Secure Data in Wireless Sensor Network By Using DES

Jagbir Dhillon , Krishna Prasad , Rajesh Kumar, Ashok Gill

jagbirdhillon@yahoo.co.in

ABSTRACT

The main goal of sensor networks is to provide precise information about a sensing field for an extended period of time. The emergence of sensor networks is one of the dominant technical trend has posed challenges to explorers. As sensor networks may interact with sensitive data and operate in hostile insecure environment, it is clear that these security concerns can be addressed from the basic system design. These networks are likely to be composed of hundreds, and potentially thousands of small sensor nodes, functioning independently .The challenges in sensor networks are diverse, we concentrate on security of Wireless Sensor Network in this paper [1,2,3,4,5]. Some of the security goals are proposed by our self for Wireless Sensor Network and use of sensor networks for many applications. We also propose some techniques against these threats in Wireless Sensor Network. So, in this paper we have implemented Encryption Algorithm like - DES to provide sufficient levels of security for protecting the confidentiality of the data in the WSN network. This paper also analyzes the performance of DES algorithm against Attacks in WSN Network [3,5].

KEYWORDS**:** WSN, Sensor node, Gateway, Security, DES.

1. INTRODUCTION:

Wireless sensor networks are very popular because of the fact that they are offer low cost solutions to a variety of real-world challenges. Due to low cost one can deploy large sensor arrays in both military and civilian areas. But sensor networks also face severe resource constraints due to their lack of data storage and power and hence implementation of traditional computer security techniques in a wireless sensor network become difficult [8, 9, 11]. The unreliable and unattended communication channel makes the security defenses even difficult. Often wireless sensors have the processing characteristics of machines that are very old, whereas the industry wants to reduce the cost of wireless sensors while maintaining similar computing power. Researchers have begun to maximize the processing capabilities and energy efficiency of wireless sensor nodes while also securing them against attacks. All aspects regarding wireless sensor network are being analyzed including secure and optimal routing, data aggregation, cluster formation, and so on. Apart from these traditional security issues, many sensor network techniques assumed that all nodes are trustworthy. Some of the researchers began to concentrate on building a sensor network model to solve the desired problems by using cryptographic schemes. Due to unattended feature of wireless sensor networks, we see that physical attacks to sensors play an important role in the operation of wireless sensor networks. Thus, we include a detailed discussion of the physical attacks and their corresponding defenses, topics typically ignored in most of the current research on sensor security. We classify wireless sensor network security in four categories: the obstacles to sensor network security, the need of a secure wireless sensor network, attacks, and defensive measures. We also give a brief introduction of related security techniques and summarize the

DOI : 10.5121/ijwmn.2011.3315

obstacles for the sensor network security [13, 14, 15]. The security requirements of a wireless sensor network are listed as below:

1.1. Obstacles of Sensor Security

A wireless sensor network is a network which has many constraints compared to a traditional computer network and these constraints make it difficult to use the existing security techniques to wireless sensor networks. However, it is necessary to develop useful security mechanisms by getting ideas from security techniques like (DES, AES).

2. WSN ARCHITECTURE

In a typical WSN we see following network components –

[A]. Sensor motes– Routers mounted in the process must be capable of routing packets on behalf of other devices. They control the process and process equipments. A router is a field device which do not have process sensor or control equipment and does not interface with the process.

[B]. Gateway or Access points – A Gateway provides communication between Host application and field devices.

[C].Network manager –To maintain the scheduled communication between devices and configuration of the network for which Network Manager is essential. Also manages the routing tables and monitoring the condition of the network.

[D].Security manager – The Security Manager manages the storage and management of the Cryptographic keys like DES and AES. [5, 18, 19].

