Probabilistic Encryption for Secure Routing in WSN

Harish. M. S.
M.E. Scholar, Department of ECE
Government College of Technology
Coimbatore, India

Dr. V. Sumathy
Associate Professor, Department of ECE
Government College of Technology
Coimbatore, India

***Abstract*—— Recent technology advances in low-cost, low-power chip design have made the deployment of large-scale sensor networks economically feasible. Data forwarding algorithms and protocols have been among the first set of issues explored in sensor networking. In wireless sensor network we consider the problem of secure data transmission in the presence of a passive eavesdropper. It is assumed that the enemy fusion center (EFC) attempts to intercept the transmission of the sensors and detect the state of nature. Before transmission to the ally fusion center (AFC) the sensor nodes encrypt their data using probabilistic encryption scheme based on the Advanced Encryption Standard (AES) in the CBC (Cipher Block Chaining) mode. The communication between the sensors and each fusion center is assumed to be over a parallel access channel. The proposed probabilistic encryption scheme offers more semantic level security when compared to the asymmetric encryption algorithms and has minimal processing and communication overhead suitable for the sensor networks with limited resources.**

Keywords—Advanced Encryption Standard, Information Security, Probabilistic Encryption, Wireless Sensor Networks.

I. INTRODUCTION

Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real world problems. Their low cost provides a means to deploy large sensor nodes in a variety of conditions capable of performing both military and civilian tasks. There are many attacks designed to exploit the insecure communication channels and unattended operation of wireless sensor networks makes the security defenses even harder. There are many cryptographic approaches for providing secure data transmission in wireless sensor networks Due to their resource scarcity traditional cryptographic algorithms based on public key ciphers are not suitable due to their higher computational complexity. The deterministic symmetric key algorithms also offer limited semantic level security in the resource constrained environments. This raises the need for an encryption scheme which is based on probabilistic approach which gives more semantic level security. In this work the probabilistic encryption is based on the advanced encryption standard algorithm in the cipher block chaining mode. Passive eavesdropper (EFC) Enemy Fusion Center is chosen as the adversary. The (AFC) Ally Fusion Center which is assumed to be a very few wavelengths away from the EFC is the data fusion node. The major goal of the proposed work is to provide secure data transmission in the presence of a passive eavesdropper which is an obvious attack to data privacy and very serious problem in military communications. The organization of this paper is as follows section II discuss the related work followed by section III which describes our proposed work. Section IV deals with the simulation and results followed by section V which elaborates our future work.

II. RELATED WORK

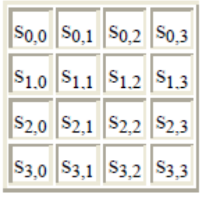
The broadcasting nature of wireless communications makes the distributed routing and detection prone to passive eavesdropping. Many researchers have designed a physical layer secure routing scheme based on simple bit flipping encryption [2]. The authors aimed at achieving information theoretic perfect secrecy without the use of traditional cryptographic techniques. They have used the grouping of sensor node scheme to provide secure detection scheme in their research work. Stefano et al and Vincenzo et al repeated the work of secure routing in wireless sensor networks in the presence of byzantine nodes in the network. The Probabilistic ciphers in their work were based on the RC4 encryption algorithm [3]. The authors have taken the probability of bit error analysis as the routing performance metric. The use of RC4 enciphering scheme have lower computational overhead and they work faster in software. They have used the probability of bit error analysis as the routing metric for both the AFC and EFC. Reeza Shooshabi et al, Mort et al have studied the counter measures against passive eavesdropping in military communications. [4] The authors have mainly focused their research work against the data confidentiality issues. They have taken a stream based probabilistic ciphers as their encryption scheme. The major part of their work involves in the optimal key management issues.

The disadvantage of using RC4 probabilistic ciphers is that we cannot reuse the same key as we do with block ciphers. To provide the probabilistic nature in RC4 encryption we need an additional input called the initialization vector (IV) which is 24 bit long. Large key lengths are needed to prevent the network from a brute force attack. So we need an efficient probabilistic encryption scheme to overcome the cryptanalysis attack at the physical layer.

