RESEARCHERID
THOMSON REUTERS

*[Nitnaware *,* 5(11): November 2018]
DOI- 10.5281/zenodo.1495289

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

INVESTIGATION OF DETECTION AND PREVENTION SCHEME FOR BLACK HOLE ATTACK IN AODV FOR MANET

Dhiraj Nitnaware
Assistant Professor, Department of Electronics and Telecommunication, Institute of Engineering and Technology, DAVV, Indore (M.P.), India

ABSTRACT

Black hole attack is one of the security challenges in MANET where the traffic is redirected to a node that actually does not exist in the network. The node drops the packet similar to real world equivalence to the Universe black hole where things disappear. The black hole node presents itself in such a way to the other nodes and networks that it knows the shortest path. This paper proposed detection and mitigation scheme to avoid black hole attack and improve the network performance. The complete work is simulated and evaluated on Qualnet simulator. Variable parameters taken are mobile node, pause time speed and area. Improved Throughput and Packet delivery ratio has been observed in proposed solution in compare with black hole attack. Performance of proposed solution is similar with original AODV and tries to maintain privacy of content.

Keywords*: Black hole attack, AODV, Detection, Prevention, Qualnet 5.2 simulator, performance parameter*

I. INTRODUCTION

MANET consists of group of devices or nodes that can transmit data through a wireless communication medium with the help of radio frequency without any fixed infrastructure or centralized control. Cooperation of nodes is important to forward packets on behalf of every different once other destinations are out of their direct wireless transmission vary. The nodes facility to move generously ensures a flexible and handy vibrant network topology which is another important feature of a MANET [2]. MANET found its applications in emergency disaster relief, military operations and health monitoring using medical sensor network (MSN).

Each nodeacts as a host or router in MANET that can move, join or leave the network. Thus give rise to a protocol which can overcome this topological insecurity.The main advantage of MANET is that it can be deployed in areas where a convectional wired infrastructure network cannot work. This can be quickly deployed to support emergency requirements, instant needs and coverage in emergent areas.

Z. Alishahiet.al. have proposed a method in which collaboration of a group of nodesare used to detect black hole attack. Here intermediate node's validity is check who is forwarding the control packets RREQ and RREP.The source node then selects the secured path to destination based on this validated RREP. This technique suffers routing overhead problem as control packets has to be ACK by the intermediate node.

IDS node scheme is suggested by A. Sharma et.al. to secure AODV protocol[5]. This IDS node keeps a track of all nodes who are updating their routing table and sending higher sequence number to the source. The source node is then instructed by IDS to discover new route to destination. Thus IDS node detects the black hole attack. But limitation is that the malicious node should be in communication range of IDS node.Security-Aware Routing protocol (SAR) is suggested by S. Yi et al. [6] in which RREQ packets have a security metric or trust level. The intermediate nodes will forward RREQ packet this metric of level is satisfied else it will be dropped.

*[Nitnaware *, 5(11): November 2018]* ISSN 2348 – 8034
DOI- 10.5281/zenodo.1495289 Impact Factor- 5.070

II. BLACK HOLE ATTACK IN AODV

In this section, first we explain the black hole attack and then its type in AODV protocol.

A. Black Hole Attack

Black hole attack is one of the attacks in MANET which can disrupt the performance of the network. Here we explain the working of Black Hole attack that is carried out against MANETs. The malicious nodes in black hole attack advertise that they have shortest and high bandwidth path to the destination. One of the most arising issues in MANET is the limited battery, attackers take an advantage of this flaw and try to keep the nodes awake until all its energy is lost and went to permanent sleep.

The working of black hole attack is given in fig. 1.1.Here node "A" is source node while node "D" is destination node. Node "C" is a malicious node who titles that it has an active route towards the destination when it receives RREQ packets. It will respond immediately to source node "A" before any other node will. Now node "A" will send data through node "C" and ignore all other route. Thus node "C" will drop the data packets.

