Efficient Technique For Detecting Malicious Node In Wireless Sensor Networks

Mrs. Poonam Rana
Dept of Computer Application
Chandigarh Group of Colleges Landran

Abstract- *Wireless sensor networks are typically installed in unprotected and harsh environments where security is a significant concern. In such insecure environments, wireless sensor networks are open to many physical and logical attacks. Wireless sensor network security is very important, as these types of networks usually trigger alerts that require sudden attention.*

There are misdirection attacks which occur due to the presence of malicious nodes within the paths. Due to this there is an increment of delay within the network. This paper focuses on identifying and isolating malicious nodes from the network, the selective forwarding attack within the network.

I. INTRODUCTION

There are different sensor nodes in wireless sensor networks that are located in a specific area in different applications. Loss of information along with energy expenditure occurs when denial of service (DoS) attacks occur on the network. There are a finite number of sensor nodes deployed in this network that use the LEACH protocol to divide the entire network. A fixed cluster size is generated here. Depending on the distance and energy, there is a choice of cluster heads for each group. The smallest path is chosen between the source and destination, which basically depends on the reactive routing protocol. There are redirect attacks that occur because of the presence of malicious nodes on paths. Because of this, there is a delay increase in the network. In this work, in order to identify and isolate malicious nodes from the network, an selective relaying attack on the network.

II. OBJECTIVES

1. Investigation and analysis of various types of security attacks that are possible in a wireless sensor network
2. Propose an innovative technique for detecting and isolating malicious nodes from the network, which is responsible for selective redirection attack
3. The proposed technique will be based on the technique based on the detection and isolation thresholds of malicious nodes
4. Implement the proposed and existing techniques and graphically compare the results in terms of throughput, delay and energy consumption.

III. RESEARCH METHODOLOGY

An active attack that is responsible for dropping data and control packets on the network is known as selective forwarding. There is a minimization of network performance in terms of various parameters when a malicious node is present in the network. Parameters such as power consumption, bandwidth and delay determine the network's performance, which may change according to modifications made to the network. This work proposes a technique to recognize and remove malicious nodes from the network. A technique was proposed based on the traffic analyzer and threshold values present in the network. The central controller is selected in the network depending on the node trust value. Depending on the data packets that are retransmitted on the network, the node's trust value is calculated. There is a central controller node that registers each node according to the IP address, MAC address and current data. The bandwidth required for communication related to the base station is assigned via the central controller node. Depending on the hop count and sequence number, a safe and efficient path is generated from the sensor node to the base station. Data is sent from the sensor node. In addition, the central node randomly checks each node individually. Nodes whose threshold is different from the threshold set must be detected and presented as a malicious node in the network. In order to remove such malicious nodes from the network, the multi-path routing method is presented here.

IV. PROPOSED ALGORITHM

PROPOSED ALGORITHM

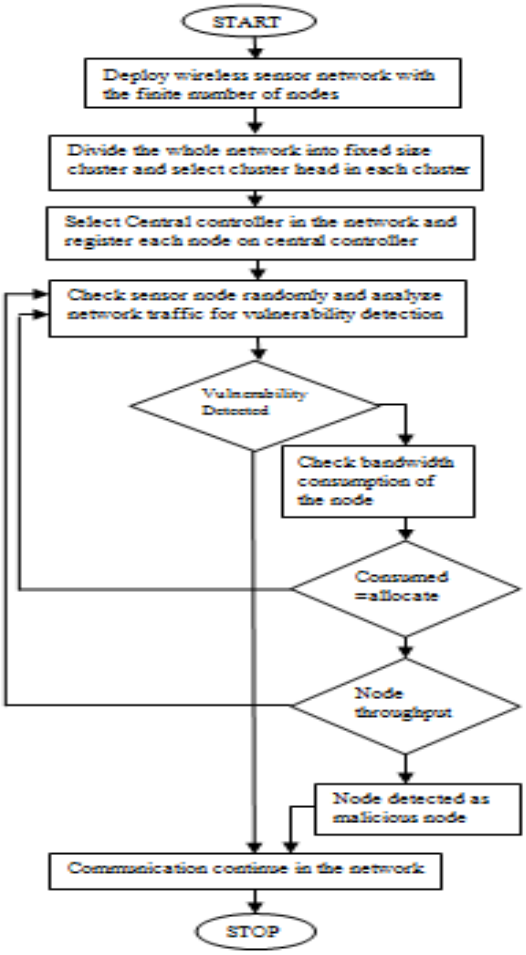
Input data: sensor nodes

Output: Detection of malicious nodes

1. Deploy a wireless sensor node with a finite number of sensor nodes
2. Select the central node ()
1. For (i = 0; i = n; i ++)

