RESEARCH PAPER | Engineering | Volume : 3 | Issue : 8 | Aug 2013 | ISSN - 2249-555X

FHSS Based Anti-Jamming Method for Secure Communication in Wireless Sensor Networks

KEYWORDS: Wireless Sensor network, jamming, anti-jamming, energy efficiency, channel efficiency

Prakash J. Parmar
Sinhgad Institute of Technology, Lonavala Pune University India

Sachin D. Babar
Sinhgad Institute of Technology, Lonavala Pune University India

ABSTRACT *Jamming is the biggest threat to wireless network security, especially to wireless sensor networks where a network consists of small nodes with limited energy and computing resources. So it is very difficult to adopt the available anti jamming methods to implement over Wireless sensor networks. In this article we propose a frequency hopping spread –spectrum (FHSS) based anti-jamming method for secure communication in wireless sensor network. Our analytic results show the improvement of channel efficiency in the presence of jammer node(s).*

INTRODUCTION

Sensor networks using distributed wireless technology are utilized in many applications, such as health monitoring system, building or infrastructure access systems, disaster relief and tsunami warning systems. Some of these applications lack security due to resource constraints, thus, resulting in reduced Quality of Service (QoS). In resource constrained network such as WSN, traditional security schemes cannot be applied. Hence, need for new security measures to maintain network functionality without sacrificing network performance. In this paper, different jamming attack on WSN is considered, and a defense mechanism is proposed.

In WSN, a multitude of wireless sensors are interconnected by means of RF communication links. The functionality of the nodes in this application includes sensing, collecting and distributing dynamic information within the network. Energy usage is a key issue as the sensors are typically tiny and wireless with limited memory and functionality given the fact that the batteries have a limited power supply. Hence, difficulties arise during computation [2]. A network or node can be affected by many kinds of DoS attacks including those, forcing nodes to be in idle or stand-by mode. This affects the performance of the node and the network. In worst cases, the attacked node continues to communicate to its neighbors and finally depletes all its power and declares itself dead, which reduces the networks coverage area. Hence, WSN need to be adaptable with minimal wait period (network set up need to be modified). The communication links in such an unpredictable environment (node failures) are kept functional by applying a robust routing algorithm.

In this paper a novel approach is proposed, we use a frequency hopping spread –spectrum (FHSS) based anti-jamming method for secure communication in wireless sensor network. Finally our paper organizes as, in section 2 we analyze previous work and compare their result and show their constraint. We proposed our method in section 3 with mathematical model in section 4. In Section 5 Numerical Analysis result and their graph shows. We conclude the paper with the section 6 discussing the conclusion and future work.

RELATED WORKS

Broadly we can categories security and jamming in three categories: Transmission security, Attack Security and Hybrid Security. Transmission security includes eavesdropping and privacy threats. In Attack security, the main objective of a node is to listen the ongoing communication and attack on the network Hybrid Security includes the characteristic of both transmission and attack security issues. In this paper our main objective is to tackle with the hybrid security issue. Fig 1 shows brief classification of all these three categories

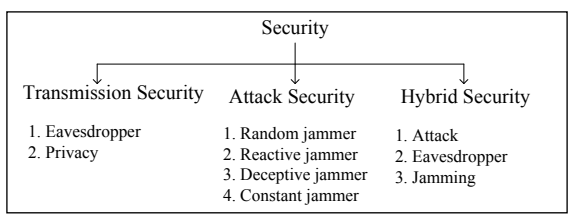

Figure 1: General classification of jamming and security

JAMMING ATTACKS

There are many different attack strategies an adversary can use to jam wireless communications [6], as depicted in Fig. 1.

Constant jammer: The constant jammer continually emits a radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal or a normal wireless device that continuously sends out random bits to the channel without following any MAC-layer etiquette. In general, the MAC protocol allows legitimate to send data packet if channel is sensed idle. Thus a constant jammer holds the channel by sending constantly dumpy packets.

Deceptive jammer: Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions.

As a result, a normal communicator will be deceived into believing there is a legitimate packet and be duped to remain in the receive state. For example, in Tiny OS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected.

