Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement

Gulshan Kumar [1], Mritunjay Rai [1] and Gang-soo Lee [2]

[1] *Department of Computer Science,*
Lovely Professional University, Jalandhar, India

[2] *Department of Computer Engineering, Hannam University, Korea*
gulshan_acet@yahoo.com, raimritunjay@gmail.com, jslee@hannam.ac.kr

Abstract

Wireless Sensor Networks have been a great effect in our real life. With its various types of applications WSN is also a matter of concern for its existing vulnerabilities. To prevent those loopholes we need to provide some effective mechanism for providing better security and authentication issues. Wireless Sensor Networks also have a constraint of resources as the nodes work on battery power. In our paper, we have shown such an effective mechanism using a combination of DES and Blowfish in CBC mode for security enhancement which provides high data confidentiality and authentication.

Keywords: *Wireless Sensor Network, CBC, Security, Blowfish, DES, Confidentiality*

1. Introduction

Wireless sensor network is a network comprised of autonomous sensor devices that are geographically installed to sense physical or environmental factors like temperature, pressure, vibrations, sound etc. Wireless Sensor Networks provides different types of applications such as healthcare, military surveillance, logistics, energy plants, inventory etc. A sensor can be divided among three different parts: a radio transceiver, a battery and a micro controller (Sink node) shown in Table 1.The radio transceiver is responsible for transmitting, microcontroller accumulates and processes the data and battery is the only power resource for transceiver and microcontroller.

Table 1. Component Description

Componet		Description
Sensor Node	MICAz	Mote module
	MDA300CA	Data acquisition board
	Echo20	Soil moisture sensor
Sink Node	MIB510	Serial interface board
	Terminal	A single board computer

As WSN is structure-less network it is more vulnerable to the active and passive attacks. These attacks should be prevented for providing data confidentiality in wireless sensor transmission. We also have to keep in mind that the wireless sensor network must be functioning efficiently with low power consumption so that services can be provided for a long duration. To provide security we can use symmetric key encryption techniques such as Blowfish and DES in block cipher mode operation.

2. Various Attacks on WSN

There are several attacks that often happen in wireless sensor networks some of which are described below.

2.1. Denial of Service attack

The main aim of this kind of attack is to make the service or resources unavailable to the authorized users. It is mainly occurred due to the sending of unnecessary data packets in huge amount to the victim node such that it gets exhausted and the network gets disrupted. In a wireless sensor network DoS can be of several forms: in physical layer it takes the form of jamming and tampering; at link layer it is like collision, exhaustion; at network layer it is neglect and greed, homing, misdirection, black hole; at transport layer it takes the form of flooding and desynchronization. DoS is shown in Figure 1.

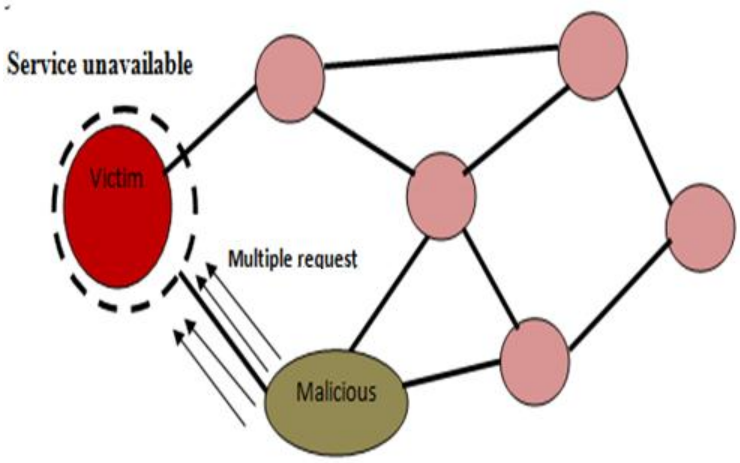

Figure 1. Denial of Service

2.2. Sinkhole Attack

Sinkhole attack deals with a node that disguises itself as an important node for communication by accessing useful routing information so that all the data transmission with the base station can be passed through the sinkhole node. It then selectively forwards the data. This attack is shown in Figure 2.

