JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Black Hole Attacks and Their Impact on Wireless Sensor Network using AODV Protocol

Rikshit Narseth*, A.J Singh**
**MTech, Dept. of Computer Science, Himachal Pradesh University, Shimla (H.P), India.*
Email: -narsethrikshit@gmail.com
*** Professor, Dept. of Computer Science, Himachal Pradesh University, Shimla (H.P), India.*

Abstract: -WSN is a very essential topic for research nowadays and it is used in many basic to critical applications like military operations, Health Analysis, etc. So, Security becomes a very important parameter in WSN for transferring data from one location to other. It is very difficult to keep an eye on every node in the Network because it depends upon the size of the network. To maintain the normal flow of data it's very prominent to keep sensor nodes secure from all the threads coming into the network. Small changes in the network data can degrade the network's performance metrics depending upon the attack type that happened, active or passive. A blackhole attack is introduced in this paper, which attracts the flow from the source with fake routing information given to the source. The source sends the data without knowing that the destination is an attacker and can drop the selected packets or all the packets. If the attacker drops only the selected packets it's very difficult to detect this attack. In this paper, blackhole attack and its influence is stated in the result analysis using AODV protocol with and without attack as the 7 nodes are taken into the consideration for the simulation. Results are the same as expected that there is a huge impact on WSN when this attack comes into play and is described in the graph.

Keywords: -WSN, Blackhole, RREQ, RREP, PDR, AODV.

1. INTRODUCTION

WSN contains the largely positioned nodes and base station, where all-networks information is received and then broadcasted to the internet. A sensor node consists of a Processing Unit, Power Unit, Sensing Unit, and transceiver unit to work with the data [1]. These nodes should be made attack free so that data is received confidentially. Security becomes very important to block in WSN. Data must be secure between the nodes.

1.1 Blackhole Attack

An attacker disables the connection of the communication between the sender and the destination. There can be more than one attacker node present in WSN depending upon the requirement of the attacker. A malicious node has two main possibilities after collecting the packets from its neighboring node:

a) It can drop all the packets received from its neighbor node

b) It can drop the selected packets of some type

In this attack, attacker node inappropriately advertises the best path to reach the destination when sender is calculating the route [2]. Firstly, source node finds best path to reach the receiver, and path which delivers least hops is set as the best route for data transmission.

For transferring data from sender to receiver, the RREQ is sent to receiver via adjacency nodes. Sender waits for RREP (Routing Reply) to send the packets to receiver. All packets are sent with path carrying least hops. But in black hole attack, the malicious node unicast fake RREP to sender and falsely tells, distance from the sender to the destination is short so the sender sends data from this route and the malicious node collects this data and acts receiver and drop packets sent by sender [3].

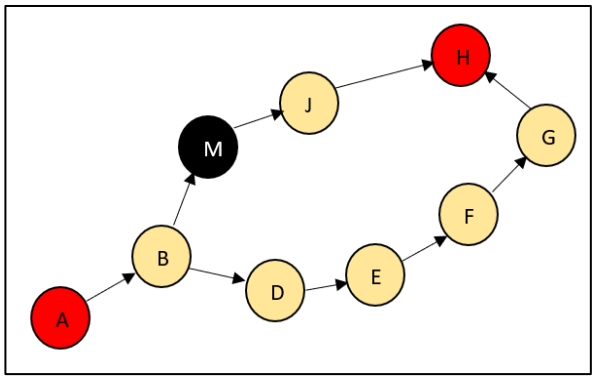

Fig.1.1 Blockhole Attack [2, 4]

In Fig.1.1, A is sender and H is receiver. A doesn't know the appropriate path to reach H. A sends the RREQ to its neighbor nods B and D which further sends the RREQ to its neighboring nodes. M is the malicious node that drops all the packets sent by node A or drops selected packets. When the RREQ is sent by A and the RREQ reached M it will send a fake RREP to A that the routing path from node M to H is very nearby.

