Threshold Technique for Isolation of Sinkhole Attack in WSN

Manvita Singh[1], Mrs. Amandeep Kaur[2], Leena Mahajan[3]
[1]Research Scholar, [23]Assistant Professor
[12]Punjabi University, Patiala, Punjab, India
[3]Indo Global College, Mohali, India

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. With the advancement of this technology, one of the major concerns these days is of security. The attacks are triggered within the network due to the presence of such kind of malicious nodes in the network. The sinkhole is an active type of attack. When the sink hole 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 sink hole attack, a novel approach is to be proposed in this research work.

keywords- WSN, LEACH, Sink Hole, Active, Passive, Attack

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 [1]. 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 [2]. 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 [3]. Attacker impacts on the wireless sensor network are possible due to two factors such as vulnerabilities and opportunities. 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 [4]. 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. There are various ways like in-band and out of band ways for the creation of a tunnel. 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. Denial of Service (DOS) attack can be triggered at different layers but the primary motive of these attacks is to temporarily make the network resources unavailable. The complete programming of the sensors can be manipulated by the attackers [5]. The attackers can be so influential that they can even place a false sensor in place of a legitimate sensor, resulting in the modification of whole circuitry. Sinkhole Attack is the attack in which base station is being prohibited so that it cannot access correct data or information, also known as dangerous attack. This attack occurs in the higher layer application of the network. The main objective of this attack is to attract all the traffic from the area using a malicious node and at the center it creates a metaphorical sinkhole. 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. There is of two types of jamming [6]. 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), analyzed wide range of application of wireless sensor networks in this paper that has been utilized for the data gathering and data transmission process. In this paper [8], authors have proposed an improved Co-FAIS immune system for DoS attack in WSN. 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. 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.

RakshaUpadhyaya, et.al, (2016), analyzed that open nature of wireless sensor networks (WSN) results in more vulnerability to outside attacks. In this paper [9], authors have proposed an optimal solution for the prevention of DDOS attack from sensor networks. In proposed solution they have used dynamic source routing. For the detection and prevention of attacks, the disturbed nodes energy was utilized. 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. 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) presented the issue of DDoS attack and its multilevel analysis in the wireless sensor network as it degrades the functionality of the whole system. They 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]. 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 [11]. 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 order 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]. 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 results to 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

This research work, is based on the detection and isolation of malicious nodes from the network which are responsible to trigger sink hole 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 sink hole 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 sink hole attack in the network.

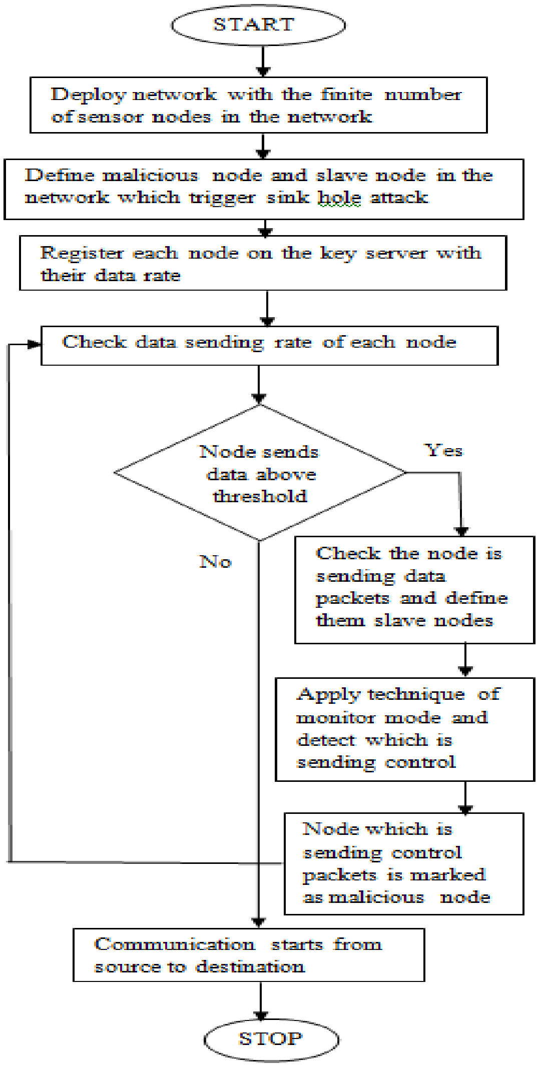
START
Deploy network with the finite number of sensor nodes in the network
Define malicious node and slave node in the network which trigger sink hole attack
Register each node on the key server with their data rate
Check data sending rate of each node
Node sends data above threshold
Yes
No
Check the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

Fig.1: Proposed Flowchart

IV. EXPERIMENTAL RESULTS

The proposed algorithm is implemented in MATLAB and the results are evaluated by making comparison against proposed and existing algorithms with respect to certain parameters.

