International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Threshold Based Algorithm for the Detection of DDOS Attack in Wireless Sensor Networks

Poonam Sharma, Megha Sharma

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. The nodes start communicating with each other in order to transmit important information within the network. As this type of network is decentralized in nature there are numerous malicious nodes which might enter the network. There are so many attacks possible on WSN, in Distributed Denial of Service (DDOS) attacks, malicious nodes adapts many attacks such as flooding attack, black hole attack and warm hole attack, to halt the overall functioning of network. The risks are even more when we talk about military and industrial applications. The DDoS 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: DdoS, WSN, Threshold

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 [1]. 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. The transmitting of important information which is received by the base station from the sensor nodes is its major task [2].

Manuscript published on November 30, 2019.
* Correspondence Author
Poonam Sharma*, Research Scholar, Sirda Group of Institutions Naulakha, Himachal Pradesh, India. E-mail: poonamsharma8945@gmail.com
Megha Sharma, Assistant Professor, Sirda Group of Institutions Naulakha, Himachal Pradesh, India. E-mail: megha1110sharma@gmail.com

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 [3]. Thus, the lifetime of the network reduces which is a major concern. Wireless sensor network has emerged numerous applications in various fields with huge classification. It is difficult to avoid overlap and systematic arrangement is difficult. It is divided into two complimentary steps from functional point of view such as in first, data is collected from the SNs and in second, distribution of the data to the desired system in order to perform the action, hence it is utilized as an actuator. In the first step, the location of the SNs is determined selecting location an adequate data rate is selected. For the transfer of the data harmonization between is required such as SN clock synchronization, coordination between the sleep and awake cycle sequence, increase in the volume of collected data and transfer of data to base station through storage. Second step, all the accumulated data must be delivered to preferred devices along with actuators [4]. Security is the major concern in the wireless sensor network which completes all the fundamental requirements of the network. Protections are provided to the sensitive data with these requirements as well as minimize the issue of the constrained resources in each node due to which sensor network remains active. 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 [5]. Blackhole 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. Multipath routing distributed systems are very prone to this attack due to absence of centralized network which is utilized to identify each node. The term jamming is used to define an attack in which the radio signals are transferred is interfered by radio frequencies which has been utilized by the sensor network [6].

There is of two types of jamming. There is intersection of transmission of a radio signal with radio frequencies in the distributed denial of service attack that has been utilized by 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. By refusing routing messages a multi-hop network advantage is taken by node in routing layer [7]. 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. In this attack excessive amount of packets are sent are sent to a server to slow down its pace or to make the scarcity of resources to the users so that a user cannot access the facility.

II. LITERATURE REVIEW

ShitalPatila et.al, (2016) proposed an improved Co-FAIS immune system for DoS attack in WSN [8]. Co-FAIS immune system is the intrusion detection model first real time system that compares current system with normal system to recognize the attack by using fuzzy logic. But it has some disadvantages such as lacks in capability of easy learning and based model i.e. single which do not changes with change in time during the process of detection. So, 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. As per simulation result, concluded that accuracy rate of attack prevention has been improved due to this proposed system and minimizes the false alarm rate that helps in recognizing different DoS attack.

Raksha Upadhyaya, et.al, (2016) proposed an optimal solution for the prevention of DDOS attack from sensor networks [9]. In proposed solution they have used dynamic source routing. For the detection and prevention of attacks, the disturbed nodes energy was utilized. The modification in DSR along with some security mechanism for DDOS attack has been proposed in this paper. For this purpose, they carried out four steps. The examination of battery charge of each node prevents the above mentioned attack by identifying malicious nodes. Since a sensor network does not have any blacklist to detect malicious nodes therefore a shutdown method can be applied to minimize these infectious nodes. With the help of this infectious nodes are removed from the communication and start using alternative ways to transfer data or packets. Qualnet 5.2 simulator was utilized in this paper for the implementation of the proposed scheme.

Katarzyna Mazur, et.al (2016) proposed the two security levels with eight defined scenarios and different number of compromised devices. Author in this paper investigated the sink's performance and energy consumption under the DDoS attack using simulations. After obtaining all the results from the simulations, a new kind of (DDoS) attack is identified [10]. All the processed packets in the network are not encrypted hence, there impacts on the network is dangerous as it bring down the whole network down and draining valuable energy resources. On the basis of conclusion it is also known that the security level can be possibly adjusted on the basis of the type of the DDoS attack as it prevents different types of attacks. It is also possible to avoid DDoS or delay in the network by lowering security level in certain conditions.

Chunnu Lal, (2017) proposed various techniques that has been utilized by various researchers in order to detect the presence of the denial-of-service attack in WSN. Due to the limited resources for the WSN devices, these attacks are more vulnerable to the consumption and destruction of these inadequate resources [11]. 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 due to the limited power and processing capability of sensor nodes in oreder to reduce the power consumption hence, it is necessary to design an energy preserving DoS detection mechanism in WSNs.