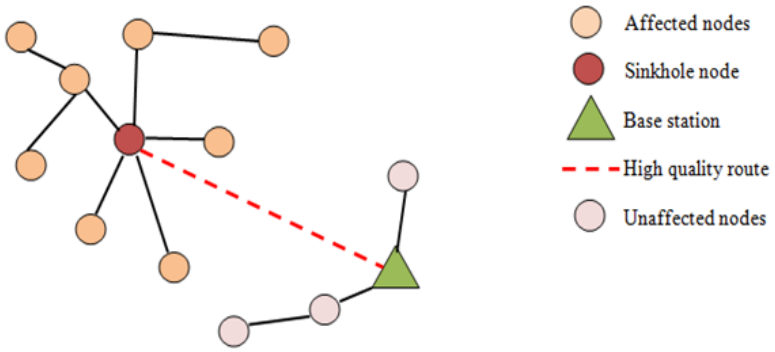

Figure 2. Sinkhole Attack

2.3. Wormhole Attack

Wormhole attack is a very important attack to prevent in sensor networks. It is based on one kind of partnership among one or more number of attackers. Source sends request packets which are transmitted through the attackers' zone. The attacker nodes pass these packets to the destination through a high-speed link faster than any other link. The destination node also selects the same route to send its reply packets. When reply packets are arrived at the source through the attackers' zone the source node starts transmitting data through the path in which the attackers are in. As a result all the data passes through the unauthorized zone and security of the transmission is compromised. Figure.3 shows a diagram for the wormhole attack.

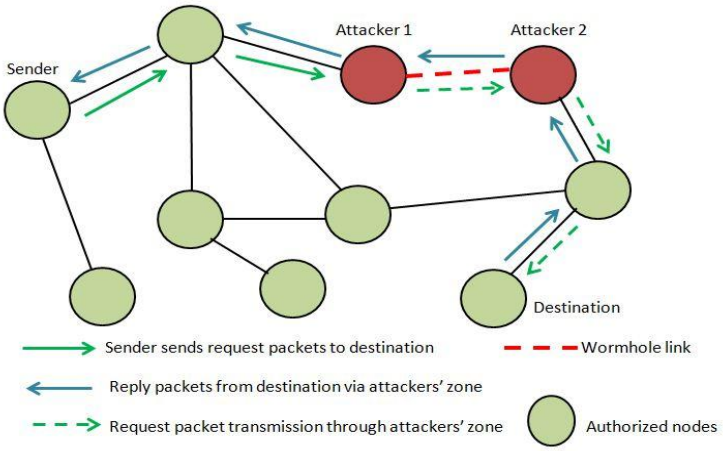

Figure 3. Wormhole Attack

2.4. Sybil Attack

In this attack a faulty or malicious node appears to be a group of nodes i.e. it has the capability of presenting itself as different identities in a WSN to function as distinct nodes. It can send false information like position of nodes, strength of signal, node formation to a node. By masquerading and disguising as multiple identities, a malicious node can gain control over a sensor network.

2.5. Passive Information Gathering

In this attack, the intruder gets equipped with strong receiver and well designed antenna to intercept the data stream transmitting to and fro in a sensor network. A lot of information, therefore, can be easily accessed and used in further direct attacks to the network. It also makes the intruder capable of locating and destroying the sensors in the network. Figure 4 depicts this attack.

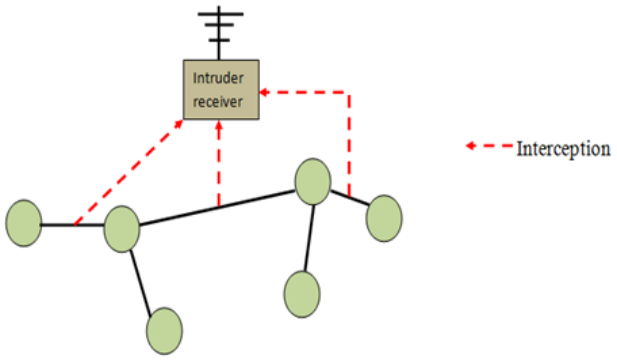

Figure 4. Passive Information Gathering

2.6. Eavesdropping

This attack is a severe attack in wireless sensor network where the intruder just deletes the packets selectively. The sender sends message to the receiver and on the way of transmission some message packets may be deleted by the intruder or may be delayed without the awareness of the receiver. As a result, the receiver receives a false information or delayed information which in case of wireless sensor network is considered to be useless.

2.7. Traffic Analysis

This passive attack is severe as the detection of this kind of attack is hard. The unauthorized entity sits far from the original network and only observes the traffic flowing through the network. As a circumstance, it then can decide where to attack in the network for destroying the functioning of the network.

3. Security on WSN

Authentication confirms the identity of the parties participating in a connection. It can be classified into two types. *Peer entity authentication* provides identity proofs at establishment or at runtime of a data transfer phase in a connection. *Data origin authentication* confirms the identity of the source that generates a data or a message.

Confidentiality ensures the protection of the data being transmitted between sender and receiver such that the data will never be disclosed to a third party.

Data Integrity means that the data sent by the sender should remain same while it reaches to the receiver and there should not be any sort of alteration or fabrication during the transmission.

Availability ensures the presence of network services in spite of the security attacks.

Non-repudiation ensures that neither of the communicating parties can deny the responsibility of a particular message transmission.