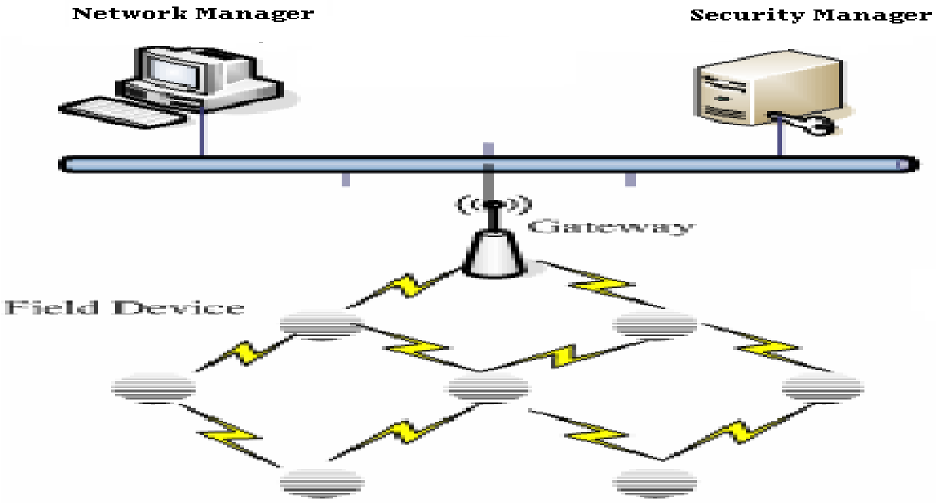

Figure 1 WSN Architecture

3. WSN SECURITY ANALYSIS

Wireless Sensor Network are vulnerable to variety of attacks due to their simplicity. To secure wireless sensor network the network should support all security issues: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware configuration as the genuine nodes that might plan to attack the system. Attackers may approach malicious nodes by purchasing these separately. Also, these nodes have better communications links for coordinating these attack. Sensor nodes if attacked , one can extract all key materials, data, and code . So tamper resistance might be a defense for some networks, we do not see it as a general purpose solution. On the other hand sensor nodes are intended to be very inexpensive [21, 23]

3.1 Overview

The Data Encryption Standard is the Federal Information Processing Standard, which gives the data encryption algorithm. As per ANSI standard X3.92, data encryption algorithm is an improvement of the algorithm Lucifer developed by IBM in 1970s. IBM and the National Security Agency developed the algorithm. The DES has studied in depth and is the most widely used symmetric algorithm in the world. [15, 5, 19]. DES has a 64-bit block size and uses a 56-bit key during execution. DES is a symmetric cryptosystem, specifically a 16-round Feistel cipher.

As we know that WSN is mostly used for the application of collection of information from the surrounding environment, so it is necessary to protect the sensitive data from unauthorized parties. WSNs are susceptible to security attacks due to the broadcast radio transmission. It is very clear to all of us that some of the sensor nodes are physically captured or destroyed by the enemies. The main role of sensor network in security for various applications depends on secure routing. The resources of sensor network show many challenges for its security. As sensor nodes are very limited for computing power and it is very difficult to provide security in WSN using public-key cryptography because it is very costly. So security solutions for various applications are based on symmetric key cryptography. In this paper we have used DES for the security purpose of wireless sensor network. [22, 23]

3.2 OVERVIEW OF SECURITY ISSUES

3.2.1. Attack and attacker

An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. As we know that all the attackers are the originator of an attack. Main weaknesses in a system are security design, configuration, implementation or limitations which can be exploited by the attackers are known as vulnerability or flaw. Any event or attacker which impacts a system through the security breach is called threat. So the attacker will exploit a particular vulnerability and causing harm to a system asset is called as risk.

3.2.2. Security requirements

A sensor network is a type of Ad hoc network. The security requirements of a wireless sensor network can be classified as follows [26, 27, 29, 30]

Authentication: As we know that WSN communicates sensitive data that helps in making the important decision. The receiver needs to ensure that the data used originates from the desired source. During exchange of control information in the WSN, authentication is important.

Integrity: Data transit may be changed by the attackers or intruders. Data loss can also occur due to the harsh communication environment. Data integrity ensures that no information is changed in transit due to malicious node or by accident.

Data Confidentiality: Some of the applications need to rely on confidentiality like surveillance of information, industrial secrets and key distribution etc. Encryption standards are used to keep data confidentiality.

Data Freshness: We need to ensure freshness of all messages even if confidentiality and data integrity are assured. Data freshness means that the data is recent and no old messages are replayed. A time stamp can be added to the packet to ensure that no old messages are replayed.

