Securing Wireless Sensor Network from Denial of Sleep Attack by Isolating Nodes

Simerpreet Kaur
Lecturer, Department of Computer Science
Malout Institute of Management and Information Technology
Malout, Punjab

Md. Ataullah
Assistant Professor, Department of Computer Science
Lovely Professional University
Phagwara, Punjab

ABSTRACT
The Wireless Sensor Network has gained advancement in new era technology. Beside a small size, sensors have the feature of sensing and collecting the data and small and are used in many areas ranging from detecting temperature to providing security for the home. Other than these, sensors are also used for traffic management and military applications. To extend the network lifetime, sensor nodes are placed in sleep mode. Denial of sleep is a type of denial of service attack which prevent nodes from going into sleep mode and resulting in short network lifetime. To secure the system, various techniques are used. This paper represents a more efficient and feasible solution to solve the problem of denial of sleep attack of isolating the nodes to be used in hierarchical clustering.

Keywords
Denial of Sleep Attack, Hierarchical Cluster, Sleep Mode, Wireless Sensor network.

1. INTRODUCTION
The wireless sensor network (WSN) consist of several nodes where each node is connected to one or more sensors. WSN has applications in many important areas, such as the military, homeland security, health care, the environment, agriculture, and manufacturing. Providing security in Sensor networks is not an easy task. Compared to conventional desktop computers, severe constraints exist since sensor nodes have limited processing capability, storage, and energy, and wireless links have limited bandwidth.

The worst energy consumption attacks in WSN is denial of sleep attack in which attacker consumes the sensor nodes energy by making the nodes wake even when there is no traffic to hold. In this way sensor nodes energy is consumed totally and sensor nodes die. Due to which the lifetime of the wireless sensor network decreases by causing the radio of the receiver ON draining the battery in only a few days. Energy is wasted due to Collision, Overhearing, and Control packet overhead and Over-emitting. This energy consumption attacks is performed on Data link layer [11].

From this it can be understood that security against the denial of sleep attack is a very important part. Clustering is an efficient technique for sending data more efficiently and securely to access point. Network Structure is divided into Flat Based, Hierarchical Based and Location Based.

Flat routing protocols distribute information as needed to any sensor node within the sensor cloud and here all the nodes play the same role and there is no hierarchy. Flat routing uses two techniques Flooding and Gossiping where no routing algorithm is used simply the packet is sent to all the sensor nodes or sensing node decide where to send data. Hierarchical routing sets the nodes to form a cluster so as to conserve energy. The hierarchical based cluster includes Leach protocol, Pegasis protocol and TEEN protocol where cluster and chains are formed to send the data. Location-Based requires location information for sensor nodes so as to calculate the distance between two nodes. The geographic and energy aware routing protocol is used for minimum consumption of energy and local and external storage is a main consideration in Location protocol. The Energy consumption by collision, idle listening and over-emitting in cluster are common. And these attacks make the Network lifetime less.

Denial of Sleep Attack is a technique which prevents the radio from going into sleep mode. Many techniques introduced its impact on battery –powered mobile devices. An attacker might use jamming attack to consume the energy and battery of the sensor but it would take about months to completely deplete the targeted devices whereas denial of sleep attack is a clever attack that keeps the sensor node radio ON that drain the battery in only a few days. In this paper we are only concern with the denial of sleep attack which is a type of denial of service attack on data link layer [2].

The data link layer is divided into two sub layer MAC layer and Link layer. The link layer coordinates the access to the physical medium linking a network node. The link layer decides when the radio should transmit frames; listen to the channel to receive data and sleep to conserve energy.

MAC protocols operate at the link layer and these protocols are used for detecting denial of sleep attacks because they control the functionality of the transceiver, which consumes more energy than any other components. The MAC protocol is responsible for managing the radio of sensor, and radio is the main source of power consumption.

To design a secure MAC layer it is crucial to understand the normal and malicious sources of energy loss, which is essential to design the power control system [2].

The objective of the Research work is to increase the network lifetime by effectively saving the energy which to be consumed by denial of sleep attack. Although idle listening is still the problem which creates problems.

The rest of this paper is organized as follows. In Section II describe the work related to the research topic. Section III gives the detailed description of implementation with snapshots and its comparison with existing scenario. In Section IV we compared implemented protocol with leach protocol and Section V we conclude.

