© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Genetic Algorithm Based Denial of Sleep Attack Detection in WSN

Prof. Sucheta Raut[1], Priyanka Ghodmare[2], Nidhi Meshram[2], Mangesh Jibhkate[2], Vaibhao Bele[2], Pranoti Girhe[2]

[1]HOD(ETC), G.N.I.T., Nagpur, Maharashtra, India

[2]Department of Electronics and Department of Electronics and Telecommunications, G.N.I.T., Nagpur, Maharashtra, India

ABSTRACT

The wireless ad hoc networks are highly vulnerable to denial of service (DoS) attacks because of its unique characteristics such as open network architecture, shared wireless medium and stringent resource constraints. These attacks throttle the tcp throughput heavily and reduce the quality of service (QoS) to end systems gradually rather than refusing the clients from the services completely. In this paper, we discussed the DoS attacks and proposed a defence scheme to improve the performance of the ad hoc networks. Our proposed defence mechanism uses the medium access control (MAC) layer information to detect the attackers. The status values from MAC layer that can be used for detection are Frequency of receiving RTS/CTS packets, Frequency of sensing a busy channel and the number of RTS/DATA retransmissions. Once the attackers are identified, all the packets from those nodes will be blocked. The network resources are made available to the legitimate users. We perform the simulation with Network Simulator NS2 and we proved that our proposed system improves the network performance.

Keywords : Genetic Algorithm, Wireless Sensor Networks, Cross Layer Security, Denial of Sleep Attacks.

I. INTRODUCTION

Wireless Sensor Network (WSN) contains a collection of self-governing sensors that monitors the conditions such as sound, temperature, pressure, and vibration [1]. The
sensor nodes in the WSN are energized using the batteries. But, one of the major issues of WSN is energy loss. It is caused due to the following reasons

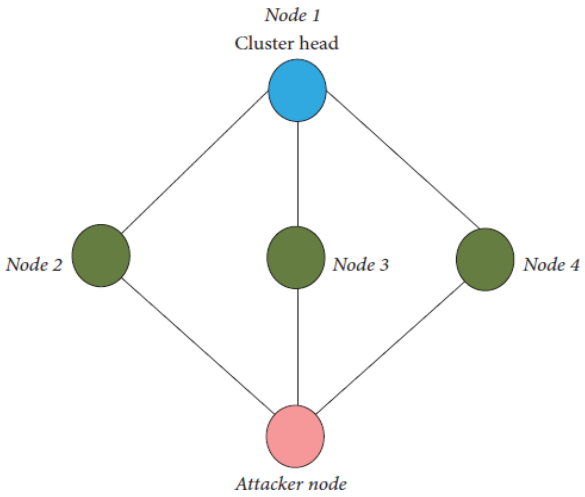
1. Collisions
2. Overhearing
3. Idle listening
4. Control packet overhead

In the collision loss, the collision of data packets in the wireless medium introduces the energy loss. In the overhearing loss, the maintenance of radios in the receiving mode during data packet transmission introduces the energy loss. The idle listening loss is created by a node's radio in just monitoring the channel. As the control packets may have to be received by all the nodes in the transmission range, the control packet overhead is introduced. Generally, the WSN is prone to two types of attacks such as invasive attack and non invasive attack. The non invasive attacks affect the power, frequency, and timing of the channel, whereas the invasive attacks affect the information transmission, routing process, and service availability [3]. Among the attacks of WSN, the denial-of service attacks make the system or service inaccessible. The important properties of the DoSL attacks are

(i) malicious,
(ii) disruptive,

(iii) remote.

When the denial-of-service attack is performed intentionally, it is termed as malicious. When the DoSL attack is successful, the capability or service in WSN is affected. Thus, disrupting the affected service is not the only goal of the attacker.



1.

Figure 1. Denial-of-sleep attack

II. RELATED WORK

1. Mansouri et al. IEEE Transaction 2015:

Mansouri et al. proposed a clustering technique for addressing the DoS attacks. The suggested technique exploited the energy consumption of the nodes. Mansouri et al. detected the compromised nodes in WSN using energy-preserving solution. The suggested algorithm detected the controlled nodes (C node) using a hierarchical clustering technique. Experimental results proved that the suggested technique achieved optimal energy balance, throughput, detection coverage, and delay between the packet transmissions. Chen et al. proposed a time-division secret key protocol for detecting the DoS attack. The simulation results proved that the cipher function was optimal for WSN. Further, the detection jamming scheme increased the network lifetime of the WSN.

2. J.Nam, Y. Cho, "Statistical En-route Filtering (SEF) Scheme ", June 2014:

Nam and Cho suggested a Statistical En-Route Filtering (SEF) scheme for detecting the false reports in the intermediate nodes. Further, the false report injection attack was defended using three types of keys such as individual key, pairwise key, and cluster key. The comparison of SEF with the suggested method proved that the proposed method enhanced the energy savings than the SEF in sensor networks. Manju et al. suggested three steps such as network organization, malicious node detection, and selective authentication for detecting the denial-of-sleep attack in WSN. Experimental results proved that the suggested method was optimal for defending the attacker from performing the task.