Availability: Due to excess computation or communication, battery power of sensor nodes may run out and become unavailable because attackers may jam communication. The requirement of security is very important in maintaining the availability of the network.

Self-Organization: As we know that in WSN every sensor node should be independent and flexible to be self-organizing and self-healing according to different environment conditions. Therefore no fixed infrastructure is available for WSN network due to random deployment of nodes & distributed sensor networks must self-organize to support optimal routing in WSN.

Time Synchronization: Most sensor network applications require time synchronization. An individual sensors radio may be turned off periodically to conserve power.

Secure Localization: The sensor network always needs information of location accurately. Therefore by reporting false signal strengths and replaying signals, an attacker can easily manipulate non-secured location information in WSN. [21, 28]

3.3 In Depth

By using a 64-bit key which gives a 64-bit block of plaintext as input and gives an output in the form of a 64-bit block of cipher text. DES operates on blocks of equal size by using permutations and substitutions in the algorithm. Because DES has 64-bit rounds, hence the main algorithm is repeated 16 times to produce the cipher text. However it has been noted that the number of rounds are always exponentially proportional to the time required. Security of the algorithm increases exponentially when the number of rounds increases which means security is maximized automatically when the number of rounds are more. [3, 4, 5].

64 bit plain text

64 bit plain text

64 bit plain text

DES

DES

DES

64 bit cipher text

64 bit cipher text

64 bit cipher text

Figure2. Conceptual working of DES

3.4 Key Scheduling

DES has 64-bits long input key but the in real practice key used by DES is of 56-bits length. A parity bit is LSB in each byte set in such a way that there should be odd number of 1s in every byte. As these parity bits are ignored, hence the seven most significant bits are used for each byte giving us 56-bits key results. Firstly the 64-bit key is passed through a Permuted Choice 1(PC1). The table is given below. All descriptions of bit numbers, 1 is the left-most bit and n is the rightmost bit.

PC -1: Permuted Choice 1							
Bit	0	1	2	3	4	5	6
1	57	49	41	33	25	17	9
8	1	58	50	42	34	26	18
15	10	2	59	51	43	35	27
22	19	11	3	60	52	44	36
29	63	55	47	39	31	23	15
36	7	62	54	46	38	30	22
43	14	6	61	53	45	37	29
50	**21**	**13**	**5**	**28**	**20**	**12**	**4**

Table 1: Permuted Choice 1

For example, PC-1 table can be used to see how bit 30 of the original 64-bit key changes to a new 56-bit key. As number 30 in the table, belongs to the column no.5 and the row no. 36. Now adding values of the row and column to know the new position of the bit. For bit 30, 36+5=41, so bit 30 becomes bit 41 of the new 56-bit key. Therefore bit 8,16,24,32,40,48,56 and 64 of the original key are not present in the table. They are the unused parity bits which are discarded if the final 56-bit key is created [17, 19, 5].

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

Figure3. Discarding of every 8th bit of Original Key (Shaded Bit Position are Discarded)

Original 64 bit Key

Key Discarding Process

Resulting 56 bit Key

Figure 4. Key Discarding Process

Now that we have the 56-bit key, the next step is to use this key to generate 16 48-bit sub keys, called K [1] – K [16], which is used in the 16 rounds of DES for encryption and decryption. The procedure for generating the sub keys – known as key scheduling – is fairly simple:

Set the round number R to 1.

Split up the present 56-bit key, K, into two 28-bit blocks, L and R.

Rotate L left by the number of bits given in the table below, and repeat the same procedure for rotating R left by the same number.

Join L and R together to get the new K.

Apply Permuted Choice 2 (PC-2) to K to get the final K[R], where R is the round number we are on.

Give increment of 1 to R and repeat its procedure until we get 16 sub keys, i.e., up to K [1] to K [16].