2. RELATED WORK

Ghugar Uma Shankar et.al (2017) [5] In this paper, the concept of Blackhole Attack is discussed working with AODV protocol. It Primarily discusses the packet delivery from sender to receiver. It talks of RREQ sent by the sender and RREP sent by the receiver and how the fake Black hole node did this.

Kaur Gurjinder et.al (2017) [6] In this paper, the basic knowledge of WSN and the different application of WSN is discussed in this section. After this section, the different types of attacks in WSN are described with their damage. After this, the existing methodologies are discussed with different algorithms which are used to solve the problem. After this, the methodology for detecting and preventing blackhole attacks is discussed. In the last section, the simulation and the result analysis are discussed with Throughput and End-To-End Delay of packets in a network.

Patel Manish et.al (2018) [7] In this paper, the different variants of Wormhole attacks are discussed and give an overview of how wormhole attacks degrade the performance of the WSN. It computes several dimensions with and without attack. Performance of WSN decreases with a malicious node comes into play as compared to an attack.

Rani Bindu et.al (2018) [8] In this paper, brief knowledge about the WSN is stated with the application. After this section, the different types of attacks in WSN are discussed with their damage level. After this, the black hole attack in WSN is discussed with its types and its working in the AODV routing protocol. After this, the detection and prevention method for blackhole attacks is discussed also with the advantages and disadvantages of different techniques described in the table format.

soni Abhishek et.al (2018) [9] It gives some description about blackhole attack. After this, the related work about the problem is discussed. After this section methodology has been discussed in single blackhole node detection and prevention. At the end of the paper, the result and discussion are discussed with a simulation that finds UDP, how data is received, how data is lost and the flowchart of the algorithm discussed earlier.

Singh Gulbir et.al (2018) [10]In this paper, the security of the wireless network is discussed. After this, the literature survey and related work are discussed. After these proposed approaches like CHEMAS and the detection mechanism of selective forwarding attack are discussed. After this section result and implementation is described, by using the ns2 simulator the results are made. In this section PDR and number of nodes present in one or multiple nodes are discussed and plotted in the graph**.**

Kumar T. Hemanth et. al (2019) [11] In this paper, the blackhole detection in AODV-based WSN and honey-pot method about black hole attack is discussed. After this, the limitation of the present systems like low calculation resources, passive assault, and active assault is discussed. In the last section, the data security system is proposed for blackhole attacks and according to that result is made.

Sidhu Navjot et.al (2020) [12] In this paper, a small description of the WSN is stated in the starting section of the paper. After that, the related work is discussed, which describes the network layer attacks efficiency when working with the use of LEACH and AODV. After this section, the AODV operation under normal and with attack conduction is discussed. The metrics such as Throughput, PDR, number of packets received, and Average inter-arrival time is discussed. In the last section, the impact of the different request drops on the network Is discussed and demonstrated in the graph format.

Saputra Riko et.al (2021) [13] In this paper, small knowledge about the blackhole attack is discussed initially. After this section the different research methods such as system design in which the different physical features like topology, connective devices, and node address are discussed. The main focus of this section is to compute the packet loss, throughput, and packet delivery with blackhole using a checking agent detection system. After this, the data collection methods are discussed. In the last section, the average delay in the network without blackhole attack is discussed which calculation of the average delay and the throughput demonstrated in the graph format.

3. PROPOSED AODV PROTOCOL

It is defined as the Ad hoc Demand Distance Vector Routing that comes category of the reactive data protocol. Reactive means before sending data to the receiver, the sender searches route to reach a destination. It means path having the minimum number of hops becomes best path to transfer data from sender to receiver. It is the extension of DSR (Dynamic Source Route). It is also called "On Demand" because routers are automatically created when needed. It contains the following parameters to do any task in the network: -

i. **A broadcast Route Discovery Mechanism**
   RREQ (Route Request Packet) [14] is broadcasting to predict an appropriate path with a minimum number of hops.
   RREP (Route Reply Packet) [15] sets path and the data is transferred according to this reply request.
ii. **Dynamic Establishment of route table Entries**
   Nodes on currently path contain the routing table information only.
iii. **Maintain Timer-based States**
   In this scenario, the entry on the routing table is expired If it is not used recently.
iv. **Destination Sequence Number**
   It prevents the routing loops occurred in the network and also avoids the very old and the betokened paths.