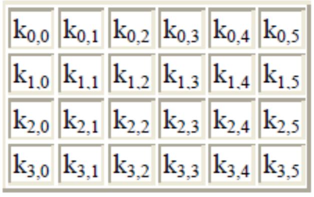
In this paper we propose a security scheme which is based on the advanced encryption standard (AES) algorithm in the (CBC) cipher block chaining mode. It offers more semantic level security when compared with the RC4 based probabilistic ciphers. We have also taken the probability of bit error analysis as the routing performance metric in our proposed work. This gives the routing analysis of the data in the presence of a passive eavesdropper. The other network performance measurable metrics such as the ally fusion center (AFC) throughput, energy analysis, packet delivery ratio are implemented and shown in our simulation results.

III. AES BASED PROBABILISTIC ENCRYPTION SCHEME

The AES (Advanced Encryption Standard) is a symmetric block cipher that can encipher or decipher information. The AES algorithm uses three different key lengths128, 192 and 256 bits to encrypt or decrypt data in blocks of 128 bits. The AES algorithm was developed by Joan-Daemen Proton World International and Vincent Rijmen Katholieke University at Leuven, Belgium.
The key length will be extended in multiples of 32 bit.
AES is an iterated block cipher, where both key the
Initial inputs undergo multiple rounds of transformation before producing the original cipher message.
The results of the intermediate cipher are the state.
The cipher key and the block are presented by array of columns, where each array has four rows and column represents a single byte.
An array representing the state will have N_b column, where the values of N_b are 4, 6 and 8 corresponding to 128, 192 and 256 bit block.
The array representing the cipher key will have N_k columns, where the N_k values of 4, 6 and 8 will represent the corresponding key length. An example of 128 bit state (N_b=4) and 192 bit cipher key (N_k=6) are show in Fig1



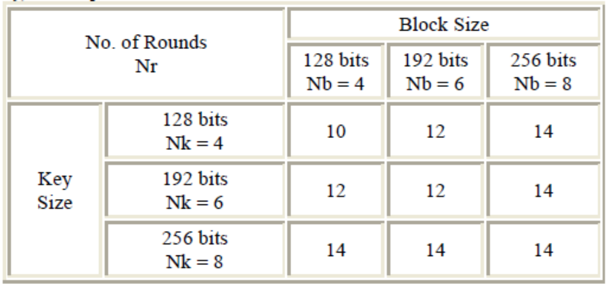
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$



$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$	$k_{0,4}$	$k_{0,5}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,4}$	$k_{1,5}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$	$k_{2,4}$	$k_{2,5}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$	$k_{3,4}$	$k_{3,5}$

Fig 1 Bit state and Cipher key in Columns

The number of transformation rounds (N_r) is a function of block length and key length and is shown in the Fig2 below.



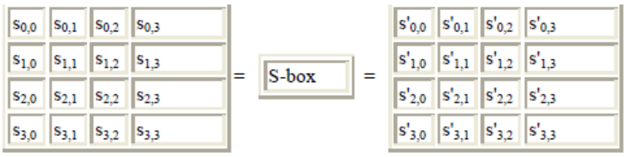
No. of Rounds Nr		Block Size 128 bits Nb = 4	 192 bits Nb = 6	 256 bits Nb = 8
Key Size	128 bits Nk = 4	10	12	14
	192 bits Nk = 6	12	12	14
	256 bits Nk = 8	14	14	14

Fig 2 Transformation rounds in AES

The AES algorithm consists of four operational stages, they are the a) Add-round key transformation b) Substitute byte stage c) Shift rows d) Mix column transformation. The arrays S and S' represents the state before and after the transformation.

a) The Substitute byte transformation:

The substitute byte transformation operates on each of the state bytes independently and changes the value. The RIJNDAEL S-box is used for the byte substitution transformation stage. The S-box specifications are available in the AES specification. For an example the input state byte value of EA will be substituted by a new value of 87 and so on. Fig3 shows the substitute byte transformation.