Here are the tables involved in these operations:

Sub Key Rotation Table:

Round Number	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Number of Bits to Rotate	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**

Table 2: Sub Key Rotation Table

P C 2 : Permuted Choice 2						
Bit	**0**	**1**	**2**	**3**	**4**	**5**
1	**14**	**17**	**11**	**24**	**1**	**5**
7	**3**	**28**	**15**	**6**	**21**	**10**
13	**23**	**19**	**12**	**4**	**26**	**8**
19	**16**	**7**	**27**	**20**	**13**	**2**
25	**41**	**52**	**31**	**37**	**47**	**55**
31	**30**	**40**	**51**	**45**	**33**	**48**
37	**44**	**49**	**39**	**56**	**34**	**53**
43	**46**	**42**	**50**	**36**	**29**	**32**

Table 3: P C 2 : Permuted Choice 2

3.5 Plaintext Preparation

After the key scheduling has been done, the next step is to encrypt. The plaintext is passed through a permutation called as the Initial Permutation (IP). This table also has the Inverse Initial Permutation, or IP^ (-1) known as the Final Permutation. These are given below.

IP: Initial Permutation								
Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	58	50	42	34	26	18	10	2
9	60	52	44	36	28	20	12	4
17	62	54	46	38	30	22	14	6
25	64	56	48	40	32	24	16	8
33	57	49	41	33	25	17	9	1
41	59	51	43	35	27	19	11	3
49	61	53	45	37	29	21	13	5
57	**63**	**55**	**47**	**39**	**31**	**23**	**15**	**7**

Table 4: IP(Initial Permutation)

IP^(-1):Inverse Initial Permutation								
Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	40	8	48	16	56	24	64	32
9	39	7	47	15	55	23	63	31

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

Table 5: IP^(-1) Inverse Initial Permutation

Tables mentioned above are used for the key scheduling. By looking at the tables it is very clear why one permutation is called the inverse of the other. For example, how bits 32 are transformed under IP. Bit 32 available at the intersection of the column 4 and row 25 as shown above, apply IP^ (-1). In IP^ (-1), bit 29 which is located at the intersection of the column no. 7 and the row no. 25. So this bit becomes bit 32 (25+7) after the permutation is done which is the same bit position that we have started before permutation. So inverse of IP^ (-1) is IP. It does the exact opposite of IP. We will end up with the original block.

3.6 DES Core Function

Once key scheduling and plaintext preparation are over, then actual encryption or decryption is performed by using DES main algorithm. The 64-bit block of input data is first split into two halves, L and R. L is the left-most 32 bits, and R is the right-most 32 bits.

64 Bit block Input data

L	**R**

Left Most 32 bit **Right Most 32 Bit**

Figure 5. Splitting 64-bit block input data

The following is repeated 16 times for making up the 16 rounds of standard. We call the 16 sets of halves L[0] to L[15] and R[0] to R[15].

L	**R**

16 Rounds	**16 Rounds**

Keys **Keys**

Figure 6. 16 Rounds

The following process is repeated 16 times for making up the 16 rounds of standard DES. We call the 16 sets of halves L [0] – L [15] and R [0] – R [15].

This expands the number R [I-1] from 32 to 48 bits to prepare for the next step.

E-Bit Selection Table						
Bit	0	1	2	3	4	5
1	32	1	2	3	4	5
7	4	5	6	7	8	9
13	8	9	10	11	12	13
19	12	13	14	15	16	17
25	16	17	18	19	20	21
31	20	21	22	23	24	25
37	24	25	26	27	28	29
43	28	29	30	31	32	1

Table 6: E-Bit Selection Table

The 48-bit R [I-1] is XORed with K [I] and stored in a temporary buffer so that R [I-1] is not modified.

The result from the last step is now split up into 8 parts of 6 bits each. The left-most 6 bits are denoted as B [1], and the right-most 6 bits as B [8]. These blocks from the index into the S-boxes are to be used in the next step. The Substitution boxes(S-boxes) are a set of eight 2-dimensional arrays, with 4 rows and 16 columns. The numbers in the boxes are always 4 bits in length and their values from 0 to 15. The S-boxes are numbered S [1] to S [8].

For B [1], first and last bits of the 6-bit block are used as an index into the row number of S [1], with range from 0 to 3, and middle four bits are used as an index into the column number, with its range from 0 to 15. The number from this position in the S-box is taken and stored which is repeated with B [2] and S [8]. At this point, now we have eight 4-bit numbers, which give a 32-bit result.