3.1 Route Discovery

a. **Node has 2 parameters**
   - Seq. No.
   - Broadcast_id: Add one when the sender issues a new RREQ.

b. **Sender broadcast RREQ for searching route**
   - <Source Address, Source Seq. No., Broadcast_id, Destination Address, Destination Seq.No., Hop Count>

c. **Destination Replies RREP which is Unicasting**
   - <source address, destination address, destination seq., hop count, lifetime>
   - RREP has current seq. No., hopcount=0, full lifetime

d. **Adjacency Nodes**
   - Discards the doubly sent packets and sent RREP if it contains an active path with bigger seq. no.

4. TOOLS USED

The following tools are used to accomplish the task and find the appropriate results: -

1) **ns-2.35: -**It is the basic simulation tool used in Linux to find the result in the network. It consists of many libraries inside it like nam-1.15, x-graph, gnu plot, and many awk files to find the appropriate results.
2) **nam-1.15: -**It is the library in the ns-2.35 used for looking at the simulation of packets in the NAM file of any TCL file. It gives the real-time experience of packets flowing from the sender to the destination with animation.
3) **x-graph: -**It is also the library in ns-2.35 used for making the graphs of the resulting data.
4) **gnu plot: -**It is also used to plot the data into a graphical form and it is much more advanced as compared to the x-graph.
5) **NSG2.1: -**It is defined as Scenario generator 2 and is a JAVA-based ns2 scenario generator. It establishes different networks. It was written in java and has compatible to run on every platform.

5. PERFORMANCE METRICS

It is the basic parameter on which the network relies. It gives the values after the simulation and according to those values, the results are made. In the result analysis section, the values of different performance metrics are calculated which shows the impact on the network with and without attack. The following are the metrics used to compute the performance of WSN: -

a) **Avg_throughput** [16]**:-**It is the ratio between the sum of all the packets generated by the source node to the sum of all the packets received at the destination.
   Avg_throughput (TP) [16]=**∑All the packets generated by the source node/∑All the packets received at the destination.**
b) **Packet Delivery Ratio** [17]**: -**It is defined as the ratio between the sum of all the packets received by the destination node to the sum of all the packets sent by the source node. **PDR** [17]= **∑All the packets received by the destination node/∑All the packets sent by the sender node.**
c) **Packets dropped** [18]=**∑Packets received by the destination-∑Packets sent by the source**
d) **Instant Throughput** [19]**: -**It is defined as the throughput at a particular period. As time grows what impact on the throughput of WSN at an instant period.
e) **End-to-End Delay** [20]**: -**It the total sum of time taken by a packet to reach from the source to the destination.
   End-to-end delay [20]=**Receiving Time-Sending Time**

6. RESULTS

The results of workflows of blackhole attack impact on the whole network using AODV is taken into the consideration. The whole experiment is performed using ns2 simulator and analyzed by nam1.15. The results analysis is done on the different performance metrics: Avg_throughput, Instant throughput, packets dropped, END-TO-END delay, and PDR. Different simulations scenarios with different environments are considered below: -

6.1 Nodes with and without blackhole attack using AODV

a) In the first scenario only 7 nodes are taken into the consideration for simulation without a blackhole attack and the whole performance metrics are calculated using ns2. According to the values comes the result is calculated and analyzed.