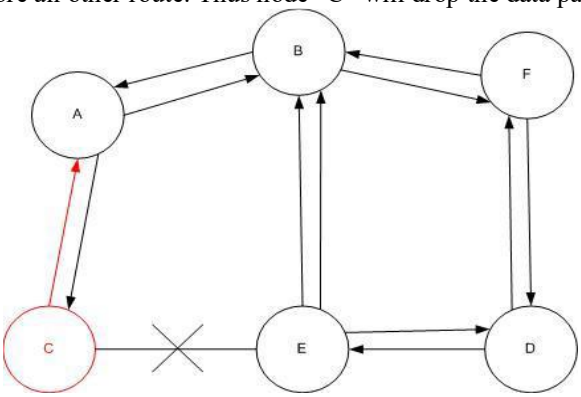

Figure 1.1 Black Hole Attack

B. Black Hole Attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

- *Internal Black hole attack:*Here an internal malicious node will fits in between source-destination path. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.
- *External Black hole attack:* Here the malicious node who is outside the network, attacks by denying access to network traffic, creating congestion in network or by disrupting the entire network. It may become internal when it have control of internal malicious node to attack other nodes in MANET.

  A malicious node can carry out the following attacks in AODV.

  i. Source node can be impersonated by the malicious node by modifying the source address with its address in the RREQ packet.
  ii. To analyze the communication in the route and become a part of it, malicious node can change the othercontents of RREQ packet such as hop count. The hop count can be reduced to increase the chances of being selected in the route between source and destination.
  iii. Destination node can also be impersonated by forging the destination address by its own address in a RREP.
  iv. Malicious node can capture an entire network and act as a network leader by broadcasting the biggest sequence number. It can become a black hole to the entire sub network.
  v. It can selectively forward certain RREQ packets and RREP packets and avoid other packets.
  vi. It can forge a RERR message and avoid further communication between nodes as they cannot reach the destination with different sequence number.

*[Nitnaware *, 5(11): November 2018]* **ISSN 2348 – 8034**
DOI- 10.5281/zenodo.1495289 **Impact Factor- 5.070**

vii. To create delay in the communication, malicious node can send two different RREQs to the neighboring node with different sequence numbers.

III. PROPOSED SCHEME

Black hole attack adversely affects the performance of AODV routing protocol. An adaptive technique is presented in this paper which can detect and prevent black hole attack. In the proposed scheme, every AODV node executes a BDS mechanism, i.e. each node in the network has a BDS agent in-built in the form of module with AODV routing protocol. BDS module estimates the suspicious value called *Transmission Power and Antenna Height* of each node to recognize the high capability node into network. When a suspicious value for a neighboring node exceeds a threshold, then that node is isolated from the network as other nodes do not forward packets through the suspected malicious node. The complete phenomena are shows in figure 1.2 and 1.3.