Random jammer: Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for a while, it turns off its radio and enters a "sleeping" mode. It will resume jamming after sleeping for some time. During its jamming phase, it can behave like either a constant jammer or a deceptive jammer.

Volume : 3 | Issue : 8 | Aug 2013 | ISSN - 2249-555X

This jammer model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply.

Reactive jammer: The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. As we shall see in the following section, these methods are relatively easy to detect. An alternative approach to jamming wireless communication is to employ a reactive strategy. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. One advantage of a reactive jammer is that it is harder to detect.

As given in [6] , Figure 2 shows the different types of jammers in attack category.

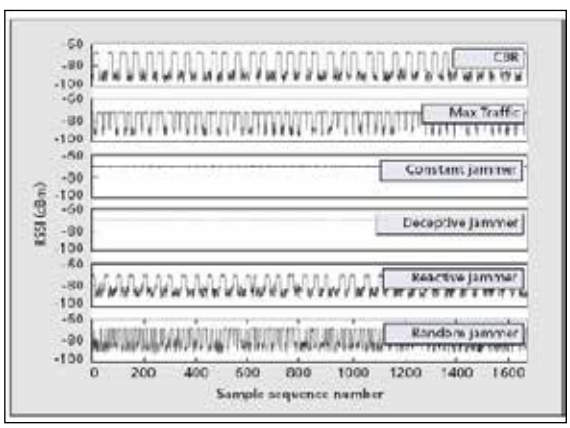

Figure 2: Jamming Type [6]

In this paper we have studied various jamming and security technique which we briefly summaries as

Paper [1] work at physical layer to provided security using OFDM signal, which provided high security. In this [1] proposed method is fast and channel independent which uses cooperative jamming technique but it is not suitable for WSN since it energy consumption and power for computation is more also system is complex.

Paper [2] proposed a game theory solution for physical layer security work on un-trusted rely friendly jammer. Advantage of this is non zero secrecy rate can be achievable but is is difficult to implement also system complexity is more so it is also not suitable for WSN.

Paper [3] uses artificial Eigen vector method for channel estimation to provided security at physical layer but included estimation that required statistical data optimization which required high energy consumption.

Paper [4] cooperative jammer power allocation method which power management nice but scalability is big issue to implement it on WSN.

Paper [5] work on link layer attack security using minimal protocol knowledge requirement, this provide energy efficiency and improve scalability of system but in this proposed method based on TDM which required high degree of synchronization.

From above discussion it is clear that we cannot adopt any jamming and security technique over wireless sensor network so we need to develop a new to scheme to tackle a jamming an attack issues in WSN this is the key motivation of our research work.

PROPOSED SYSTEM

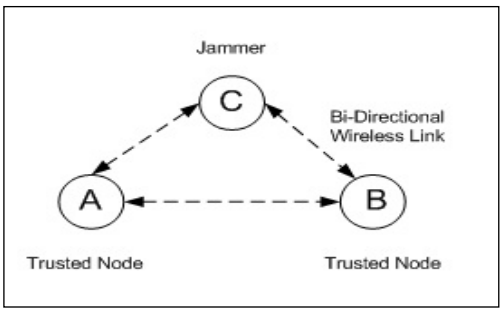

Figure 3: An Example Topology

Our propose system model is based on frequency hopping spread –spectrum (FHSS) technique with anti-jamming method for secure communication in wireless sensor network. In this we are proposeing a secrete sequence of frequency hopping between two trusted node to provider immunity against hybrid attack for a simplicity we assume network of three node as shown in fig-3 where node A and B are trusted pair and node C is working as an attacker/jammer. Figure 4 shows the self explanatory flow chart of proposed system.

