Novel Technique for Detection of Malicious Nodes in Wireless Sensor Networks

[1]Ashish Singh,[2]Dr. Vishal Pareek,[3]Dr. Surendra Yadav
[1]M. Tech (student),[2]Assistant Professor,[3]Professor
[1,2,3]Sri Ganganagar Engineering College, Sri Ganganagar

Abstract-The self-configuring type of network in which the sensor node are deployed in such a manner that they can join or leave the network when they want is known as wireless sensor network. As this type of network is decentralized in nature, there are numerous malicious nodes which might enter the network. Due to the presence of such malicious nodes, the attacks can be triggered which are classified as active and passive types of attacks. The type of attack in which the raw packets are flood to the victim node is known as DDoS type of attack. It is an active type of attack. When the DDoS attack occurs in the network, it minimizes the lifetime of the network and also increases the overall energy consumption of the network. In order to detect the malicious nodes from the network which cause the DDoS attack, a novel approach is to be proposed in this research work.

Keywords- *WSN; Threshold; Delay*

I. INTRODUCTION

There are numerous sensor nodes deployed within a wireless sensor network (WSN) along with one base station in it. The sensor nodes are small sized devices which have very less power, and cost along with constrained memory, computational and communication resources. There are numerous spatially distributed autonomous sensors present within the network which gather the information from their surroundings and pass it to the base station. The nodes deployed within these networks collect the information from surrounding environmental areas. All the gathered information is transmitted to the base station present in the network which acts as a gateway amongst the sensor networks and the external environment. The storage capacity of base stations is very high and it also consists of numerous data processing capabilities which can be useful in the network [1]. The transmitting of important information which is received from the sensor nodes by the base station is its major task. This information can be accessed by the end user and can be utilized as per its requirement. Within the area of base station basically the sensor nodes are deployed which can form groups as per the requirement of the application. Due to the smaller sizes of the sensor nodes, the sizes of their batteries are also small. Due to this, the batteries of the sensor not deplete very easily and cannot be recharged easily as they are deployed in very large areas. Thus, the lifetime of the network reduces which is a major concern. Security in wireless sensor networks has to be comprehensives a fundamental of requirements. These requirements are not only guarantee safeguard of sensitive data but also to achieve bounded resources in each sensor node, which remains the sensor network alive. In order to perform numerous operations within the wireless sensor networks, the basic requirement is power [5]. Within numerous activities such as gathering or data, its processing and communication require energy. Even when the nodes are not performing any tasks, there is a need of huge amount of energy in the components of nodes when some dedicated operations are to be performed. Once, the energy of the nodes is consumed completely, the batteries of these nodes need to be changed or recharged. However, as the nodes are deployed in large areas where it’s not possible for the humans to go, the replacement of these batteries is almost impossible. Thus, within the design and development of wireless sensor networks, this issue is very major. The energy efficient hardware and software protocols are proposed which are applied within these networks. Another challenging issue within the designing of WSN is the maintenance of security of these networks. Not only within the military applications but also in the huge buildings in order to provide alarms and monitor the surroundings, the WSNs are deployed. Attacker motivation and vulnerabilities, and opportunities are two factors, which give the attacker possibility impact to the wireless sensor networks [2]. There are number of attacks in WSN. Wormhole is a type of attack in which there is a formation of a tunnel by the malicious nodes and it is kept hidden from other legitimate nodes. This tunnel is used to send data packets from one malicious node to other. A malicious node in one area attracts the packets from its area and transmits them to the malicious node of other area [3]. There are various ways like in-band and out of band ways for the creation of a tunnel. This kind of attack can put a very huge effect on the procedure of routing and localization as there is no need to make any changes in other genuine networks to trigger this attack. Black hole is again a very dangerous kind of attack as in this attack re-programming in different set of nodes can be done by the attacker. This may lead to the blockage of packets or the attacker can do anything else with the captured packets like generating false messages but does not forward them to the base station in WSN. Sybil attack is an attack in which a malicious node can reshape itself like other different nodes [4]. Multipath routing distributed systems are very prone to this attack as they have no centralized entity which can be used to verify the identity of each node. With the advent in the technology, wireless sensor networks emerged as growing technology in many applications such as weather, military aim tracking, and patient monitoring. Hence, protection is necessary for such types of sensor network from prohibited attackers. It is necessary for the senor networks to have some security measures to mitigate the effects of the attacks [5]. The term jamming is used to define an attack in which the transmission of a radio signal is interfered by radio frequencies which are being used by sensor network. In Distributed Denial of service attack, the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network is called jamming. The communication protocols can be intentionally violated by attacker in link layer, e.g., ZigBee or IEEE 802.11b protocol and in order to attempt collisions messages are continuously transmitted. The packets lost by collision are needed to retransmit [6]. By refusing routing messages a multi-hop network advantage is taken by node in routing layer. The conclusion is that any node that is affected by attacker will not be able to exchange messages with the part of network. In case of flooding, that transport layer is also affected by attack. Number of connection requests is send to malicious node in case of flooding. The connection requests are handled by allocating resources.

