International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-6)

Research Article

June 2015

Mechanisms for Detecting and Preventing Denial of Sleep Attacks and Strengthening Signals in Wireless Sensor Networks

Chandrakala. P. Goudar[1], Shubhada. S. Kulkarni[2]
[1]P G Student, Gogte Institute of Technology, Belagavi, Karnataka, India
[2]Asst Prof, Dept of C S E, Gogte Institute of Technology, Belagavi, Karnataka, India

Abstract-

Wireless sensor network is a partially scattered self-governing sensor to supervise various substantial characteristics such as temperature, pressure, vibration and sound. Sensor nodes are energized through batteries which cannot be recharged frequently. Low processing power and wireless connectivity makes the networks vulnerable to various attacks like sink hole, black hole, Sybil attacks, selective forwarding, worm hole, hello flood etc. Capacity can be conserved by designing different protocols and keeping the antenna in sleep mode 90% of time. Sleep time of the nodes are varied by designing MAC protocols depending on the communication need. However sleep time and life time of sensor node are diminished when attackers tries to use their knowledge of their basic MAC protocol. This problem is referred as Denial of sleep attack. The project is focused on two aspects like identifying malicious node and strengthening signals by detecting and preventing hello flood attack on a sensor network.

Keywords- Security, Sensor networks, Denial of sleep attack, MAC protocols.

I. INTRODUCTION

Wireless sensor network contains number of nodes which are connected to one another, that are partially scattered self-governing sensors that inspect physical conditions like temperature, sound, vibration, pressure, motion. The applications are varied; it supports a different application which includes auditing, tracing and supervising of objects. Particular functions include habitat monitoring, object tracing, nuclear reactor, fire revelation, and traffic supervising etc[1].

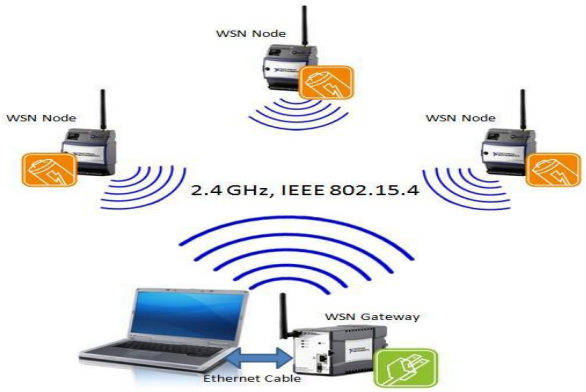

Fig .1: Communication between WSN nodes

Above given fig no.1 shows that the communication between the nodes, are executed by using the gateway[1]. Wireless sensor network (WSN) is prone to invasion as a result of its energy constraints. By a reason of narrow boundary, energy, processing constraints and cost sensors are out of scope of real world. It contains large number of nodes in a network where proper global id cannot be generated and are prostrate to breakdowns. The different modes of WSN are active mode and sleep mode which are used to conserve energy. Active mode displays that it is equipped to accept and dispatch data. In case of sleep mode it shows that node is not qualified to accept or dispatch the data. Energy utilised during sleep mode is minor than compared to energy utilised during the idle state of the sensor node. When no packet are message is arriving its advantageous to place the sensor node in sleep mode. However the issue arises when the sensor nodes are to kept in sleep mode because if the packet arrives then it will not be in a position to forward[6]. The key design considerations of wireless sensor network application are energy efficiency of MAC protocol wherein the radio must be maintained in a low-power sleep mode. Hence research is more concentrated on MAC protocols .Various MAC protocol with different objectives was proposed for wireless sensor networks. By reducing energy waste the proposed MAC protocol can be maintained in an energy efficient way[5].
The various reasons of energy loss in WSN are as follows[5]:

- Collision: If the receiver node accepts more than one packet at the same time, crash occurs. The packets that cause crash have to be discarded, and the re-transmissions are performed.
- Overhearing: The nodes receive packets that has to be detonated to other nodes and the energy is wasted by keeping its radio in receive mode.