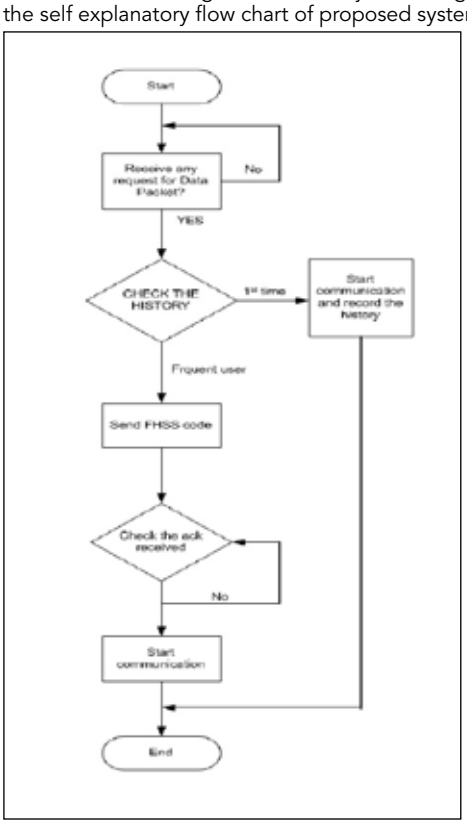

Figure 4: Flow Chart of Proposed System

SYSTEM MODEL

In this section we are developing system model based on [7]. To make our system model we made following assumptions:

- In general traffic pattern in the sensor network is of unsaturated traffic. So it is practical to assume that we will not face any collisions of packets due to low competition however we assume that we have a jammer within the network will be responsible for collision of transmitted message.
- The collision probability needed to compute τ (Transmission Probability) can be found considering aforementioned network topology. a packet from a transmitting

Volume : 3 | Issue : 8 | Aug 2013 | ISSN - 2249-555X

node encounters a collision if in a given time slot, at least one of the remaining (N − 1) node transmits simultaneously another packet, and there is no capture effect.

$$P_{col} = 1 - (1 - \tau)^{N-1} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

- We consider a scenario in which N nodes are uniformly distributed in a circular area of radius R, and transmit toward a common base node in the center of such an area.
- From [7], we compute normalize the channel efficiency defined as fraction of time the channel is used to successfully transmit payload bits:

$$S = \frac{P_t P_s E[PL]}{(1-P_t)\sigma + P_t(1-P_s)T_c + P_t P_s T_s} \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Where,

- P_t is the probability that there is at least one transmission in the considered time slot, with N stations contending for the channel, each transmitting with probability

$$P_t = 1 - (1 - \tau)^N \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

- P_s is the conditional probability that a packet transmission occurring on the channel is successful. This event corresponds to the case in which exactly one station transmits in a given time slot. This condition yields the following probability:

$$P_s = \frac{N\tau(1-\tau)^{N-1}}{P_t} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

- Tc and Ts are the average times a channel is sensed busy due to a jamming data frame transmission time and successful data frame transmission times, respectively. Knowing the time durations for ACK frames, ACK timeout, $\sigma\sigma$, data packet length (PL) and PHY and MAC headers duration (H), and propagation delay, $\tau_p\tau_p$ Tc and Ts can be computed as follows:

$$Tc = H + PL + ACK\ timeout \quad \ldots\ldots\ldots\ldots (5)$$

$$Ts = H + PL + SIFS + \tau_p + ACK \quad \ldots\ldots\ldots\ldots (6)$$

- E[PL] is the average packet payload length.
- $\sigma\sigma$ is the duration of an empty time slot.
- We are assuming BEB backoff algorithm for sensor network
- We assume that packet will be drop after few retried
- We are assuming packet format as shown in figure-5 [8].

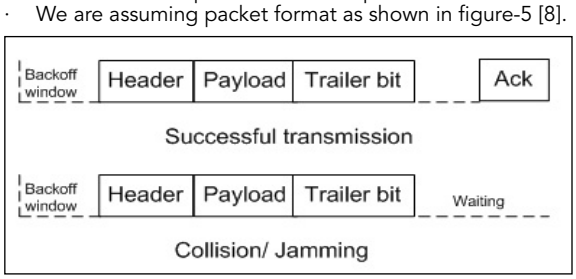

Figure 5: Packet diagram

NUMERICAL ANLYSIS

In this section we consider one toy topology, as shown in figure 3, to show the analysis of our propose system. For our calculation we have consider the following parameter, as summarized in table-2, based on [7]. We have done our all calculation based on aforementioned formulas. In nut shell our result are showing the jamming / attacked effect on various network performance matrix.

Fig -6 illustrates the calculation between channel capacity and number of nodes. From the figure-6 we can conclude that as the number of nodes is increasing the channel capacity starts decreasing. The reason is that increasing number of nodes also increase the competition and hence collision. In this paper jammer nodes are giving the same result as increase in channel access competition. This result is the main motivation of our work.