Table 6.1: (without blackhole Attack)

Performance Metrics	Values
Avg_throughput	0.153846
PDR (Packet Delivery Ratio)	89.6373
No. of Packets dropped	8
Average end-to-end delay	498.276ms
Generated Packets	193
Received Packets	173

In above table 6.1, Observations are taken without inserting the blackhole node into the network. The different performance metrics are taken and the corresponding results are mentioned in the table itself. These results screenshots on ns-2.35 running on ubuntu 22.04 version are inserted below: -

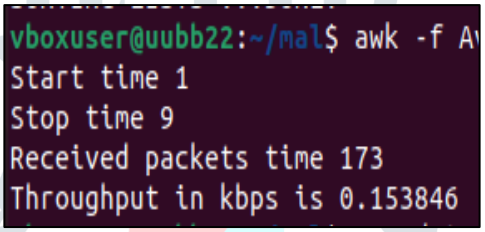

Fig.6.1 Avg_throughput without Blackhole attack

As in the above fig 6.1 gives the results of the network which contains the 7 nodes with source and the destination. The node n0 is sender and the n6 is receiver which collects the packets from the source n0.In between, there is no black hole node inserted to understand the impact on the performance with blackhole attack.

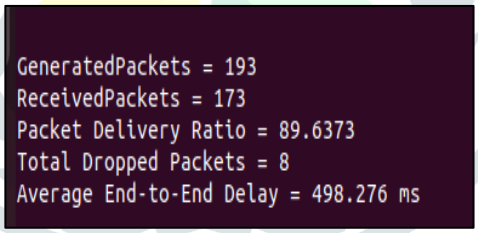

Fig.6.2 Dropped Packets, PDR and Avg_END-TO-END Delay

In above fig 6.2, results of dropped packets, PDR, and the average END-TO-END Delay without blackhole attack are discussed and analyzed. These results are generated in the ns2 on the ubuntu 22.04 version.

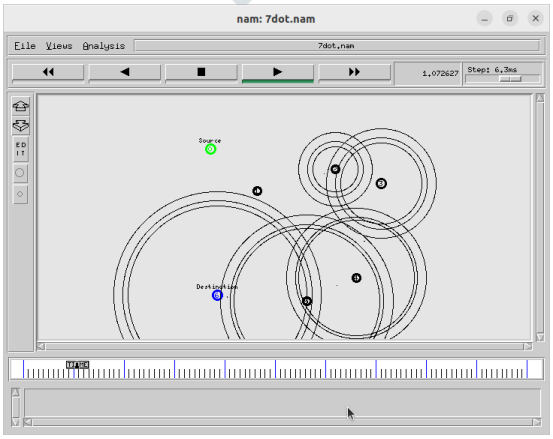

Fig.6.3 Simulation of Packets

As in the above fig 6.3 different nodes are scattered in a different position in the network. As in the above figure node, n0 is sender, n6 is receiver. This is the simulation done without blackhole attack in the network and all the performance metrics are calculated after the simulation. The above TCL file 7dotmal.tcl is used to simulate this 7dot.Nam file for simulation. All the results of this simulation are discussed in the above tables and the figures.

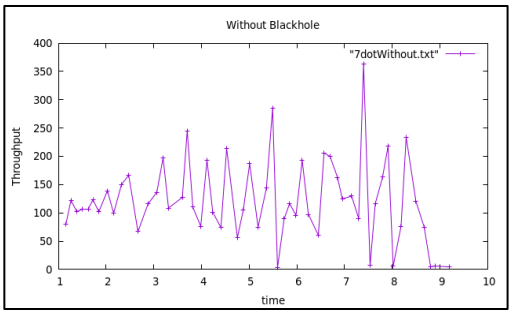

Fig.6.4 Instant Throughput without Blackhole

b) In the second scenario 7 nodes are taken into the consideration for simulation with a blackhole attack and the whole performance metrics are calculated using ns2. The node n5 is set as the blackhole node or the attacker node in the simulator. According to the values comes the result is calculated and analyzed.

Table 6.2: (with Blackhole Attack)

Performance Metrics	Values
Avg_throughput	0.148338
PDR (Packet Delivery Ratio)	88.3721
No. of Packets dropped	18
Average end-to-end delay	451.499ms
Generated Packets	172
Received Packets	152

In above table 6.2, Observations are taken by inserting the blackhole node into the network. The different performance metrics are taken and the corresponding results are mentioned in the table itself. These results screenshots on ns-2.35 running on ubuntu 22.04 version are inserted below: -

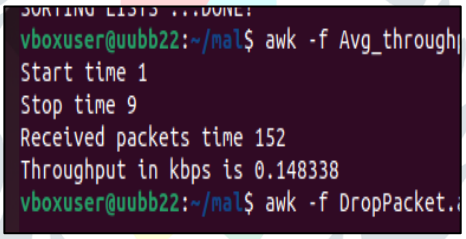

Fig.6.5 Avg_throughput with blackhole

As in the above fig 6.5 gives the results of the network which contains the 7 nodes with source and the destination. The node n0 is source and n6 is receiver which collects packets from the source n0.In between, there is a blackhole node n5 inserted. After insertion, the simulation is done and the impact values of the black hole attack in WSN is observed.