- Control Packet Overhead: Only few number of control packets are allowed to broadcast the data. The battery life can be greatly impacted if the nodes are forced to stay awake for spurious control packets. Control packets used by the protocols are request to-send (RTS), and clear to- send (CTS).
- Over Emitting: The energy loss occurs due to the transmission of a message when the destination node is not ready.

A. DIFFERENT KINDS OF ATTACKS ON WSN

The different kinds of attacks on sensor networks are[3]:

1) *Denial of Sleep Attack:* This attack averts the radio from moving into sleep mode where the battery power will be completely drained. It causes consumption of the energy and battery of the sensor would take about months to completely deplete the targeted devices whereas denial of sleep attack is a clever attack that keeps the sensor nodes radio ON that drain the battery in only few days. Several solutions have been proposed to solve these types of attack but each has limited feature which are only concern to the particular layer.
2) *Wormhole Attacks:* In this attack an illegal node builds an imaginary tunnel through a low latency link that takes the messages from one part to another part of the network.
3) *Hello Flood Attacks:* Some protocols require nodes to send HELLO packets to advertise themselves to their neighbors. If a node receives such packet then it would assume that it is inside the RF range of the node that sent that packet. However, this assumption could be false because a laptop class adversary could easily send these packets with enough power to convince all the network nodes that the adversary is their neighbor. But the packets would get lost and would create a state of confusion, since the transmission power of those nodes is much less that the adversary node.
4) *Sybil Attacks:* The node has many identities and the coordinates are interchanged for productive packet routing so Sybil attack is considered as a risk to geographical routing protocols. Adversary node assumes to be in multiple places at same time.
5) *Selective Forwarding Attack:* In a selective forwarding attack, the messages would not propagate through the network because the malicious node avoids reaching destination or eliminate them.
6) *Sinkhole Attacks:* In a sinkhole attack, the compromised node will attract all the traffic to a certain area or the network creating a sinkhole.

B. ENERGY CONSUMPTION IN WSN

The two different modes are active mode and sleep mode that are used for energy conservation. Active mode of WSN node indicates that WSN node is in a position to accept and dispatch data. Sleep mode shows that WSN node is not ready to accept or dispatch the data[8]. The energy consumption in different level is show below.

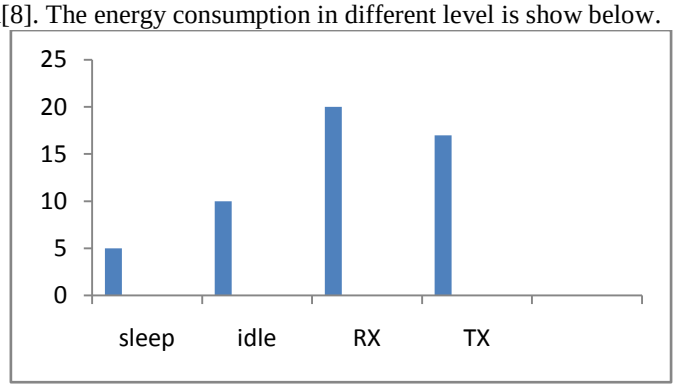

Fig . 2 Energy Consumption

Fig 2 indicates that the energy consumed during sleep mode is very less compared to the idle state of the sensor node. This tells that it is better to keep the sensor node in sleep mode when there are no packets.

II. BACKGROUND STUDY

In Denial of Sleep attack the nodes are awake when there is no traffic and the energy of the battery is completely utilized and the node will die. This act will lower the lifetime to a few days. The energy is wasted due to collision, overhearing, and over-emitting. Collision occurs when the receiver node receives more than one packet at a time and has to be discarded and retransmitted which increases the energy consumptions. Overhearing occurs when the node receive a packet destined for other node which causes the receiving node energy consumption by keeping its radio ON. The third energy consumption problem is control packet overhead where the minimum number of control packets are send for the data transmission as the staying the node wake for control packets consume the battery life. Another reason for energy consumption is trying to transmit the message when the destination node is not ready to accept which is performed on Data link layer[7]. MAC layer is used to overcoming this energy consumption attack. This clearly provides an idea the need of security in WSN. Due to the importance of this problem, there have been different distinct solutions that are proposed to solve it[8].