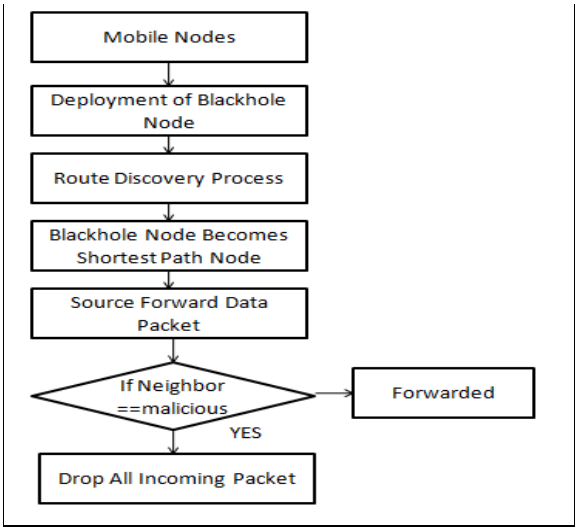

Figure 1.2: Deployment of Black hole Attack

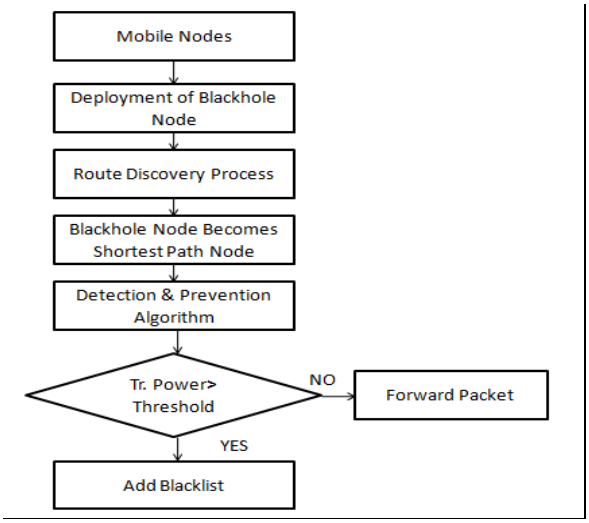

Figure 1.3: Detection & Prevention of Black hole Attack

*[Nitnaware *, 5(11): November 2018]* ISSN 2348 – 8034
DOI- 10.5281/zenodo.1495289 Impact Factor- 5.070

IV. RESULTS AND ANALYSIS

The performance parameter which we have taken for analysis of the proposed scheme are throughput, packet delivery ratio (PDR) and end to end delay against various varying parameter like number of nodes, speed, pause time and area. Implemented in four different sections are listed below:

A. Varying Number of Nodes

The configuration of scenarios is based on the number of nodes are deployed and the position of the source node and destination node.

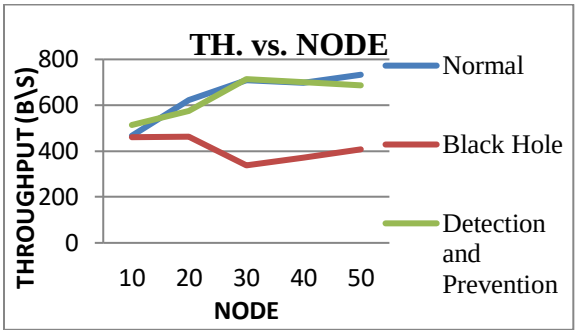

Figure 1.4 Throughput at variable Node

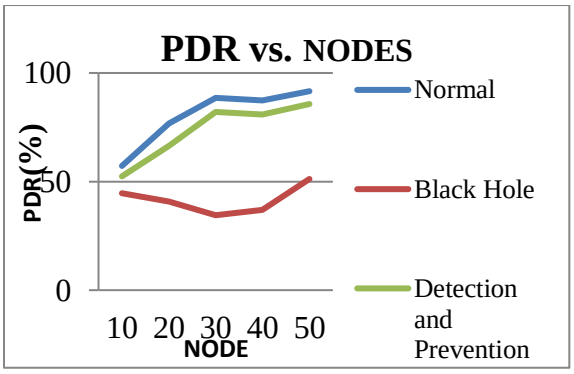

Figure 1.5 Packet delivery ratio at variable Node

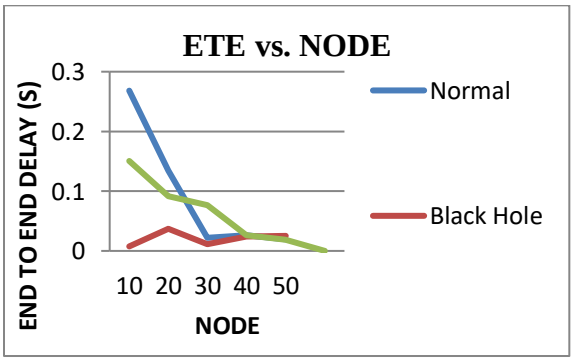

Figure 1.6 End to End Delay at variable Node

Figure 1.4, 1.5 and 1.6 shows that increment in number of mobile nodes increases the throughput and packet delivery ratio with respect to enhancement. Subsequently, it decreases the performance during black hole attack. It is

ISSN 2348 – 8034
Impact Factor- 5.070

also observe that end-to-end delay is degraded with respect to scaling. A similar result hasbeen observed between normal AODV and modified preventive AODV.