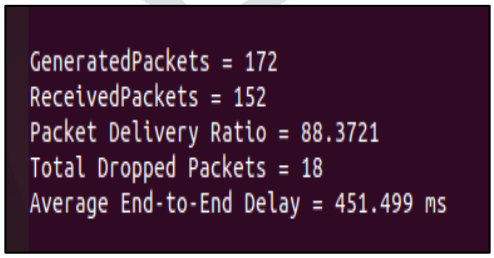

Fig.6.6 Dropped Packets, PDR and Avg_END-TO-END Delay

In above Fig.6.6, results of dropped packets, PDR and average END-TO-END Delay with blackhole attack is discussed and analyzed. These results are generated in the ns2 on the ubuntu 22.04 version.

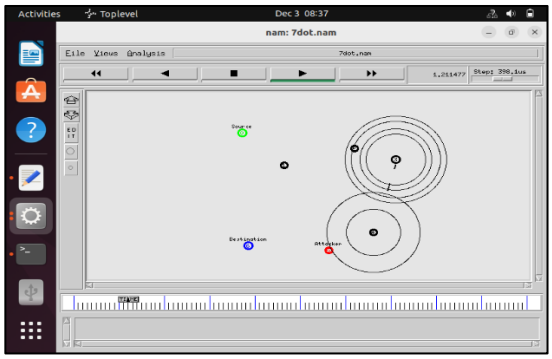

Fig.6.7 Simulation of Packets

In the above fig 6.7 different nodes are scattered in different positions in the network. As in the above figure node, n0 is sender, n6 is the receiver and node n5 is the attacker node or blackhole node. This is the simulation done with blackhole attack in the network and all the performance metrics are calculated after the simulation. The above TCL file 7dotmal.tcl is used to simulate this 7dot.nam file for simulation. All the results of this simulation are discussed in the above tables and the figures.

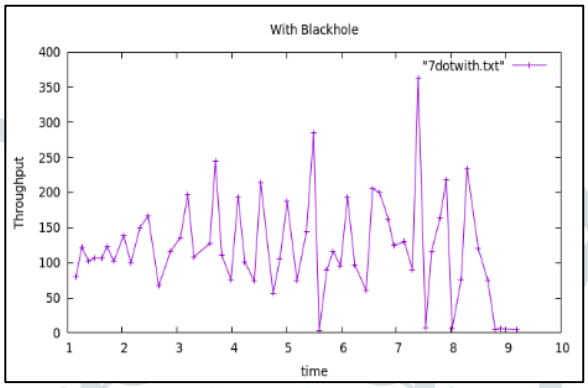

Fig.6.8 Instant Throughput without Blackhole

6.2.2 Comparison of Performance metrics

a) Avg_throughput (with and without attack)

Average throughput between nodes with and without blackhole attacks is given in this graph.

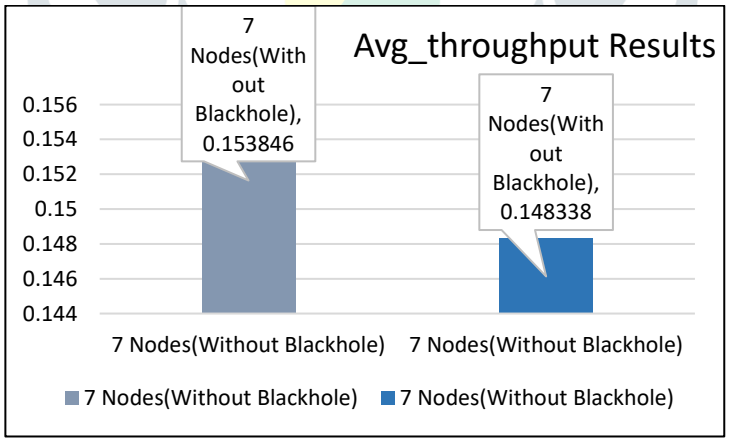

Fig.6.9 Avg_throughput Results

b) PDR (with and without attack)

PDR between nodes with and without blackhole attacks is given in this graph.