The different defending techniques to defend against denial of sleep attack and also tackles with the topics like behavior of compromised nodes, predefined time, one hop communication, cluster head selection and scalability.

- Absorbing Markov Chain (AMC) Model: The normal death time of each and every node in the network is used to detect sleep attack. It provides details of negotiated nodes and the action of every node can be analyzed using AMC model[1].
- Storm control mechanism: It was used for the purpose of lessening flooding and denial of sleep attacks. System tracks the frequency of accepted packets and an alert is triggered if frequency reaches above the accepted limit. Wireless transceiver is shut for a specified time as the node sends alert to the base station[1].
- An ant-based routing algorithm: Using guidelines such as age, energy and reliability, denial of sleep attack are identified.. The denial of sleep attack is prevented by using the concept of Packet authentication[1] .
- Scalable Secure Topology Maintenance Protocol (Sec-TMP): The protocol was volatile to sleep deprivation attacks which includes clustering. The nodes can be easily added into the network though there are existences of previous nodes, hence it was scalable. Sec-TMP takes help of one-hop communications[1].
- Random vote, round robin and hash-based scheme: Curtailing the impact of sleep deprivation charge and avoiding cluster head creation are taken care by these methods. The random vote scheme probable's in electing the cluster head. Addition of new nodes is achieved by using random vote clustering algorithm[1].

The different approaches to defend against sleep attack like hierarchical framework, clustered adaptive rate Limiting are elaborated below.

- A hierarchical framework based on distributed collaborative approach: There were two approaches in order to minimize the probability of false intrusion and to provide a stable and energy compelling composite WSN. The obtained values are analyzed with respect to the specified parameters to identify the adversary[2].
- Clustered Adaptive Rate Limiting (CARL): The attack was noticed by restraining the traffic when there is presence of abundant dangerous packets. Even in the presence of an attack the scheme provides improved throughput and enhances network period. It is performed implemented in S-MAC protocol[2].

A new MAC protocol which mitigates many of the effects of denial of sleep attacks by centralizing cluster management. MAC has several energy saving features which not only extend the network lifetime, but the centralized architecture makes the network lifetime more resistant to denial of sleep attacks. Other than single period and synchronization message, it has two contention period and different networks for sending the message within the clusters and outside the cluster through the gateway node. The MAC protocol Performance results show that G-MAC performs significantly better than other protocols in every traffic situations. The empty network case shows the protocol overhead and idle listening effects determined by the effective duty cycle-MAC has 95% duty cycle is weighted average of duty cycle of gateway node and other nodes. Attacker can gain access to network through gateway node. But attacker can only affect one node at a time because nodes alternate the gate way responsibilities based upon incremental increase in battery levels[4].

III. DENIAL OF SLEEP ATTACKS ON WIRELESS SENSOR NETWORK

Due to limited resources WSN is exposed to different attacks. Security on WSN becomes a priority steps. Sensor networks are amenable to certain malicious attacks due to severe constraints like limited processing capability, storage, energy, and limited bandwidth . It is recognized as one of the most dangerous threats and it was defined by Stajano and Anderson in 1999 and calls it as "sleep Deprivation torture"[[11]. The DS attack is a pruned to battery powered devices power supply to exhaust and decrease the lifetime. Defensive strategies are developed in MAC layer which safeguards radio usage in a productive manner. Functionality of transceivers are been controlled by MAC protocols present in the link layer and hence used to detect denial of sleep attacks, which utilizes extra power compared to neighbouring component[10].