TABLE 2-: SYSTEM PARAMETER

Parameter	Size (Bytes)	Time duration (micro sec) = Bits*4
Payload size	128	4096
	256	8192
	512	16384
	1024	32768
MAC header	12	384
PHY header	10	320
ACK	10	320
Back-off window time	-	250
Collision time	-	150

***Note: For Calculation Speed = 250 kbps i. e. 4 micro sec per bits**

Figure 7 shows the graph between Pt and tau. It is important to note that increasing in tau value will increase the Pt value which represents jammer effect in the network. Similarly, figure 8 shows the graph between Ps and tau. As shown in the figure 8 increases in tau decrease the Ps value. The reason is that this increase in tau will increase the competition i.e. Channel is captured by Jammer node.

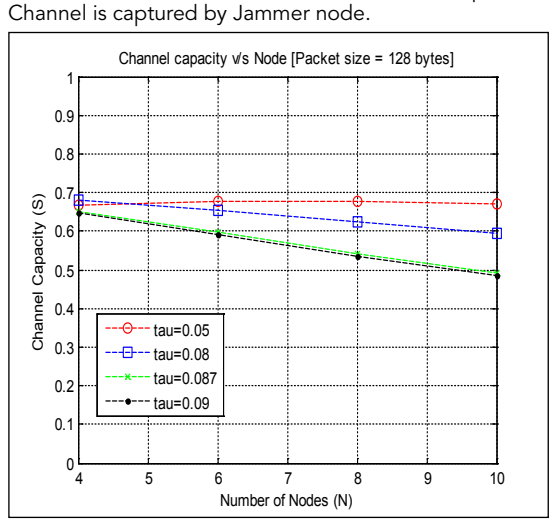

Figure 6(a): Channel Capacity versus Node [Packet size = 128 bytes]

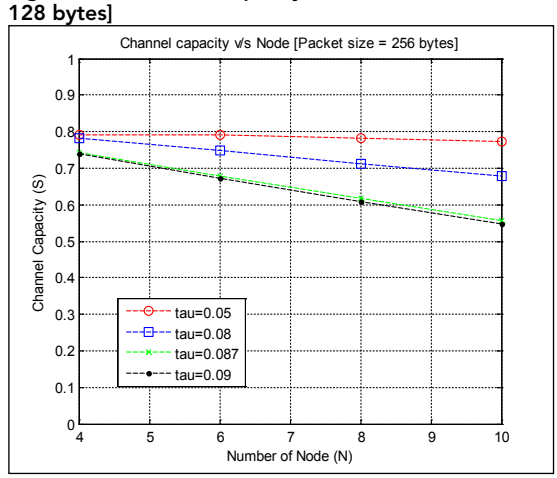

Figure 6(b): Channel Capacity versus Node [Packet size = 256 bytes]

Volume : 3 | Issue : 8 | Aug 2013 | ISSN - 2249-555X

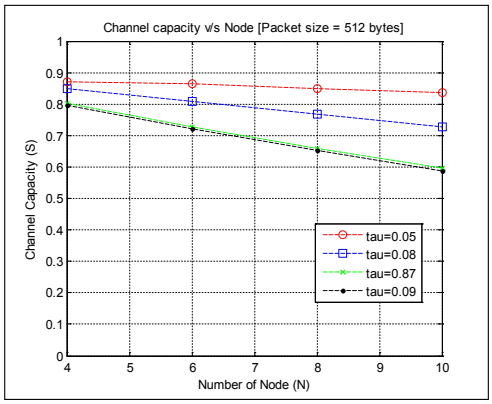

Figure 6(c): Channel Capacity versus Node [Packet size = 512 bytes]

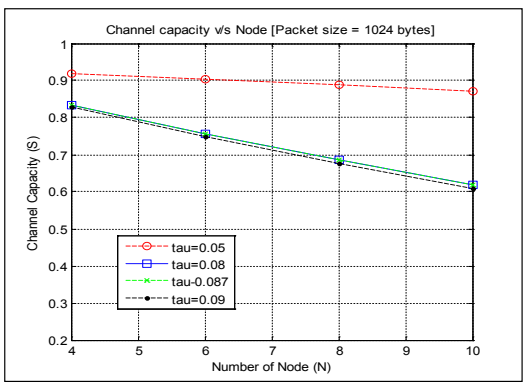

Figure- 6(d): Channel Capacity versus Node [Packet size = 1024 bytes]

