International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

Detection & Isolation of Malicious Nodes in a WSN Using LEACH Protocol

Er. Himanshi Vashisht, Sanjay Bharadwaj, Sushma Sharma
[1]CSE, Haryana Engineering College, Jagadhri, Haryana, India
[2]Computer, DAV College for girls, Yamunanagar, Haryana, India
[3] Computer, DAV College for girls, Yamunanagar, Haryana, India

ABSTRACT

A wireless sensor networks (WSN) is a recent advancement of technology of computer networks and electronics. They have a wide variety of applications ranging from data gathering to data transmission through wireless media. Along with these applications, WSN also has some weakness due to which its sensor nodes are vulnerable to most of the security threats. Denial-of-Service (DoS) attack is one of the most popular attack. This attack affects different layers of WSN and each layer has different type of DoS attack. A malicious node interferes in the system that needs to be detected and eliminated. For this we need a proper strategy. This is been studied in this paper.

Keywords : DoS attack, LEACH protocol, Malicious nodes, Throughput

I. INTRODUCTION

Sensor Networks (WSN) are becoming popular these days due to its wide range of applications ranging from military appliactions to household applications [1]. These applications require some sensitive and critical data that is collected over by sensor nodes in WSN. This sensitive data is very critical to attacks. As a result, security of WSN is a well discussed area[2].

The sensor nodes deployed in a WSN are small, low cost devices with limited energy and transmission bandwidth. These weakness results in various attacks on WSN. One of such attack is Denial or Service (DoS) attack that may be present in various layers of WSN. In this paper, We will try to eliminate any malicious node that has occurred due to this attack.

II. LEACH PROTOCOL

LEACH or Low Energy Adaptive Clustering Hierarchy is one of the most popular hierarchical routing algorithms for WSNs. The basic idea is to form clusters of the sensor nodes based on the received signal strength and use local cluster heads as routers to the BS. This will save energy since the transmissions will only be done only by cluster heads rather than all sensor nodes.

LEACH has two phases- Set-up of cluster phase and steady data transmission state. To conserve the energy, the duration of stable phrase is longer than the time required for the establishment.

The algorithm for LEACH protocol is as follows:

1. SET-UP PHASE- The first phase of LEACH is Set-up phase and it has three fundamental steps.
   i. Cluster Head advertisement
   ii. Cluster setup
   iii. Creation of Transmission Schedule

During the first step, the cluster head sends an advertisement packet to inform the cluster nodes that they have become a cluster head now.

In the second step, the non-cluster head nodes receive this advertisement. They send a join request to the cluster head informing that they are members of the cluster under that cluster head.

In the third step, each of the chosen cluster head creates a transmission schedule for the member nodes.Each node then transmits its data in the allocated time schedule.

2. STEADY PHASE- During this phase, the cluster nodes send their data to the cluster head. Sensor nodes in each cluster communicate only with the cluster head via a single hop transmission. The cluster head then aggregates all this collected data and forwards this data to the base station either directly or via other cluster heads along a defined route . After the certain predefined time, the network again goes back to the Set-up phase.

III. PROPOSED STRATERGY

An active attack which is in charge of dropping the information and control bundles inside the system is known as the specific sending assault. There is a minimization of execution of system and its performance as far as different parameters are concerned when a malignant hub is available inside the system. The parameters, such as vitality utilization, throughput and deferral/delay characterize the execution of the system which can change according to the adjustments made inside the system.

In this work, with a specific end goal to perceive and expel the pernicious hubs from the system, a method has been proposed. Based on activity analyzer and limit esteems introduce inside the system, there is a procedure proposed. The focal controller is picked inside the system relying upon the confide in estimations of the hubs. Contingent upon the information parcels that are re-transmitted inside the system, the trust estimation of the hub is registered. There is a focal controller hub that registers every hub as per IP, MAC address and the present information. The data transmission required for correspondence identified with the base station is doled out utilizing the focal controller hub. Contingent upon the bounce check and arrangement number, a protected and effective way is produced from sensor hub to base station. The information is transmitted from the sensor hub. Assist the focal hub checks independently every hub in an irregular way. The hubs that have edge unequal to the chose limit esteem are to be identified and exhibited as pernicious hub inside the system. For expelling such malignant hubs from the system, a multipath directing technique is exhibited here.

