International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 4 (2014), pp. 381-388

http://www. irphouse.com /ijict.htm

# Review of Prevention and Detection Methods of Black Hole Attack in AODV- based on Mobile Ad Hoc Network

**Sakshi Jain**

*Department of Computer Science, Poornima College of Engineering Sitapura, Jaipur.*

**Abstract**

Mobile Ad Hoc Network (MANET) is a Self Configuring, infrastructure less Network in which Autonomous nodes forms a multi hope network for purpose of communication. Nodes act as a host and a router by forwarding unrelated data packets. Due to the undefined boundary, no centralized administrator, changing topology and wireless links it is vulnerable to many kinds of attacks. Blackhole attack is a kind of denial of service attack, in which a malicious node advertises itself as having a shortest path to a Destination node and then purposely drops the packets. This attack awfully reduces the network performance. This paper studies Blackhole attack in AODV routing protocol. Study of literature indicates many modifications have been offered in the AODV protocol to detect and prevent Blackhole attack. These methods are studied in the paper with their pros and cons and their future scope is also studied. The performance of the network parameters like routing overhead, end to end delay, throughput, packet delivery ratio are compared in all the scenarios.

**Keywords**: Mobile Ad hoc Network (MANET); Blackhole Attack; AODV Routing Protocol.

## 1. Introduction

A mobile Ad hoc Network is a self configuration decentralized network in which Nodes are dynamic in nature and can move during the communication. Nodes can communicate with each other without any infrastructure. Multihope communication takes place between the nodes which are not in each other range. Due to the following characteristics it draw an attention from many researches and are used in places where

infrastructure networks do not work well like disaster management, battle field, virtual classrooms and places where due to less population setting an infrastructure network in costly.

For Communication between nodes many routing protocols have been designed in MANET which is categorized as Reactive, Proactive and Hybrid. Reactive protocols look for route only when route is requested by any node for ex (AODV, DSR). In Proactive protocol routes between different nodes are searched from time to time ex. DSDV and Hybrid is the combination of both the reactive and proactive protocols ex. ZRP.

AODV is one of the most efficient routing protocols for MANET, it offers several benefits as compared to others such as dynamic, self starting, Supports Multihope routing, loop free and automatically detects inactive routes [15]. Instead of all these features it is vulnerable to many attacks. Blackhole is a kind of denial of service attack in which the attacker advertise itself as having the fresh route between the nodes whose packets it want to interrupt. This attack highly reduces the packet delivery ratio and hinders the network performance.

Many modifications have been made in the algorithm to improve the performance of Network under Blackhole attack by preventing or detecting that. This Paper includes many methods and the comparison among them based on some parameters.

The rest of the paper is organized as follows: Section 2 describes the AODV protocol under influence of Blackhole attack. Section 3 outlines the related work. Section 4 shows the comparison among different methods and section 5 concludes the paper with future scope.

## 2. Adhoc on Demand Distance Routing Protocol (AODV) Under Blackhole Attack

AODV is a reactive routing protocol for Mobile Adhoc network. It has two phases route discovery and route maintenance. Whenever a node wants to send data to destination node whose address is not present in its cache.

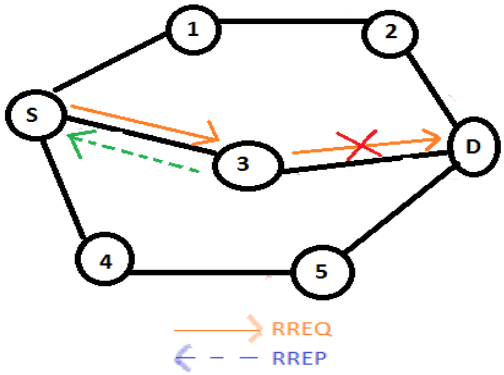


**Fig. 1**: Propagation of Route Request and Route Reply.

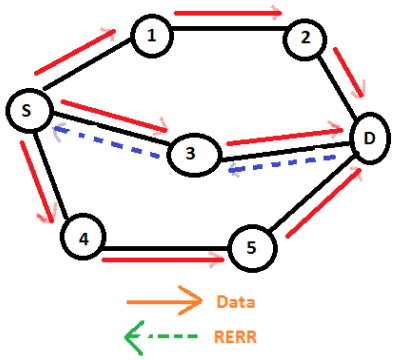


**Fig. 2**: Route Error Detection Between S and D.

It broadcast a RREQ (Route request) packet; neighbor nodes check if it is destination or have a route to destination in their routing table. In that case it will send a RREP (Route reply) packet on the reverse path as shown in Fig. 1. If path is not available, it will increment the hop count by one and further broadcast a RREQ. During the transmission of data if any node identifies route break, it will send a RERR (Route Error) message as shown in Fig. 2. Freshness of the path is measured by destination sequence number. Source node choose path with a higher destination sequence number and low hop count.