In medium access control protocol, sensor node frequently moves to the fixed listen/sleep cycle. A time frame in S-MAC is divided into two parts: listening period and a sleeping period. During listen period the nodes interact with each other and dispatches some control packets such as SYNC, RTS (Request to Send), CTS (Clear to Send) and ACK (Acknowledgement)[6]. The sensor nodes can synchronize with all its neighbours by using a SYNC packet exchange. The purpose of the intruder in the DS attack is to enhance energy usage of the sensor node and reduce the battery life time. The attack prevents the node from going into negligible power sleep mode by ensuring sensor node working all the time. An attacker can change the MAC protocol and make the nodes to utilize more[9]

A. EFFECTS OF DENIAL OF SLEEP ATTACKS ON WIRELESS SENSOR NETWORK MAC PROTOCOL

Classification of Sensor network denial-of-sleep attack is performed on the basis of attackers knowledge of MAC layer protocol and overcoming authentication and encryption protocols. The four different sensor network MAC protocols, i.e., Sensor MAC, Timeout MAC, Berkeley MAC, and Gateway MAC[9]. Effectiveness and productivity can be quantified based on reasoning of selected attacks on S-MAC, T-MAC, and B-MAC. Though the attacker sleeps 99% of period, the cluster of nodes are active 100% of the period which is ensured by S-MAC. Even though attacker sleeps 92% of time, the victim node are active 100% of period by utilizing T-MAC. Without having the capability to infuse encryption, subtle attacks can be performed to lessen the battery power to a certain level. To reach current predictions, the sensor network must be powerful aganist denial-of-sleep which increases the network overhead[12].

B. WHY DOS IS IMPORTANT COMPARED TO OTHER ATTACKS

Denial of sleep attacks is the most fatal power consumption attack where in energy of nodes are utilized by the attacker and ensuring the nodes to be active where there is nil traffic. Loss of Energy is because of collision, overhearing, and control packet overhead and over-emitting which is performed on Data link layer .power management system has few scope to change into lower power category which is caused by penetration DOS attack and intentionally depleting the from years to days[10]. A jamming attack can be used by an attacker to drain energy and battery of sensor nodes, which takes about months to drain it completely the targeted device. Whereas the battery is drained in few days by sleep attack. In case of Denial of Sleep attack if the attacker knows the protocol used in the respective network, then it is not necessary to break link-layer encryption[5].

IV. THE PROPOSED SIMULATION METHODOLOGY

The architecture of proposed system for detection and prevention of hello flood attack and denial of sleep attack. The proposed method consists of three main steps :

- Network organization
- Identifying malicious node
- Selective authentication.

A. NETWORK ORGANIZATION

The process of nodes creation is started by writing the tcl script for the application.

The proposed system first creates the nodes using tcl script where the number nodes are to be is decided and fixed which is of fifty, then among the fifty nodes the source node and destination has to decided by the user by entering the node number along with attacker node number. The properties of the network are applied to the simulator and the node where the node are configured using the parameters specified in define options. The nodes are created using above parameters, provide initial (X,Y, for now Z=0) co-ordinates for mobile nodes It displays the nam window along the deployed number of nodes, sources and destination nodes .

B. IDENTIFYING MALICIOUS NODE

Once the ids are generated and assigned and identification of malicious node is performed. In the next process two options are provided for flood check status that is OFF and ON options. After deciding with the source destination and attacker node if flood check status is set with OFF mode then normal broadcasting process takes place where after every 0.1 second broadcasting of packets is performed and source will flood packets by using best path to reach destination. If the flood check status is ON then identification of malicious node is performed. If broadcasting takes place before 0.1 sec then it is considered as malicious node and those packets are not broadcasted. Whenever the attacker tries to flood the packets ,it updates with the message as found attacker and interrupts in normal broad casting it drops those packets and changes its path ,but slow rate in identifying the path till that there will be no flooding of packets from source to destination . Here the details of the attacker are obtained like its id and stored in the result file.