B. Varying Speed

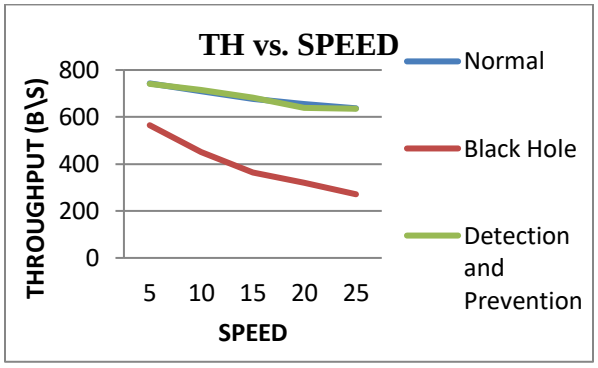

Figure 1.7 Throughputs at variable Speed

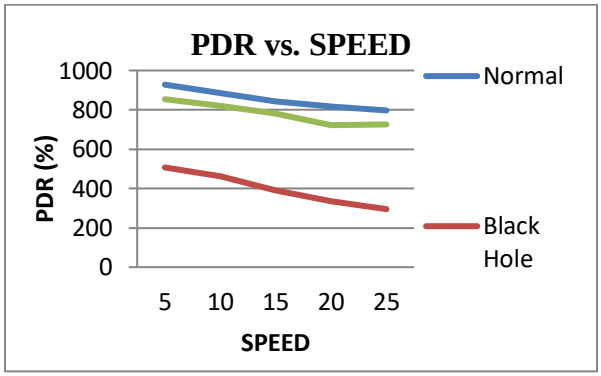

Figure 1.8 Packet Delivery ratio at Variable Speed

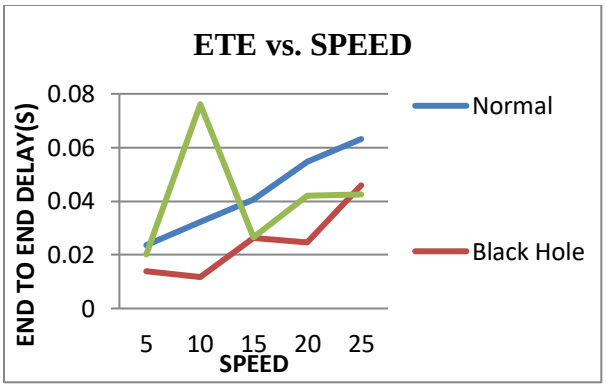

Figure 1.9 End to End Delay at variable Speed

Figure 1.7, 1.8 and 1.9gives that increment in mobile nodes speed decrease the throughput and packet delivery ratio with respect to enhancement. High speed frequently moves the node from one place to another which lead to degrade the possibility of node as intermediate node for long time. Movements into mobile node demand change the route design and generates various fresh route request and reply process. It is also observed there is increase in end-to-end delay.

