Journal of Engineering Science and Technology
Vol. 4, No. 2 (2009) 243 - 250


# SIMULATION STUDY OF BLACKHOLE ATTACK IN THE MOBILE AD HOC NETWORKS

SHEENU SHARMA[1,*], ROOPAM GUPTA[2]

[1]SOIT, RGPV Bhopal, India
[2]UIT, RGPV Bhopal, India
*Corresponding Author: sheenu142002@gmail.com

**Abstract**

A wireless ad hoc network is a temporary network set up by wireless nodes usually moving randomly and communicating without a network infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. In this study we investigated the effects of Blackhole attacks on the network performance. We simulated Blackhole attacks in Qualnet Simulator and measured the packet loss in the network with and without a blackhole. The simulation is done on AODV (Ad hoc On Demand Distance Vector) Routing Protocol. The network performance in the presence of a blackhole is reduced up to 26%.

Keywords: Ad hoc networks, Routing protocols, AODV, Blackhole

## 1. Introduction

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this is communicating with rest of the world while being mobile. The disadvantages are their limited bandwidth, memory, processing capabilities and open medium. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET). An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of ad hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes [1].

**Abbreviations**

| | |
|---|---|
| AODV | Ad hoc On-demand Distance Vector Protocol |
| CBR | Constant Bit Rate |
| DSR | Dynamic Source Routing Protocol |
| E-E delay | End to End delay |
| IP | Internet Protocol |
| MAC | Medium Access Control |
| MANET | Mobile Ad hoc Network |
| PDR | Packet Delivery Ratio |
| RREP | Route Reply |
| RREQ | Route Request |
| RRER | Route Error |
| UDP/IP | User Datagram Protocol / Internet Protocol |

In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. To support this connectivity nodes use routing protocols such as AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing).

Wireless ad hoc networks are usually susceptible to different security threats and Blackhole attack is one of these. In our study, we simulated Blackhole attacks in wireless ad hoc networks and evaluated their effects on the network performance. We chose AODV protocol because it is widely used and it is vulnerable to these attacks because of the mechanisms it employs. We made our simulations using Qualnet Simulator and compare the network performance with and without Blackholes in the network. As expected, the throughput in the network deteriorated considerably in the presence of a blackhole.

The paper is organized as follows: section 2 describes the AODV protocol and Blackhole attacks are described in section 3. Network simulation results are presented in section 4 followed by conclusions in section 5.

## 2. AODV Routing Protocols

The AODV routing protocol [1] is an adaptation of the DSDV protocol for dynamic link conditions. Every node in an ad hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This

Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. This is illustrated in Figs. 1a and b. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'BlackHole' attacks.

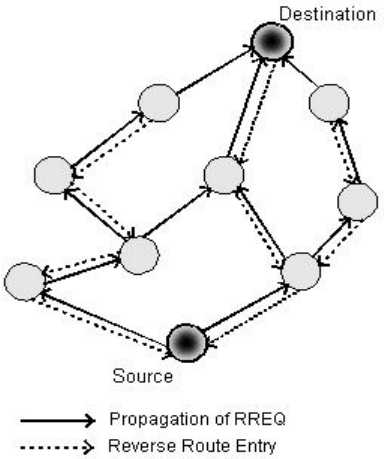


**Fig. 1a. Propagation of RREQ.**

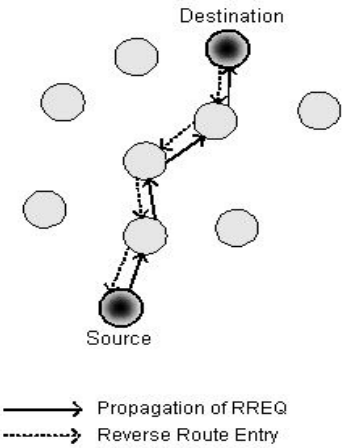


**Fig. 1b. Propagation of RREP.**

## 3. Blackhole Attack and Classification

In Blackhole attack [2], all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node as the matter disappears into Blackhole in universe. So the specific node is named as a Blackhole. A Blackhole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. Blackhole attacks in AODV protocol routing level can be classified into two categories: RREQ Blackhole attack and RREP Blackhole attack.

### 3.1. Blackhole attack caused by RREQ

An attacker can send fake RREQ messages to form Blackhole attack [2]. In RREQ Blackhole attack, the attacker pretends to rebroadcast a RREQ message

with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will be broken down. The attacker can generate Blackhole attack by faked RREQ message as follows:

- Set the type field to RREQ (1);
- Set the originator IP address to the originating node's IP address;
- Set the destination IP address to the destination node's IP address;
- Set the source IP address (in the IP header) to a non-existent IP address (Blackhole);
- Increase the source sequence number by at least one, or decrease the hop count to 1.