IV. PROPOSED ALGORITHM

Input: Sensor nodes

Output: Detection of malicious nodes

1. Deploy the wireless sensor node with the finite number of sensor nodes
2. Select Central node ()
1. For (i=0;i=n;i++)
2. No.pkts=node(i)
3. If (node(np.pkts(i)> np.pkts(i+1)))
4. Central node=node(i)
5. End
3. Each node register with the central node with their IP and MAC address
4. Assign Bandwidth ()
5. For (i=0;i=n;i++)
6. Bandwidth node(i+1)=total bandwidth-bandwidth node(i+1)
7. End
8. Central controller node check the sensor nodes randomly
9. if (node(bandwidth use=bandwidth assigned)
   1. if(Node(throughput < thrashold throughput)
   2. malicious =Node(i)

3. else
4. repeat step 8 to 9 until malicious node get detected

10. End of for
11. End of if
12. End of if

V. IMPLEMENTATION FRAMEWORK

For the purpose of analyzing the performance of the model that has been developed in real time it is made to be performed within a simulation. The simulators are classified into two types that are event based and the time based. An event based simulator using which the generated events can be triggered at certain defined duration is known as the network simulator version two. For simulating the network models, the network simulator is utilized. There are a lot of versions of NS simulator however NS2-2.35 is the latest version which fits best along with the Ubuntu 12.04. at the front end, the tool command languages are utilized within the NS2 and at the backend, the C++ language is used as a programming language.

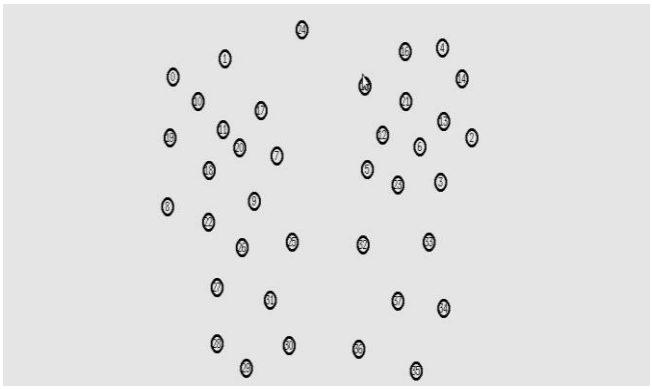

Figure 1. Deployment of Sensor nodes

In this figure, the network is deployed with the finite number of sensor nodes and the whole network is divided into fixed size clusters using location based clustering. The technique of LEACH protocol is applied to select cluster head in each cluster

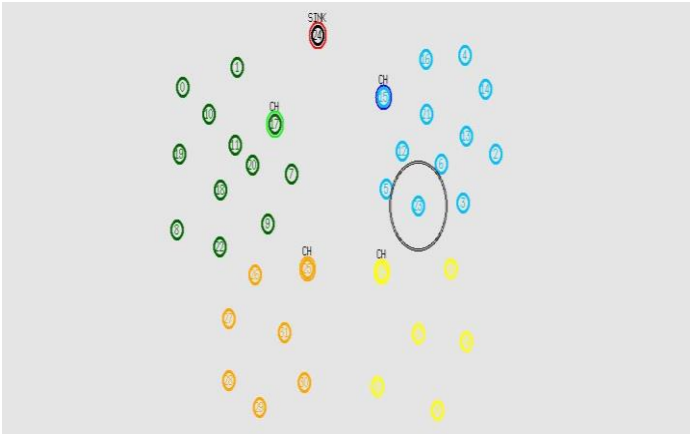

Figure 2. Deployment of Sensor nodes

In this figure, the network is deployed with the finite number of sensor nodes and the whole network is divided into fixed size clusters using location based clustering. The technique of LEACH protocol is applied to select cluster head in each cluster.

