International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 03 | March - 2021 ISSN: 2582-3930

# Black Hole Attack In Wireless Sensor Networks

**Neha Mathur[1], Dr. Pramod Sharma[2]**

[1]*MTech Student, Department of Electronics and Communication, RCERT, Jaipur, Rajasthan, India*
[2]*Professor, Department of Electronics and Communication, RCERT, Jaipur, Rajasthan, India*

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract - The wireless sensor network is formed of a colossal range of sensors that are scattered around a geographical area wherever we tend to keep track of the developments. Sensor hubs typically usually include sensors, actuators, memory and a processor, as well as the ability to speak with other sensors. The sensor network is liable to a variety of active and passive attacks. Black hole is the most well-known and damaging active attack of all the chances. This black hole attack delays down network execution and triggers a denial of service attack. The attack is started by a malicious hub/node that's present on the network. In this article, a unique methodology for identifying and eliminating malicious nodes from the network that are responsible for initiating/creating the attack is presented. The new approach is based on the Delphi scheme. The proposed strategy detects and separates the malicious nodes from the network proficiently; this exploratory result will demonstrate that. Network effectiveness will enhance as far as bundle misfortune, defer and expand throughput of the network. NS2 simulator tool will be used as a part of it.**

***Key Words***: optics, photonics, light, lasers, templates, journals

## 1.INTRODUCTION

With the development in the technology of network and communication, the inconvenience of wiring is resolved with Wireless sensor networks (WSN) into people's life; especially it has huge perspective and practicability in the area of remote sensing, industrial automation control, and domestic appliance and so on. 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 are 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. Able to operate devices like motors actuators and switches that control conditions.

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.

At the first occurrence of an acronym, spell it out followed by the acronym in parentheses, e.g., charge-coupled diode (CCD). **Misdirection Attack in WSN:** It is the most popular denial of service attack. This attack can be performed in different ways [5]. A malicious node could deny a substantial course to a specific node in this way 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 delivers 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.

## 2. 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, WSNs are vulnerable to various routing attacks, data authenticity, confidentiality, integrity, and availability, a security protocol was created by focusing a particular attack in WSN, most renowned attacks were Sybil attack, Denial of Service attack, wormhole attack, selective attack, HELLO Flooding attack, Sinkhole attack etc. This survey majorly focuses on the most challenging Sinkhole attack detection, prevention strategies, and attack techniques and also highlights open challenges in dealing with such attacks.

Kaur and Kumar (2018) studied mitigation of blackhole attacks and wormhole attacks 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 complex and easy to implement, also consumes less battery power, hence enhances network lifetime.

Kamble *et.al.* (2017) discussed in this paper [9], that within WSN data sending directly to the sink node raise various problems. Information gathering technique is the center of the WSN. In this information aggregation technique is used to decrease the energy consumption as well as enhance the network lifetime. In this paper data aggregation is performed to avoid such problems related to energy. An energy effective system in which data collection nodes are utilized for gathering data from cluster head inside the cluster. The lifetime 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 both of the parameters is very important and so the various methods have been proposed which can prevent the attacks to happen. The main degradation of energy occurs due to the attacks that are caused by the intruders. Approaches like cluster-based approach are explained in this article which will prevent the energy from being destroyed. Through this the maintenance of the throughput is also done. The article has proposed various such methods which will help in prevention of all the attacks and will help maintain 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, it is found to use the unified methodology in a WSN and make utilization of the all the more powerful Base Station 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) proposed in this paper [12] that because of the scattered way of WSNs, resource constraints, the radio link for multi-bounce communications and their remote region deployment, Dissent of Service (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. In the proposed mechanism, a methodology has been created to determine the issue of DoS attacks by actualizing wordings, for example, Intruder Detection System, validating nodes with a key mechanism and retracing routing path as a sly activity from the path required with the victim node as an internal attacker in the network. The essential center of this proposed work is to contribute secure and reliable data transmission over source and destination by determining 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. To assess 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.