4. Applications of WSN

In today's world wireless sensor network performs a huge amount of crucial tasks. Some of the important applications are listed below.

4.1 Battlefield

In case of warfare, sensor networks play an important role in sensing the enemy strategy with observing the aircrafts, radio signals and other means. It also includes the intelligent system of detecting and launching missiles or other attacks by weapons for destruction.

4.2 Medical Help

In case medical environment, now a days wireless sensor network is paid a great attention for patient monitoring system. It helps in sensing the current status with various factors of a patient and alerts the medical team at different levels.

4.3 Home Environment

With the advancement of technology, human beings are also becoming luxury minded. In today's technological environment total autonomous home environment is possible to create with the sensor networks. Example: clapping electronics, talking washing machine, theft alarms etc.

4.4 Environment Monitoring

In this kind application, the wireless sensor network sense the environmental factors such as temperature, rainfall, humidity, wind flow, waves height etc. and alerts about the possible weather or natural hazards such as earthquake, flood, tsunami, volcano eruption etc.

5. Data Encryption Standard

5.1. Encryption

Data Encryption Standard (DES) is one of the encryption techniques used for the block cipher. It takes 64 bits data block as input with 56 bit key (after randomly generated from 64 bits). DES is comprised of three stages. Firstly, an initial permutation is done on the 64 bits input block which generates a permuted input to work with further. The second stage deals with the 16 rounds of iteration of same function with randomly generated keys at each round and a pre-output is generated. The third stage consists of an inverse initial permutation that gives us our desired cipher block. Figure 5 shows the overall DES algorithm and Figure 6 shows a detailed single round of operation. We shall now explain each stage in the following.
Initial Permutation (IP) : It is the first stage of data block computation. IP reorders the bits in the data block. It arranges the even bits in left half L0 shown in blue color in Table 2 and odd bits in right halfR0 shown in red color in Table 2.In this permutation, the data bits are

permuted in the pattern showed in Table 2. This reordering is necessary for bit synchronization and bit error checking. It also includes redundancy check error.

Table 2. Initial Permutation

58	50	42	34	26	18	10	2	Even bits as L0
60	52	44	36	28	20	12	4	
62	54	46	38	30	22	14	6	
64	56	48	40	32	24	16	8	
57	49	41	33	25	17	9	1	Odd bits as R0
59	51	43	35	27	19	11	3	
61	53	45	37	29	21	13	5	
63	55	47	39	31	23	15	7	