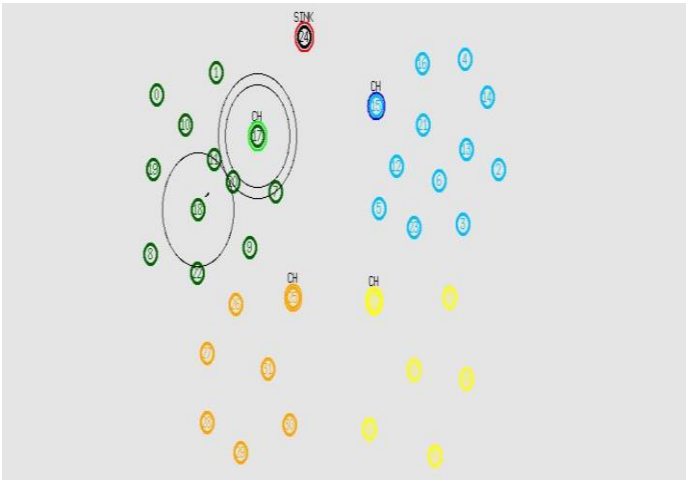

Figure 3. Delay per hop

In this figure, there are different quantities of hubs that convey the system and the area based grouping strategy is utilized to parcel the entire system into settled size of bunches. The bunch head is chosen based on LEACH convention. With the assistance of base station, the best way is picked that gives association inside two group heads. There are some noxious hubs introduce inside the system that bring about causing the confusion assault. The postponement per bounce is figured for isolating the malignant hub from the system.

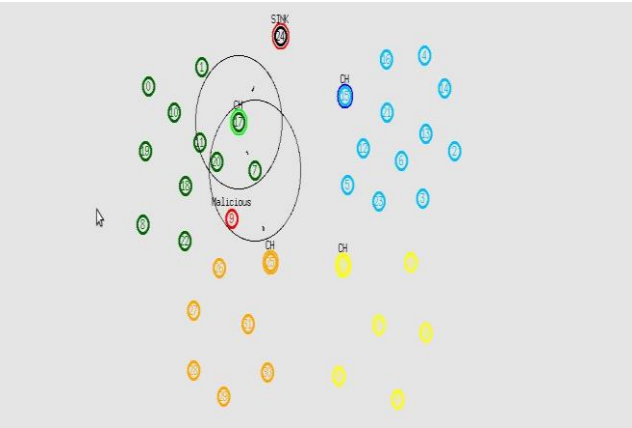

Figure 4. Malicious node isolation

In this figure, with the presence of finite number of sensor nodes, a network is deployed and the complete network is partitioned into fixed size of clusters. A location based clustering method is utilized here for partitioning the network. In order to select the cluster head for each cluster, the LEACH protocol is utilized. Amongst the two cluster heads, the best path possible is chosen. There are various malicious nodes present within the network that trigger misdirection attack within the networks. The delay per hop is counted from the base station within this figure. The malicious node is isolated from the network in this complete scenario.

VI. METRICS APPLICATION

Various metrices will be applied on our proposed method to evaluate the performance. The basic metrices to be applied are-

1. **End-to-end Delay-** End-to-end delay can be defined as time(delay) taken by node to reach from the source to destination over a Wireless sensor network.

   $$\text{End-to-end delay} = T_r - T_s$$

   Where, T_r is the time at which packet is received and T_s is time at which packet was sent.
2. **Energy consumption-** One of the main concerns while designing and implementing a WSN is energy consumption. In a WSN , energy is a limited and valuable resource. Therefore, Energy consumption is an important parameter to be estimated that depends upon hardware constraints and protocols implemented.
3. **Throughput-** Throughput can be defined as rate of successful message delivery over the network.

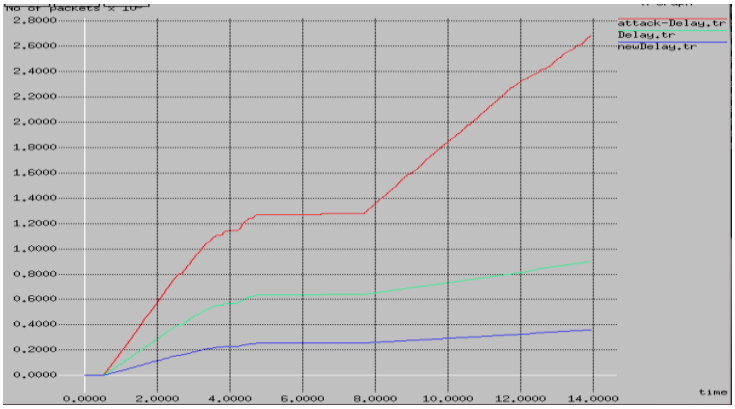

Figure 5. Delay graph

In this figure, in terms of the delay parameters, there is a comparison made amongst the LEACH, the attack as well as the proposed technique. There is maximum delay caused during the presence of attacks. There is least delay within the proposed method as there is no attack present in that network.