II. LITERATURE REVIEW

Shivam Dhuria et.al (2018) proposed two techniques in this paper amongst which the majority of attacks occurring within WSN are prevented through light-weight two-way authentication method. The DDoS attacks are identified and prevented from WSN with the help of another technique which is traffic analysis that is based on data filtering method. Various parameters which include throughput, delay, packet loss, energy consumption and PDR are verified through the Network Simulator 2 (NS2) [7]. This evaluation shows that the proposed technique is very simple and at each node it has been deployed. The DDoS attacks cause whole drainage of battery source which can be prevented with the help of small computations of tracking the data rates from neighbor nodes.

Taranpreet Kaur, et.al, (2016), have analyzed that Wireless Sensor Networks (WSNs) is a collection of large number of sensor nodes that have limited capabilities for collecting sensitive information. There is advancement in this technology that leads to security as major concerns. In WSN, there are number of attacks like Distributed Denial of Service (DDOS) attacks. In order to detect and prevent DDOS attacks, number of researchers has proposed new mechanisms. In this paper [8], authors did a survey on different existing approaches on basis of various parameters. This survey will help researchers to improve the existing techniques that have low false alarm problem and less energy consumption.

Shital Patila, et.al, (2016) proposed an improved Co-FAIS immune system for DoS attack in WSN [9]. Co-FAIS immune system is the first real time intrusion detection model that compares current system with normal system to recognize the attack by using fuzzy logic. Authors have improved the current Co-FAIS system by adding two learning parameters in fuzzy system that helps in improving the accuracy rate of detection and improves learning capabilities. The simulation results show that the proposed system will improve the accuracy rate of attack prevention, reduce the false alarm rate that helps in recognizing different DoS attack.

Raksha Upadhyaya, et.al, (2016), proposed a solution to prevent WSN from DDOS attack [10]. In proposed solution they have used dynamic source routing (DSR). The concerned nodes energy is used for detecting and preventing attacks. The proposed scheme provides a modified DSR with security aware mechanism for DDOS attack. The whole process is carried out in four steps. The DDOS attack is prevented by examine battery charge of each node that provides identification of malicious node. This will help in removing the malicious node from communication and start transferring packet transmission from alternative routes. The proposed scheme is implemented using Qualnet 5.2 simulator.

Raksha Upadhyay, et.al, (2015), have recommended that wireless network with sensing and processing information merit is known as wireless sensor network (WSN). In network, the information and sensor node information is compromised due to different security attacks. The goal of DDOS attack is to infect the network by the drainage of resource capability. Meaningless messages in large numbers are sent by the attacker to increase the network congestion and also degrade the life of node and network. In this paper [11], severe problems have been observed by authors and a solution is proposed a solution to overcome the problem of power draining due to DDOS attack. In order to simulate and evaluating the performance of proposed solution for AODV and DSR routing protocols in WSN they have used Qualnet 5.0 simulator.