The attacker forms a Blackhole attack between the source node and the destination node by faked RREQ message as it is shown in Fig. 2.

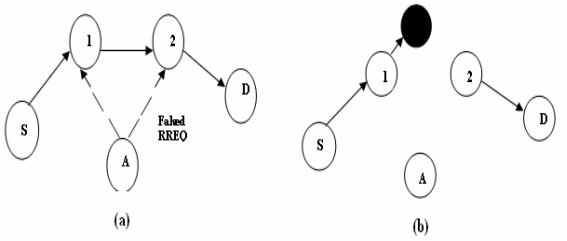


**Fig. 2. Blackhole is Formed by Faked RREQ.**

### 3.2. Blackhole attack caused by RREP

The attacker may generate a RREP message to form Blackhole as follows:

- Set the type field to RREP (2);
- Set the hop count field to 1;
- Set the originator IP address as the originating node of the route and the destination IP address as the destination node of the route;
- Increase the destination sequence number by at least one;
- Set the source IP address (in the IP header) to a non-existent IP address (Blackhole).

The attacker unicasts the faked RREP message to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non-existent node. Then RREP Blackhole is formed as it is shown in Fig. 3.

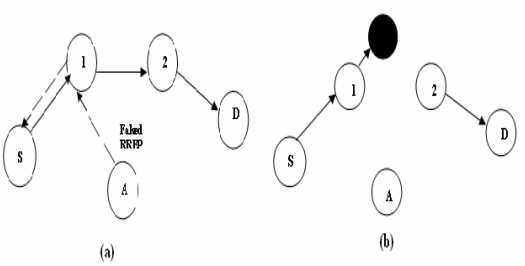


**Fig. 3 Blackhole is Formed by Faked RREP.**

## 4. Simulation Environment

We have implemented Blackhole attack in a Qualnet simulator [4]. For our simulations, we use CBR (Constant Bit Rate) application, UDP/IP, IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 40 randomly allocated wireless nodes in a 1500 by 1500 square meter flat space. The node transmission range is 250 m power range. Random waypoint model is used for scenarios with node mobility. The selected pause time is 30 s. A traffic generator was developed to simulate constant bit rate (CBR) sources. The size of data payload is 512 bytes. In our scenario we take 40 nodes in which nodes 1-27 and 29-40 are simple nodes, and node 28 is a malicious node or Blackhole node.

The simulation is done using Qualnet [4], to analyze the performance of the network by varying the nodes mobility. The metrics used to evaluate the performance are given below.

**i) Packet Delivery Ratio**: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

**ii) Throughput**: Throughput is the average rate of successful message delivery over a communication channel.

**iii) Node Mobility**: Node mobility indicates the mobility speed of nodes.

Simulation results are shown in Figs. 4 to 7 and Tables 1 and 2. Figure 4 shows the effect to the Packet Delivery Ratio (PDR) measured for the AODV protocol when the node mobility is increased. The result shows both the cases, with the Blackhole attack and without the Blackhole attack. It is measured that the packet delivery ratio is dramatically decreases when there is the malicious nodes in the network. For example, the packet delivery ratio is 100% when there is no effect of Blackhole attack and when the node moving at the speed 10 m/s. But due to effect of the Blackhole attack the packet delivery ratio decreases to 92%, because some of the packets are dropped by the blackhole node.