2. RELATED WORK

Various papers which are defining solution for solving the denial of sleep attack for adding security to WSN. Some of the techniques are mentioned below:

G-MAC protocol is proposed which mitigates many of the effects of denial of sleep attack by centralizing cluster management. G-Mac is a standard protocol used in various applications. This protocol increases the network lifetime and make the network more resistant to denial of sleep attack [4].

Cluster Adaptive Rate Limiting techniques based on the rate limiting approach at MAC layer. The technique effectively used in B-MAC protocol and it maintain the network lifetime and better throughput at a time even in sleep deprivation attack [6].

Effective scheme is proposed employing fake schedule switch with RSSI measurement aid. The sensor nodes can reduce and weaken the harm from exhaustion attack and on the contrary make the attackers lose their energy so as to die. Here the energy consumed and the packet drop ratio has been less compared to a scenario without fake schedule [7].

Sleep deprivation attack detection technique also uses the hierarchical framework with detection mode where the cluster is further divided into the sector. This technique gives the effective way to solve the Denial of sleep attack and also increases the network lifetime but with problem of leaf node can be easily affected by the attackers [8].

Dynamic Sleep Time is proposed, where rather than the using fixed sleep time which minimizes the energy wasted in idle channel which increases the network lifetime but less effective for denial of sleep attack [9].

Distributed Wake-up scheduling scheme for data collection is used which increases both energy conservation and low reporting latency. This scheme is proposed for 1-hop and 2-hop neighbors. Power Saving and latency are improved to prolong the network lifetime and freshness of data [10].

3. IMPLEMENTATION

In WSN, leach protocol is used as hierarchical cluster for sending data where the only single cluster head is used, other than leach there are various multilevel clustering where two cluster heads are used for energy efficiency. We have created a hierarchical cluster with no particular cluster head but with nodes having different energy levels. Nodes having greater energy can detect any anomalous packet using detection mode.

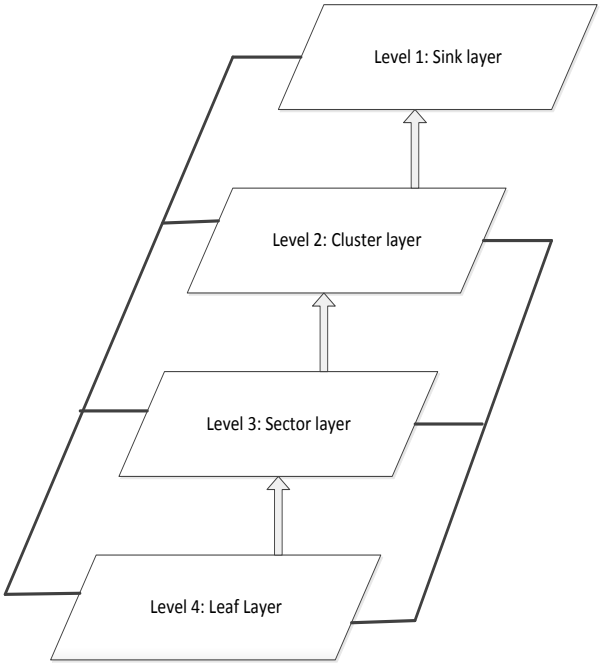

Fig1: Hierarchical level of cluster

Following steps shows cluster formation:-

Step I: A Sink gateway node sends the message to neighboring nodes and forms a cluster to send the data.

Step II: We have made 4 levels in the decreasing order of energy.

Step III: Set detection mode for higher order Energy levels nodes for checking the packet as anomalous or not and accordingly set the tag as valid or invalid for packet.

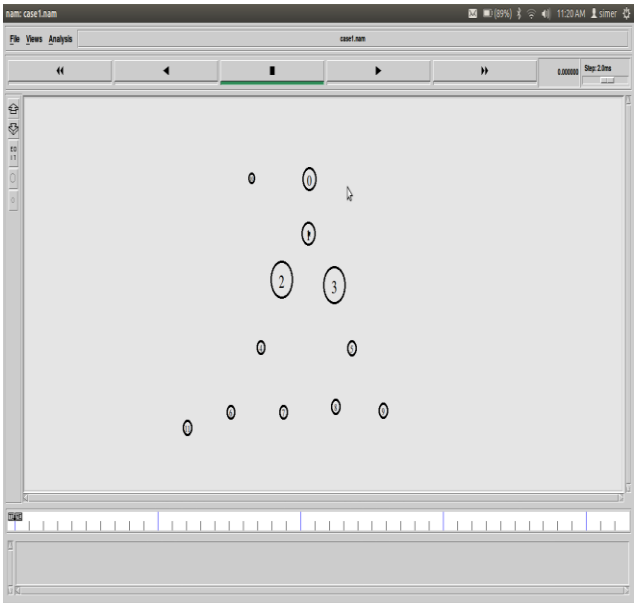

Fig 2: Cluster Formation

Sensor node is differentiated from a simple mobile node as they are having schedule time which contains node's active and sleep schedule time. Sensor node can transmit and receive messages in its active schedule and goes to sleep schedule in order to conserve energy. As the lower level nodes have less energy so their task is only to sense the data and goes to sleep mode when there is no packet to sense. We have included three cases on the basis of leaf nodes schedule time.

