The Threshold Technique for the Isolation of Denial of Service Attack in Wireless Sensor Networks

Yogesh Sharma[1], Bimaljeet Kaur[2]
[12]*Computer Science and Engineering, ARSA College of Engineering and Technology, Punjab, India*

Abstract- A wireless sensor network consist of wide variety of sensors over a geographical region, where proper evaluation is necessary to known the progressions going ahead there. They are more prone to attacks as appropriate algorithms are not generated for such networks. In the sensor network there are many feasible attacks such as active and passive attacks. The most widely recognized and critical attack among all the plausible active attacks is sinkhole attack. This attack hamper the functioning of the network by seize all the execution process as well increase the effects of denial of service attack. A novel technique is proposed in this paper that is used to separate or identify all the embedded malicious nodes attacks from the network. The proposed technique is based on the threshold technique for detection of malicious nodes. As per the performed experiments the proposed method identifies and removes all the malicious nodes from the network accurately. NS2 simulator instrument has been utilized in this network that provides the effective performance as well remove the errors and expand throughput of the network.

Keywords- WSN, DOS, Threshold

I. INTRODUCTION

Wireless Sensor Network is a combination of tiny lightweight wireless sensors with computing elements. These sensor nodes are generally cheaper in price, with limited energy storage and limited processing capabilities. Wireless sensor network consists of a large number of these sensor nodes (usually hundred or thousand of nodes). These types of networks are highly distributed and deployed in hostile environments [1]. In order to measure the physical parameters such as moisture, weight, and temperature wireless sensor networks are required to monitor the surroundings. Sensor nodes use battery power as an energy source. The battery is a constrained force asset and as wireless sensor networks are normally conveyed at threatening ecological it is about illogical to supplant batteries of the sensor nodes, so control utilization in wireless sensor networks is dependably a noteworthy concern [2]. In this manner, it is frequently required to have energy proficient strategies which can build the life of these wireless sensor networks. An inbuilt exchange off system ought to be made so that the end-client ought to decide on dragging out network lifetime at the decrement of lower throughput or higher transmission delay [3]. The movement in Wireless Sensor Network relies on upon a number of queries created per Meantime. The sink node transmits the data to be detected by sending a query all through the sensor field. The sensor nodes react to the query by social event the data utilizing their sensors. At last when the sensor nodes have the consequence of the infused query will answer to the sink node through some directing convention. A sensor node likewise totals the answers to a solitary reaction which spares some of the packets to send back to the sink node. Wireless sensor networks are usually installed at unprotected and bitter environments where security is an essential issue. In such unprotected environments, wireless sensor networks are open to many physical as well as logical attacks [4]. Security of Wireless sensor network is very important as such types of networks are generally causing alerts which require sudden attention. False alerts generated by the wireless sensor networks may lead to unwanted actions. The security issue is the main concern in a sensor network. A misdirection attack is basically a type of DoS attack which can occur at various instants. A communication that is to occur within the network is denied due to the presence of malicious nodes due to which the service is also further not provided to the destination. Misdirection attack can occur in two ways. First is Packets Forwarded to a Node Near to the Destination [5]. This sort of misdirection assault is less serious, on the grounds that packets compass to the destination however from an alternate course which assists delivers long delay, consequently diminishing throughput of the system (bit exchange every second). Second is Packets Forwarded to a Node Far Away from the Destination. In order to send the node away from the network, the misdirection attack can be very problematic here. The destination of the nodes is modified and so they never reach the desired destination. This results in continuous delay within the network and negligible throughput is also generated [6]. As these attacks results in degrading the performance of the networks, the misdirection attacks are very harmful for providing reliable networks. There are a number of nodes deployed in the network. There is a source which sends data to the destination. In this attack, one node attack acts as a malicious node which sinks all the packets and drops to forward it. The path is established between source and destination using AODV protocol. Data is transmitted from source to destination [7]. During data transmission, one intermediate node acts as a malicious node which triggers misdirection attack in the network. When the Sinkhole attack occur in the WSN, the performance of WSN starting to

decrease in term of some performance metrics such as packet delivery ratio, the end to end delay and packet loss.