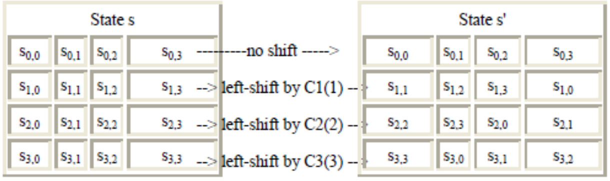


$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$					$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	=	S-box	=		$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$					$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$					$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

Fig 3 S-box transformation

b) Shift row transformation

It is a simple permutation on the substitute by transformed matrix. The first row of the state is not altered. For the second row, a 1-byte circular left shift is performed. In the third row a 2-byte circular left shift is performed and so on. Fig4 represents the forward shift row transformation.



State s					State s'			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$	---------no shift ----->	$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	--> left-shift by C1(1) -->	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$	--> left-shift by C2(2) -->	$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$	--> left-shift by C3(3) -->	$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

Fig 4 Shift row transformation

c) Mix Column transformation

The forward mix column transformation operates on each column individually. Each byte of a column is mapped into a new value that is a function of all the four bytes in that column. The mix column operation uses a predefined polynomial acting on the four values at one time in the Galois field GF (2^8). Here the addition is represented by the bitwise XOR operation and multiplication is by 1-bit left shift operation followed by the conditional bitwise XOR operation.

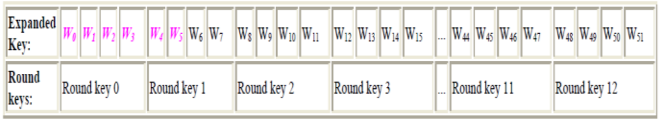
d) Add Round Key Transformation

In the forward add round key transformation, called the Add Round Key, the 128 bits of the state or bitwise XORed with the 128 bits of the round key. We need to derive different key for each round which is to be applied during each round of the encryption operation.
These keys are called as the round keys and each will be the same length of the block. N_b 32bit words are denoted by W.
The AES original specifications define a key schedule by which the original cipher key is used to form an expanded key.
The expanded key size is equal to the block size times the number of encryption rounds incremented by a value of 1, which will provide N_r+1 different key.

For example a 128 bit AES key will be expanded to a 44 32bit word key that can be used for 10 rounds of transformation.

The original cipher key occupies the first portion of the expanded key and is used to produce the remaining key material.

The AES 192 bit key will 52 32 bit -word key and the 256 bit version will have 60 32 bit word key that can be used for the 14 rounds of transformation. Fig 4 represents the expanded key version used in the AES 128 bit key length. Recall that the round key is the length of the block used. The key expansion algorithm [4] is used to derive the expanded key that is used as a key material for each round of transformation.



Expanded Key:	W_0	W_1	W_2	W_3	W_4	W_5	W_6	W_7	W_8	W_9	W_{10}	W_{11}	W_{12}	W_{13}	W_{14}	W_{15}	...	W_{44}	W_{45}	W_{46}	W_{47}	W_{48}	W_{49}	W_{50}	W_{51}
Round keys:	Round key 0				Round key 1				Round key 2				Round key 3				...	Round key 11				Round key 12			

Fig 4 Key Expansion Process

To make the AES encryption algorithm to be probabilistic in nature we need to use an additional input value called the initialization vector. For a 128 bit AES key length the initialization vector used is 16 bytes. The AES in the Cipher Block Chaining mode (CBC) makes the encryption algorithm to behave as probabilistic, for the same plain text data we will be obtaining different cipher text. In the CBC mode each block of the plain text data is XORed with previous cipher text blocks before being encrypted. This way each cipher text blocks depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector is used in the first block. The mathematical equation representing the CBC encryption is given below.

$$C_i = E_K(P_i) \oplus C_{i-1}, \quad C_0 = \text{Initialization vector.}$$

The Mathematical equation for the decryption in the CBC mode is given below.

$$P_i = D_k(C_i) \oplus C_{i-1}, C_0 = \text{Initialization vector.}$$

An initialization vector is added to the first plain text block to make each CBC encryption nondeterministic. The first cipher c1 depends on the plain text P1 and the initialization vector. The second cipher text c2 depends on c1 and P2 and so on. The third cipher text c3 depends on c2 and P3. Fig 5 represents the AES probabilistic encryption in the cipher block chaining mode.