Following steps shows three cases:-

1. When the packet comes to a leaf node, in its active schedule.

a) Leaf node will sense the data, sector level nodes collect the data and detect the data to be anomalous or not.

b) By anomalous we mean that packet is sent in the leaf node's sleep schedule. And set the tag as valid tag.

c) And passes the packet to cluster level nodes whose task is to take the final decision for valid and invalid tag and passes the packet to sink level node in order to reach the packets to the access point.

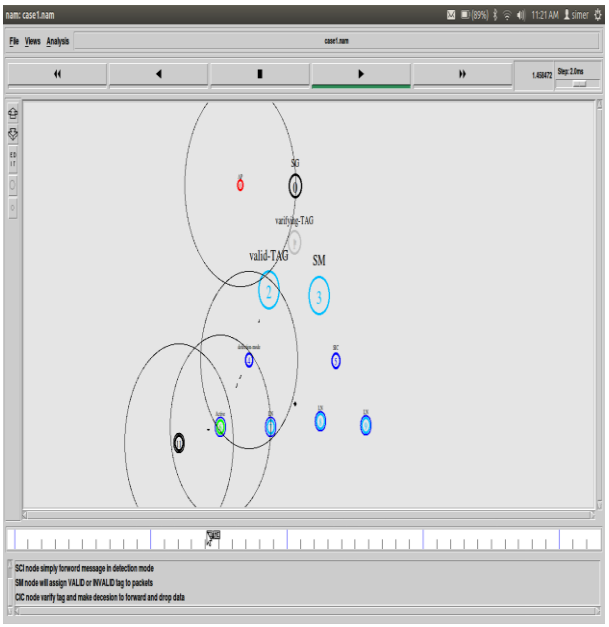

Fig 3: Active schedule of leaf node

Fig. 3 shows the active scenario for the cluster. Here node outside the cluster send the packet to leaf node of cluster in its active schedule sector in charge node detect the packet using the detection mode and detect that packet is sent in leaf node active schedule due to sector monitor set the tag as valid and passes the packet to cluster in charge which further check the tag as in valid and invalid and passes the packet to sink then to the access pointing message.

2. When the packet comes to a leaf node, in its sleep schedule.

a) It forces the leaf node to come to active mode and forward the packet.

b) Leaf node will then sense the packet, and sector level nodes collect the packet and detect that packet is anomalous. And set the tag as invalid.

c) And passes the packet to cluster level nodes which will drop the packet after detecting the invalid tag of the packet.

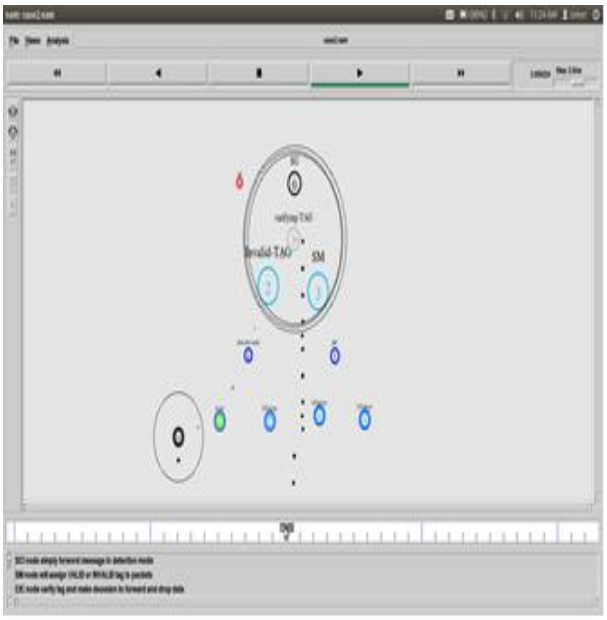

Fig 4: Sleep Scenario of leaf nodes

Now the problem with above two cases is that sector level

3. Nodes are not able to detect when the random message arrives at the leaf node.

a) Leaf node will send continuous packets to the higher level nodes.

b) When the higher level node buffer is full, it will start dropping the packets as well as send the signal to all its neighboring nodes

c) Neighboring node will start sending packet to the outside node so as to deplete the outside node energy.

d) And outside node dies.