Chunnu Lal, (2017) presented that in the wireless senor networks there are various attacks that degrade the functionality of the network but among those attacks denial of services attack is considered as the major attack [12]. Therefore, it becomes major challenge for many researchers to develop effective and lightweight security mechanism that minimizes and prevents the various attacks for WSN such as Denial-of-Service (DoS) attack. Author in this paper consider only effective detection techniques in order to detect the presence of the DoS attack and reduce the power consumption in the wireless sensor network. There is large number of detection mechanisms that exists in the network but sensor nodes has limited power and processing capability to reduce the power consumption hence, it is necessary to design an energy preserving DoS detection mechanism in WSNs.

III. RESEARCH METHODOLOGY

The wireless sensor network is the decentralized type of network in which sensor nodes can join or leave the network when they want. Due to dynamic nature of the network malicious nodes enter the network which is responsible to trigger various types of active and passive attacks. The active attacks are those which affect the network performance in terms of certain parameters. The Denial of service is the active type of attack in which malicious node flood the legitimate nodes with the rough packets to reduce network performance. The distributed denial of service is the advance type of DOS attack in which malicious node choose its slave and slaves will flood the legitimate node which the rough packets and it reduce network performance. This research work, is based on the detection and isolation of malicious nodes from the network which are responsible to trigger DDOS attack in the network. In the proposed technique, the key servers are formed in the network and each node in the network will register itself to the key server node with their data rate and bandwidth consumption. When all the nodes start transmitting data in the network, and when the DDOS attack is triggered in the network and throughput of the network get reduced to threshold value then malicious node detection process starts. In the process of malicious node detection, the nodes which are sending data above the threshold value are considered as malicious node and technique of watch dog is applied that whether these nodes are sending data packets or control packets. When the nodes are sending the data packets, then that nodes are considered as the slave nodes. The technique of monitor mode is applied on the slave nodes which can then analyze the network traffic. When the slave nodes receive the control packets from the other node, then the node which send control packet is detected as the malicious node in the network. The proposed technique is applied under the simulated environment to detect malicious nodes from the network which are responsible to trigger DDOS attack in the network.

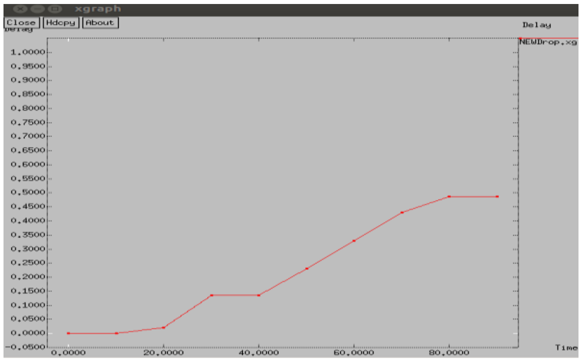
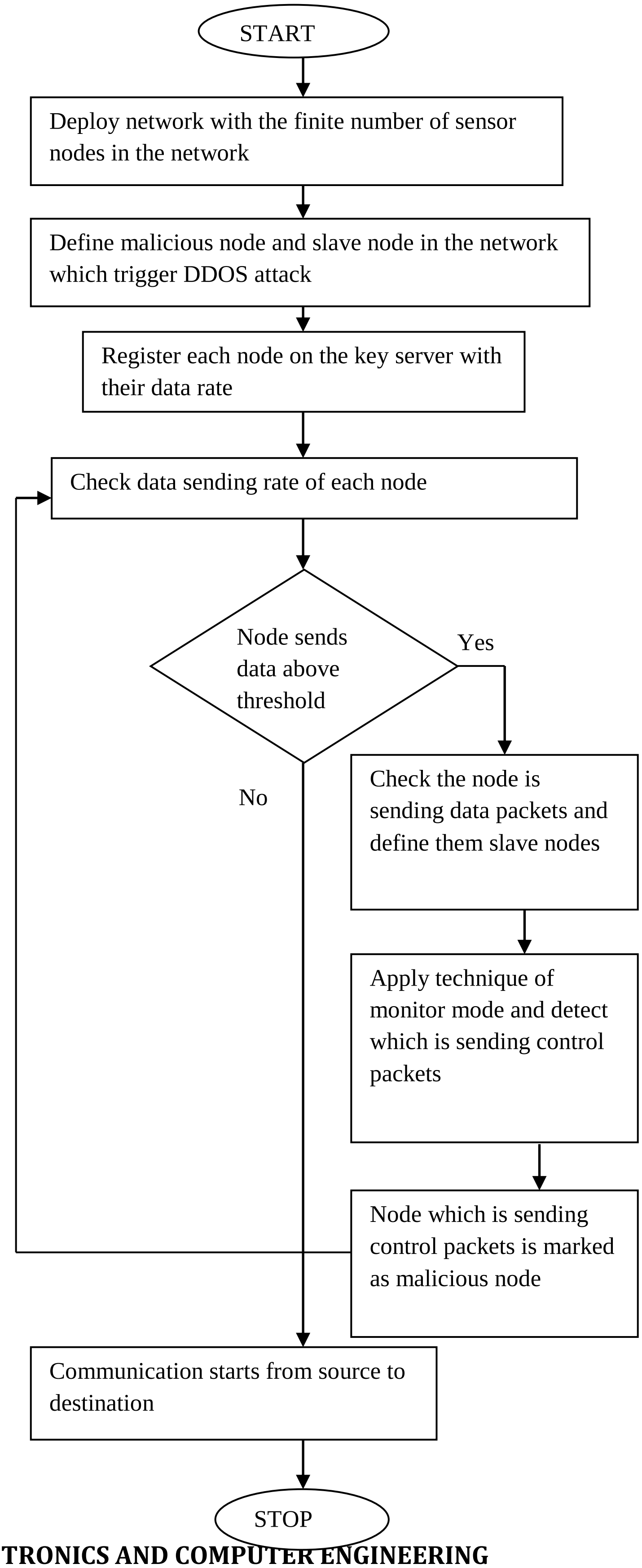