III. MECHANISM FOR DOS PREVENTION

Proposed method to defend denial of sleep attack consists of two parts.

3.1 Network organization: Sensor Network was built in tree like structure and organizes the nodes. Sink node is at the root of the tree. Each node must know its parent node to which it needs to send packets to reach to sink. Also the parent node must know the child node from which it can receive SYNC packets.

3.2 Selective level authentication: There are two different formats for SYNC packet. One is without authentication and other one is with authentication Token. During normal operation if the SYNC is under threshold SYNC without authentication is used. If there is a threshold cross over there is a chance of denial of sleep attack and enforces SYNC with authentication token for authentication

IV. MODULES

- **Network Configuration and Creation:** This module will involve designing the network structure to be used for transmission.
- **Attack Execution:** This module will demonstrate

execution of attack wherein the node energy will be lost due to existence of an invalid node. Due to this loss of energy, the overall performance of the network will be affected and therefore, improper transmission executes. It will involve transmission of data from source to destination node and its analysis to track the details of nodes.

- **Attack Detection using hash analysis:** This module will facilitate the execution of attack and its detection using authentication mechanism. This mechanism will involve attachment of a hash analysis with the data transmitted will be distributed using an Authentication Node.

- **Analysis Module:** This module will facilitate the generation of analysis of simulation time of the above executions and get an overall view of the current energy of the network at a particular time.

V. ARCHITECTURE

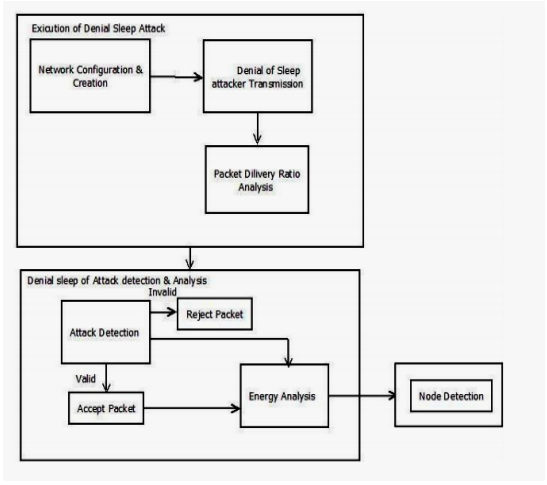


Figure 2. Architecture of challenge and response method

The main goal of this architectural process is to detect the denial-of-sleep attack, analyse energy consumed and calculate the Packet Delivery Ratio with detection and without detection of attack. This architectural process
is divided into two stages:-

5.1 Execution of Denial-Of-Sleep:

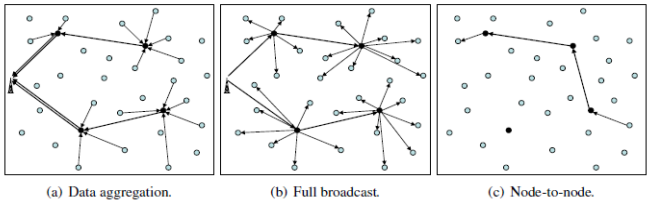
Initially in this stage network is created and configured. Then demonstration of execution of attack will be done wherein the node energy will be lost due to existence of an invalid node..Due to this loss of energy, the overall performance of the network will be affected and therefore, improper transmission executes. It will involve transmission of data from source to destination node and its analysis to track the details of nodes.

5.2 Denial-Of-Sleep Attack Detection Analysis:

This stage executes and detects the attack using authentication mechanism. This mechanism will involve attachment of a hash analysis with the data transmitted. Attack detection will be done by comparing the response calculated by the destination node with the response received from the main station. If the received response matches the calculated response then the node is valid node.

VI. CLUSTERING IN WSN

Some form of clustering is almost always required for scalablability in large-scale ad-hoc WSN deployments. Clustering reduces network contention by deconflicting inter-cluster interferencethrough lower transmit power, separate channels, or spread-spectrum techniques, thereby improvingspatial reuse. Reducing contention conserves energy and reduces latency in the network. Clustering can also conserve energy by aggregating and fusing data at clusterheads for transmission to
a base station. Figure 3 depicts routine modes of cluster-based communication in WSNs



Figuew 3. Routine communication models for cluster-based WSNs.

Although different in the details of their execution, clustering algorithms generally follow the sequence of events outlined here.

1. Some subset of network nodes volunteer (or are elected) to become clusterheads. This decision is often randomized, but is based upon current energy reserves, the number of times a node has served as clusterhead, some desired clusterhead node-degree, or other parameters.
2. Each remaining node in the network "joins" a cluster by communicating its intent to do so
to one of the clusterheads. Deciding which cluster to join is often done by using received
signal strength values to decide which clusterhead can be reached with the lowest transmit power.
3. Clusterheads establish routes to other clusterheads or to a base station according to the communication model used by the network.

