SECURE TECHNIQUE FOR DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

Neha Mathur*1, Dr. Pramod Sharma*2

*1MTech Student, Department of Electronics and Communication Engineering, RCERT, Jaipur, Rajasthan, India.

*2Professor, Department of Electronics and Communication Engineering, RCERT, Jaipur, Rajasthan, India.

ABSTRACT

The wireless sensor network is made up of a vast number of sensors that are scattered around a geographic region where we must keep track of the developments. Sensor hubs typically include sensors, actuators, memory, and a processor, as well as the ability to communicate with other sensors. The sensor network is vulnerable to a number of active and passive attacks. Black hole is the most well-known and damaging active attack of all the possibilities. This attack delays down network execution and triggers a denial of service attack. The attack is started by a malicious hub that is present on the network. In this article, a novel method for identifying and eliminating malicious nodes from the network that are responsible for initiating the attack is presented. The new approach is based on the Delphi scheme. The exploratory results will demonstrate that proposed strategy detects and separate the malicious nodes from the network proficiently. It will enhance network effectiveness as was as bundle misfortune, defer and expand outturn of the network. NS2 machine tools are used as a locality of it.

Keywords: LEACH, WSN, mutual authentication, misdirection attack.

I. INTRODUCTION

Wireless Sensor Network may be a set of lightweight and small wireless type sensors with shrewd calculative components. Element nodes are a unit cheaper, having restricted processing capabilities and energy storage. The WSN consists of an oversized range (hundreds or thousands) of those sensor elements. These styles of network area unit extremely distributed and deployed in hostile environments [1]. WSN monitors the surroundings as well as system via taking physical parameters, like, Temperature, moisture and weight. These wireless sensing elements are a unit best suitable for applications like military order, natural life checking, shrewd interchanges, trendy control, circulated apply autonomy, perception of essential bases, sensible structures, movement perceptive, checking human heart ranges, etc. So, WSN is an assortment of tiny devices that gives:

1. Efficient and reliable communications.
2. Able to measure physical and environmental conditions like humidity, pressure and temperature.
3. For control conditions, Wireless Sensor Network is able to drive devices, such as switches & motors actuators.

WSN has 2 kinds of sensor nodes that's - sink node, and a sensor element node. A large number of sensing element nodes are found in WSN that sense or collect the information and transmit it through multiple hops to the sink.

Misdirection attack in Wireless Sensor Network: - It is the most popular DoS. The Misdirection attack can be executed in many ways [5]. A malicious node may deny a considerable course to a selected node during this manner denying service to the destination.

Misdirection attack can occur in two ways:

1) Packets Forwarded to a Node Near to the Destination: This sort of misdirection assault is less serious, on the grounds that packets compass to the destination however from an alternate course which assist deliver long delay, consequently diminishing throughput of system (bit exchange every second).
2). Packets Forwarded to a Node Far Away from the Destination: This sort of misdirection assault is extremely destructive in light of the fact that all packets are sent to a node far away, averting them to achieve the destination so packets won’t achieve destination. Because of the assault the delay gets to be unending and assist results in zero throughputs.

Consequently, misdirection attacks are harmful in nature as they cause degradation in the performance of network. There are number of nodes deployed in the network. The data is transferred to the destination by the source. All the packets are sinks by the malicious node which drop all the packets to forward it [6]. Path is established between source and destination using AODV protocol.

II. LITERATURE REVIEW

Rehman et. al. (2019) performed sinkhole attacks in wireless sensor networks: a survey, they took around 40 cases based on sinkhole attacks in WSN, in this survey they reviewed all work related on detection, prevention strategies and attack techniques on sinkhole attack that also highlights open challenges in dealing with such attacks, Wireless Sensor Networks are at high risk like, various routing strikes, data genuineness, secrecy, integrity, and proximity, a security protocol was created by focusing a particular attack in WSN, most renowned attacks were denial of service, selective; sink hole; work hole; attack etc. This survey majorly focuses on the most challenging Sinkhole attack detection; prevention strategies; & attack techniques that also highlights open challenges in dealing with such attacks.