Biswas *et.al.* (2015) proposed in this paper [14] the fundamental objective of the paper which is to show distinctive sorts of Security attacks, their effects and defense mechanisms in Wireless Sensor Network which is vulnerable to security attacks and dangers because of its attributes and restrictions. This overview paper concentrates on different parts of various security attacks, their effects and defense mechanisms comparing to every attack and so on. So this paper helps analysts to have an extremely solid thought regarding the security issues, existing attacks and they can likewise utilize the ideas and ideas to construct more secure wireless sensor network framework in future. A bearing can be gotten to grow new security mechanisms to protect new conceivable attacks alongside existing ones.

Fotohi *et. al.* (2020) studied Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol, they used

Sensor Detection Accuracy (ASDA-RSA) method that is utilized to counteract DoS attacks to reduce the amount of energy consumed, the ASDA-RSA schema in this paper consists of two phases to enhancement security in the WSNs, in the first phase, a clustering approach based on energy and distance is used to select the proper cluster head and in the second phase, the RSA cryptography algorithm and interlock protocol were used along with an authentication method, to prevent DoS attacks. They concluded that the WSN network performance metrics can be improved in terms of average throughput, Packet Delivery Ratio (PDR), network lifetime, detection ratio, and average residual energy.

## 3. 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 utilized for the selection of cluster head within each cluster. In the LEACH protocol, energy and distance of each node is checked, node which has maximum energy and minimum distance from the other nodes is selected as the cluster head. All the nodes in the network will aggregate its data to its cluster head. The cluster head will establish path through other cluster heads and transmit data to 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 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 selected 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 and isolate malicious nodes, the base station will apply technique of node localization.

## 4. 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 the base station due to which node lead to increase delay in the network as well identify the present malicious nodes.

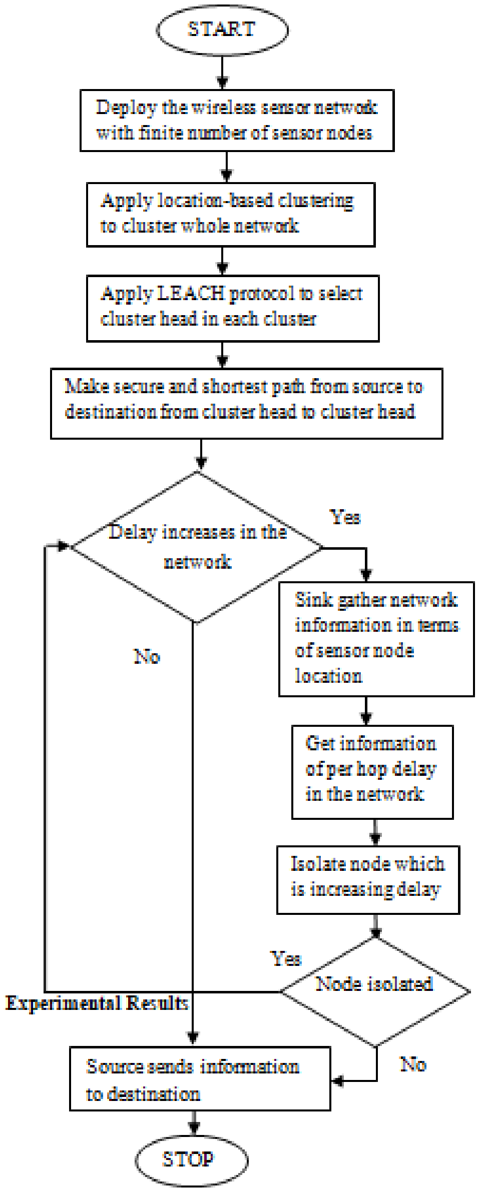
START
Deploy the wireless sensor network with finite number of sensor nodes
Apply location-based clustering to cluster whole network
Apply LEACH protocol to select cluster head in each cluster
Make secure and shortest path from source to destination from cluster head to cluster head
Delay increases in the network
Yes
No
Sink gather network information in terms of sensor node location
Get information of per hop delay in the network
Isolate node which is increasing delay
Yes
Node isolated
Experimental Results
No
Source sends information to destination
STOP

**Figure 1:** 3D view of building.

## 5. RESULTS AND DISCUSSION

The proposed approach is implemented in NS2 and results are evaluated in terms of delay, energy consumption and packet loss.