Now applying permutation in the result of previous stage as all details given in next step

This number is now XORed with L [I-1], and moved into R [I]. R [I-1] is moved into L [I].

At this point we have a new L [T] and R [I]. Here, increment is given to I and same core function is repeated until we get I = 17, So that 16 rounds have been executed and all the keys K[I] to K[16] are used.

When L [16] and R [16] have been obtained, they are joined back together in the same fashion they were split apart (L [16] is the left-hand half, R [16] is the right-half hand), then the two halves are swapped, R [16] becomes the left-most 32 bits and L [16] becomes the right-most 32 bits of the pre-output block and the resultant 64- bit number is called the pre-output.

P- Permutation				
Bit	0	1	2	3
1	16	7	20	21
5	29	12	28	17
9	1	15	23	26
13	5	18	31	10
17	2	8	24	14
21	32	27	3	9
25	19	13	30	6
29	22	11	4	25

S-Box 1:Substitution Box 1																
Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	**15**	**12**	**8**	**2**	**4**	**9**	**1**	**7**	**5**	**11**	**3**	**14**	**10**	**0**	**6**	**13**

S-Box 2:Substitution Box 2																
Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	**13**	**8**	**10**	**1**	**3**	**15**	**4**	**2**	**11**	**6**	**7**	**12**	**0**	**5**	**1**	**4**

S-Box 3:Substitution Box 3																
Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	**1**	**10**	**13**	**0**	**6**	**9**	**8**	**7**	**4**	**15**	**14**	**3**	**11**	**15**	**2**	**12**

S-Box 4:Substitution Box 4																
Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	**3**	**15**	**0**	**6**	**10**	**1**	**13**	**8**	**9**	**4**	**5**	**11**	**12**	**7**	**2**	**14**

S-Box 5:Substitution Box 5

Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	**11**	**8**	**12**	**7**	**1**	**14**	**2**	**13**	**6**	**15**	**0**	**9**	**10**	**4**	**5**	**3**

S-Box 6:Substitution Box 6

Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	12	1	10	15	9	2	6	8	0	3	13	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	**4**	**3**	**2**	**12**	**9**	**5**	**15**	**10**	**11**	**14**	**1**	**7**	**6**	**0**	**8**	**13**

S-Box 7:Substitution Box 7

Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	**6**	**11**	**13**	**8**	**1**	**4**	**10**	**7**	**9**	**5**	**0**	**15**	**14**	**2**	**3**	**12**

S-Box 8:Substitution Box 8

Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	**2**	**1**	**14**	**7**	**4**	**10**	**8**	**13**	**15**	**12**	**9**	**0**	**3**	**5**	**6**	**11**

Table 7: S-Boxes

3.7 How to use the S-boxes

The aim of the example is to explain the working of the S-boxes. Suppose we have the following 48-bit binary number:

011101000101110101000111101000011100101101011101

In order to pass this through steps 3 and 4 of the Core Function as outlined above, the number is split up into 8 6-bit blocks, labeled B[1] to B[8] from left to right:

011101 000101 110101 000111 101000 011100 101101 011101

Now, eight numbers are extracted from the S- boxes – one from each box:

B[1] = S[1](01,1110) = S[1][1][14] = 3 = 0011

B[2] = S[2](01,0010) = S[2][1][2] = 4 = 0100

B[3] = S[3](11,1010) = S[3][3][10] = 14 = 1110

B[4] = S[4](01,0011) = S[4][1][3] = 5 =0101

B[5] = S[5](10,0100) = S[5][2][4] = 10 = 1010

B[6] = S[6](00,1110) = S[6][0][14] = 5 = 0101

B[7] = S[7](11,0110) = S[7][3][6] = 10 = 1010

B[8] = S[8](01,1110) = S[8][1][14] = 9 = 1001

Row index of B[n] is first and last bit and column index of S[n] are the middle four bits.