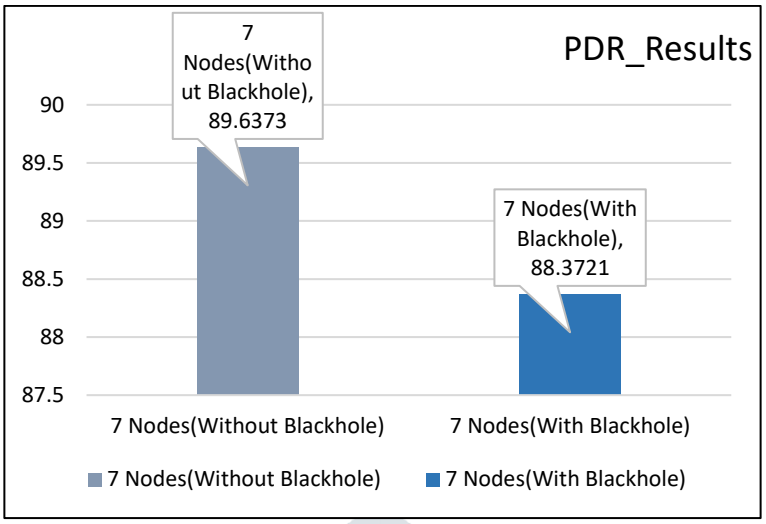

Fig.6.10 PDR_Results

c) Avg_End-To-End Delay (with and without attack)

The End-To-End Delay between the nodes with and without blackhole attacks is given in this graph.

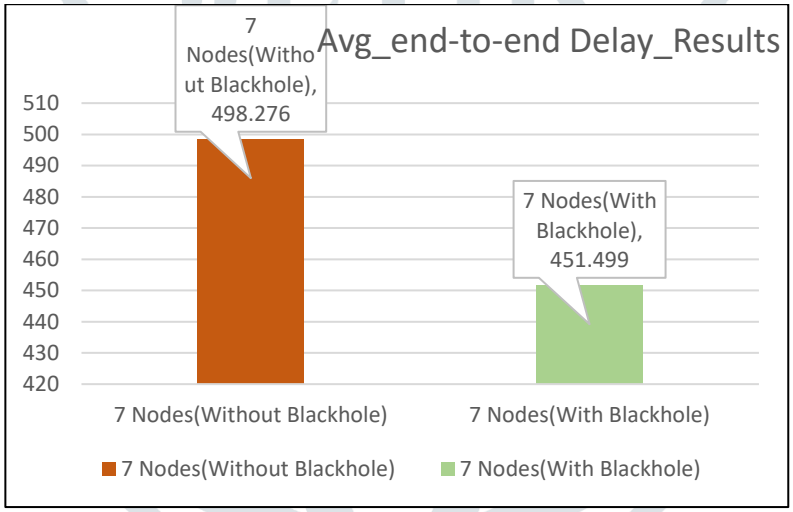

Fig.6.11 Avg_End -To-End Delay Results

d) Packets Dropped (with and without attack)

Packets dropped between the nodes with and without blackhole attacks is given in this graph.