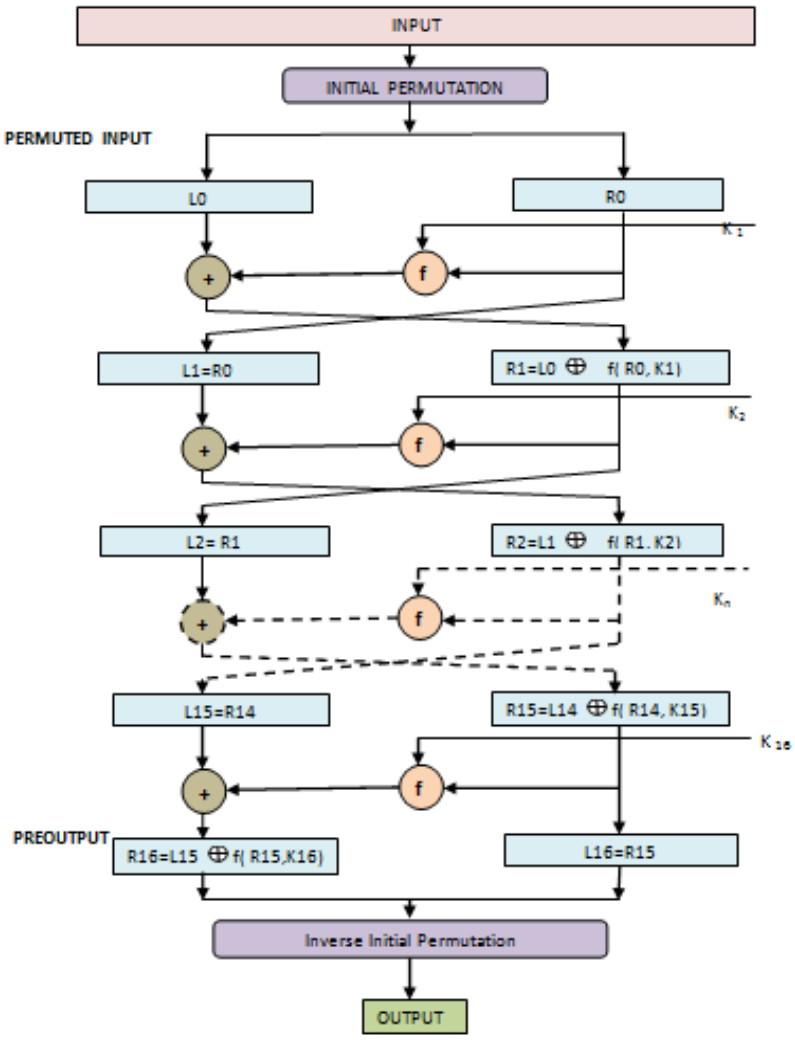

Fig.5 DES Algorithm

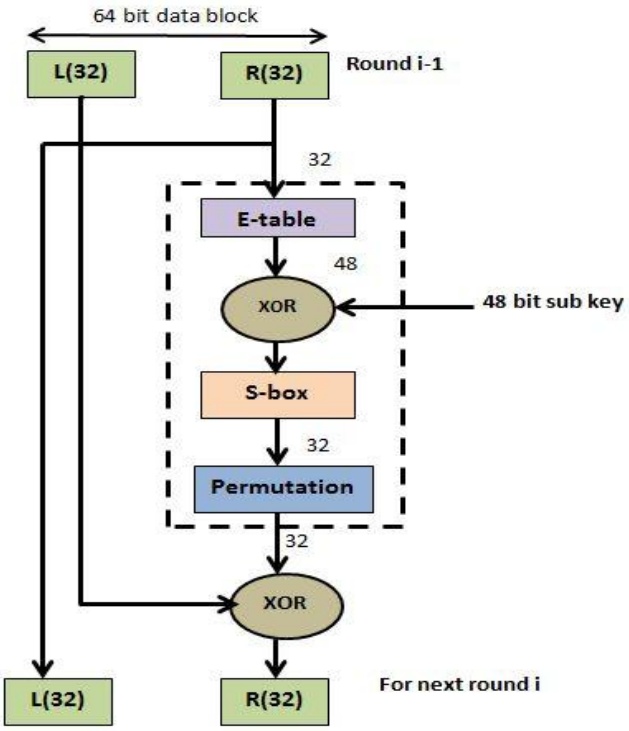

Figure 6. Single Round Structure

Round Structure: This is the second stage for cipher block computation in DES. It consists of 16 same rounds each of which takes input of two halves of data block L_{i-1} and R_{i-1} and randomly generated key K_i where i= 1 to 16. In each round, the 32 bit right half of the previous round and the 48 bit key is given input to a function f whose output and the left half is XOR ed. The right half directly and the output of the XOR function is then interchanged to get the left and right halves respectively for the next round. The formulae for left and right halves are given below.

$$L_i = R_{i-1} \quad (1)$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \text{ for } i = 1 \text{ to } 16$$

The function f takes input of 32 bits right half and 48 bits sub key. The 32 bits right half is expanded to make it 48 bits according to the E-Table in Table 3 to work in the following way. After the expansion, the 48 bits are XOR ed with 48 bits of sub key. The resultant 48 bits are then subdivided into 8 substitution box. Each of them takes 6 bits input and gives 4 bits of output. As a result, we get total 32 bits of output which is again permuted and we get 32 bits from the function f shown in Figure 7. The output of the function f is XOR ed with the left half of the data and the output of the XOR and the right half are interchanged to get the right half and left half for the next round. Thus, 16 rounds occur.

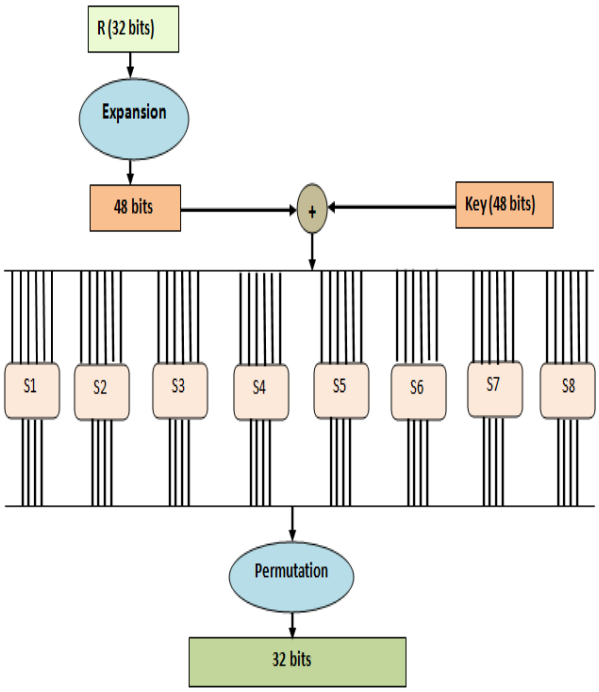

Fig. 7 Round Function F

Table 3 Expansion(E) Table

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Inverse Initial Permutation (IP -1): The output of the 16 rounds, called *PREOUTPUT* is then inversely permuted according to the Table 4. Thus we get 64 bit encrypted data block.

