Neutralization of Denial of Service Attack in Wireless Sensor Networks

N.TAMILARASI,
Research Scholar, Department of Computer &Information Sciences, Faculty of Science, Annamalai University, Annamalainagar.

Dr.S.G.SANTHI ,
Assistant Professor, Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, Annamalainagar.

Abstract

Wireless Sensor Network (WSN) has large expansion in the various applications on real time unfair incident detection. The capability of identifying the nodes in WSN is an important property. Each and every sensor nodes in the network has some restrictions on consumption of power and resource. This leads to many susceptible actions or attacks in WSN. These actions include Denial of sleep (DoS) as one of the attack. There are different types of DoS attack based on the nodes located at various layers. Efficiently facing this attack needs knowledge about types of DoS and also various security mechanisms applied to overtake the problems. Denial of Sleep is a kind of denial of service attacks which prevents the sensor nodes to enter in to sleep mode and this leads to small network lifetime. Network lifetime of the sensor node is extended by placing the inactive nodes under sleep mode. In this paper, a Hierarchical Clustering System (HCS) is proposed for the improvement of accurate rate of prevention of DoS attack and the extension of network lifetime.

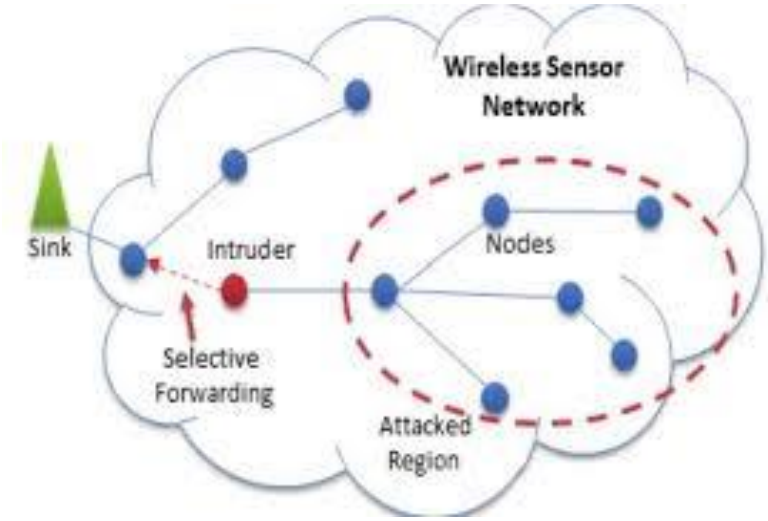
Keywords: DoS attack, sleep mode, wireless sensor nodes and Hierarchical Clustering System (HCS)

1. Introduction

The wireless sensor network (WSN) consists of a number of sensor nodes in which each node is interconnected to one another [1]. WSNs are used in many applications in different areas, which includes defense, medical care, environment, factory and agriculture. Security providing in sensor network is an uneasy task. When comparing with conventional desktop computers, rigorous constraints survive while sensor nodes contains restricted processing competence, energy, storage and wireless links include bandwidth[2].

The WSNs are classified into structured and unstructured networks. Sensor nodes can also be deployed in an ad hoc network into many fields. WSN propose a connection between the real and virtual worlds. The WSN have the capacity to supervise the broad array of potential applications to science, industry, security, civil infrastructure and transportation.

Wireless sensor networks have the potential for applications to inspect and react to events, but their segregation initiate various challenges and unfair actions for network administrator and power consumption [3]. Wireless networks are interconnected in open RF connections and communications are done in an equal frequency bandwidth. So radio probing or intelligence works are very simple to perform. Sensor nodes are available at low cost and minimum consumption of resources such as bandwidth, power and storage. It is a complex one to include any new security algorithms which leads to failure during implementations. As an impact, sensor networks accept low cost self-effacing security protocols.



