Varying Data Rate Based on Black Hole Attack in MANET using NS-3

Jigyasa Rajak[1], Ashish Chaurasia[2], Ashok Verma[3]

[1]Student, Dept of CSE, [2]Asst.Professor, Dept of CSE, [3]HOD, Dept of CSE.

Gyan Ganga Institute of Tech & Science, JBP, M.P, India

Abstract - Black hole attack is one of the security menace in which the traffic is readdress to such a node that drops all the packets or the node really does not exist in the set-up. Black holes points to the places in the network where incoming traffic is peacefully discarded or dropped. Now days, these course of Mobile ad hoc networks (MANETs) are fetching more and more importance in many paths. In this paper, we estimate the various parameters which come across the process of black hole attack. Therefore, we are mainly highlighted on the effect of Black Hole attack in MANET using AODV routing Protocol. Thus, as a result we come to a point that the throughput of the network increases with the increase in data rate.

Keywords - Black hole attack, AODV, MANET, Routing Protocol, Malicious node.

1. INTRODUCTION

The various security threats are rising in the meadow of MANET. One of these security threats is black hole attack which drops all customary data packets proposed for forwarding. A mobile ad-hoc network (MANET) is a set of mobile strategies that used wireless communications ability without any central network power. The mobile devices can effortlessly communicate with another device by forwarding packets over themselves. The network nodes in a MANET not only pretend as the normal network nodes but also as the routers for other stared devices. Lack of a fixed infrastructure, dynamic topology and the wireless character make MANETs vulnerable to the security attacks. Wireless ad hoc networks are swiftly gaining fame as an approach of communication, particularly among highly mobile sectors of society. A Mobile Ad hoc Network (MANET) is shaped with wireless mobile devices without the necessity for existing network infrastructure. As a outcome, such networks are comparatively simple to deploy and use for a very small time. In addition to providing a suitable mode of communication for business purposes, wireless ad hoc networks are very pleasing for use in emergency situations in disaster-stricken areas. In such cases, where no network infrastructure exists, it provides a decisive mode of communication. A high level of cooperation is necessary for applications that need real-time data transmission. Though, the partial energy supply of mobile devices raises queries about the skill of every node to be entirely cooperative. As an outcome, packet delivery cannot be assured even when malicious nodes are not present, and redirecting data packets does not provide a superior solution.

If malicious nodes are present in a mobile ad-hoc network, they may try to reduce the network connectivity by pretending to be cooperative but as a conclusion dropping any data they are meant to pass on. These actions may result in defragmented networks, inaccessible nodes, and radically reduced network performance.

2. RELATED WORK

Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan had studied that Mobile Ad hoc Network (MANET) is a collection of wireless nodes that are distributed without relying on any position of network infrastructure. MANET routing protocols were planned to put up the properties of a self organized environment without guarding against any inside or outside network attacks. Latha Tamilselvan, V Sankaranarayanan had discussed an approach in which the requesting node waits for the responses counting the next hop details, from other neighboring nodes for a preprogrammed time value. H. Deng, W. Li, and D. P. Agrawal had under done through a protocol that requires the midway nodes to send RREP message along with the next hop information. When the source node gets this information, it sends a RREQ to the next hop to stand out that the target node really has a route to the midway node and to the destination. When the next hop receives a Further Request, it sends a Further Reply which contains the check result to the source node. Based on information in Further Reply, the source node judges the validity of the route.

3. ROUTING PROTOCOL

As we know, protocols are the set of rules. As such, the Routing protocols are mainly used to transport the data

cogently and for route discovery and discover the network topology. The basic job of routing protocols in the ad-hoc network is to give groundwork of optimal paths between source and destination with the least overhead so that packets are delivered in an appropriate succession with the least obstructions. These protocols are vital because of the mobility of the nodes. A MANET protocol should function lucidly over a wide range of networking context from small ad-hoc group to larger mobile Multihop networks. fig 1 shows the categorization of these routing protocols.