Kaur and Kumar (2018) studied mitigation of black-hole attack & worm-hole attack in wireless sensor networks using AODV protocol, they proposed techniques used to defend from the Denial-of-service attacks that are described and for detection and defending from the black-hole attack and worm-hole attack. The proposed technology is less complicated & easy to apply; as well as require less power; thus increases network life-span.

Kamble et.al. in [2017] as discussed in paper [9], is that sending data directly to the sink node within Wireless Sensor increases various issues. Information collecting method is the midpoint of the wireless sensor network. To decrease the energy utilization and also increase in network life-span, Information aggregation method is used. In this paper data aggregation is done to avoid such problems related to energy. For collecting data from cluster head inside the cluster, an system which is energy effective and in which data collection nodes are utilized. The lifespan of the wireless network is improved by forwarding the data in aggregated format.

Rani et.al. (2015) presented in this paper [10] that when there is a change in the network topology, there is a change in the energy efficiency and the fault tolerance protocols. The maintenance of the two parameters is very crucial and so the many techniques have been suggested, that can help to put a stop to the attacks to occur. The main degradation of energy happens because of the attacks which are originated by the intruders. Approaches like cluster-based methods are described in this article that will stop the energy from being ruined. With help of this; throughput maintenance can also be done. Many techniques & methods are proposed through this article which will help to put a stop to all the attacks and also to keep the network secure.

Joshi et.al. (2015) proposed in this paper [11] that late improvements in Micro-Electro-Mechanical Systems (MEMS), wireless communications, and digital hardware have enabled advancement of ease, low power; multifunctional sensor nodes are small and opportunity to impart in short separations. In this paper, a definite study has been carried out identified with different investigation strategies, which could be utilized to address present uncertain issues in wireless sensor networks. The greater part of the studied papers concentrates on various strategies to ascertain trust and reputation and give security to the wireless sensor network. In any case, To make utilization of all available powerful base stations and also using the unified methodology, it has be observed that, to play out these calculations and diminish the weight of the power consuming reputation request and the calculations on the sensor nodes.

Anand et.al (2016) Suggested in the paper [12] that because of the scattered way of WSNs, resource constraints, the radio link for multi-bounce communications and their remote region deployment, DoS attacks is an arrangement of attacks started by individual node or group of nodes by misusing the transmission to deny different nodes from legitimate access to resources. To determine the problems in DoS attacks by actualizing wordings, a creation of a methodology took place in proposed mechanism. E.g. the validating nodes with a key mechanism & intruder detection method, as a sly activity from the path needed with the victim node; as an
internal striker inside network. The main requirement of this proposed work is to come-up with a secure and dependable data transmission above originated and destination by identifying DoS attack.

Said et al. (2015) proposed in this paper [13], another model that deploys heterogeneous sensors in 3D wireless sensor networks (WSNs). The model handles the two sensing situations, single sensing and multiple sensing. WSN proficiency under various probabilistic distributions is additionally illustrated. For the evaluation of the proposed model; a simulation domain is built utilizing OPNET and NS2. The simulation results demonstrated that Gaussian distribution gives the best proficiency and execution. The outcomes demonstrated that Gaussian WSN have the best execution in both evaluation approaches, then uniform WSN. The beta and the chi-square WSNs have the most minimal execution. Additionally, the end-to-end deferral is the main parameter where the uniform WSN gives preferable execution over the Gaussian WSN. Simulation consequences of the proposed model demonstrate that Gaussian sensors distribution in WSN is suggested in 3D situations.

Biswa et al. (2015) proposed in this paper [14] the main propose of the paper which is to show different sorts of Security attacks, defense mechanisms and effects of security attack in Wireless Sensor Network which is unprotected to security attacks and dangers because of its attributes and restrictions. This overview paper concentrates on different parts of many security attacks, their effects and defense mechanisms comparing to every attack and so on. Hence, this paper helps analysts to have an extremely solid thought regarding the existing attack, security issues and they can similarly utilize the ideas and ideas to construct more protected framework of WSN in future. A bearing can be gotten to grow new protected mechanisms to prevent new conceivable attacks along with existing ones.