WSN is located in tremendous climatic conditions and large area coverage. It is hard to constantly monitor the networks for possible attacks [4]. The main purpose of this paper is to increase the life time of the network by minimal consumption of energy and making the inactive node in to sleep mode which is referred as Denial of sleep attack.

This paper is organized as follows: Section 2 presents the related work of Denial of sleep, Section 3 classifies the implementation of proposed patterns on Denial of sleep, section 4 deals with the comparison of previous work and finally Section 5 concludes this paper.

2. Related work

A variety of papers are which defining the solutions for solving the denial of sleep attack which adds protection to WSN. a number of techniques are given below:

Brownfield, M., Gupta, Y., & Davis, N [5]. Proposed a G-MAC protocol which reduces a lot of effects of denial of sleep attack by cluster management through centralizing. G-Mac is a regular protocol that is used in a variety of applications. This protocol lead to increase of network lifetime and formulate the network more opposing to denial of sleep attack.

Raymond D. R and Midkiff S. F [6] proposed a Cluster Adaptive Rate Limiting method based on rate warning approach at MAC layer. The system efficiently used in the B-MAC

protocol and it also maintains the network lifetime as consistent and improved throughput even during the time of sleep deprivation attack.

Chen, C., Hui, L., Pei, Q., Ning, L., and Qingquan, P [7] projected an efficient scheme by employing forged schedule switch with the help of RSSI measurement aid. The sensor nodes can be reduced and weaken that harm from collapse attack and on the dissimilar construct of attackers misplaces their energy so as to expire. Here the energy consumption and the drop ratio of packets has been very less compared to that of scenario without any forged schedule.

Bhattasali, T., Chaki, R., & Sanyal, S.[8] developed a Sleep deficiency attack finding technique that uses the hierarchical structure with revealing mode where the clusters are later classified into various sectors. This method gives an efficient approach to resolve the Denial of sleep attack and also increases the network lifetime but with the problem of leaf node can be easily affected by the attackers.

Kaur, T & Baek, J. [9] proposed a Dynamic Sleep Time, to a certain extent than the permanent sleep time which minimizes the energy wastage in the idle channel which increases the network lifetime but less efficient for denial of sleep attack.

Wu, F. J., & Tseng, Y. C [10] Distributed Wake up scheduling system for collection of data is used which expands both energy conservation and low exposure latency. This system is proposed for 1-hop and 2- hop neighbors. Power reduction and latency are enhanced to lengthen the network lifetime and originality of data.

3. Proposed Mechanism

3.1 Hierarchical clustering System:

In Wireless Sensor Network, usually a hierarchical cluster based routing protocols like leach is used for sending data in which it uses single cluster head for data transmission. Apart from leach, there are also a variety of multilevel clustering, where couple of cluster heads is used for energy conservation. In the proposed mechanism we have formed a Hierarchical Clustering System (HCS) without any particular cluster head but it is formed based on the sensor nodes energy levels. Nodes having superior energy can detect any abnormal packet by means of detection mode.

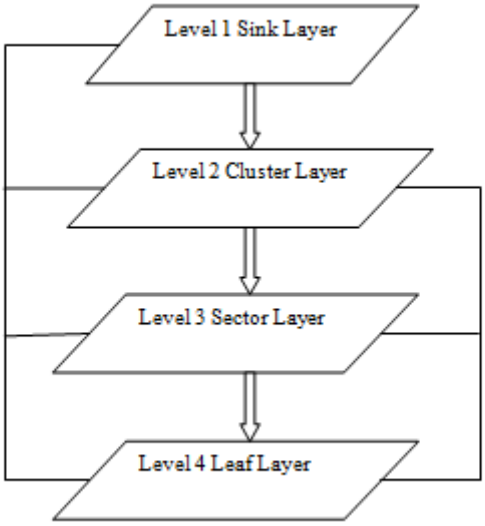


Fig . 1 Hierarchical clustering system

3.2 Working Mechanism:

Step 1: Sink layer node is responsible for the formation of cluster. It sends an advertisement message to the neighbor nodes in the network. Sending and receiving of data is done via the sink layer

Step 2 : Based on the energy level, sensor nodes are arranged in four levels from the highest to the lowest.