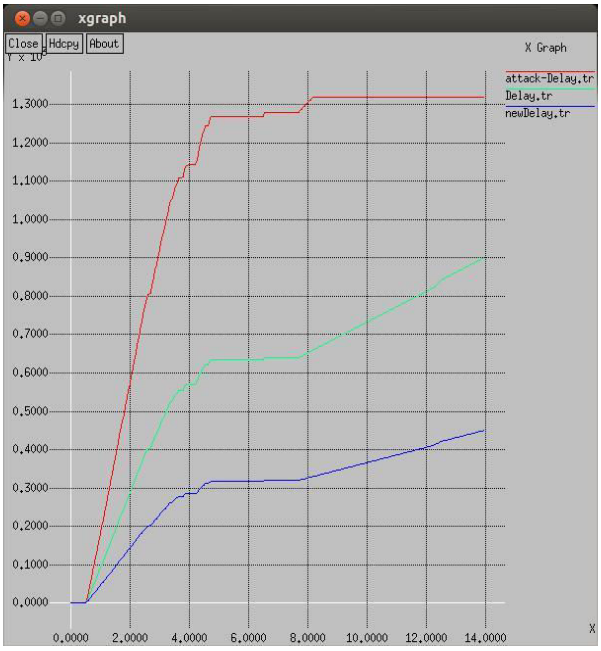

**Figure 2: Delay graph**

As shown in the figure 2, the comparison of LEACH, Attack and proposed technique is shown in terms of delay. In 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.

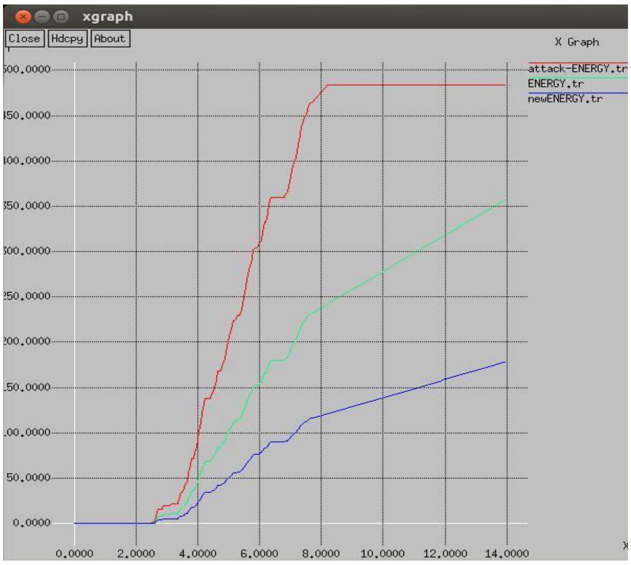

**Figure 3: Energy graph**

As shown in figure 3, 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.

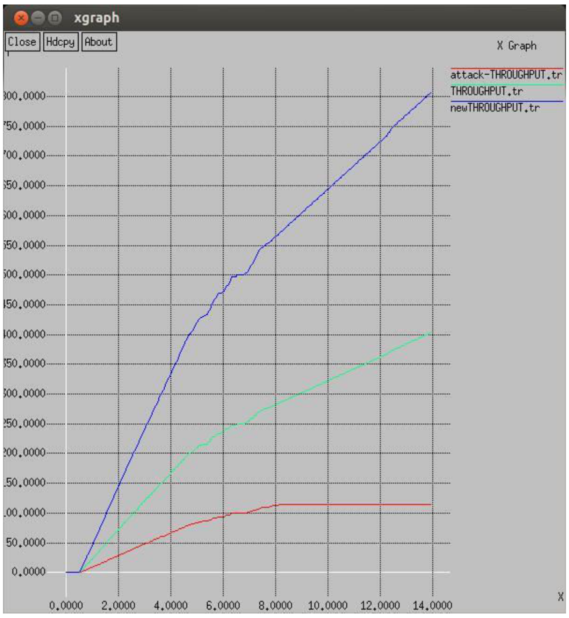

**Figure 4: Throughput Graph**

As shown in figure 4, 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.