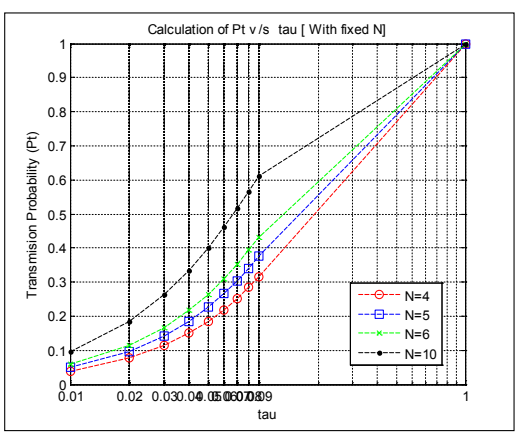

Figure 7: Pt versus tau [with fixed N]

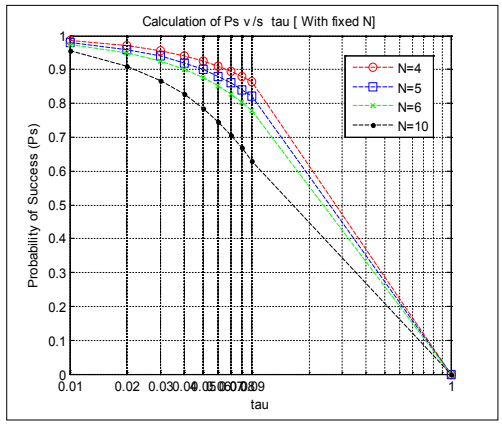

Figure 8: Ps versus tau [with fixed N]

Finally, figure 9 shows the clear affect of jamming in the given analysis. From equation (2) we can see that channel capacity is proportional to Ps and decrees in Ps and vice-versa. This is nothing but the jamming affect in the given network.

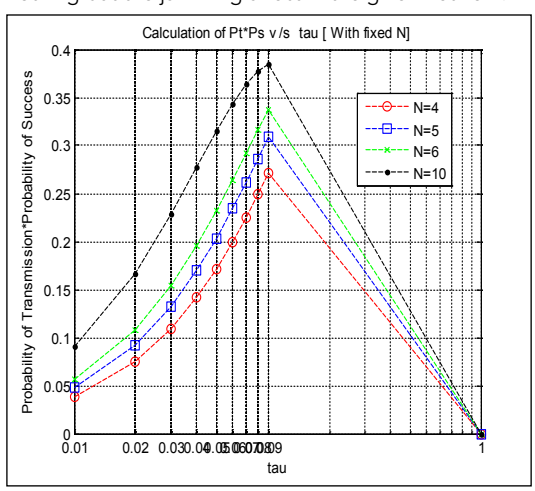

Figure 9: Pt*Ps versus tau [with fixed N]

CONCLUSIONS

In this paper we have studied security and jamming problems in WSN. We have reviewed several related works on security and jamming and proposed a frequency hopping spread –spectrum (FHSS) based anti-jamming method for secure communication in wireless sensor network. We also developed a mathematical model for our proposed method and based on that we have done exhaustive numerical analysis. Our results showed an improvement in throughput result under the jamming condition. Currently we are implementing our proposed method for simulation and expecting a good match between theoretical and simulation results.