Surendra Nagar, et.al (2017) proposed routing protocol to provide security to wireless sensor network, in order to prevent the DDoS attack from the network. With the help of this proposed protocol infectious nodes within the network is scanned and scanned node is blocked to prevent further activities in the network. Intrusion prevention scheme has been utilized by the author to protect the network in which the specific node of the network acts as IPS node [12]. When a malicious node is identified by the IPS node that involved in passing messages to nodes other than UDP and TCP messages, this malicious node is blocked by the IPS node for further sending empty messages. NS 2.35 has been utilized in this paper for the simulation process. On the basis of obtained results, it is concluded that proposed method give feasible resultsto protect the network against DDoS attack as compared to other methods.

ShivamDhuriaand Monika Sachdeva (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) [13]. Majority of the DDoS attacks are identified and prevented on the basis of authentication and data filtering technique. 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.

III. RESEARCH METHODOLOGY

In the wireless sensor network, sensor nodes can connect or dissert the network anytime when they want due to property of decentralization. Due to the decentralization property any node can enter into the network that node can be the legitimate node or the malicious node. Presence of malicious node within the network is responsible of triggering active and passive attacks this is due to dynamic nature of the networks. The malicious node can degrade the performance of the network. The network performance in terms of certain parameters has been affected by the active attacks. There are so many attacks possible on WSN, in Distributed-Denial of Service (DDOS) attacks, malicious nodes adapts many attacks such as flooding attack, black hole attack and warm hole attack to halt the overall functioning of network. 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 so that presence of malicious nodes can be determined easily which is responsible of causing DDOS attack in the network.

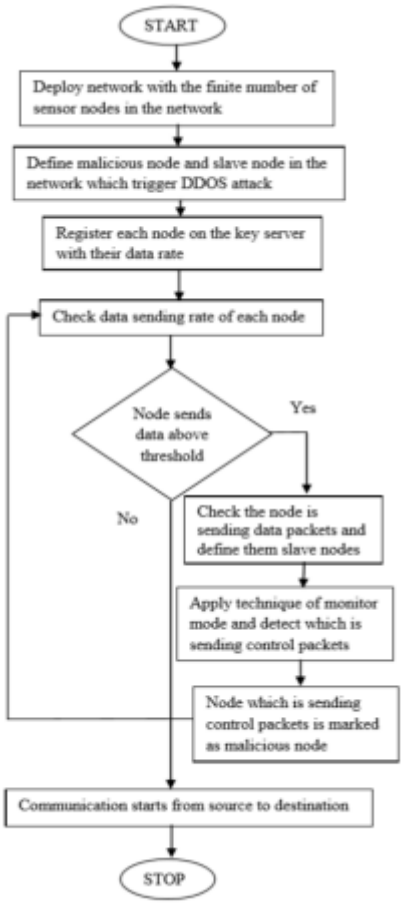

Figure 1: Proposed Flowchart

IV. EXPERIMENTAL RESULTS

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

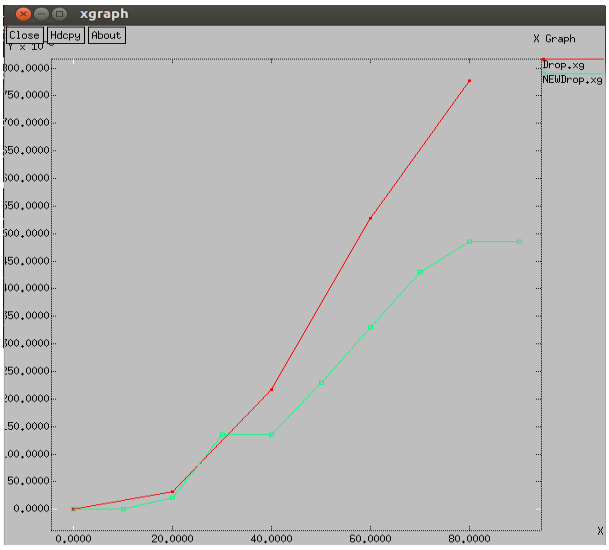

Fig 2: Packetloss Graph

This fig.2 shows the condition of the network at the time of the attack and when the attack is prevented.

The red line shows the packet loss at the time of attack and the other one show the packet loss at the time when the attack is being prevented. Hence after the attack has been prevented the packet loss of the network is reduced.