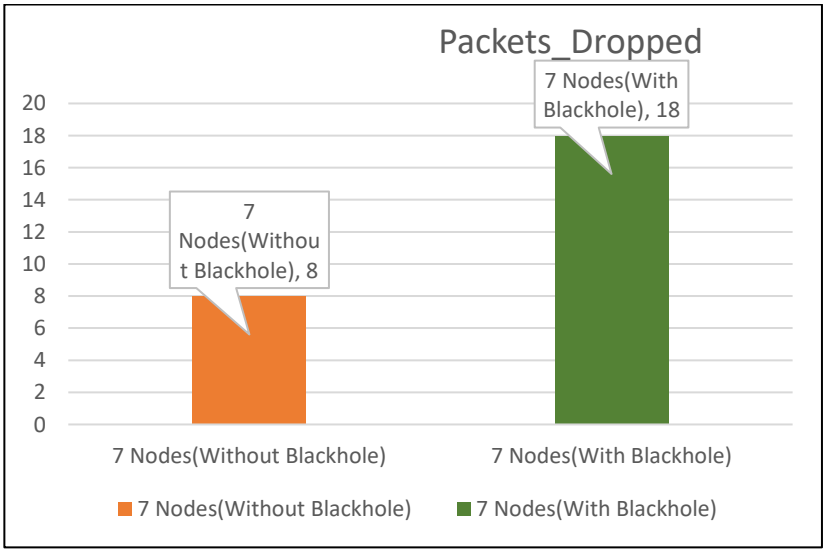

Fig.6.12 Packets Dropped

7. RESULT ANALYSIS

The results section discusses the impact of the different metrics. This section discusses the analysis gathered from the above result section and is discussed below with data: -

Case 1: - Impact on Average throughput

The throughput of 7 nodes without attack is 0.153846 and reduced when a blackhole attack exists to 0. 148338. So, the analysis comes that when an attacker is present in WSN it degrades throughput of WSN.

Case 2: -Impact on PDR

The PDR in 7 nodes without attack is 89.6373 and reduced when blackhole attacks exist to 88.3721. So, the analysis comes that when an attacker is present in WSN it also degrades the PDR of WSN.

Case 3: -Impact on End-To-End Delay

The End-To-End delay in 7 nodes without attack is 498.276 and reduced when blackhole attacks exist to 451.499. So, the analysis comes that when an attacker is present in WSN it also degrades the End-To-End Delay of WSN.

Case 4: -Packets Dropped

Packets dropped in 7 nodes without attack is 8 and increases when blackhole attacks exist to 18. So, the analysis comes that when a blackhole node is present in WSN the packet drops increase.

8. CONCLUSION AND FUTURE SCOPE

In this paper, we discussed the impact of blackhole attacks on WSNs using the AODV protocol. All the metrics like Avg_throughput, PDR, End-to-End Delay, and Instant throughput are taken into consideration. The graph depicted that number of packets dropped increased and values of other metrics decreased when the network was under the blackhole attack. All outcomes are captured using the ns2 simulator. This shows that there is also a huge impact on the working of the AODV protocol when an attack happens. So, it becomes very essential to prevent this attack using different methods, and is a very challenging task to achieve because of the wide and critical use of WSN. For this research work, there are a few areas left to research. By using this work one can know the importance of performance metrics and how their values decreases while the network is under the blackhole attack. This work will clear Questions like what are the factors that influence the Wireless sensor network when a blackhole attack comes into play? The second biggest challenge is power consumption because the node's battery power is very limited. All the power goes into sending and computing data. Sometimes there may be a chance of an attack that may dead the power of the battery by giving a certain task to that node by the attacker. So, one can work to maintain the power of nodes in WSN.

References

[1] J. Grover and . S. Sharma, "Security Issues in Wireless Sensor Network - A Review," *International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)* , pp. 397-404, 2016.

[2] S. Solapure, . N. Mete, P. Dodake, . S. Jadhav and P. D. Mehetre, "Comparative Survey of Routing Attacks in WSN's," *International Research Journal of Engineering and Technology (IRJET)* , vol. 5, no. 5, pp. 3210-3217, 2018.

[3] R. . W. Anwar, M. Bakhtiari, . A. Zainal, A. H. Abdullah and K. N. Qureshi, "Security Issues and Attacks in Wireless Sensor Network," *World Applied Sciences Journal 30 (10),* pp. 1224-1227, 2014.