ISSN 2348 – 8034
Impact Factor- 5.070

C. Varying Pause Time

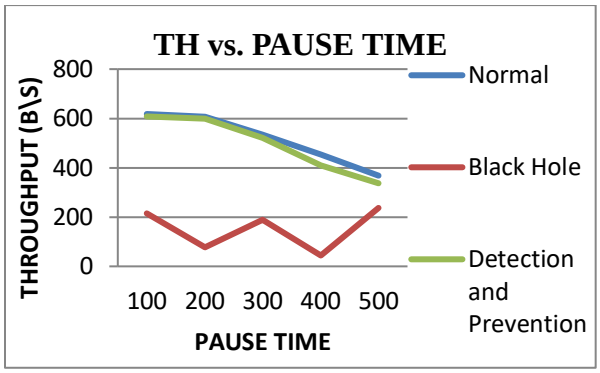

Figure 1.10 Throughput at variable Pause Time

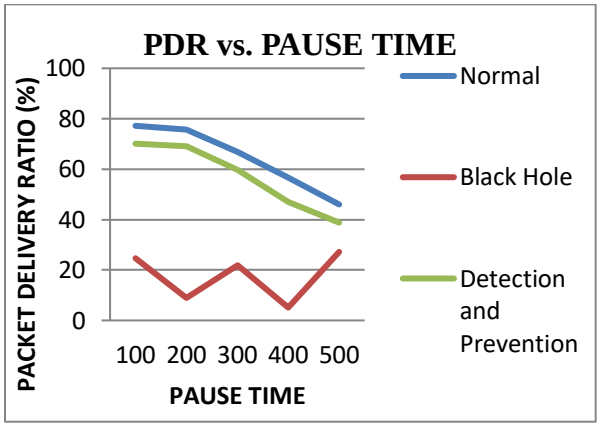

Figure 1.11 Packet Delivery Ratio at variable Pause Time

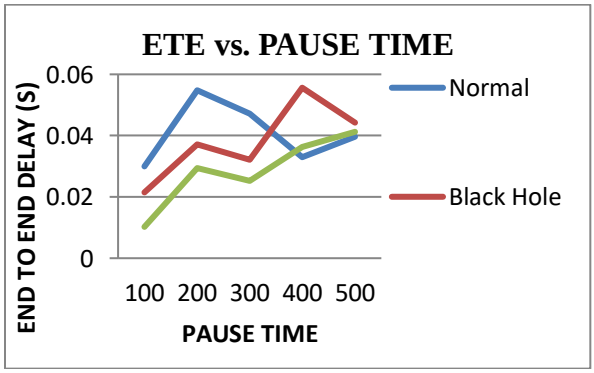

Figure 1.12 End to End delay at variable Pause Time

Performance parameter against pause time is shown in figure 1.10, 1.11 and 1.12. Here we observed that increment in pause time degrade the node speed and cause slow node movement. This slow movement stable the route design for a time period and call for recreate after pause time over. The complete phenomena lead to degrade the network throughout and packet delivery ratio. Subsequently, it saturates the End-to-End delay with respect to pause time increment.

*[Nitnaware *, 5(11): November 2018]*
DOI- 10.5281/zenodo.1495289
ISSN 2348 – 8034
Impact Factor- 5.070