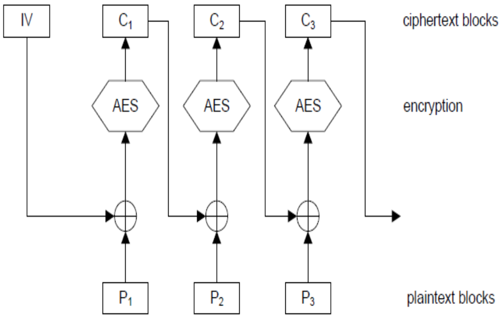


Fig 5 AES Probabilistic encryption

The Cipher block chaining mode is very efficient to implement in hardware. The properties of the IV depend on the cryptographic scheme used. The randomized IV's to provide the property of uniqueness. In the stateful based encryption schemes the sender and the receiver can use a common initialization vector state, which is updated in a predefined way at both the sides. In the stream cipher based encryption schemes like the RC4 uniqueness is crucially important as plaintext be trivially be recovered. The pseudo code for the AES probabilistic encryption based on the CBC mode is given in Fig 6

```
Rijndael (State ⊕IV, Cipher key)  /* for
block 1
     {
   Key expansion (Cipher key, Expanded Key); /*i/p
4 word key and o/p 44 word expanded-key (1408bits)
     Add Round Key (State, Expanded Key); /* Initial
round with first 4 words of expanded-key (128bits)
         for(i=1; i<Nr; i++) {
           Round(State,ExpandedKey + Nb*i) ; /* upto 9
           rounds
         Final Round (State, Expanded Key + Nb*Nr);/
           *10th round
         Out (Final Round) = C1;
         }
Rijndael (C1 ⊕ State, Cipher key) / * for block2
         {
         Key expansion ();
         Add round key ();
         Round ();
         Final round ();
         Out () =
         }
```

Fig 6 Pseudo code for AES-CBC

IV SIMULATION RESULTS

Network Simulator-2 (NS2) is used as the simulation tool. The performance metrics such as the throughput, energy and the pack delivery ratio in terms of the AFC (Ally Fusion Center) is determined. The simulation parameters are as follows.

MAC layer protocol with priority extension	MAC 802.11.15.4
Number of nodes	21
Simulation area	1000 x 1000 m
Initial energy of the nodes	100 J
Data rate	2 packets/ sec
Data packet size	512 bytes
Routing protocol	DSR
Channel type	Channel/Wireless
Antenna type	Omni directional
Simulation time	30 seconds

Table 1 Simulation Parameters

SNR (db)	P_b^{EFC}	P_b^{AFC}
0	0.930	0.470
1.9	0.900	0.462
2.6	0.880	0.458
3.4	0.850	0.450
4.0	0.800	0.440
5.0	0.730	0.432
6.5	0.650	0.350
7.0	0.550	0.250
8.5	0.200	0.200
9.4	0.100	0.100
10	0.090	0.010

Table 2 Probability bit error analysis

The simulation result of Ally Fusion Center (AFC) throughput analysis in presence of the passive eavesdropper (EFC) is shown in the Fig 6. The glitches that occur in our simulation results are due to the eavesdropping activity of the enemy fusion center, while the data packets encrypted by using the probabilistic encryption scheme.