Table 1: Comparisons between Different Proposed Security Method

Reference Number	[1]	[2]	[3]	[4]	[5]
Characteristics	Physical layer ,OFDM Signal	Un-trusted rely Friendly jammer, game theory solution	Physical layer, Channel estimation, Eigen vector, artificial intelligence	Physical layer, Cooperative jammer, power allocation method	Link layer, attack security, minimal protocol knowledge required
Advantage	High Security ,Channel Independent and non-cooperative Method	Non zero secrecy rate possible, cooperative method	Estimation error included, cooperative method, artificial method	Power management, suboptimal power allocation solution	Energy efficient , scalable, minimal protocol knowledge required, Simple algorithm,
Disadvantages	Need Statistical data, time synchronization,	Difficult solution, optimization	Statistical data required, optimization	scalability overhead	TDM based system, high degree of synchronization, suboptimal solution

Volume : 3 | Issue : 8 | Aug 2013 | ISSN - 2249-555X

Complexity	High	High	High	< low	low
Adoptable for sensor network	No [energy efficiency & Computation power]	No [energy efficiency & Computation power]	No [energy efficiency & Computation power, scalability]	Could be very difficult to adapt[energy efficient and scalability]	Adaptable but required s synchronization,

REFERENCE [1]Gollakota, S.; Katabi, D.; , "Physical layer wireless security made fast and channel independent," INFOCOM, 2011 Proceedings IEEE , vol., no., pp.1125-1133, 10-15 April 2011 | [2]Rongqing Zhang, Lingyang Song, Zhu Han and Bingli Jiao "Physical Layer Security for Two-Way Un trusted Relaying with Friendly Jammers" IEEE 2012 | [3]James M. Taylor, Jr., Michael Hempel, Hamid Sharif, Yang "Impact of Channel Estimation Errors on Effectiveness of Eigenvector-Based Jamming for Physical Layer Security in Wireless Networks", IEEE CAMAD 2011 | [4]Lun Dong Homayoun Yousefi'zadeh Hamid Jafarkhani "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper",IEEE ICC 2011 | [5]Yee Wei Law, Lodwijk van Hoesel, Jeroen Doumen, Pieter Hartel and Paul havinga "Energy Efficient Link Layer Jamming Attack against Wireless Sensor Network MAC Protocol" , ACM , SACN November 7, 2005 | [6]Wenyuan Xu, Ke Ma, Wade Trappe and Yanyoung Zhang "Jamming Sensor networks: Attack and Defense Strategies" , IEEE network, , vol,pp 41-47 , May/June 2006 | [7]F. Daneshgaran, M. Laddomada. F. Mesiti, and M. Mondin, "Unsaturated Throughput Analysis of IEEE 802.11 in Presence of Non Ideal Transmission Channel and Capture Effect " ,wireless communication IEEE 27 Oct 2008 | [8]Alejandro Proa¯no, Loukas Lazos "Selective Jamming Attacks in Wireless Networks", IEEE 2009 | [9]Le Wang and Alexander M. Wyglinski"A Combined Approach for Distinguishing Different Types of Jamming Attacks against Wireless Networks" | [10]Faraz Ahsan, Ali Zahir , Sajjad Mohsin, Khalid Hussain "Survey on survival approaches in Wireless network against Jamming attack" - jatit 2009 | [11]M. Strasser, B. Danev, and S. Capkun. Detection of reactive jamming in sensor networks. ACM TOSN, 2010 | [12]Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou "Survey on Jamming Attacks and Countermeasures in WSNs" ,IEEE 2009 | [13]A. Arora and L. Sang. Dialog codes for Secure Wireless Communications. In IPSN, 2009 | [14]L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. "Cooperative jamming for wireless physical layer security", RXIV: 0907.4996, 2009 | [15]D. Tse and P. Vishwanath. Fundamentals of Wireless Communications. Cambridge University Press, 2005 | [16]L. Lai and H. E. Gamal. The relay-eavesdropper channel:Cooperation for secrecy. IEEE Trans. on Info. Theory, 2008 | [17]M. Tahir, Sigit P.W Jarot and M.U Siddiqi "Wireless Physical Layer Security Using Encryption and Channel Pre-Compensation" International Conference on Computer Applications and Industrial Electronics (ICCAIE 2010), December 5-7, 2010, Kuala Lumpur, Malaysia | [18] YI-SHENG SHIU AND SHIH YU CHANG "PHYSICAL LAYER SECURITY IN WIRELESS NETWORKS: A TUTORIAL" IEEE April 2011 | [19] J. Croft, N. Patwari, and S. Kasera. Robust uncorrelated bit extraction methodologies for wireless sensors. IPSN 2010 | [20] D. Tse and P. Vishwanath. Fundamentals of Wireless Communications. Cambridge University Press, 2005 |