II. LITERATURE REVIEW

R Sowmya et.al [2000] proposed that these sensor nodes are battery-powered with a constrained lifetime and additional energy can be collected from the outer environment. Wireless sensor networks are vulnerable to various types of attack. As Denial of Service Attack (DoS) attack covers an expansive number of attacks and dangers in WSN, finding productive mechanisms for the powerful counteractive action of Denial of Service Attack (DoS) circumstances still stays as an open examination issue. Misdirection attack is one of the Denial of Service Attack, which causes the nodes to course information on long paths and ultimately makes circumstances of network jam. The work proposed here is the creation of CH-buffer database and Received-buffer database which can identify the malicious node and protect the data.

Michael Collins et.al [2009] proposed a secure lightweight architecture, ASLAN in this paper to provide which provides the constraints related to the sensor networks. In order to provide reliable connection amongst the nodes, a hierarchical network topology is presented in this paper. The malicious sensor nodes are identified and separated from the ASLAN method. A protocol is presented here for recognition and separation of such attacks. There are two segments present within this protocol which are node-to-node and cluster head-to-node. They both work together in relation to each other. Any node that has identified the trade off and removed the attack is done with the help of this protocol.

Megha Joshi et.al [2015] proposed that the sensor nodes are small and have less impact of the smaller regions due which there is a need to enhance the Micro-Electro-Mechanical Systems (MEMS) wireless communications. Due to these methods, there are simple and low power sensor nodes provided within the networks. In order to address such issues, various methods have been proposed and a study has been conducted related to them in this paper. In order to gain trust and provide a reputed solution to such issues, various studies have been analyzed and with the help of this, the wireless sensor network has been secured. A unified methodology has been proposed here within these networks and the reliable base station has been selected here in order to provide better calculations. This also helps in minimizing the power consumption and various calculations being made for the sensor nodes.

Omar Said et.al [2015] proposed in this paper a model within which the heterogeneous sensors are deployed within the 3D WSNs. The two broader classifications of sensing are the single and multiple sensing. There are probabilities generated in order to propose intrusion detection with the help of various methods such as Gaussian, uniform, beta and chi-squared methods. A simulation domain is generated with the help of OPNET and NS2 in order to access the proposed model. The best efficiency and execution related results are generated within the Gaussian distribution method. There is very less execution within the various techniques such as beta and chi-square. The various outcomes are achieved within these methods which show that these methods have improved the results in comparison to the exiting methods. Within the WSN in 3D conditions, the various simulation results of the proposed model are presented with the help of Gaussian sensors distribution method.

Suparna Biswas et.al [2015] proposed in this paper the various types of security attacks, the effects they cause and the defense methods to be applied in order to remove them. Depending on the various security attacks, their effects and the methods that are required to prevent them, a study is proposed which is presented in this paper. In relation to the various security issues and the existing attacks present within the network, there is a very improved method proposed for analysis in this paper. There are presented various ways in which a secure wireless sensor network can be generated in future. Various security methods are also provided for protecting the network from other attacks.

C. Anand et.al [2016] proposed that there is a need to provide radio link multi-hop communications in order to provide services of wireless sensor networks that have various resource constraints. In order to prevent such attacks from degrading the performance of the network, various security measures are to be proposed. Hello flood attacks are also the type of DoS attacks which are often identified within the WSNs. Due to the presence of such attacks, there is a lack of resources within the networks for each node. In order to determine the problems faced by DoS attacks, a methodology has been generated in this paper. It is to be ensured that a secure and reliable type of data transmission occurs within the network by eliminating the DoS attack from the path established between the source and destination.