D. Varying Area

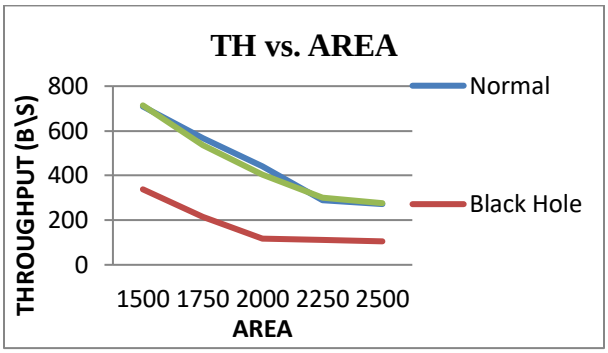

Figure 1.13 Throughputs at variable Area

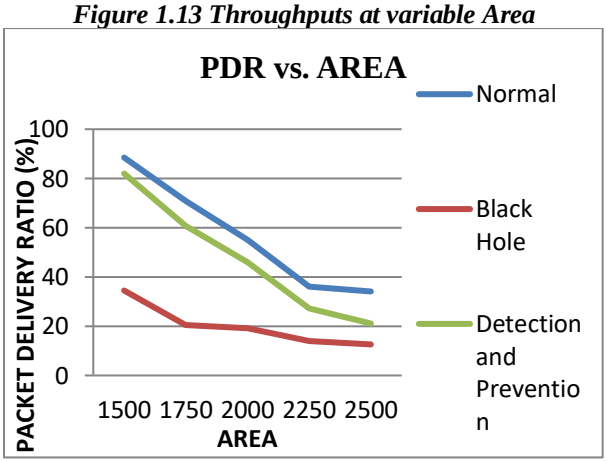

Figure 1.14 Packet Delivery Ratio at variable Area

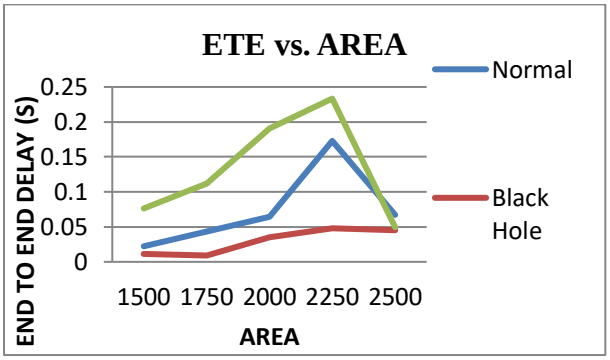

Figure 1.15 End to End Delay at variable Area

From figure 1.13, 1.14 and 1.15, we observed that increment in area size decreases throughput and packet delivery ratio while saturated end-to-end delay has been observed.

V. CONCLUSION

We conclude that proposed scheme successfully detect and mitigate the black hole attack in MANET. It is also observe that proposed algorithm help to improve the network performance during attacking situation. Following points are observed from simulation analysis:

- Throughput and PDR increases on average 40.758 % and 80.904 % with respect to Black Hole against number of nodes.
- Throughput and PDR increases on average 82.162 % and 100.68 % with respect to Black Hole against speed while it also saturates the E2E delay.
- An almost same result is observed against pause time and area size.

REFERENCES

1. *KitsakOsathanunkul, "A Countermeasure to Black hole Attack in Mobile Ad Hoc Networks" International Conference on Networking, Sensing and Control, 2011.*
2. *Panagiotis Papadimitratos and Zugmunt J. Haas, "Secure routing for Mobile Ad Hoc Networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS-2002), 2002, pp 1-13.*
3. *Y. C. Hu, A. Perrig and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols", in Proceedings of the ACM Workshop on Wireless Security, 2003, pp 30–40..*
4. *Z. Alishahi, J. Mirabedini and M. K. Rafsanjani, "A new method for improving security in MANETs AODV Protocol", Management Science Letters 2, 2012, pp 2271–2280.*
5. *A. Sharma, R. Singh and G. Pandey, "Detection and Prevention from Black Hole attack in AODV protocol for MANET", published in International Journal of Computer Applications, Vol. 50, No.5, 2012, pp 1-4.*
6. *S. Yi, P. Naldurg and R. Kravets, "Security-Aware Ad-hoc Routing for Wireless Networks", Report No.UIUCDCS-R-2002-2290, UIUC, 2002.*
7. *Y. F. Alem and Z. C. Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" 2nd International Conference on Future Computer and Communication, IEEE, Vol. 3, 2010, pp 672-676..*
8. *M. Medadian, A. Mebadi and E. Shahri, "Combat with Black Hole Attack in AODV Routing Protocol" in Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, 2009, pp 530-535.*
9. *L. Himral, V. Vig and N. Chand, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST) Vol. 3, No. 5, 2011.*
10. *P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", In Proceeding of IFIP Sixth Joint Working Conference on Communication and Multimedia Security, 2002, pp 107-121.*
11. *H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security In Mobile Ad Hoc Networks:Challenges And Solutions", published in IEEE Wireless Communications, 2004, pp 38-47.*
12. *Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-hoc Networks", in Proceedings of the 6th International Conference on Mobile Computing and Networking, MobiCom, 2000, pp 275–283.*