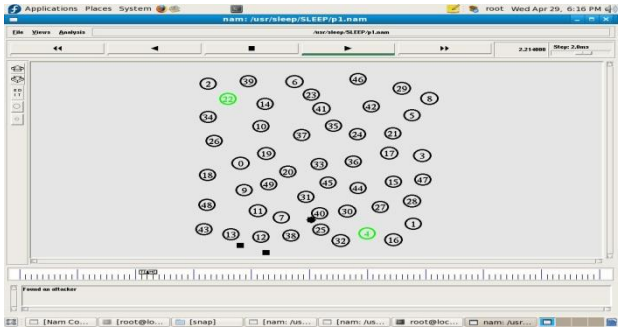

Fig. 3 No broadcasting of packets

The figure indicates source and destination node in green color. After every 0.1 second broadcasting of packets is done from the source to destination. It also indicates broadcasting of packets is stopped after 0.1 second since it is in slow rate in identifying the path.

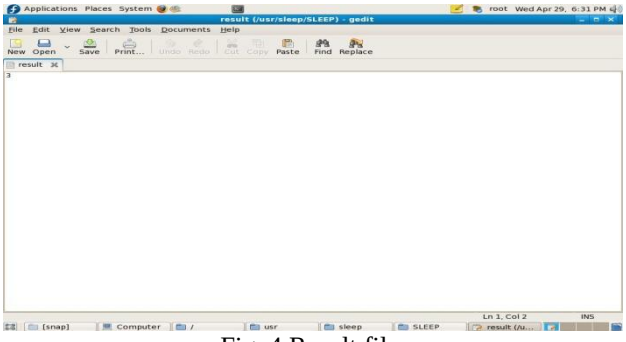

Fig .4 Result file

The above file displays a result file which provides the details of the attacker node which identified when the flood check status is ON. It provides the node number of the attacker node.

C. SELECTIVE AUTHENTICATION PROCESS

In selective authentication process it carries the details of the attacker from previous stage who tries to keep the nodes busy by sending the packets and avoiding them from entering into sleep mode. When source trys to broad cast packets it finds best path and forwards packets to destination. By using bootstrapping technique it also selects three category of nodes as 0,1,2 which acts as firewall , these firewalls identifies the packets send from the attacker and stops the node from flooding packets to destination.This way it avoids sleep attack.

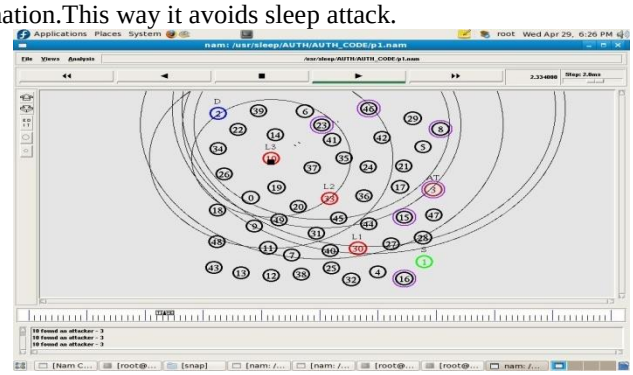

Fig .5 Broadcasting of packets

The figurer displays the source node in green colour and the destination node in blue colour. The attacker node in maroon colour and the firewalls are generated in red colour. It also indicates that the source node is broadcasting packets using a selected path to destination and the attacker node is also trying to broad cast packets using a certain path. Firewalls are taking care that the packets sent by attacker node are being dropped.