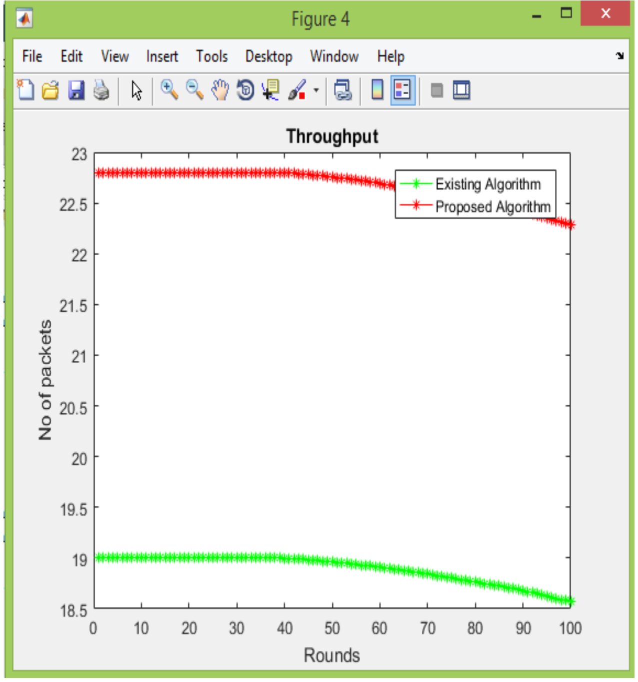

Fig.2: Throughput Comparison

As shown in figure 2, the throughput of the proposed technique in which threshold is applied for the secure channel is analyzed. It is analyzed that throughput is increased at steady rate.

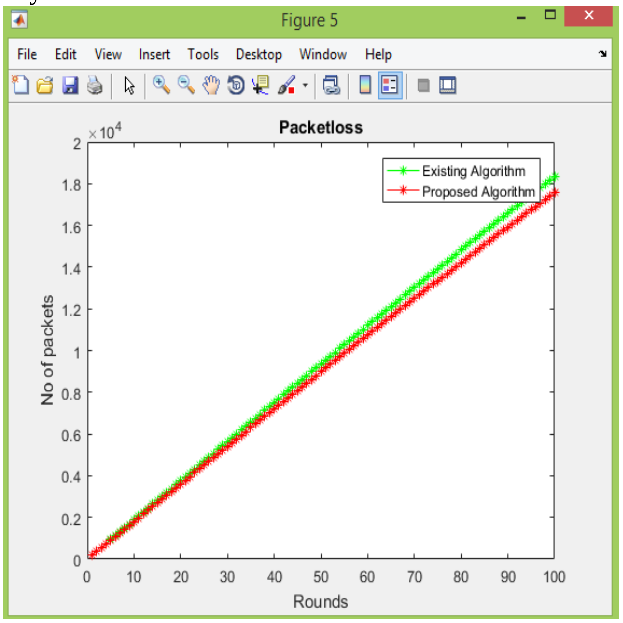

Fig.3: Packet loss Comparison

As shown in figure 3, when the threshold technique is applied, the malicious node is detected from the network which reduces packet loss. In the figure, the x axis shows number of rounds and y axis shows number of packets.

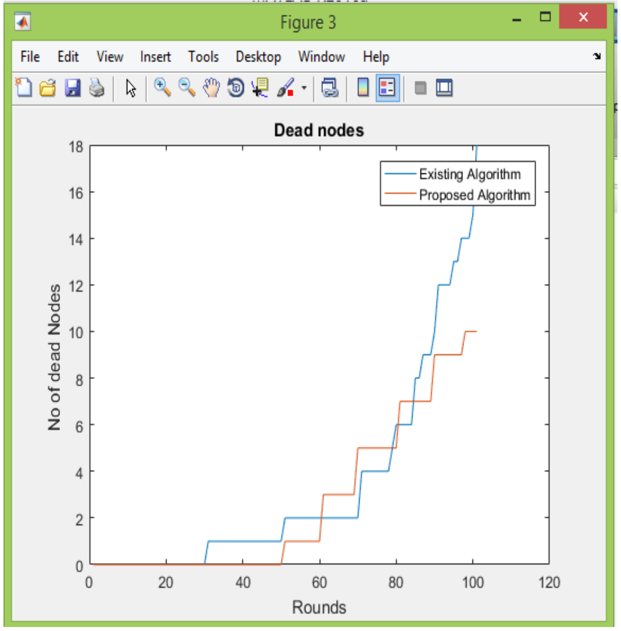

Fig.4: Comparison of Dead Node

As shown in figure 4, the graph is shown in which number of dead nodes are shown versus number of rounds. On the x-axis the numbers of rounds are shown and on the y-axis the numbers of dead nodes are illustrated. The proposed technique has less number of dead nodes as compared to existing technique.

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 sink hole 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

VI. REFERENCES

[1]. MahsaSeyyedtaj, Mohammad Ali JabraeilJamali, “Different Types of Attacks and Detection Techniques in Mobile Ad Hoc Network”, International Journal of Computer Applications Technology and Research vol.3, pp. 541 – 546, 2014.

[2]. G. Kumar, “Understanding denial of service (dos) attacks using osi reference model,”international Journal of Education and Science Research, vol. 1, no. 5, 2014.

[3]. Varsha Nigam, Saurabh Jain, Dr. Kavita Burse, “Profile based Scheme against DDoS Attack in WSN”, IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies, vol. 5, pp. 112-116, 2014.

[4]. RakshaUpadhyay, Salman Khan, HarendraTripathi, 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.

[5]. William Hurst, Nathan Shone, Quentin Monnet, “Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures”, 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications.

[6]. Monika Malik, Dr. Yudhvir Singh, “A Review: DoS and DDoS Attacks”, 2015, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 6, pg.260 – 265.

[7]. 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.

[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.