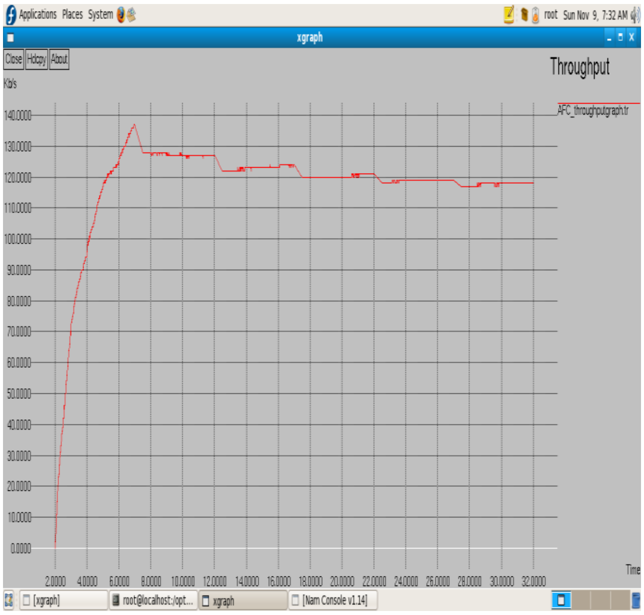


Fig 6 AFC throughput analysis

The simulation result of the packet delivery ratio of the AFC in the presence of passive eavesdopper is given in the Fig 7.

The eavesdropping activity by the enemy fusion center will reduce the packet delivery ratio. As the data packets from the sensor nodes are intercepted by the EFC through the wireless broadcasting channel, the ratio of the successful packets that reach the destination (Base station) via the the ally fusion center is given in the AFC packet delivery ratio simulation result. The glitches that occur in our simulation results are due to the passive eavesdropping action by the enemy fusion center.

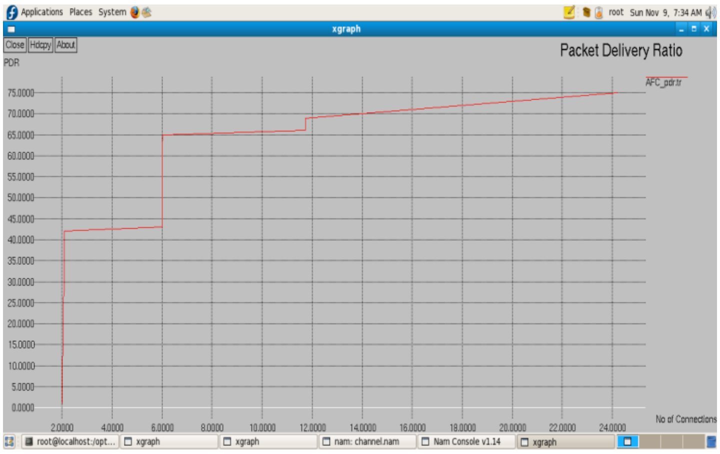


Fig 7 AFC Packet delivery ratio

The AFC energy analysis simulation result is show in the Fig 8. encryption and decryption consumes most of the battery power in the sensor network. The network life time depends upon how we are degrading the performance of the enemy fusion center.