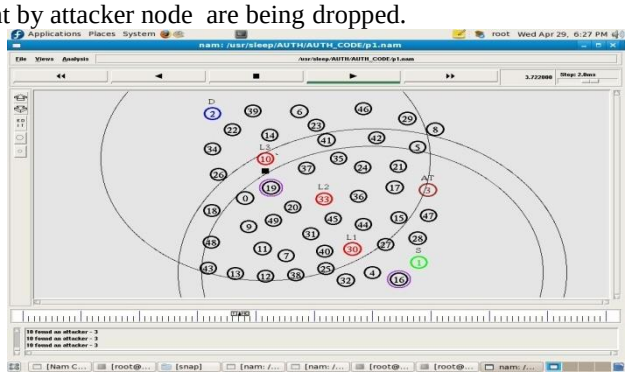

Fig. 6 Message displayed by firewall

The source node is broadcasting packets to the destination, as previously the attacker tried to broadcast the packets and the firewall node number 10 has identified and prevented the process. A message is displayed below indicating firewall found an attacker.

V. SIMULATION RESULTS

A. END TO END DELAY: The average time taken to route the packet from source to destination.

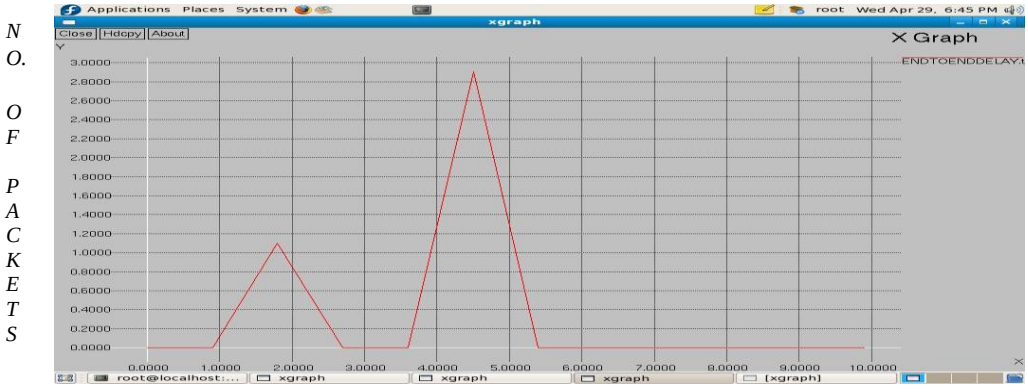

Fig.7 End To End Delay

B. PACKET LOSS: It is the measure of number of packets dropped by nodes due to various reasons.The lower value of the packet lost means the better performance of the protocol.

Packet lost = No. of packet send – No. Of packet receive

Fig.8 Packet Loss

C. PACKET DELIVERY RATIO: The packet delivery fraction is defined as the ratio of number of data packets received at the destinations over the number of data packets sent by the sources. In other words, fraction of successfully received packets, which survive while finding their destination, is called as packet delivery ratio.