The results are now joined together to form a 32 – bit number which serves as the input to stage 5 of the Core Function (the P Permutation):

00110100111001011010010110101001

4. Conclusion:

Data encryption is utilized in various applications and environments. The specific utilization of encryption and the implementation of the DES will be based on many factors particularly to the WSN and its associated components like sensor node, Gateway, Secure routing in WSN etc. Cryptography is used to protect data while it is communicating between two points or while it is stored in a medium vulnerable to physical theft. So data encryption standard is very useful for secure routing in wireless sensor network. For security point of view, we can also use Advanced encryption standard (AES) to secure routing in wireless sensor network. As we know that none of the protocol is designed to keep security in mind, so there should be a proper implementation and design in routing protocol for security purpose in wireless sensor network. I will concentrate on DES for security purpose in my research topic of WSN.

References:

[1]. International Journal of Technology and Applied Science, Vol. 2, pp. 5-11, 2011. ISSN: 2230-9004 © 2011 IJTAS 5 Repairing the Gaps in Connectivity of Wireless Sensor Network & WiMAX Using Robots: Jagbir Dhillon, Krishna Parsad, Rajesh Kumar.

[2].International Journal of VLSI and Signal Processing Applications, Vol. 1, Issue 1 (48- 61),ISSN 2231-3133 48A Survey on the state of the art of secure and optimal routing issues in wireless sensor networks. *Jagbir Dhillon, Prasad K.P, Krishan Kumar* jagbirdhillon@yahoo.co.in

[3]. Distributed Recovery from Network Partitioning in Movable Sensor/Actor Networks via Controlled Mobility, Kemal Akkaya, Member, IEEE, Fatih Senel, Aravind Thimmapuram, and Suleyman Uludag, Member, IEEE, IEEE transactions on computers, vol. 59, no. 2, february 2010.

[4]. IEEE journal on selected areas in communications, vol. 28, no. 5, june 2010 Cross Layer QoS-Aware Communication for Ultra Wide Band Wireless Multimedia Sensor Networks Tommaso Melodia, Member, IEEE, and Ian F. Akyildiz, Fellow, IEEE.

[5]. IEEE journal on selected areas in communications, vol. 28, no. 7, september 2010. Handling Inelastic Traffic in Wireless Sensor Networks Jiong Jin, Student Member, IEEE, Avinash Sridharan, Bhaskar Krishnamachari, Member, IEEE and Marimuthu Palaniswami, Senior Member, IEEE.

[6]. Constrained Relay Node Placement in Wireless Sensor Networks: Formulation and Approximations, Satyajayant Misra, Member, IEEE, Seung Don Hong, Guoliang (Larry) Xue, Senior Member, IEEE, and Jian Tang, Member, IEEE; IEEE/ACM transactions on networking, vol. 18, no. 2, April 2010.

[7]. Deploying Sensor Networks With Guaranteed Fault Tolerance; Jonathan L. Bredin, Erik D. Demaine, Mohammad Taghi Hajiaghayi, and Daniela Rus; IEEE/ACM transactions on networking, vol. 18, no. 1, february 2010.

[8]. A Distributed Node Localization Scheme for Wireless Sensor Networks; Qinqin Shi, Hong Huo, Tao Fang, Deren Li; Published online: 26 March 2009 © Springer Science+Business Media, LLC. 2009.

[9]. High Reliable In-Network Data Verification in Wireless Sensor Networks; Dong-Wook Lee, Jai-Hoon Kim; Published online: 29 May 2009 © Springer Science+Business Media, LLC. 2009.

[10]. Secure and Efficient Localization Scheme in Ultra-Wideband Sensor Networks; Daojing He, Lin Cui, Hejiao Huang, Maode Ma; Published online: 4 November 2008 © Springer Science+Business Media, LLC. 2008.

[11]. TMH Book of Cryptography & System Security.

[12]. Phalguni Gupta Internet & Protection Security Book.

[13] Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks” Communications of the ACM, Page53-57.

[14] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, International conference on Advanced Computing Technologies, Page1043-1045.

[15] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, pp. 324-328.

[16] D. C. Schleher, Electronic Warfare in the Information Age. Artech.