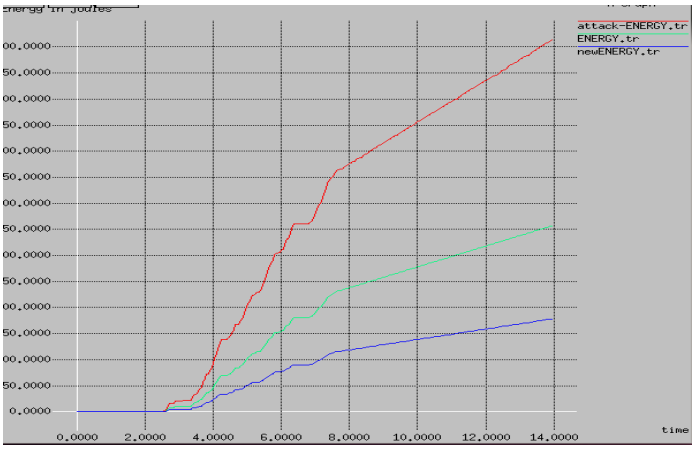

Figure 6. Energy graph

In this figure, the comparison of the proposed, attack scenario is shown in terms of energy. It is been analyzed that energy consumption of the proposed scenario is least as compared to attack scenario.

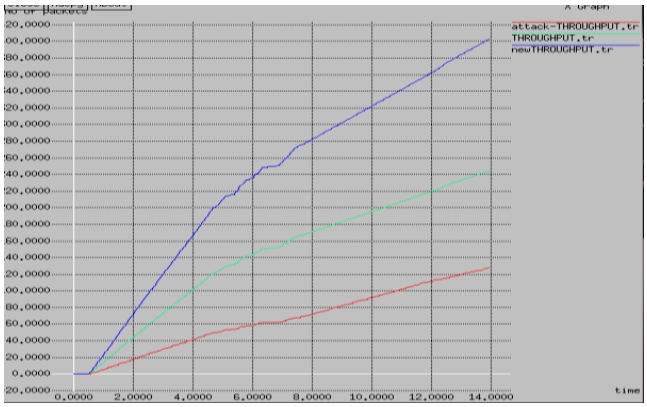

Figure 7. Throughput Graph

In this figure, a comparison has been made for the attack and the proposed method in terms of throughput. In comparison to the other methods, the throughput of proposed method is the highest.

VII. CONCLUSION AND FUTURE WORK

WSN due to its applicational variety is an emerging technology. It is vulnerable to various types of security attacks. Since there are many types of attacks, the most commonly attack type is Denial of Service (DoS) attack. In this paper, we have presented a way of detection and isolation of malicious nodes caused due to these attacks.

In the future, we can create a security mechanism for other attacks such as wormhole attack.

VIII. REFERENCES

[1]. I.F. Akyildiz, W. Su, Y. S. Subramaniam, E. Cayirci. "Wireless Sensor Networks: A Survey" Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA 20 December 2001, pp. 392-422.

[2]. R Sowmya, Mrs. Shoba. M," DETECTION AND PREVENTION OF MISDIRECTION ATTACK BY THIRD PARTY MONITORING IN WSN", 2000 IJRSE

[3]. Roshan Singh Sachan, Mohammad Wazid, Avita Katal, D P Singh, R H Goudar," A Cluster-Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN", 2013 IEEE 978-1-4673-4866-9/13/

[4]. Hero Modraes, Rosli Salleh and Amir hossein Moravjosharieh, "Overview of Security Issues in Wireless Sensor Networks", Third International Conference on Computational Intelligence, Modelling and Simulation (CIM SIM), IEEE 2012, pp. 308-311.

[5]. Roshan Singh Sachan, Mohammad Wazid, D.P. Singh, Avita Katal and R.H. Goudar, "Misdirection Attack in WSN: Topological Analysis and an Algorithm for Delay and Throughput Prediction", 2012 IEEE 978-1-4673-4603.

[6]. Yi-Ying ZHANG, Xiang-Zhen LI, Yuan-an LIU, "The detection and defense of DoS attack for wireless sensor network", Elsevier Journal of China Universities of Posts and Telecommunications, Vol19, pp. 52-56, Oct-2012.

[7]. Hossein Jadidoleslamy," A Hierarchical Intrusion Detection Architecture for wireless sensor networks", 2011 Vol.3, No.5.

[8]. Teodar-Grigopou, "Main Types of Attacks in Wireless Sensor Network", Recent Advances in Signals and Systems, ISSN: 1790-5109, 2009.

[9]. Dr. G. Padma vathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, pp. 1-9.