Fig.2: Packetloss Graph

Fig.1: Proposed Flowchart


START
Deploy network with the finite number of sensor nodes in the network
Define malicious node and slave node in the network which trigger DDOS attack
Register each node on the key server with their data rate
Check data sending rate of each node
Node sends data above threshold
Yes
No
Check the node is sending data packets and define them slave nodes
Apply technique of monitor mode and detect which is sending control packets
Node which is sending control packets is marked as malicious node
Communication starts from source to destination
STOP

IV. EXPERIMENTAL RESULTS

The proposed approach is implemented in NS2 and the results are analyzed by making comparisons amongst proposed and existing approaches in terms of packet loss, throughput and energy consumption in the networks.

As shown in figure 2, the technique of neural networks is applied in this research work. The proposed improvement leads detection of malicious nodes due to which packet loss get reduced in the network.

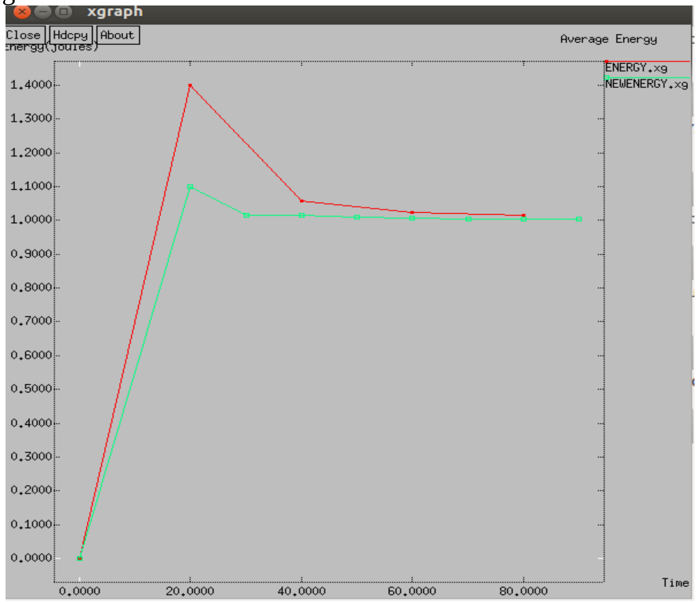


Fig.3: Energy Consumption

As shown in figure 3, the sensor nodes have very small size and it is self configuring in nature. Due to which energy consumption needs to reduce to increase network lifetime. In this graph the energy consumption graph is represented.