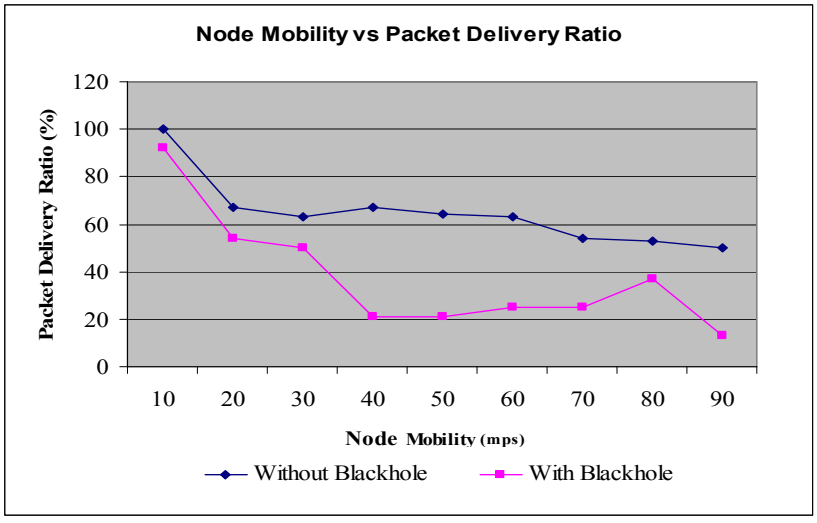


**Fig. 4. Impact of Blackhole Attack on Packet Delivery Ratio.**

Figure 5 shows the impact of the Blackhole attack to the networks throughput. The throughput of the network also decreases due to blackhole effect as compared to that without the effect of Blackhole attack. We vary the speed of the node and take the result to the different node speed.

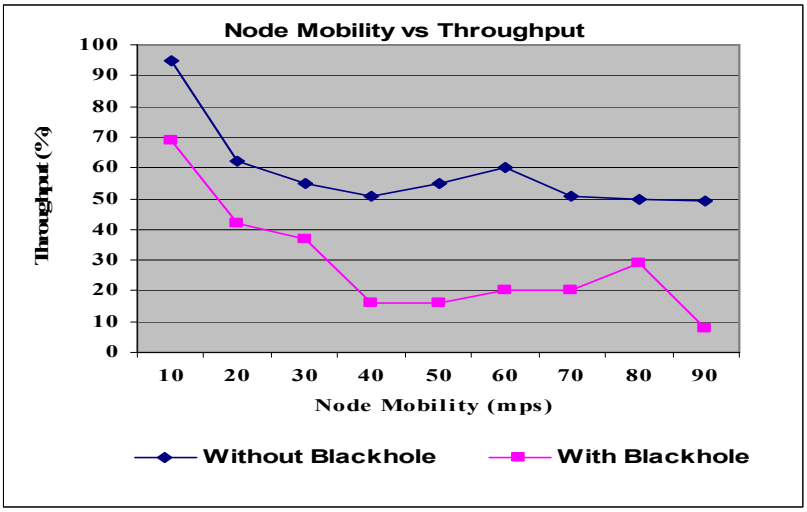


**Fig. 5. Impact of Blackhole Attack on the Network Throughput.**

It can be observed from Fig. 6 that, there is a slight increase in the average end-to-end delay without the effect of blackhole, as compared to the effect of Blackhole attack. This is due to the immediate reply from the malicious node, i.e., the nature of malicious node here is it would not check its routing table.

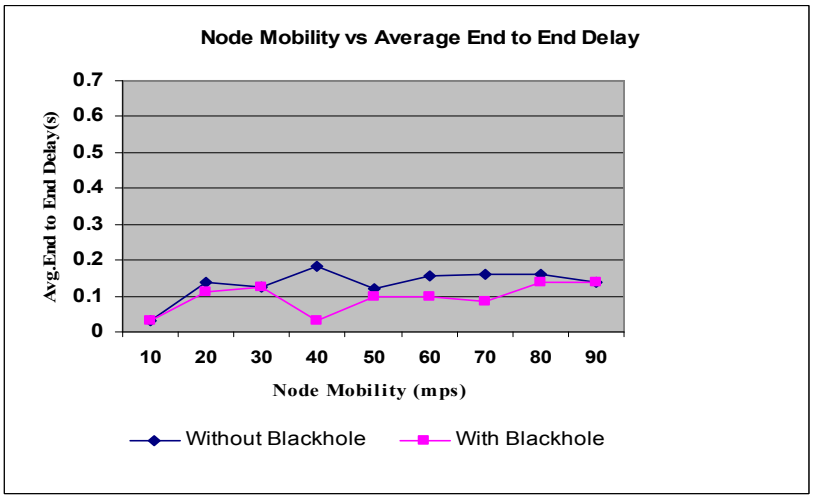


**Fig. 6. Impact of Blackhole Attack on the Avgerage E-E Delay.**

It is observed from Fig. 7 that average jitter between the nodes is more without the Blackhole attack, as compared to the average jitter between the nodes with the effect of Blackhole attack. This is due to the malicious nodes provides the path with fewer number of nodes, or smaller path. Thus average jitter between the nodes is reduced.