## 6. CONCLUSION

The wireless sensor networks is the type of network in which sensor nodes can sense environmental conditions and sensed information will be passed to base station. The size of the sensor nodes is very small due to which battery life of the sensor nodes is limited. The wireless sensor networks are the self-configuring type of network due to which some malicious nodes may join the network. These malicious nodes are responsible to trigger misdirection attack in the network. In this work, technique is proposed which 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.

## 7. REFERENCES

[1] Joseph, J.,Vijayan, V. P. (2014) Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression-using-Longer-Path-Protocol, *International Journal Of Computer Applications(IJCA)*,ISSN 2250-1797, *Volume 4(**4**)*,

[2] Padmavathi, G., Shanmugapriya, D. (2009) A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, *International Journal of Computer Science and Information Security*, ISSN 1947- 5500, Vol. 4 (**1/2**), 1-9.

[3] Younis, Abdullah, M., Hua, G. W., Alsharabi, N. (2008) Wireless sensor networks misdirection attacker challenges and

solutions, *International Conference on Information and Automation,* ISSN 1050-4729, 369-373.

[4] Sachan, R. S., Wazid, M., Singh, D. P., Katal, A., Goudar, R. H. (2013) Misdirection attack in WSN: Topological analysis and an algorithm for delay and throughput prediction, *International Conference on Intelligent Systems and Control (ISCO)*, Vol. 7, 427-432.

[5] Kim, J., Caytiles, R. D., Kim, K. J. (2012) A review of the vulnerabilities and attacks for wireless sensor networks, *Journal of Security Engineering*, ISSN 2041-903, Vol. *9*(**3**),241-250.

[6] Sharma, K., Ghose, M. K. (2010) Wireless sensor networks: An overview on its security threats, *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs*, ISSN 0890-8044,42-45.

[7] Rehman, A. U., Rehman, S. U., Raheem, H. (2019) Sinkhole attacks in wireless sensor networks: A survey, *Wireless Personal Communications*, ISSN 0929-6212 Vol. *106*(**4**), 2291-2313.

[8] Kaur, Taranpreet., Kumar, Rajeev. (2018) Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol, *IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, ISSN 00002016, Vol.6, 288-292.

[9] Kamble, S., Dhope, T. (2016) Reliable routing data aggregation using efficient clustering in WSN, *International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, ISSN 00002017,46-250.

[10] Rani, L.,Rani, E. V. (2015) A Novel Study on Data Flow Routing with Energy Optimization under Different Attacks in WSN, *International Journal of Engineering and Technical Research (IJETR),* ISSN: 2321-0869, Volume-3(5), 134-138.

[11] Joshi, M., Patel, S. (2015) Centralized Signature Based Approach for Wireless Sensor Network Using RSA Algorithm, *International Journal for Technological Research in Engineering,* ISSN 2347 – 4718, Volume 2 (**8**), 1442-1445.

[12] Anand, C., Gnanamurthy, R. K. (2016) Localized DoS attack detection architecture for reliable data transmission over wireless sensor network, *Wireless Personal Communications*, ISSN 0929-6212, Vol. *90*(**2**), 847-859.

[13] Said, O., Elnashar, A. (2015) Scaling of wireless sensor network intrusion detection probability: 3D sensors, 3D intruders, and 3D environments. *EURASIP Journal on Wireless Communications and Networking*, ISSN 1687-1472 Vol. 1, 1-12.

[14] Biswas, S.,Adhikari, S. (2015) A survey of security attacks, defenses and security mechanisms in wireless sensor network, *International Journal of Computer Applications*, ISSN 2250-1797, Vol. *131*(**17**), 28-35.

[15] Fotohi, R., Firoozi Bari, S., Yusefi, M. (2020) Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, ISSN 1099-1131, Vol. 33(**4**), 4234.