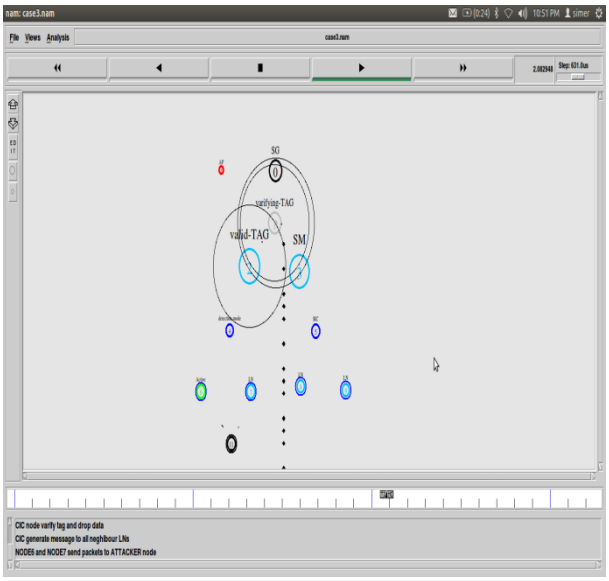

Fig 5: Isolation Scenario for leaf node

4. FLOWCHART AND METHODOLOGY

Following flowchart describes the steps which followed while using the above technique. Where 1to n is the no. of messages outside node send to the leaf node and is the message when send in the sleep mode. By n number of message we mean the rate of message which comes.

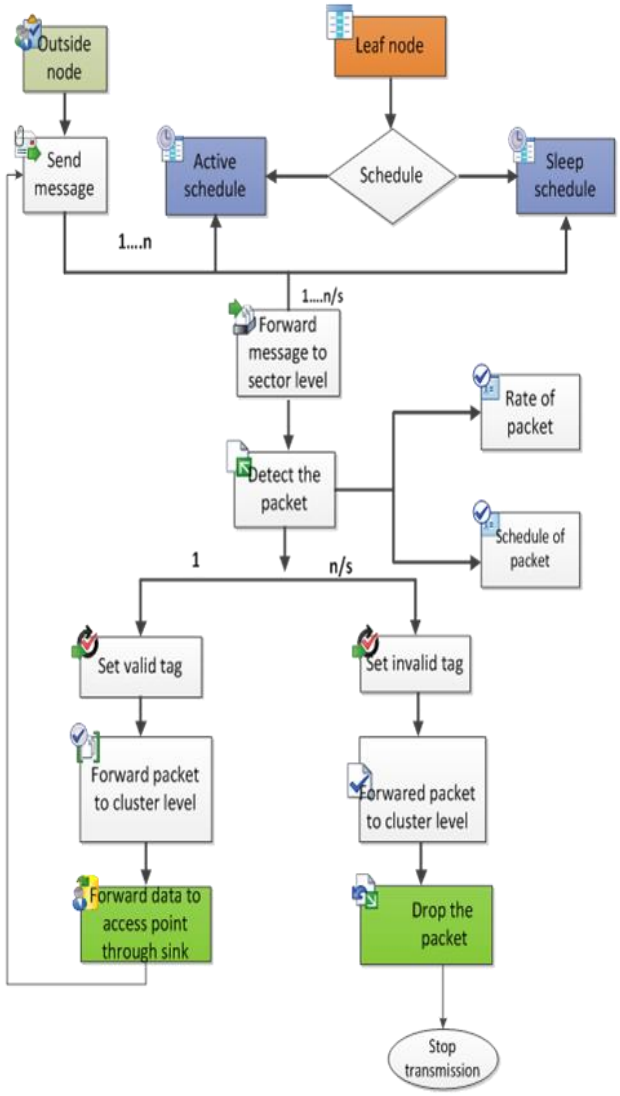

Fig 6: A flowchart for the procedure to be followed

This protocol is implemented on NS-2 tool under the Linux environment. Various tools are available for implementation of wireless sensor network simulation like Omnetpp, Opnet, and Simnet. Ns-2 is an effective tool for showing the how the attacks are formed and its prevention as the motivation of the research work is to secure the cluster from denial of sleep attack. Using the Ns-2 firstly network is created from which cluster is formed. The cluster is then attacked by the outside node which is shown using TCL script. In NS-2 there are various input files which can be used for further modification of any protocol.

