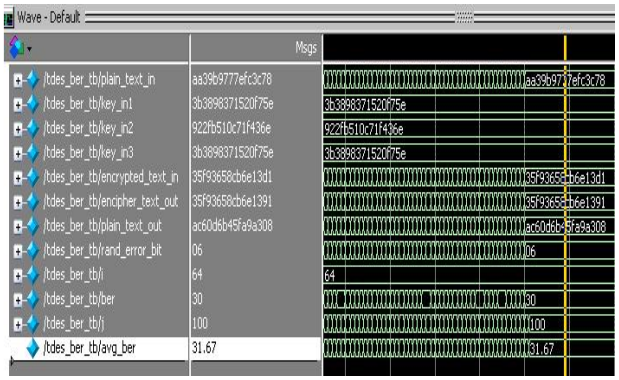

Fig.7. Average BER output for Triple DES algorithm

Similarly, we can observe the results for the triple DES algorithm (Fig.7); in this the DES algorithm is used three times. So, the average ber calculated for triple DES is 31.67, which is almost same as for the standard DES. Similarly, if we use M-DES in triple DES, i.e if we use three M-DES instead of standard DES than the average ber is obtained as 14.02(Fig.8). This is better than normal triple DES. Thus the ber performance is much more improved and the security is also increased using triple modified DES.

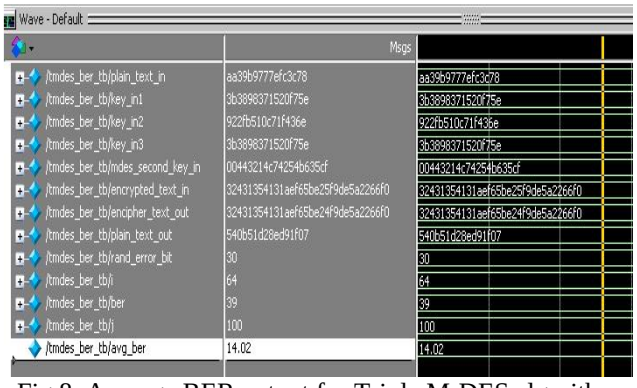

Fig.8. Average BER output for Triple M-DES algorithm

The BER comparison table for different algorithms is shown below

Architecture	Standard		Modified	
	DES	T-DES	DES	T-DES
BER	31.62	31.67	18.16	14.02

V. CONCLUSION

In this paper, we showed how well known block cipher encryption algorithms are not sufficient for the use in wireless applications. Because in these applications, the signal may experience severe degradations and attenuations, which causes wrong reception of the signal and hence a catastrophic effect on the decryption process. In this paper, we proposed a new encryption mechanism based on modified DES. Using simulation we quantified the performance of the proposed M-DES versus the known standard DES and Triple DES versus Triple M-DES for encryption in a wireless communication channel. We showed that the new algorithm outperforms the standard DES and Triple DES algorithms in terms of error performance. We also showed that the new algorithm enhanced the security to a high security level which is prone to all applicable types of attacks.

REFERENCES

[1] M. Haleem, C. Chetan, R. Chandramouli and K.P.Subbalakshmi, “Opportunistic Encryption: A Trade-Off between Security and Throughput in Wireless Networks,” IEEE Transaction on Dependaple and Secure Computing, vol. 4, no. 4, pp.313-324, Oct 2007.

[2] Reason, “End-to-End Confidentiality for Continuous-Media Applications in Wireless Systems,” PhD dissertation, UC Berkeley, Dec.2000.

[3] “Technical specification group services and system aspects,” 3GPP TS 55.216 V6.2.0, September 2003.

[4] Sedat Akleylek, “On the avalanche effect of MISTY1, KASUMI and KASUMI-R,” Master’s thesis, Middle East Technical University, Feb 2008.

[5] O. Dunkelman, N. Keller and A. Shamir, “A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony,” Cryptology ePrint Archive, Report 2010/013, Feb 2010.

[6] Behrouz A. Forouzan, Cryptography and Network Security, 1st Edition, Mc Graw Hill, 2008.

[7] M. Matsui, “On correlation between the order of S-boxes and the strength of DES,” in Proceedings of Eurocrypt94 (A. De Santis, ed.),no. 950 in Lecture Notes in Computer Science, pp. 366375, Springer-Verlag, 1995.

[8] E.Biham and A.Shamir, “Differential Cryptanalysis of the Full 16-round DES,” Proceedings of Crypto’92, vol. 740, Santa Barbara, CA, December 1991.

AUTHOR'S PROFILE

K. Charan Kumar

received the B. Tech. degree in Electronics and Communication Engineering from Bharat Institute of Engineering and Technology, JNTU University, Hyderabad, in 2009, and currently pursuing the M. Tech. degree in VLSI System Design from CVSR College of Engineering, JNTU University, Hyderabad respectively.

He is currently a Lab Assistant with the College. He was with the Department of Electronics and Communication Engineering, JNTU University. He worked in Bharat Electronics Limited as Graduate Apprentice trainee in Radar and Communication field. His research interests include microprocessor, Embedded design, and hardware/ software co-verification. He has been actively involved in academic, educational and industrial activities

P. Ramakrishna

received the B. Tech. degree in Electronics and Communication Engineering from NIIT, Warangal in 2006, and the M. Tech. degree in VLSI System Design from CVR College of Engineering, JNTU University, Hyderabad in 2009 respectively.

He is currently an Associate Professor with the CVSR College of Engineering with 3 years experience. He was with the Department of Electronics and Communication Engineering, JNTU University. His research interests include system on a chip design, hardware/ software co-design/ verification.