Fotohi et al. (2020) studied that wireless sensor networks should be secured against denial-of-sleep attacks with the help of RSA cryptography algorithm and interlock protocol, they used Sensor Detection Accuracy (ASDA-RSA) method that is utilized to counteract DoS attacks to reduce the energy consumption amount, in this paper the ASDA-RSA schema consists of two phases to increase security in the WSNs, in first one, a clustering method depends on distance and energy which is used to select the proper cluster head and in second one, the interlock protocol and RSA cryptography algorithm were used along with an authentication method, to protect from DoS attacks. They concluded that the Wireless network performance metrics can be improvised in terms of Packet delivery ration (PDR), average throughput, average residual energy, network lifetime and detection ratio.

III. RESEARCH METHODOLOGY

As shown in the flowchart, the whole network is deployed with the finite number of sensor nodes and the whole network is divided into fixed size clusters. The location-based clustering is applied to divide the whole network in the clusters. The techniques of LEACH protocol have been used for selection of the cluster head within each cluster. In the LEACH protocol, energy and distance of each node is checked, node which has minimum distance and maximum energy from the other nodes is chosen as the cluster head. All nodes of the network will aggregate its data to its cluster head. Then, this cluster head will establish path through other cluster heads and transmit data to the base station. To establish path from source to destination, AODV routing protocol is used. In AODV routing protocol the source node will flood the route request of packets, the adjacent nodes of the destination will respond back with the route reply packets. The source node selects best path on the basis of hop count and sequence number. The path which has minimum hop count and maximum sequence number will be chosen as the best path to destination. The source node starts transmitting data to destination on the path. Malicious nodes are responsible for triggering misdirection attack, using the selected path. To detect & isolate malicious-nodes, the base station will apply technique of node localization.

IV. MODELING AND ANALYSIS

In the technique of node localization, base station will gather node information in terms of their location. The gathered information also contains the distance of each other from the base station. The distance factor leads to count delay on each hop which is on the established path. The base station when detect that delay is increased on the established path. Delay on each hop is counted by base station due to which delay in node increased in the network as well identify the present malicious nodes.
Figure 1: 3D view of building.

V. RESULTS AND DISCUSSION

The given approach is implemented in Network Simulator-2 and results are derived in terms of delay, energy consumption and packet loss.
In figure 2 as shown, the comparison of LEACH, Attack and proposed technique is shown in terms of delay. It is been analyzed that delay in the attack scenario is maximum and delay is reduced in proposed scenario due to isolation of attack in the network.

![Energy Graph](image1)

**Figure 3: Energy graph**

In figure 3 as shown, the comparison of the proposed, LEACH and attack scenario is shown in terms of energy. It is been analyzed that energy consumption of the proposed scenario is least as compared to LEACH and attack scenario.

![Throughput Graph](image2)

**Figure 4: Throughput Graph**

In figure 4 as shown, the comparison of leach, attack and proposed scenario is shown in terms of throughput. It is been analyzed that throughput of the proposed scenario is maximum as compared to other two scenarios.

VI. Conclusion

The WSNs is the kind of network in which sensor nodes can sense environmental conditions and sensed information will be passed to base station. The sensor nodes are very in small size due to which battery life of the sensor nodes is limited. The WSNs are the self-configuring type of network due to which some malicious nodes may join the network. These malicious nodes are responsible to activate misdirection attack in the network. In this work, technique is given that will detect and isolate malicious nodes from the network. The proposed technique is based on node localization in this technique base station will analyze the delay per hop. The node which can increase delay maximum times will be detected as malicious nodes in the network. It is analyzed that energy consumption of the network get reduced, throughput get increased and delay get reduced in the network.
VII. REFERENCES