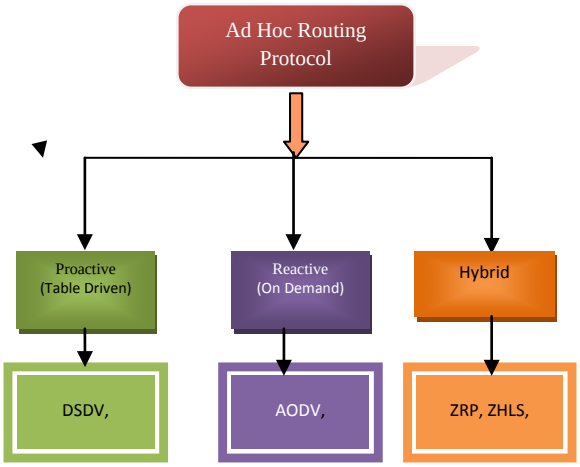

Fig-1: Hierarchy of Routing Protocols

The Routing protocols can be divided into Proactive, Reactive and Hybrid protocols, depending on the routing topology. The Proactive protocols are classically table-driven. Examples are Destination Sequence Distance Vector (DSDV). On the additional hand, the Reactive protocols do not suitably update the routing information. It is spread more widely to the nodes only when necessary. Example of such type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Examples are Zone Routing Protocol (ZRP) etc.

4. THEORETICAL BACKGROUND OF AODV ROUTING PROTOCOL

AODV routing protocol is a method of routing messages between mutable computers. It allows these mobile computers, or nodes, to pass messages through their neighbors to nodes with which they cannot straightly communicate. AODV does this by finding out the routes along which messages can be approved. AODV makes sure these routes do not hold loops and tries to find the shortest route which is feasible. AODV is also able to grip the changes in routes and can craft new routes if there is a fault.

The diagram below shows a lay out of four nodes on a wireless network. The circles demonstrate the range of communication for each node. Because of the limited range, each node can only communicate with the nodes next to it.

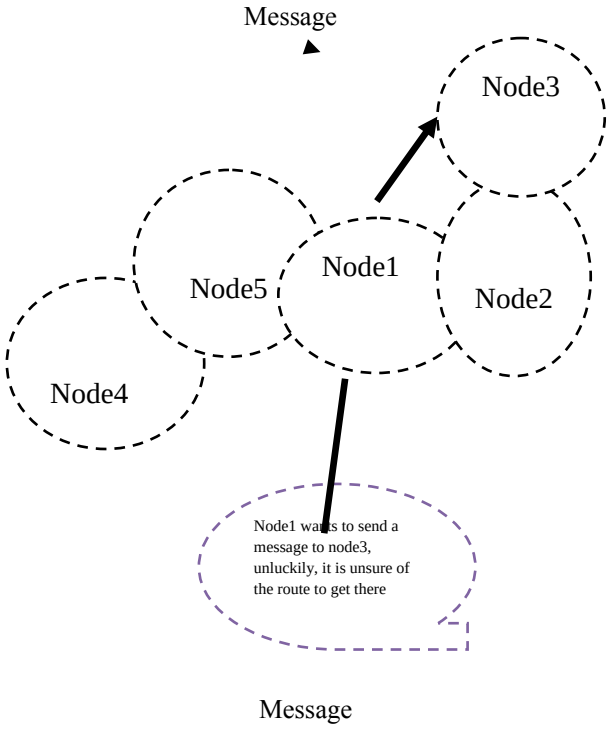

Fig-2: A set up of four nodes on a wireless network

5. BLACK HOLE ATTACK

In the Black hole attack, all network noises are redirected to a specific node which does not exist at all. The noises fade away into the particular node as the matter fades away into Black hole in universe. Therefore, the précised node is named as a Black hole. A Black hole has mainly two properties: Firstly, the node utilize the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node; even the route is spurious, with the intend of intercepting packets. Secondly, the node consumes the intercepted packets.