Table 4 IP –1

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Key Generation : At first 64 bit key is given as input in which every 8th bit is ignored. So, key input becomes from 64 bits to 56 bits. This 56 bit key is first subjected to a permutation called Permuted Choice 1 according to a permutation table PC 1 (Table 5). After this permutation 56 bits are divided into two parts $\mathbf{C}_{i-1}$ and $\mathbf{D}_{i-1}$ where i= 1 to 16 rounds. At each round, both the halves of 56 bits separately undergo the circular left shift of 1 bit for round number 1, 2, 9, 16 respectively and 2 bits for rest of the rounds.

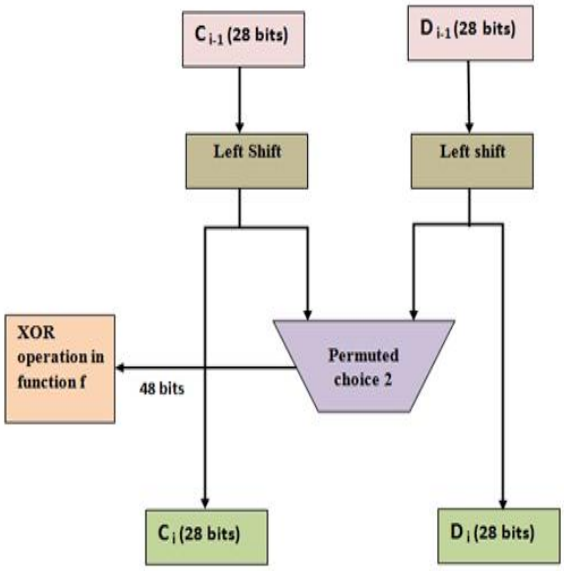

Figure 8. Key Generation

These shifted values serve as the inputs for the next round as well as go for the next step of permutation called Permutation Choice 2 according to the table of PC 2(shown in Table 6), which produces 48 bit subkey for each round used in the function f. Key generation is shown in Figure 8.

Table 5 PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
60	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Permuted Choice 1 (PC 1)

[Numbers signify bit positions]

Table 6 PC-2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Permuted Choice 2 (PC 2)

[Numbers signify bit positions]

5.2. Decryption in DES

The decryption technique in the DES is the same as encryption one with the only the difference that the application of the sub keys are reversed.

6. Blowfish Algorithm

Blowfish a symmetric key block cipher. It uses 64 bits of data blocks and a variable size key maximum up to 448 bits. It is a version of Feistel Network having 16 times of iteration of a simple encryption function. The main features of Blowfish algorithm is that it includes key dependent S-boxes and has a complex key schedule which makes the algorithm stronger.

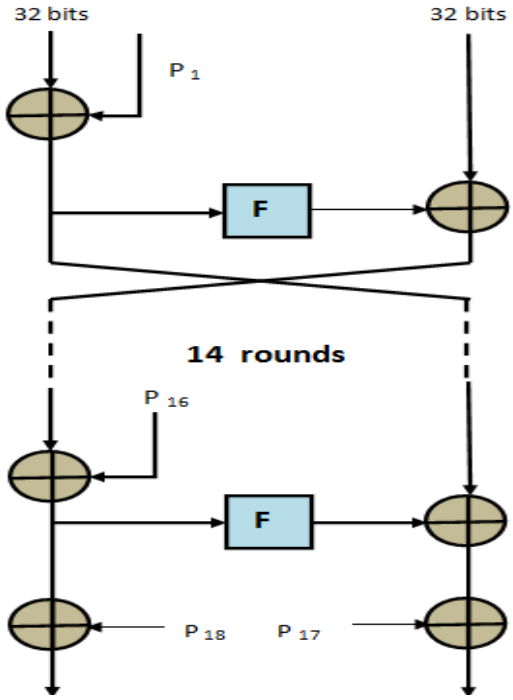

Figure 9. Blowfish Algorithm

6.1. Encryption

The data block of 64 bits are first divided into two halves of 32 bits each. Each line in the diagram (Figure 9) of the Blowfish algorithm represents 32 bit data. This algorithm uses two sub key arrays 18-entry P-array and 256-entry S-boxes. The S-boxes maps the 8 bit input into 32 bits output. One entry of P-array is compulsory for each of 16 rounds. The remaining 2 entries of P-array are used after the final round to separately XOR the outputs of each of the halves of the data block.