5. COMPARISON

The objective of research is to optimize the energy utilization in WSN. The battery driven sensor nodes has lack of sufficient energy, which greatly reduces the network lifetime. All the nodes are heterogeneous having different initial energy. The comparative protocol (Leach) initial energy is set. Energy in a node is consumed in sensing and transmission of receiving signals, and decreases with simulation time. Using LEACH and proposed trace files, residual energy of LEACH protocol is found and it shows that residual energy become zero at the 800 seconds of time whereas for proposed protocol it remains at time 800 seconds.

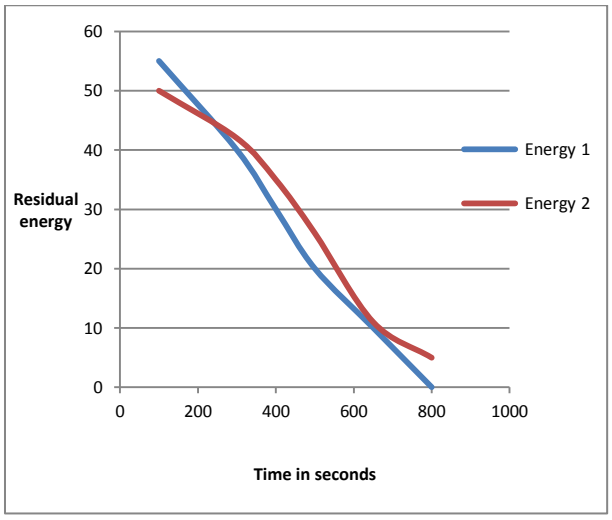

Fig 7: Graph for comparing Leach and Proposed protocol residual energy

6. CONCLUSION

Denial of sleep attack is a serious problem in wireless sensor network. We have implemented the solution to solve this problem. Above implemented protocol is efficient for large scale sensor networks for e.g. in military application where it is difficult to form a small clusters and electing the cluster head for each cluster. The above protocol is also efficient to cope with denial of sleep attack by setting the detection mode for detecting the nodes sending packets in its sleep schedule. And also isolating the nodes with lower energy from attacks. This work can be extend by securing the higher energy nodes and finding more secure method for securing nodes from attack.

7. REFERENCES

[1] Zheng, J., &Jamalipour, A. (2009):*Wireless sensor networks: a networking perspective*. Wiley-IEEE Press (2009).

[2] David R.Raymond and Scott F.Midkiff Virginia tech : "Denial of service in wireless sensor networks; attacks and defenses", published by IEEE CS 2008(2008)

[3] Manju.V.C: "Analysis of Denial of Sleep Attack in WSN", International conference on Recent Development in Engineering and technology(2005).systems.

[4] Brownfield, M., Gupta, Y., & Davis, N. :Wireless sensor network denial of sleep attack. In Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC (pp. 356-364). IEEE(2005, June).

[5] Raymond, D. R., Marchany, R. C., Brownfield, M. I., &Midkiff, S. F. : Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. Vehicular Technology, IEEE Transaction on, 58(1), 367-380(2009)

[6] Raymond D. R., Midkiff S. F : Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks, Military Communications Conference, 2007, MILCOM 2007, IEEE, pp. 1-7(2007)

[7] Chen, C., Hui, L., Pei, Q., Ning, L., &Qingquan, P. :An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks. In Information Assurance and Security, 2009. IAS'09. Fifth International Conference on (Vol. 2, pp. 446-449). IEEE(2009, August).

[8] Bhattasali, T., Chaki, R., &Sanyal, S. (2012). Sleep Deprivation Attack Detection in Wireless Sensor Network. arXiv preprint arXiv:1203.0231(2012).Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[9] Kaur, T., &Baek, J.: A strategic deployment and cluster-header selection for wireless sensor networks. Consumer Electronics, IEEE Transactions on, 55(4), 1890-1897.(2009)

[10] Wu, F. J., & Tseng, Y. C.: Distributed wake-up scheduling for data collection in tree-based wireless sensor networks. Communications Letters, IEEE, 13(11), 850-852(2009).

[11] Kaur, S., Ataullah, M., & Garg, M. Security from Denial of Sleep Attack in Wireless Sensor Network. International journal of computers & technology, 4(2), 419-425 (2013).