[17] D. Djenouri, L. Khelladi, and N. Badache, “A Survey of Security Issues in Mobile ad hoc and Sensor Networks,” IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28.

[18] D.Ganesan, R.Govindan, S.Shenker, and D.Estrin, "Highly resilient, energy efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review (MC2R), vol. 1, no. 2.

[19] F. Nait-Abdesselam, B. Bensaou, T. Taleb, “Detecting and avoiding wormhole attacks in wireless Ad hoc networks,” IEEE Communication Magazine, Vol.46, Issue 4, pp. 127-133, April 2008.

[20] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38- 47.

[21] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine.

[22] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15.

[23] Mohit Saxena, “Security In Wireless Sensor Networks - A Layer Based Classification”, Cerias Tech Report 2007-04. [24] S. Khan, K-k. Loo, T. Naeem, M.A. Khan, “Denial of service attacks and challenges in broadband wireless network,” International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp.1-6.

[25] Wang, B-T. and Schulzrinne, H., “An IP trace back mechanism for reflective DoS attacks”, Canadian M. Conference on Electrical and Computer Engineering, Volume 2, pp. 901 – 904. ISSN : 0975-3397 1835

[26] Y.Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks” IEEE Communication. Survey Tutorials, vol. 8, pp. 2–23.

[27] Y.Mun and C. Shin, “Secure routing in sensor networks: Security problem analysis and countermeasures,” in International Conference on Computational Science and Its Applications - ICCSA 2005, vol. 3480 of Lecture Notes in Computer Science, (Singapore), pp. 459–467, Springer Verlag, Heidelberg, D-69121, Germany.

[28] Thomas Haenselmann. Sensornetworks. GFDL Wireless Sensor Network textbook

[29] Secure and Efficient Broadcast Authentication in Wireless Sensor Networks Taekyoung Kwon, Member, IEEE, and Jin Hong.

[30] World Academy of Science, Engineering and Technology 51 2009 Secure Data Aggregation Using Clusters in Sensor Networks Prakash G L, Thejaswini M, S H Manjula, K R Venugopal, L M Patnaik

Author's Profile

Jagbir singh Dhillon is working as Assistant Professor, in Deptt. of Electronics & Communication Engineering, St. Margaret Engineering College,Neemrana, NH-8 Delhi- Jaipur. He has done M-tech in ECE deptt. From MDU Rohtak and pursuing Phd from Manav Rachana International University, Faridabad. He has a number of publications in some journal of well repute. His research area is security in wireless sensor network. He has more than 14 years of experience in teaching & industry

Dr. Krishna Prasad Pamulapati, Professor & Head of IT Deptt. ,Faculty of Engineering and Technology, Manav Rachna International University, Faridabad has got 22 years experience in teaching Computer Science and guiding projects at Graduate and Post-Graduate levels. Experienced in guiding Ph.D. students. Previously he was M.Sc. program Coordinator for De Montfort University,UK in Singapore and Malaysia. Experienced with various universities in Bosnia & Herzegovina,Singapore, Malaysia, Sri Lanka and India. He has many papers to his credit in various journals of repute. His research area is artificial intelligence, soft computing, mobile network and wireless sensor network.

Dr. Rajesh Kumar, Ph.D., MIEEE, FIETE, MIE (I), LMISTE, MIAENG is working as Associate Professor, in Department of Electrical Engineering, MNIT, Jaipur INDIA (On Leave) presently Post Doctorate Research Fellow National University Singapore, 1175756, SINGAPORE. His research area is Intelligent Systems, Evolutionary and Bio-inspired Algorithms and applications, Wireless Sensor Networks, Optimization Algorithms. He is reviewer / Editor of many journals viz. IEEE,IJAIS etc. He has many papers to his credit in various journals of repute. He has more than 15 years of experience in teaching field.

Ashok Gill is working as Assistant Professor, in Deptt. of Electronics & Communication Engineering, St. Margaret Engineering College,Neemrana, NH-8 Delhi- Jaipur. He has done M-tech in D&C deptt. From RGPV Bhopal and. He has a number of publications in some journal of well repute. His research area is image processing & security in wireless sensor network. He has more than 4 years of experience in teaching.