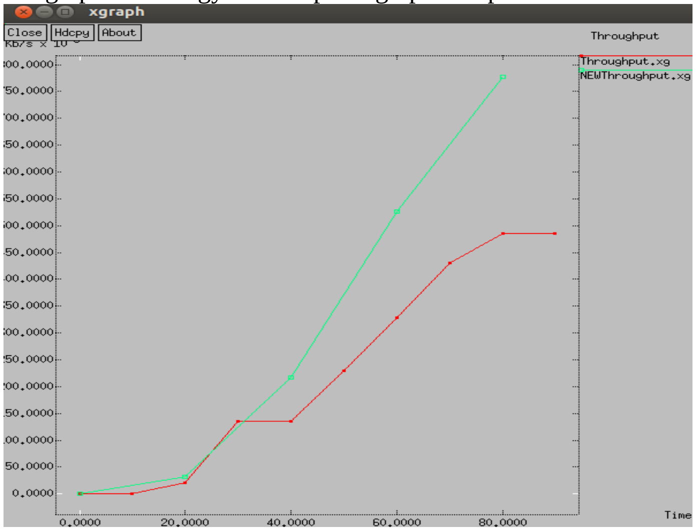


Fig.4: Throughput Comparison

As shown in figure 4, the throughput of the proposed scenario is compared with the existing scenario. It is analyzed that when attack is isolated from the network, then throughput is increased at steady rate.

V. CONCLUSION

In this research work, it has been concluded that Wireless Sensor Network is the self-configuring network due to which some malicious nodes enter the network which are responsible to trigger active and passive attacks in the network. The DDoS attack is the Distributed Denial of Service attack in which the malicious nodes flood the victim with the raw packets. The technique of threshold will be proposed which detects and isolated malicious node from the network. The proposed improvement leads to increase network lifetime, throughput and reduce network delay.

REFERENCES

[1] M.H. Anisi, A.H. Abdullah, S.A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", Wireless Sensor Networks, vol. 3, pp. 329-333, 2011.

[2] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, vol. 13, pp. 14-27, 2010.

[3] M.K. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, pp. 62-67, 2011.

[4] A.K. Pathan, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. 8th International Conf. Advanced Communication Technology, vol. 2, pp. 1043-1048, 2006.

[5] Patel MM, Aggarwal A, "Two phase wormhole detection approach for dynamic wireless sensor networks in Wireless Communications Signal Processing and Networking (WiSPNET)", 2016 International Conference on IEEE, vol. 5, pp. 2109-2112, 2016.

[6] Krishnan NS, Srinivasan P, "A qos parameter based solution for black hole denial of service attack in wireless sensor networks", Indian J Sci Technol, vol. 9, pp. 1001-1010, 2016.

[7] Shivam Dhuria and Monika Sachdeva, "Detection and Prevention of DDoS Attacks in Wireless Sensor Networks" Springer Nature Singapore Pte Ltd. 2018

[8] Taranpreet Kaur, Dr. Krishan Kumar Saluja, Dr Anuj Kumar Sharma, "DDOS Attack in WSN: A Survey", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), vol. 4, pp. 131-140, 2016.

[9] Shital Patila, Sangita Chaudhari, "DoS attack prevention technique in Wireless Sensor Networks", Elsevier 7th International Conference on Communication, Computing and Virtualization 2016, vol. 79, pp. 715-721, 2016.

[10] Raksha Upadhyaya, Uma Rathore Bhatta, Harendra Tripathia, "DDOS Attack Aware DSR Routing Protocol in WSN", ELSEVIER International Conference on Information Security & Privacy (ICISP2015), vol. 78, pp. 68-74, 2016.

[11] Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt, “Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain”, 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), vol. 3, pp. 446-451, 2015.

[12] Chunnu Lal, “A SURVEY ON DENIAL-OF-SERVICE ATTACKS DETECTION AND PREVENTION MECHANISMS IN WIRELESS SENSOR NETWORKS”, 2017, INTERNATIONAL JOURNAL OF CURRENT ENGINEERING AND SCIENTIFIC RESEARCH (IJCESR), VOLUME-4, ISSUE-10