In the function F, four S-boxes are used and two types of bit operations: XOR and addition of modulo 2^{32} are used. The function divides the input of 32 bits into four S-boxes of 8 bits each. The outputs of first and second S-boxes are first added to modulo 2^{32} and the output of the addition is XOR-ed with the output of third S-box output. The result of XOR operation and the output of fourth S-box is finally added to modulo 2^{32} to get the final output from the function F. The key schedule of Blowfish algorithm starts by initializing the P-array and S-boxes with values derived from the hexadecimal value of pi. The secret key is then byte wise XOR-ed with all the P-entries in order. Because the P-array is 576 bits long (18 P-entries * 32 bits) and the bytes are XOR-ed with all these bits, many implementations may support 576 bit key size. The function F in Blowfish S-box is shown in Figure 10.

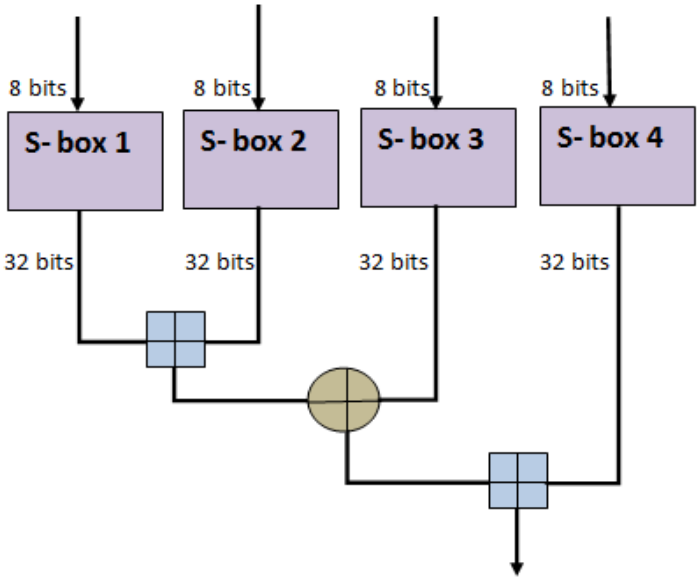

Figure 10. Function of S-box

6.2. Decryption

Decryption is exactly the same as encryption technique except the P1, P2 ……. P18 are used in reverse order.

7. Cipher Block Chaining

CBC is the most commonly used block mode operation for generating cipher blocks using fixed size of plaintext blocks of 64 bits. In CBC, an initialization vector (IV) is used for the first block of plaintext. While encryption each block of plaintext is XOR -ed with the

previous cipher text block before being encrypted and while decryption the XOR is done after the decryption of the cipher text block. Two formulae are used here for encryption and decryption.

$$C_i = E_k(P_i) \bigoplus C_{i-1},\ C0 = IV \text{ [Encryption]} \qquad (2)$$

$$P_i = D_k(C_i) \bigoplus C_{i-1},\ C0 = IV \text{ [Decryption]}$$

The data i.e. the plaintext that is to be sent is firstly divided into small blocks of 8 bytes or 64 bits each. The final block is to be padded to get the complete 8 bytes block. The final n bytes plaintext (data) $0 \leq n \leq 7$ are to be followed by $(8 - n)$ bytes for padding. It means that each block of plaintext must be of 64 bits for the encryption purpose. Figure 10a and 10b show the operation of encryption [CBC (E)] and decryption in CBC mode [CBC (D)] respectively.

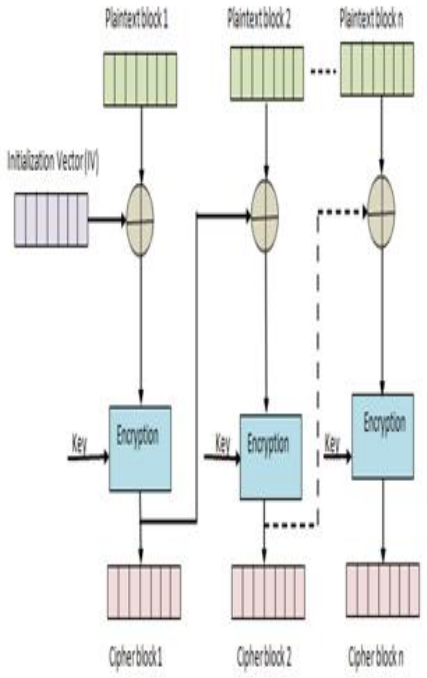

Figure 11a. CBC (Encryption)

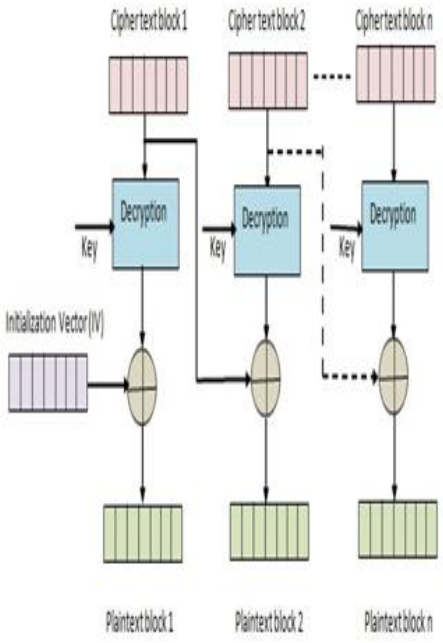

Figure11b. CBC (Decryption)

7.1. Advantages of CBC Mode

In CBC parallel encryption is restricted as encryption process cannot be processed further until the previous block of message is encrypted and passed to the next encryption process. Though this is a drawback in cipher block chaining mode this mode of block cipher has several advantages which are listed below.