Step 3: Using detection mode, check whether the packet flow is normal or not and set the label as legal or illegal. This is done only through higher level sensor nodes because they are having the highest energy to do this task.

Sensor nodes send and receive information only in their active mode. If they are idle, they move on to sleep mode in order to conserve energy. Sensor nodes are different from mobile nodes as they are having schedule time for active and sleep. In the proposed mechanism, sensor nodes are arranged in to four levels such as leaf layer, sector layer, cluster layer and sink layer in the top down manner. The bottom level layer of sensor nodes have lowest energy so it is used for sensing the packets and move on to sleep mode, when there is nothing to sense. Three cases are specified based on the leaf nodes schedule time.

Following steps shows three cases:-

1. When a leaf node sense a packet in its active mode, the following will happens:

a) The leaf node sense the packet and forward it to Sector level nodes. Then It collects the sensed packets and check whether the packets are abnormal or not.

b) At its normal mode, sector layer sets the tag as legal for the particular packet.

c) And the packet is passed on to the cluster level, whose work is to decide whether the packet is accepted or not. If it is accepted then it is passed on to sink level node so that the packets reaches to the access point.

2. The leaf node inferred a packet in its sleep mode, the following will happens

a) The leaf node is forced to forward the packet to the next higher level.

b) By abnormality, the sector layer came to know that the packet is sent during sleep schedule of leaf node and set the tag as illegal.

c) Then the packets are passed on to cluster level nodes, where it checks the packet tag and decides for packet drop.

3. When random messages are arrived, then the leaf node will do the following

a) Leaf nodes send the random packets to the next level.

b) If the buffer occupancy of the higher level node is full, then it drops the excess packets and sends this message to all its neighboring nodes.

c) In order to reduce the outside node's energy, neighboring nodes starts sending the packet and make the outside node die.

Flowchart

The flowchart shows the pictorial representation of the proposed mechanism. The outside node and the leaf node forwards packets to the sector layer in its active and sleep schedule. The sector layer detects the packets and sets a tag and forwards it to cluster layer. Depending upon the tag the cluster layer decides which packet is to be forwarded and which one is going to be dropped.