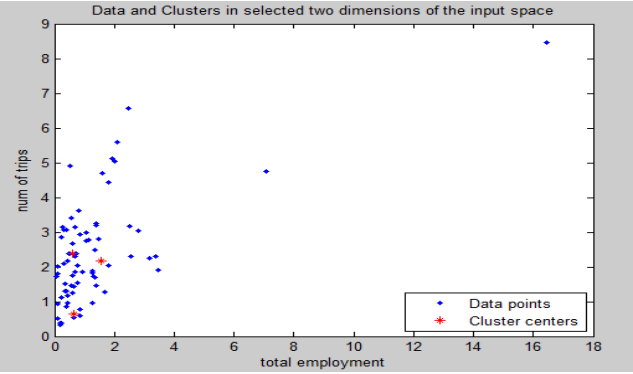


Figure 4. Data and Cluster in Selected Input Space

VII. ADVANTAGES AND DISADVANTAGE

Advantages:

1. Secure data transmission.
2. Prevent external errors and noice.
3. The strong layer authentication is a key component of the DoSL defense. On integrating this component to the WSN, the DoSL attacks can be prevented efficiently.
4. The jamming identification component is used for preventing the jamming attack that prevents the sensor nodes from accessing the wireless medium.
5. The antireplay protection component is used for preventing the replay attacks that force the nodes to forward the old traffic information.
6. The broadcast attack protection technique differentiates the legitimate traffic from the malicious traffic for minimizing the energy consumption

Disadvantage:

The existing DoSL defense mechanisms are nonoptimal energy conservation and lack of key pairing operations for preventing the attacker from implementing the attack.

VIII. CONCLUSION

In this paper, an efficient GA-DoSLD algorithm is proposed for generating the DoSL attack profiles from multiple sensor nodes such that the attacker nodes can be prevented from the communication process. Genetic algorithm is the search and optimization technique and used to find the best optimal solution with the help of some method such as initialization, selection, crossover, mutation, replacement. In these steps we first select the chromosome depend on the nature and after that selection a new offspring is produce with the help of fitness value and choose the best solution

IX. ACKNOWLEDGMENT

We express our gratitude and thanks to the Head of our department Mrs.Sucheta Raut, who has helped us a lot in the successful completion of initial phase of our project. We remember the invaluable support offered by Mrs.Sucheta Raut, our project guide and for her good suggestions and constant encouragement .

X. REFERENCES

[1]. C. Manju, S. L. Senthil Lekha, and M. Sasi Kumar, "Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks," in Proceedings of the IEEE Conference on Information and Communication Technologies (ICT '13), pp. 74–77, Tamil Nadu, India, April 2013.

[2]. D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 367–380, 2009.

[3]. R. P. Manohar and E. Baburaj, "Detection of Stealthy Denial of Service (S-DoS) attacks in wireless sensor networks," International Journal of Computer Science and Information Security (IJCSIS), vol. 14, pp. 343–348, 2016.

[4]. D. Mansouri, L. Mokddad, J. Ben-Othman, and M. Ioualalen, "Preventing denial of service attacks in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications (ICC '15), pp. 3014–3019, London, UK, June 2015.

[5]. D. Mansouri, L. Mokdad, J. Ben-Othman, and M. Ioualalen, "Detecting DoS attacks in WSN based on clustering technique," in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13), pp. 2214–2219, Shanghai, China, April 2013.

[6]. "Wireless Sensor Network" by S. Swapna Kumar.

[7]. "Protocols and Architecture for Wireless Sensor Network" by Holger Karl & Andreas Willing.

[8]. "Wireless Sensor Network" by Sunil Gupta & Dr. Harsh K. Verma.

[9]. www.wikipedia.com

Authors Profile

Ms.Priyanka Ghodmare is currently pursuing Bachelor of Engineering in Electronics and Telecommunication from Guru Nanak Institute of Technology, Nagpur, Maharashtra, India.

Ms.Nidhi Meshram is currently pursuing Bachelor of Engineering in Electronics and Telecommunication from Guru Nanak Institute of Technology, Nagpur, Maharashtra, India.

Mr.Mangesh Jibhkate is currently pursuing Bachelor of Engineering in Electronics and Telecommunication from Guru Nanak Institute of Technology, Nagpur, Maharashtra, India.

Mr.Vaibhao Bele is currently pursuing Bachelor of Engineering in Electronics and Telecommunication from Guru Nanak Institute of Technology, Nagpur, Maharashtra, India.

Ms.Pranoti Girhe is currently pursuing Bachelor of Engineering in Electronics and Telecommunication from Guru Nanak Institute of Technology, Nagpur, Maharashtra, India.