III. RESEARCH METHODOLOGY

An active attack that is responsible for dropping the data and control packets within the network is known as the selective forwarding attack. The parameters such as energy consumption, throughput and delay define the performance of the network which can change as per the modifications made within the network. In this work, in order to recognize and remove the malicious nodes from the network, a technique has been proposed. On the basis of traffic analyzer and threshold values present within the network, there is a technique proposed. The central controller is chosen within the network depending on the trust values of the nodes. Depending on the data packets that are re-transmitted within the network, the trust value of the node is computed. There is a central controller node that registers each node according to IP, MAC address and the current data. The bandwidth required for

communication related to the base station is assigned using the central controller node. Depending on the hop count and sequence number, a secure and efficient path is generated from sensor node to base station. The data is transmitted from the sensor node. Further the central node checks individually each node in a random manner. The nodes that have threshold unequal to the decided threshold value are to be detected and presented as malicious node within the network. For removing such malicious nodes from the network, a multipath routing method is presented here.

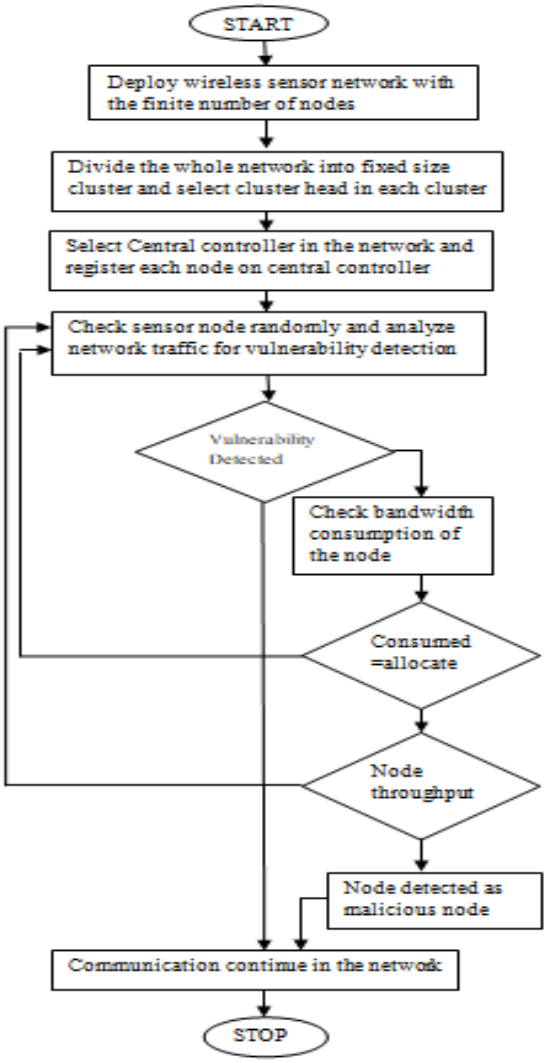

Fig.1: Proposed Algorithm

IV. EXPERIMENTAL RESULTS

The proposed work is implemented in NS2 and the results are evaluated by making comparisons against proposed and existing techniques is terms of several parameters.

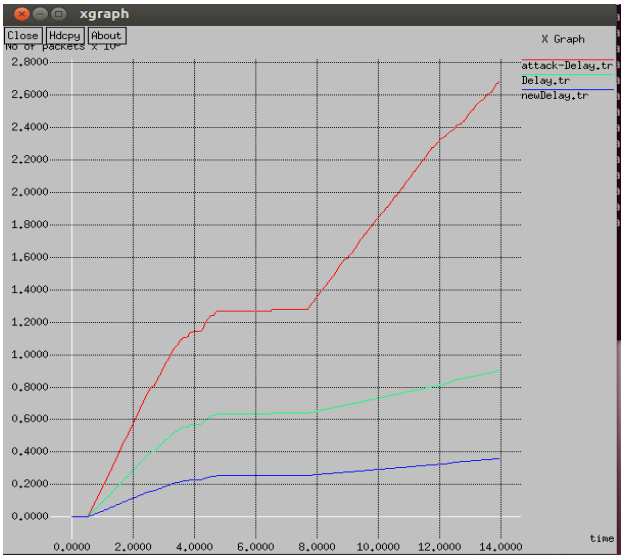

Fig.2: Delay graph

As shown in figure 2, 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.