5.1. Black Hole Problem in AODV

The black hole attack is one of the eminent security threats in wireless mobile ad hoc networks. The intruders make use of the loophole to bear out their malicious behaviors because the route discovery process is necessary and foreseeable. In networking, black holes deals with the places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not arrive at its projected recipient. When probing the topology of the network, the black holes themselves are

unseen, and can only be detected by monitoring the lost traffic; hence the name.

AOD V Characteristics:

• Will find routes only as desired.

• Use of Sequence numbers to track correctness of information.

• Only keeps track of subsequent hop for a route instead of the total route.

4. SIMULATION ATMOSPHERE

We have mocked-up the Black hole attack in MANET. In our picture we examine the throughputs with the variation of nodes at different data rates. This simulation is done using ns-3.23, to look at the performance of the network by varying the nodes mobility at dissimilar kbps. The metrics used to evaluate the performance are given below.

I).Node Mobility: The Node mobility indicates the mobility speed of nodes.

ii).Throughput: Throughput deals with the average rate of successful message delivery over a communication channel. The major parameters of our experiment are listed in Table1.

Table-1. Simulation Parameters

S.No.	Parameters	Value
1.	Simulator	NS-3.23
2.	Simulation time	Varies with nodes
3.	No. of nodes	4, 6, 16
4.	No. of Malicious node	1, 1, 1
5.	Speed	Random
6.	Traffic type	UDP
7.	Topology	Network
8.	Routing Protocol	AODV
9.	Data rate	100,250,600

6. EFFECT OF MOBILITY ON THE PERFORMANCE

This paper is applied to ns-3.23 to validate the detection and isolation efficiency of the proposed method against black hole nodes. We have analyzed the different values while coming across the Ad Hoc on Demand Distance Vector (AODV) Routing Protocol. AODV routing protocol were randomly distributed, and one malicious node performs the black-hole attack. The Simulation result is shown below with the assistance of two tables. Table 2 shows the Variation of throughput while varying the data rate with 4 nodes, Table 3 shows the Variation of throughput while varying the data rate with 6 nodes and lastly, Table 4 shows the Variation of throughput while varying the data rate with 16 nodes.

Table-2. Variation of throughput while varying the data rate with 4 nodes

S.No.	Data rate(kbps)	Throughput (Mbps)
1.	100	0.0788948
2.	250	0.185018
3.	600	0.241368

Table-3. Variation of throughput while varying the data rate with 6 nodes

S.No.	Data rate(kbps)	Throughput (Mbps)
1.	100	0.141493
2.	250	0.147322
3.	600	0.218135

Table-4. Variation of throughput while varying the data rate with 16 nodes

S.No.	Data rate(kbps)	Throughput (Mbps)
1.	100	0.0171148
2.	250	0.10858
3.	600	0.231244

7. RESULT & DISCUSSION

It is observed from the below fig. that, the impact of the Black hole attack to the Networks throughput. The throughput of the network increases with the increase in data rate.