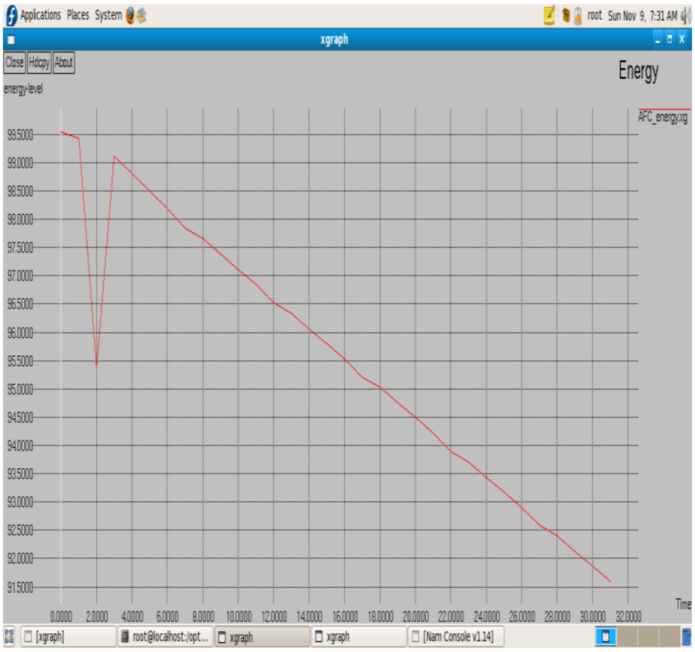


Fig 8 AFC energy analysis

The simulation result of the Probability bit analysis is given in the Fig 9. It determines the performance of both AFC and EFC with our proposed probabilistic cipher. The proposed probabilistic encryption scheme reduces the eavesdropping performance of the of the enemy fusion center and thereby reducing the detection probability of the EFC. The Routing analysis of the of the data packets in the presence of the enemy fusion center are given by probability of bit error analysis and the corresponding channel SNR.

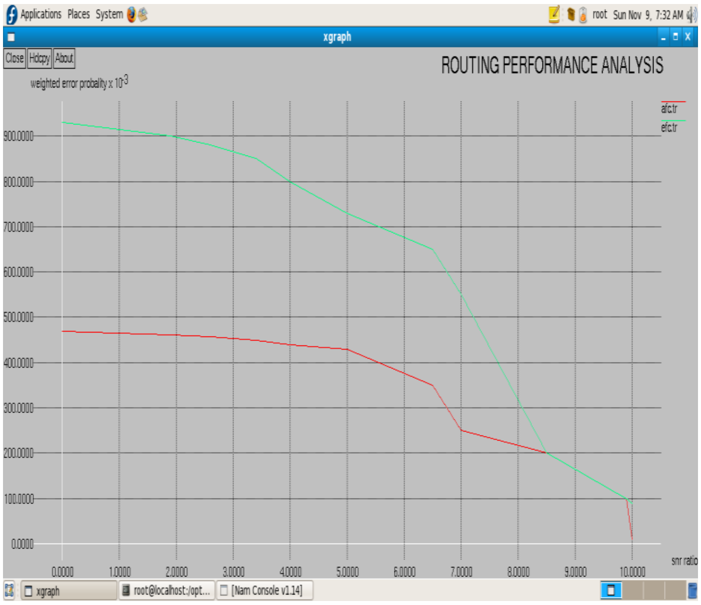


Fig 9 Probability Bit error analysis

V CONCLUSION AND FUTURE WORK

In this paper, the problem of passive eavesdropping via an enemy fusion center was investigated against secure routing of data from the sensor nodes to the ally fusion center. The probabilistic encryption scheme based on the advanced encryption standard, cipher block chaining mode is used to give more semantic level security against passive eavesdropping. The probability of bit error analysis was used as the routing performance metric for both AFC and EFC. The AES based probabilistic encryption scheme implemented gives more semantic level security.The secure detection against malicious node data transmission and the implementation shamir'secret sharing and the probability of detction by using the sub optimal and optimal decision rules will be investigated in our future work.

VI REFERENCES

[1] Reza Shooshabi, Student member IEEE "Optimal Probabilistic encryption for secure detection in wireless sensor networks, IEEE Transactions on information and forrensics and security, March 2014.

[2] Stefano Marano, Vincenzo Matta, and Lang Tong" Distributed detection in the presence of byzantine attacks" IEEE Transactions on signal processing, January 2009.

[3]. Hyoungsk, Steven W. McLaughlin "Cooperative secure transmission for distributed routing in wireless sensor networks", IEEE Transactions on signal processing,2011.

[4]. R.Shooshabi, Mort pour " Scalable PHY-layer security for distributed detection in wireless sensor networks", IEEE Transactions on information security, August 2012.

[5].http:// www.atmel.com/

[6] http://www.isi.edu/nsnam/ns/tutorial/