2. No.pkts = node (s)
3. If (node (e.g..pkts (i)> e.g..pkts (i + 1)))
4. Central node = node (s)
5. End
3. Each node registers with a central node with an IP address 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. The central controller node randomly checks the sensor nodes
9. if (node (bandwidth utilization = assigned bandwidth)
1.if (Node (throughput <threshold throughput)
2. malware = Node (s)
3. more
4. Repeat steps 8 to 9 until the malicious node is detected
10. End of deadline
11. End of if
12. End of if

V. PROPOSED FLOWCHART



VI. PROPOSED IMLEMENTATION

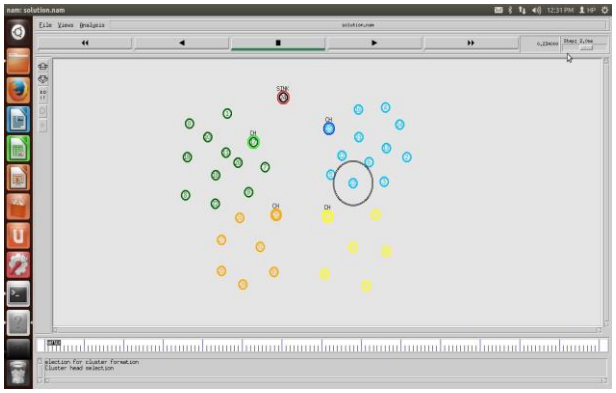


Fig 4.11: Deployment of Sensor nodes

As shown in Figure 4.11, the network is implemented with a finite number of sensor nodes, and the entire network is divided into fixed-size clusters using location-based clustering. The LEACH protocol technique is used to select the cluster head in each cluster

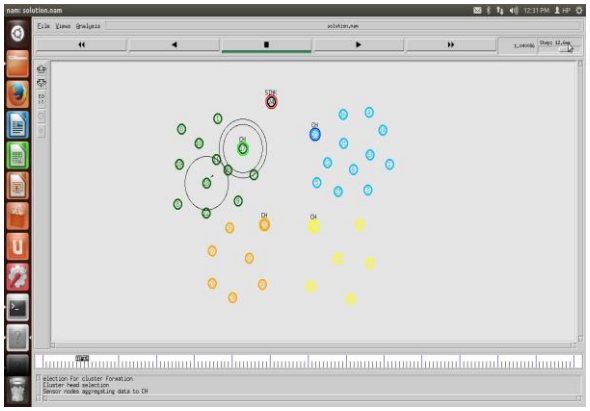


Fig 4.12: Delay per hop

As shown in figure 4.12, with the help of base station, the best path is chosen that provides connection within two cluster heads. There are some malicious nodes present within the network that result in causing the misdirection attack. The delay per hop is computed for separating the malicious node from the network.

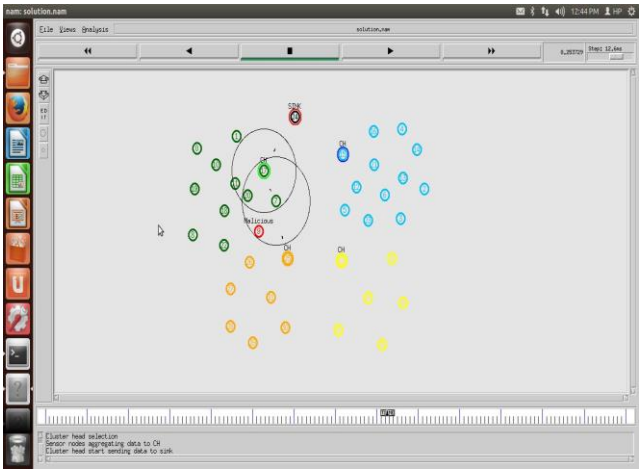


Fig 4.13: Malicious node isolation

As shown in figure 4.13, 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.

Fig 4.14: Delay graph

As shown in figure 11, 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.