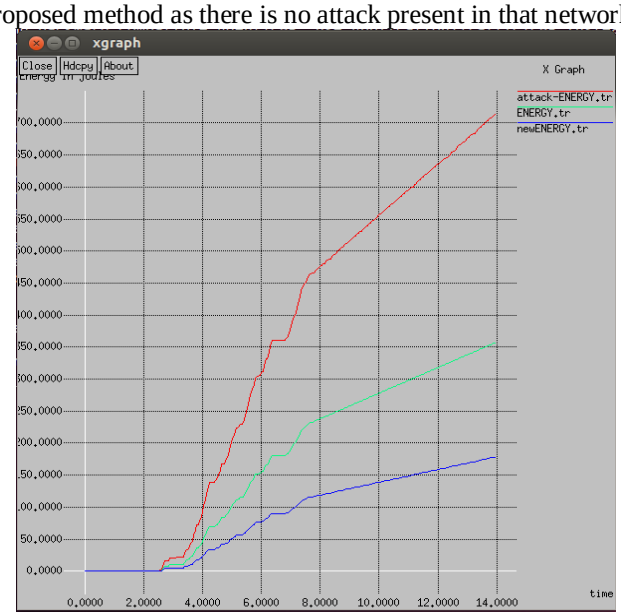

Fig.3: Energy graph

As shown in figure 3, 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

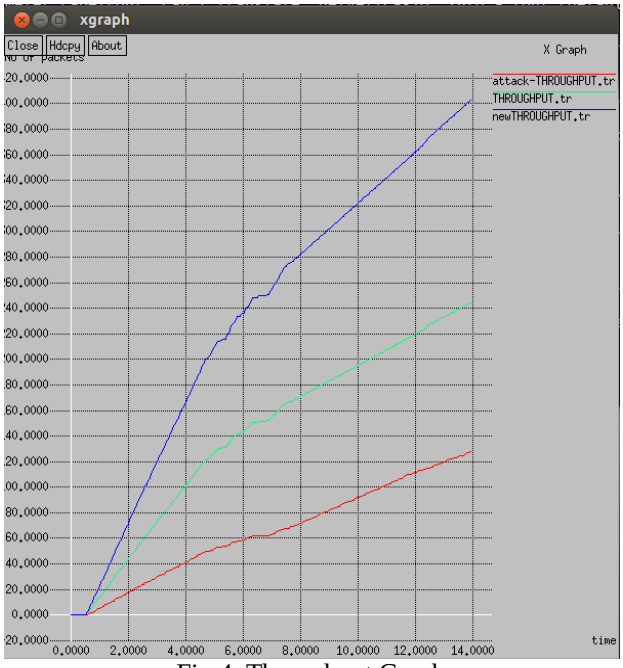

Fig.4: Throughput Graph

As shown in figure 4, 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.

V. 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 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.

VI. REFERENCES

[1]. 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

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

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

[4]. Chun-Hsin Wang and Yang-Tang Li, "Active Black Holes Detection in Ad-Hoc Wireless Networks", IEEE, 2013

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

[6]. Virendra Pal Singh Sweta Jain and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010

[7]. 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.

[8]. Megha Joshi, Saumil Patel," CENTRALIZED SIGNATURE BASED APPROACH FOR WIRELESS SENSOR NETWORK USING RSA ALGORITHM", 2015 International Journal of Technological Research In Engineering Volume 2, Issue 8

[9]. 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

[10]. Omar Said and Alaa Elnashar," Scaling of wireless sensor network intrusion detection probability: 3D sensors, 3D intruders, and 3D environments", 2015 Springer

[11]. 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

[12]. Michael Collins, Simon Dobson, Paddy Nixon," Securing Wireless Sensor Networks: Introducing ASLAN - A Secure Lightweight Architecture for WSNs", 2009 International Journal on Advances in Internet Technology, Vol. 2 No.

[13]. 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