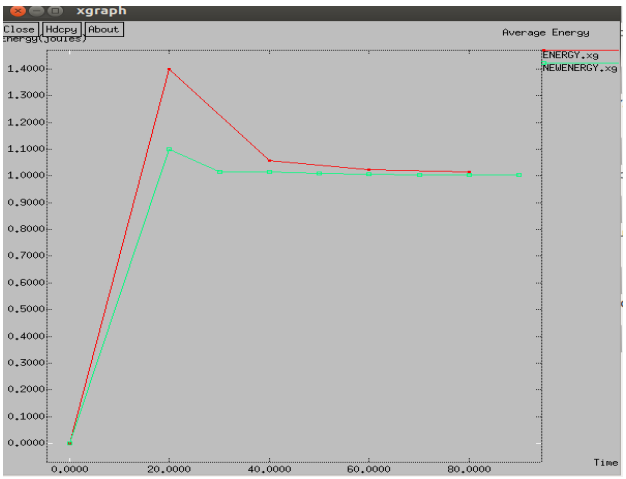

Fig 3: Energy Consumption

As shown in Fig. 3, graph the energy consumption of nodes is represented when the attack occurs and when the attack has been prevented. At the time of attack the energy consumption of nodes are high but when the attack is prevented the energy consumption of nodes are reduced.

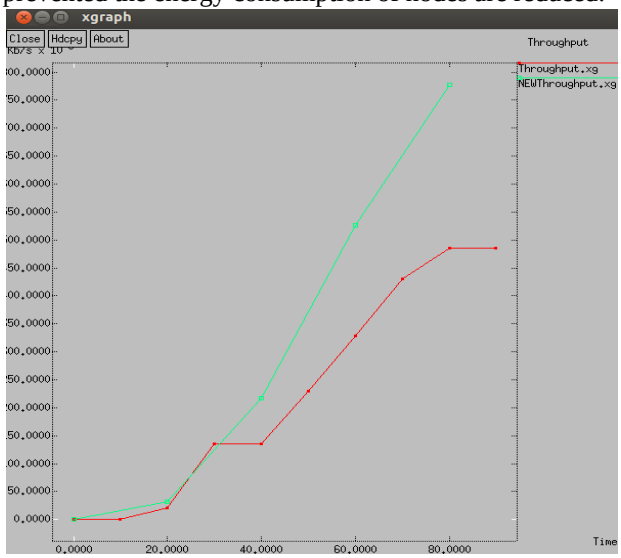

Fig 4: Throughput Comparison

As shown in Fig.4, the throughput of the proposed scenario is compared with the existing scenario. Throughput is one of the parameter to observe the performance of the network. Throughput is the number of messages delivered per unit time. In order to say that the performance of the network or any system is good then the throughput of the system should be high. In this graph both the throughputs are compared throughput before the attack and after the attack. 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. The network throughput is increased upto 20 percent in the proposed technique as compared to existing technique. The network lifetime is increased upto 10 percent and network delay is reduced upto 20 percent.

REFERENCES

1. Jiang, L., Bing Fang, & Li., "Energy optimized approach based on clustering routing Protocol for wireless sensor networks", CCD Conference. IEEE, vol. 5, pp. 181-190, 2011
2. M.K. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, pp. 62-67, 2011.
3. Jiawei Chen, "Broadcast Authentication Protocol Scheme Based on DBP-MSP and Safe Routing in WSN against DDoS Attacks", 2011 Second International Conference on Networking and Distributed Computing.
4. Omer Demir, Bilal Khan, "Finding DDoS Attack Sources: Searchlight Localization Algorithm for Network Tomography", 2011, IEEE.
5. Neamatollahi, P., Taheri, H., Naghibzadeh, M., &Yaghmaee, M., "A hybrid clustering approach for prolonging lifetime in wireless sensor networks", IEEE In Computer Networks and Distributed Systems (CNDS), 2011 International Symposium on, vol. 6, pp. 170-174, 2011.
6. ZHANG Yi-ying, LI Xiang-zhen, LIU Yuan-an, "The detection and defense of DoS attack for wireless sensor network", 2012, Science Direct, 19(Suppl. 2): 52–56.
7. Sukhwinder Sharma, Rakesh Kumar Bansal, Savina Bansal, "Issues and Challenges in Wireless Sensor Networks", IEEE International Conference on Machine Intelligence Research and Advancement, vol 4, pp.58-62, 2013.
8. ShitalPatila, SangitaChaudhari, "DoS attack prevention technique in Wireless Sensor Networks", Elsevier 7th International Conference on Communication, Computing and Virtualization 2016, vol. 79, pp. 715-721, 2016.
9. RakshaUpadhyaya, Uma Rathore Bhatta, HarendraTripathia, "DDOS Attack Aware DSR Routing Protocol in WSN", ELSEVIER International Conference on Information Security & Privacy (ICISP2015), vol. 78, pp. 68-74, 2016.
10. KatarzynaMazur, Bogdan Ksiezopolski, and RadoslawNielek, "Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks", 2016, Hindawi Publishing Corporation Journal of Sensors.
11. 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.
12. Surendra Nagar, Shyam Singh Rajput , Avadesh Kumar Gupta, Munesh Chandra Trivedi, "Secure Routing Against DDoS Attack in Wireless Sensor Network", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017).
13. ShivamDhuria and Monika Sachdeva, "Detection and Prevention of DDoS Attacks in Wireless Sensor Networks" Springer Nature Singapore Pte Ltd. 2018.