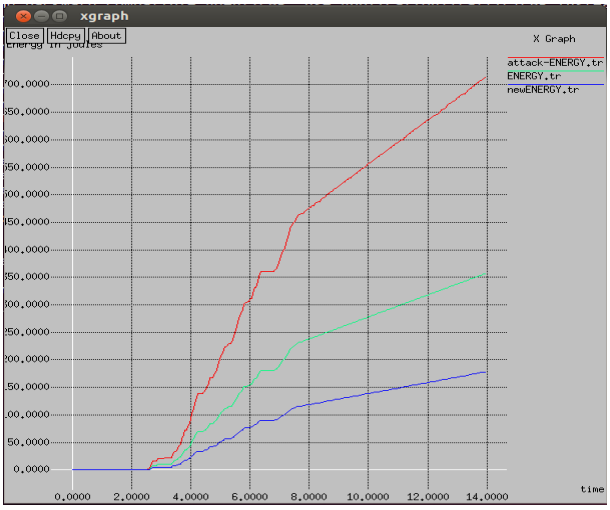


Fig 4.15: Energy graph

As shown in figure 12, 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

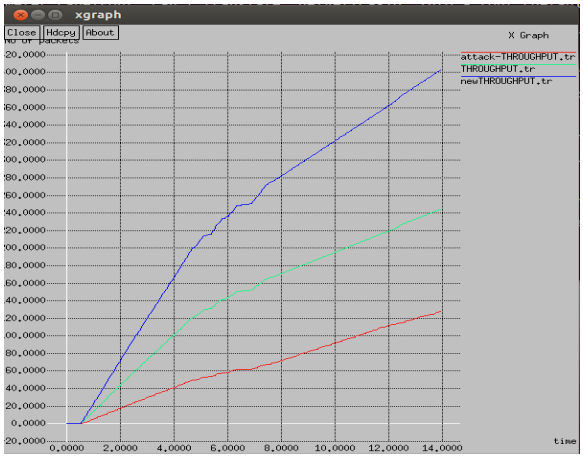


Fig 4.16: Throughput Graph

As shown in figure 13, 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

The networks that can sense the environmental conditions with the help of sensor nodes present within them are known as wireless sensor networks. The sensed information is gathered and passed further to the base station. The sensor nodes are of very small size. Therefore, the lifetime of the sensor nodes is very less and the size of battery available within them is very less. The malicious nodes can enter within the wireless sensor networks mainly due to the self-configuring nature of these networks. There can be

various attacks possible within the network due to the presence of malicious nodes within the network. Amongst these attacks is the selective forwarding attack. The technique is proposed in this paper which can identify and separate the malicious nodes from the network. On the basis of threshold mechanisms the base station analyzed the delay per hop within the network. The malicious node is identified on the basis of the delay such that the node that contributes maximum delay will be recognized as malicious node. This helps in minimizing the energy consumption of the network along with the increment in throughput and reduction of delay within the network.

VIII. FUTURE WORK

It is been analyzed that proposed technique performs well for the detection and isolation of misdirection attack in wireless sensor networks. The sinkhole is the similar type of attack in which malicious node acts like a sink and gather whole network data. In future, proposed technique can be applied in detecting and isolation of sinkhole in wireless sensor network.

REFERENCES

[1] Juby Joseph, Vinodh P Vijayan," Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol", 2014 Vol.4

[2] Dr. G. Padmavathi, 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

[3] Maan younis Abdullah, Gui Wei Hua, Naif Alsharabi, **"**Wireless Sensor Networks Misdirection Attacker Challenges and Solutions", 2008 IEEE 978-1-4244-2184-8/08/

[4] Roshan Singh Sachan, Mohammad Wazid, D.P. Singh, Avita Kata and R.H. Goudar, **"**Misdirection Attack in WSN: Topological Analysis and an Algorithm for Delay and Throughput Prediction", 2012 IEEE 978-1-4673-4603-0/12/

[5] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks" Journal of Security Engineering, 2014, pp.241-250

[6] Hero Modraes, Rosli Salleh and Amirhossein Moravjosharieh, "Overview of Security Issues in Wireless Sensor Networks", Third International Conference on Computational Intelligence, Modelling and Simulation(CIMSiM), IEEE 2011, pp. 308-311

[7] Hossein Jadidoleslamy," A HIERARCHICAL INTRUSION DETECTION ARCHITECTURE FOR WIRELESS SENSOR NETWORKS", 2011 Vol.3, No.5

[8] Ruchita Dhulkar, Ajit Pokharkar, Mrs. Rohini Pise," Survey on different attacks in Wireless Sensor Networks and their prevention system**",** 2015

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

[10] Hailun Tan, Diethelm Ostry, JohnZic, SanjayJha, "A Confidential and DoS-Resistant Multi-hop Code Dissemination Protocol for Wireless Sensor Network", ACM WiSec09, Zurich, Switzerland, March 16-18, 2009

[11] Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010

[12] R Sowmya, Mrs. Shoba. M," DETECTION AND PREVENTION OF MISDIRECTION ATTACK BY THIRD PARTY MONITORING IN WSN", 2000 International Journal of Research in Science & Engineering Volume: 1 Special Issue: 2

[13] Suparna Biswas, Subhajit Adhikari," A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network", 2015 International Journal of Computer Applications (0975 – 8887) Volume 131 – No.17

[14] C. Anand, R. K. Gnanamurthy," Localized DoS Attack Detection Architecture for Reliable Data Transmission Over Wireless Sensor Network", 2016 Springer Science + Business Media New York