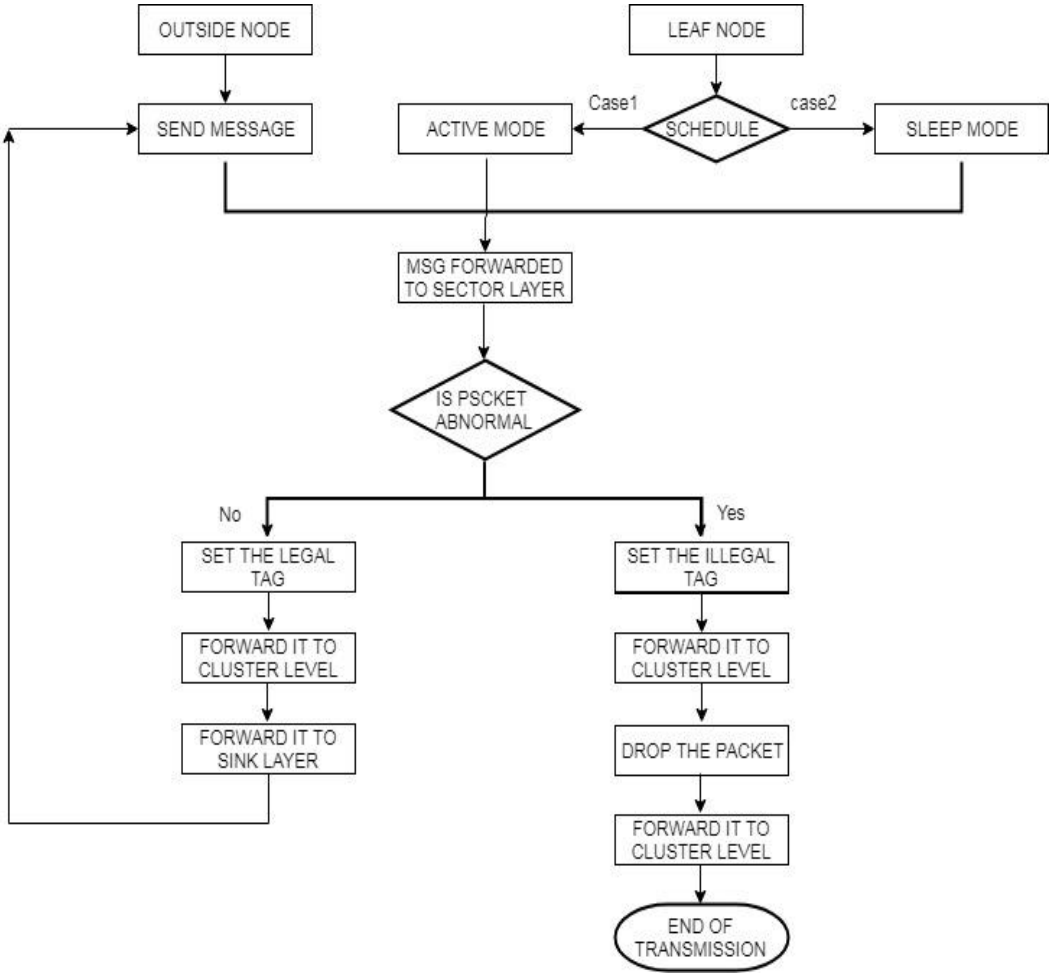


Fig.2 Flowchart – Hierarchical Clustering System

4. Results And Discussions

NS2 under Linux environment is used to implement this proposed mechanism. The intention of research is to manage the energy consumption in WSN. The lack of sufficient energy usage occurs while using battery driven sensor nodes, which leads to decrease the life time of network. Each and every node has different properties, which varies at initial energy. Nodes consume the energy while transferring, sensing and receiving of information.

The existing LEACH protocol is compared with the proposed HCS using the generated trace files. The outstanding energy of LEACH protocol is set up and it shows that the remaining energy become zero at the 900 seconds of time, At same time the proposed protocol extends the network lifetime and makes the WSN in live mode.