Firstly, this mode of operation is easy to implement and complexity is less.

Secondly, the IV used here in the first block is not constant. So, we can get different cipher text for same message.

Thirdly, CBC mode can handle larger message size easily.

Fourth, encryption and decryption operations are same in this mode.

Fifth, though error in one block can lead to a failure of subsequent blocks we can rectify the error by the XOR operation called 'limited error propagation'.

Figure 12 shows the comparison between different types of modes from which we can understand the useful factors of CBC mode.

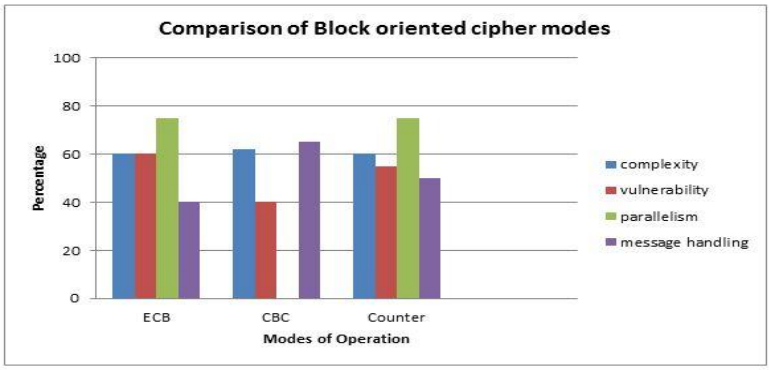

Figure 12. Comparison of Modes of Operation

8. Results

As it is important to secure our network from malicious activities performed by intruders, encryption algorithms plays an important role for achieving that goal. To have an effective encryption algorithm we must evaluate the algorithms with different issues like speed, throughput, efficiency etc. Here, we have tested our algorithms for speed and battery consumption with the parameters of 64 bit plaintext block, 64 bit key and 16 rounds of iteration in both cases.

8.1.Based on speed

The graph in Figure 13 shows clearly that Blowfish algorithm gives better throughput of generating encrypted packets than that of the DES algorithm.

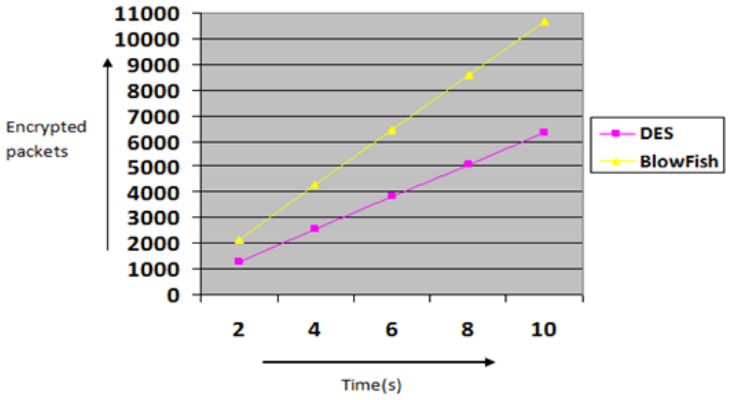

Figure 13. DES v/s Blowfish (speed)

8.2. Based on Battery Consumption

The analysis below shows that Blowfish and DES both the algorithms consume almost same amount of battery power at same levels.

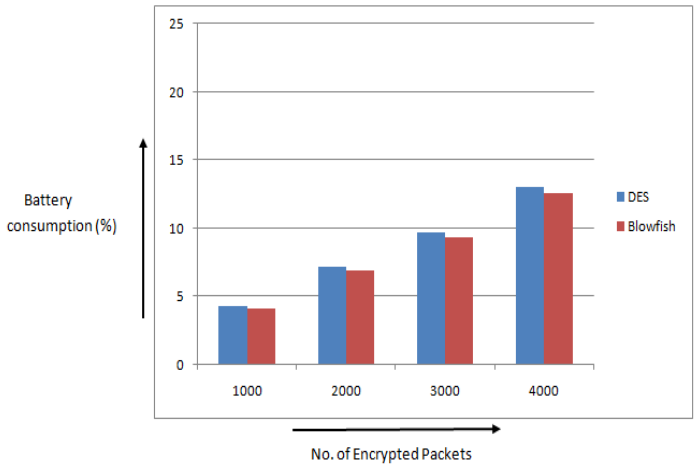

Figure 14. DES v/s Blowfish (battery consumption)