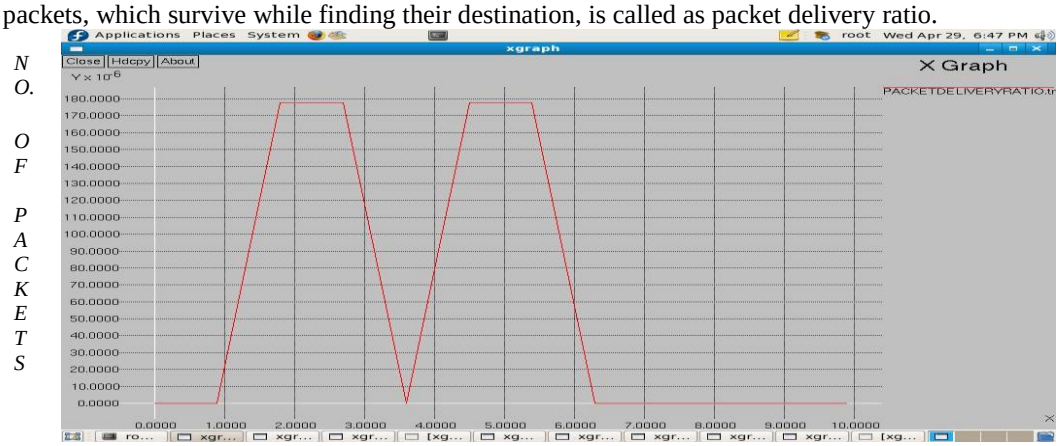

Fig .10 Packet Deliver Ratio

VI. CONCULSION

Security and energy efficiency is the most important concerns in wireless sensor networks (WSNs) designing, since they are prostrate to different types of network attacks and intrusion.The main principle of project is to identify the malicious node and collect the details of the attacker.The MAC protocols tries to reduces energy consumption of sensor nodes by keeping the antenna in sleep mode. The proposed method provides strong authentication which defends denial of sleep attack and triggers the defending mechanism only in the area of attack where the firewalls prevents the attacker from performing the task.

REFERENCES

[1] G.Mahalakshmi Assistant Professor, Department of Information Technology, NPR College of Engineering And Technology, TamilNadu, India. Dr.P.Subathra Professor, Department of Computer Science &Engineering, Kamaraj College of Engineering &Technology, Tamilnadu, India, journal of emerging technologies in web intelligence "A Survey On Prevention Approaches For Denial Of Sleep Attacks In Wireless Networks", vol. 6, no. 1, february 2014

[2] Ramandeep Kaur- Student, Dept. of C.S.E., Guru Kashi University, Talwandisabo, Punjab, India,Vinod Sharma Assistant Professor, Dept of C.S.E., Guru Kashi University, Talwandisabo, Punjab, India. International Journal of Innovative Research in Computer and Communication Engineering "A Survey on the Solutions for the Problems of Denial of sleep Attacks" , Vol. 2, Issue 1, January 2014.

[3] J.Steffi Agino, Priyanka, S. Tephillah and A.M.Balamurugan, IPASJ International Journal of Electronics & Communication (IIJEC) "Attacks And Countermeasures InWSN", Volume 2, Issue 1, January 2014

[4] SimerpreetKaur, Md. Ataullah, Monika Garg-Department of Computer Science and Engineering, Phagwara, India , Council for Innovative Research International Journal of Computers & Technology "Security from Denial of Sleep Attack in Wireless Sensor Network", Volume.4, No.2, March- April, 2013, ISSN 2277-3061.

[5] Manju.V.C,Research Student,Kerala University.Senthil Lekha.S. L,Dr.Sasi Kumar M,Kerala University, "Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks" Proceedings of2013 IEEE Conference on Information and Communication Technologies (ICT 2013).

[6] Muhammad Haneef and Zhong liang Deng, "Application specific analysis of MAC layer protocols used in Wireless sensor networks", IEEE 2010.

[7] Mohammad SayadHaghighi, Kamal Mohamedpour, "Securing Wireless Sensor Networks against Broadcast Attacks", International Symposium on Telecommunications, Aug-2008 , pp. 49-54.

[8] A Hamid, S Hong, "Defense Against Lap-top Class Attacker in Wireless Sensor Network", ICACT, Feb 2006,pp-314-318. Business Media, 2008.

[9] Luis E. Palafox, J. Antonio, "Security in Wireless Sensor Networks", IGI Global publishing, Chapter 34, pp. 547-564, 2008.

[10] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, "Effects of denial of sleep attacks on wireless sensor network MAC protocols", in Seventh Annual IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop, pp. 297304, June 2006

[11] Al-Sakib Khan Pathan-Department of Computer Engg. Kyung Hee University, Korea Hyung-Woo Lee Department of Software Hanshin University, Korea Choong Seon Hong-Department of Computer Engg Kyung Hee University, Korea "Security in Wireless Sensor Networks: Issues and Challenges" , ISBN 89-5519-129-4 ,Feb. 20-22, 2006 .

[12] W. Ye, 1. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks", IEEE/ACM Transactions on Networking, vol. 12, no. 3, pp. 493506, June 2004.

[13] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Elsevier Ad Hoc Networks 1 pp 293–315, 2003.

[14] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, "Effects of denial of sleep attacks on wireless sensor network MAC protocols", to appear in IEEE Transactions on Vehicular Technology.