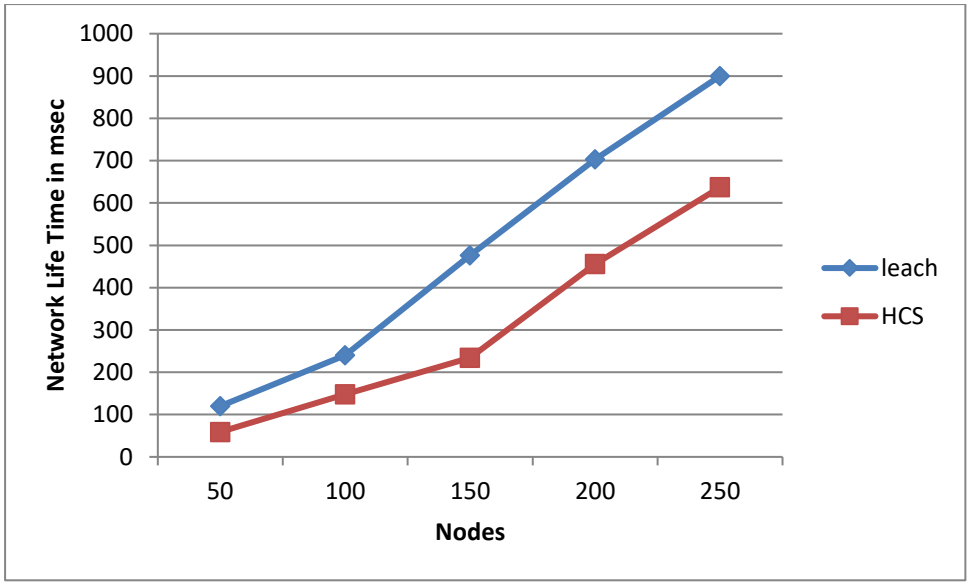


Fig.3 Nodes Vs Network Life Time

Throughput refers to the number of packets sent for a particular period of time and it is measured in kilobits / sec. From the graph it is clearly shows that the existing leach protocol sends less number of packets when compared to the proposed Hierarchical Cluster System (HCS).

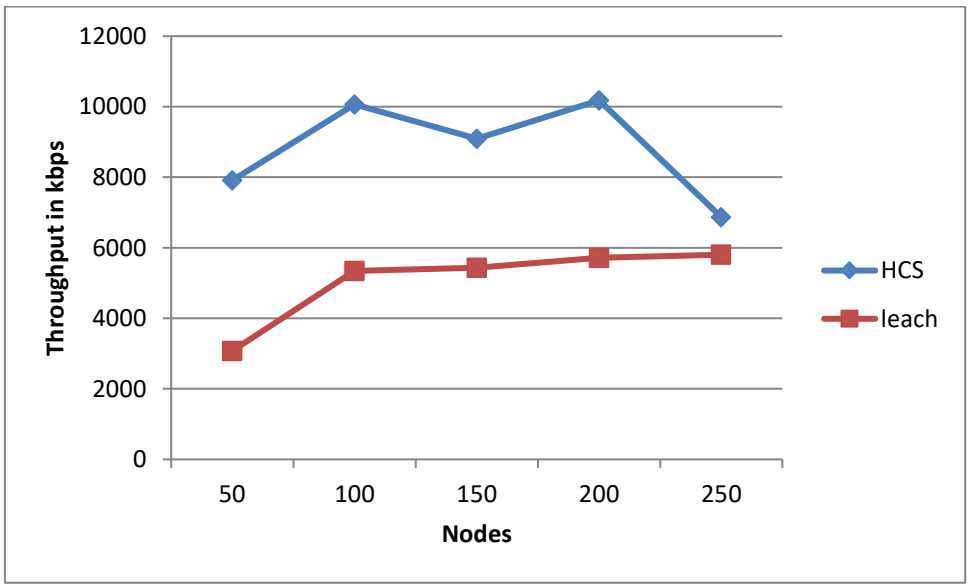


Fig. 4 Nodes Vs Throughput

5. Conclusion

Denial of sleep attack is a severe difficulty in wireless sensor network. We have implemented the result to resolve this difficulty. HCS protocol is well suited for large scale networks. The above illustrated protocol is also capable to manage denial of sleep attack by locating the detection mode in its sleep schedule. It also consume less energy because the proposed mechanism isolates the nodes depending upon their energy level. In future this work can also be extended by securing the superior energy nodes and new techniques are derived for securing the sensor nodes from attack.

References.

[1] M. Dhar and R. Singh, "A review of security issues and denial of service attacks in wireless sensor networks," International Journal of Computer Science and Information Technology Research, vol. 3, no. 1, pp. 27–33, 2015. View at Google Scholar

[2] G. Kumar, "Understanding denial of service (dos) attacks using osi reference model," International Journal of Education and Science Research, vol. 1, no. 5, 2014. View at Google Scholar

[3] Isha, A. Malik, and G. Raj, "Dos attacks on tcp/ip layers in wsn," International Journal of Computer Networks and Communications Security, vol. 1, no. 2, pp. 40–45, 2013. View at Google Scholar

[4] A. D. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in Handbook of Sensor Networks Compact Wireless and Wired Sensing Systems, M. Ilyas and I. Mahgoub, Eds., CRC Press, New York, NY, USA, 2004. View at Publisher · View at Google Scholar

[5] 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).

[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 inWireless 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).