8.3. Based on Operation Modes

The following analysis shows the comparison of the DES algorithm and Blowfish algorithm in different modes of cipher block operation

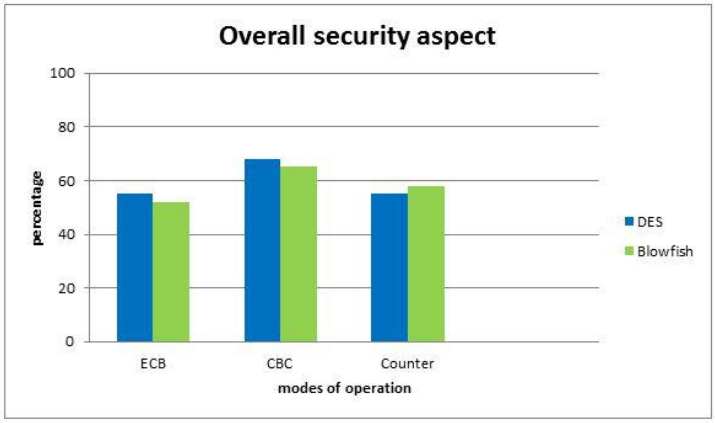

Figure15. DES v/s Blowfish (modes of operation)

As ECB mode is vulnerable to attacks, it is seen in our analysis that both DES and Blowfish algorithm are less responsive in overall security aspects. As compared to the other modes of operation, the both algorithms give the better responses in totality.

9. Conclusion

As per the above discussion we can state that the throughput i.e. the capability of generating encrypted packets and battery consumption is efficient using block cipher mode

encryption. Our approach also provides more security, confidentiality, authentication as Blowfish algorithm is strong enough to break. As using Block cipher encryption it is hard to break the security by intruder as compare to that of stream cipher. Also CBC block cipher mode of operation is most efficient as it effectively scrambles the plaintext prior to each encryption steps. In our future work we shall try to apply other block cipher encryption algorithms to optimize the security services in a sensor network.

Acknowledgement

This work was supported by the Security Engineering Research Center, granted by the Korea Ministry of Knowledge Economy.

References

[1] Shish Ahmed, Md. Rijwan Beg, Qamar Abbas. Energy Efficient Sensor Network Security Using Stream Cipher Mode of Operation, ICCCT'10, page no 348-354 **(2010)**

[2] Nadeem MYJ. A performance comparison of data encryption algorithms.In: First International Conference on Information and Communication Technologies. 2005: 84- 89 **(2005)**

[3] A. Nadeem and M. Y. Javed, \A performance comparison of data encryption algorithms," Information and Communication Technologies, ICICT 2005, pp.84-89 **(2005)**

[4] Report on the Symmetric Key Block Cipher Modes of Operation Workshop **(2000)** October 20, Baltimore Convention Center in Baltimore Maryland, sponsored by the National Institute of Standards and Technology (NIST).

[5] Mihir Bellare, Anand Desai, Eron Jokipii and Phillip Rogaway. A Concrete Security Treatment ofSymmetric Encryption: Analysis of the DES Modes of Operation. Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS '97) **(1997)**

[6] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in **(2006)** February 20-22, ICACT2006, pp(1043-1048).

[7] Salama, A. Elminaam "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vo1.10, No.3, PP.216-222 **(2010)** May.

[8] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks"MANETs **(2010)**

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermeasures,"AdHoc Networks Journal, vol. 1, no. 2–3,pp. 293–315 **(2003)** September.

[10] W. Stallings, Cryptography and Network Security, 4th Ed, pp. 58-309, Prentice Hall **(2005)**

[11] Feng Zhao,Leonidas Guibas,,"Wireless Sensor Networks", Morgan Kaufmann Publications.

[12] Schneier, The Blowfish Encryption Algorithm **(2008)** October 25 (http://www.schneier.comlblow -sh.html)

[13] P. Ekdahl, T. Johansson. A new version of the stream Cipher SNOW, available from http://www.it.lth.se/cryptology/snow/ **(2002)**

Authors

Gulshan Kumar pursuing his M. Tech degree in Computer Science and Engineering from Lovely Professional University, Jalandhar, India. His research interest includes Cryptography and Mobile Adhoc Networks.

Mritunjay Kumar Rai received his Ph.D. Degree from from ABV-Indian Institute of Information Technology and Management, Gwalior, India. Currently he is working as an Assistant Professor in Lovely Professional University.His research interest area is Mobile Adhoc Networks and Wireless Sensor Networks.