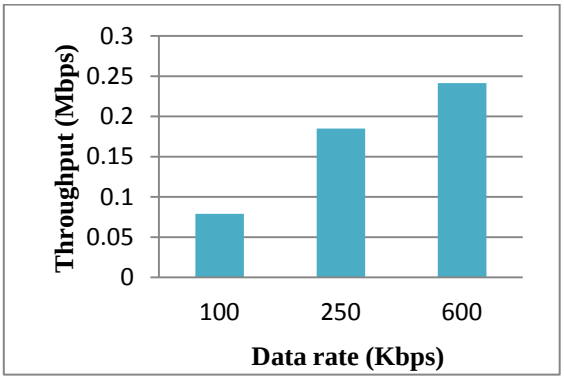

Fig-3: Variation of throughput with 4 nodes

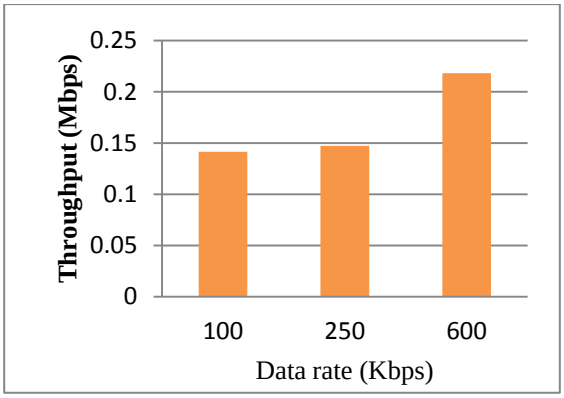

Fig-4: Variation of throughput with 6 nodes

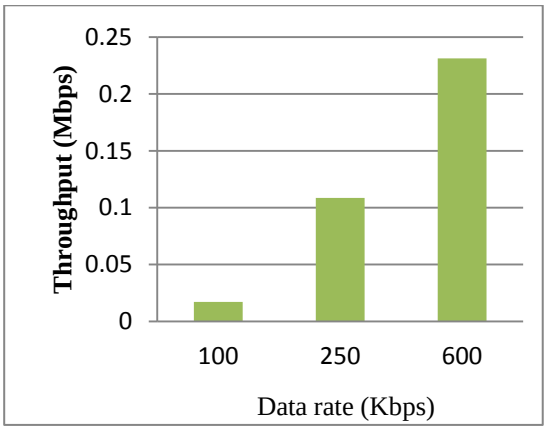

Fig-5: Variation of throughput with 16 nodes

8. CONCLUSION AND FUTURE WORK

In this paper, we have examined the throughputs which are increased while increasing the nodes with the different date rates. Black hole attack is one of the most significant security problems in MANET. In Black hole attack all network traffics are redirected to a précised node or from the malicious node causing serious harm to the networks and nodes as shown in the result of the simulation. The detection of Black holes in ad hoc networks is still considered to be a challenging task.

We simulated the Black Hole Attack and investigated its result. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be resolute. In the future work nodes can be extended and the outcomes can be estimated. In MANET applications where confirmation is not essential, there is still a need for mechanisms whereby nodes can be assured that packets will be delivered to their proposed target.

9. REFERENCES

[1]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[2]. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan. A Local Intrusion Detection Routing Security over MANET Network. 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia.

[3]. Vandna Dahiya. Analysis of Black Hole Attack on MANET Using Different Routing Protocols. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), October 2014.

[4]. Monika Verma, Dr. N. C. Barwar. A Comparative Analysis of DSR and AODV Protocols under Blackhole and Grayhole Attacks in MANET. International Journal of Computer Science and Information Technologies, 2014.

[5]. Jitendra Kumar Rout, Sourav Kumar Bhoi and Sanjaya Kumar Panda. SFTP: A Secure and Fault-Tolerant Paradigm against Blackhole Attack in MANET. International Journal of Computer Applications (0975 – 8887) Volume 64– No.4, February 2013.

[6]. Himani Yadav and Rakesh Kumar. Identification and Removal of Black Hole Attack for Secure Communication in MANETs. International Journal of Computer Science and Tele-communications, September 2012.

[7]. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao. A survey of black hole attacks in wireless mobile ad hoc networks. A Springeropen journal.

[8]. Sheenu Sharma, Roopam Gupta. Simulation Study of Blackhole Attack in the mobile Ad Hoc Network. Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 – 250 © School of Engineering, Taylor's University College.

[9]. Rashmi, Ameeta Seehra. A Novel Approach for Preventing Black-Hole Attack in MANETs. International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.3, September 2014.

[10]. Sanjay Kr. Dwivedi, Raj Shree, and Ravi Prakash Pandey. Design Enhancements in ZRP for Detecting Multiple Black Hole Nodes in Mobile Ad Hoc Networks. International Journal of Computer Applications,March2011.