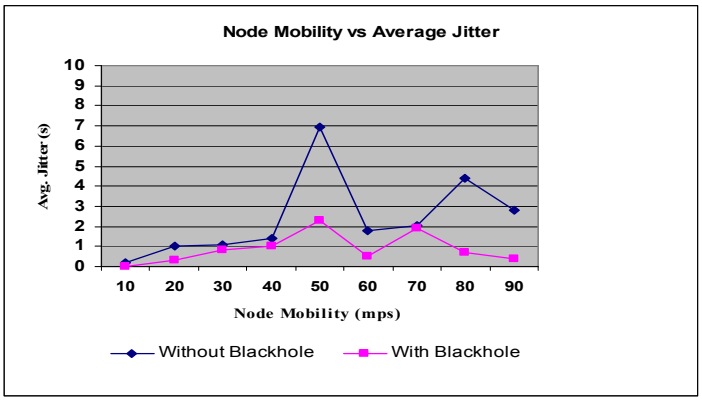


**Fig. 7. Impact of Blackhole Attack on the Average Jitter.**

**Table 1. Simulation Result without Blackhole Effect.**

| S. No. | Node Mobility (mps) | PDR % | Throughput % | Avg. E-E Delay (s) | Avg. Jitter (s) |
|---|---|---|---|---|---|
| 1 | 10 | 100 | 95 | 0.031 | 0.0213 |
| 2 | 20 | 67 | 62 | 0.13 | 1.02 |
| 3 | 30 | 63 | 55 | 0.126 | 1.087 |
| 4 | 40 | 67 | 51 | 0.183 | 1.426 |
| 5 | 50 | 64 | 55 | 0.122 | 6.97 |
| 6 | 60 | 63 | 60 | 0.155 | 1.81 |
| 7 | 70 | 54 | 51 | 0.16 | 2.047 |
| 8 | 80 | 53 | 50 | 0.16 | 4.364 |
| 9 | 90 | 50 | 49 | 0.116 | 2.78 |

**Table 2. Simulation Result with Blackhole Effect.**

| S. No. | Node Mobility (mps) | PDR % | Throughput % | Avg. E-E Delay (s) | Avg. Jitter (s) |
|---|---|---|---|---|---|
| 1 | 10 | 92 | 69 | 0.033 | 0.022 |
| 2 | 20 | 54 | 42 | 0.111 | 0.343 |
| 3 | 30 | 50 | 37 | 0.123 | 0.801 |
| 4 | 40 | 21 | 16 | 0.031 | 1.15 |
| 5 | 50 | 21 | 16 | 0.1 | 2.277 |
| 6 | 60 | 25 | 20 | 0.1 | 0.518 |
| 7 | 70 | 25 | 20 | 0.0831 | 2.047 |
| 8 | 80 | 37 | 29 | 0.137 | 0.725 |
| 9 | 90 | 13 | 8 | 0.115 | 0.343 |

## 5. Conclusion

With development in computing environments, the services based on ad hoc networks have been increased. Wireless ad hoc networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. In this paper the effect of Packet Delivery Ratio, Throughput, End-to-End Delay and Jitter has been detected with respect to the variable node mobility. There is reduction in Packet Delivery Ratio, Throughput, E-E Delay, and Jitter as shown in Figs. 4-7.

In Blackhole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes as shown in the result of the simulation. The detection of Blackholes in ad hoc networks is still considered to be a challenging task.

## References

1. Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications.* AusWireless, 21-21.
2. Chen Hongsong; Ji Zhenzhou; and Hu Mingzeng (2006). A novel security agent scheme for AODV routing protocol based on thread state transition. *Asian Journal of Information Technology,* 5(1), 54-60.
3. Dokurer, S.; Ert, Y.M.; and Acar, C.E. (2007). Performance analysis of ad hoc networks under blackhole attacks. *SoutheastCon, 2007, Proceedings IEEE*, 148 – 153.
4. Scalable Network Technologies (SNT). QualNet. http://www.qualnet.com/.
5. Sanjay Ramaswamy; Huirong Fu; Manohar Sreekantaradhya; John Dixon; and Kendall Nygard (2003). Prevention of cooperative blackhole attack in wireless Ad hoc networks. *In Proceedings of 2003 International Conference on Wireless Networks*, (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.
6. C. E. Perkins; E. M. Belding-Royer; and S. R. Das (2003). Ad hoc on-demand distance vector (AODV) routing. *RFC 3561*. The Internet Engineering Task Force, Network Working Group.
7. Satoshi Kurosawa; Hidehisa Nakayama; Nei Kato; Abbas Jamalipour; and Yoshiaki Nemoto (2007). Detecting blackhole attack on AODV based mobile Ad hoc networks by dynamic learning method. *International Journal of Network Security*, 5(3), 338–346.