[4] V. Rathod and M. Mehta, "Security in Wireless Sensor Network: A survey," *GANPAT UNIVERSITY JOURNAL OF ENGINEERING & TECHNOLOGY,* vol. 1, pp. 35-44, 2011.

[5] U. Ghugar and . D. J. Pradhan, "A Study on Black Hole Attack in Wireless Sensor Networks," *International Journal of Advance Computing Technique and Applications (IJACTA),* vol. 5, no. 1, pp. 1-3, 2017.

[6] G. Kaur , V. K. Jain and Y. Chaba, "Detection and Prevention of Blackhole Attacks in Wireless Sensor Networks," *Springer International Publishing AG,* pp. 118-126, 2017.

[7] M. Patel, A. Aggarwal and N. Chaubey, "Variants of Wormhole Attacks and Their Impact in Wireless Sensor Networks," *Springer Nature Singapore Pte Ltd.*, pp. 637-642, 2018.

[8] B. Rani and H. Sehrawat, "BLACKHOLE ATTACK DETECTION AND PREVENTION IN WIRELESS SENSOR NETWORKS: A STUDY," *Journal of Emerging Technologies and Innovative Research (JETIR),* vol. 5, no. 3, pp. 461-465, 2018.

[9] A. soni, R. Pachouri and A. Jain, "TECHNIQUE FOR DETECTING SINGLE AND MULTIPLE BLACKHOLE ATTACK ON WIRELESS SENSER NETWORKS," *International Journal of Advanced Research in Computer Science,* vol. 9, no. 5, pp. 54-63, 2018.

[10] G. Singh, D. O. P. Dubey and G. kumar, "A SOLUTION TO SELECTIVE FORWARD ATTACK IN WIRELESS SENSOR NETWORK," *International Journal of Students' Research in Technology & Management,* vol. 6, no. 4, pp. 1-6, 2018.

[11] T. H. Kumar, . K. K. Kowshik and M. Revathi, "Detection of Blackhole Attacks in Wireless Sensor Networks," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 11S, pp. 1203-1205, 2019.

[12] N. Sidhu and M. Sachdeva, "Impact Analysis of Network Layer Attacks in Real-Time Wireless Sensor Network Testbed," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, pp. 701-710, 2020.

[13] R. Saputra, J. Andika and M. Alaydrus, "Detection of Blackhole Attack in Wireless Sensor Network Using Enhanced Check Agent," *IEEE*, pp. 1-4, 2021.

[14] P. K. Maurya, . G. Sharma, V. Sahu, A. Roberts and M. Srivastava, "An Overview of AODV Routing Protocol," *International Journal of Modern Engineering Research (IJMER)*, vol. 2, no. 3, pp. 728-732, 2012.

[15] E. M. Royer and C. E. Perkins, "An Implementation Study of the AODV Routing Protocol," *IEEE*, pp. 1003-1008, 2000.

[16] R. Shyamala and S. Valli, "Impact of Blackhole and Rushing Attack on the Location-Based Routing Protocol for Wireless Sensor Networks," *Springer-Verlag Berlin Heidelberg*, pp. 349-359, 2012.

[17] C. Lal and A. Shrivastava, "An Energy Preserving Detection Mechanism for Blackhole Attack in Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 115, no. 16, pp. 32-37, 2015.

[18] S. S and J. C, "Identifying Packet Loss In Wireless Sensor Network," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 5, pp. 1178-1182, 2013.

[19] F. H. Yahaya, Y. M. Yussoff, R. A. Rahman and N. . H. Abidin, "Performance Analysis of Wireless Sensor Network," *5th International Colloquium on Signal Processing & Its Applications (CSPA)*, pp. 400-405, 2009.

[20] G. Bendale and S. Shrivastava, "An Improved Blackhole Attack Detection and Prevention Method for Wireless Ad-hoc Network," *IEEE*, pp. 1-7, 2016.

[21] C. B. Dutta and U. Biswas, "A Novel Blackhole Attack for Multipath AODV and its Mitigation," in *IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*, Jaipur,India, 2014.