In the Blackhole attack malicious node receives a route request packet and sends a RREP with a higher destination sequence number. Source node see the RREP with big sequence number and consider that the route is fresh and start sending data packets. The malicious node does not forward the data packets and drops them, thus reduces packet delivery ratio and increase network congestion.

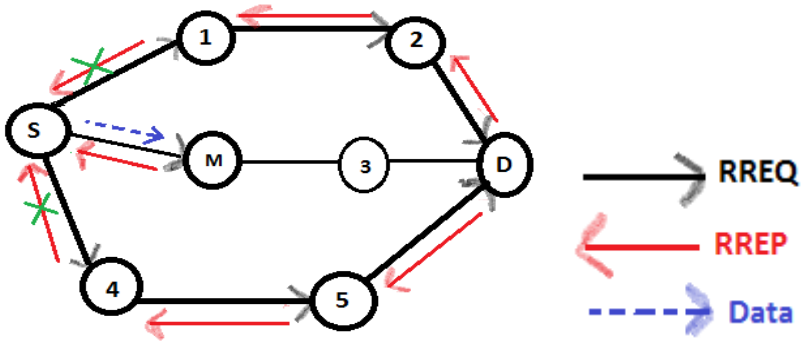


**Fig. 3**: Blackhole Attack.

In the Fig. 3 Node M (Malicious node) send a forged RREP to source node S with a higher sequence number. As source node do not have any prior information about destination in its table. It Start sending data to node M which further drop the packets.

## 3. Modified AODV Protocol Methods to Prevent and Detect Blackhole Attack

### 3.1. SAODV (Solution to Blackhole attack)

LathaTmilselvan and Dr. V Sankaranarayan[1] has proposed a solution in which source node instead of sending data packets to a node reply at once will wait and check the reply from other neighboring nodes until time outs. All the replies from neighbor node are collected in CRRT (Collect route reply table). It then checks in CRRT whether there is any repeated next hope node. If a repeated next hope node is located, it is assumed that the reply path is safe and probability of having Blackhole attack is limited.

### 3.2. Real Time Monitoring

Durgeshkshirsagar and AshwiniPatil[2]has proposed a solution, this method first identifies the neighbor of the RREP node creator i.e. suspected node. Neighbor node is instructed to listens the packets send by suspected node. Fcount and rcount are the two counters maintained by neighbor node. When a neighbor node forwards any packet to suspected node it will increase the fcount counter by 1. If suspected node forward a packet it will be overheard by the neighbor node and rcount is increased by 1. After source node receives RREP it sends packets to path to check the node is malicious node or not. Neighbor node forwards packets to suspect node until fcount reaches a threshold; thereafter if rcount is 0. RREP creator will identify as malicious node and blocked.

### 3.3. Detect and overcome Blackhole attack

Monika Y. Dangore and Santosh S. Sambare[3] proposed a solution by modifying an original AODV. To participate in Communication RREP originator must exhibit its honesty.If the node is the first receiver of the RREP packet, it will forward it to Source andcheck forthe honesty of node based on the opinion of the neighbors of RREP originator Node. Neighbors are requested to send an opinion about the RREP originator node. After receiving reply from all neighbor nodes. It checked if RREP originator node has delivered many packets to destination it a an honest node, if RREP originator node as received many packets but do not forward packets further or it has send many RREP packets, it is a misbehaving node. Such nodes are added to the quarantine list and blocked.

### 3.4. Comparing destination sequence number

Pooja Jaiswal and Dr. Rakesh Kumar [4] have proposed a method to prevent Blackhole attack in AODV. In the method source node collects all the RREP from different intermediate node. The first entry received by source is marked first entry in Route reply table (RRT). The destination sequence number (DSN) of first entry is compared with sequence number of source node. If the DSN of first entry is very large as compared to source sequence number, the node is considered as malicious node and removed from the RRT. Path is selected based on the remaining entries in RRT which is arranged according to DSN. The node with highest DSN is selected for path.

### 3.5. Secure Route Discovery For Preventing Blackhole Attack

Seryvuth Tan and KeecheonKim [5] Proposed a solution in which it has defined different threshold value for different environment like small medium and large. The threshold value defined is some percentage of the maximum destination sequence number (232) .In this two extra functions are added i.e. Source node use threshold value to verify RREP from neighbor nodes and destination Node use the defined threshold to verify the RREQ messages from source node. If the destination sequence number of RREP is greater than threshold it is considered as malicious node. Destination node also uses threshold value to identify the destination sequence number.

### 3.6. Cooperative Blackhole attack detection

Jaydipsen and sripadkoilakonda[6] proposed a solution to detect cooperative black hole attack in AODV based MANET. In this each node maintains its Data Routing Table (DRI). This is a two phase method in which node checks DRI and then cross verify the honesty of node. The proposed method relies on the reliable nodes to transfer data packets.

### 3.7 Calculation of Peak value to detect Blackhole attack

Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala[7] has proposed a solution in which malicious nodes are discovered during the route discovery process. In this in a given time interval peak value is calculated based on three parameters RREP Sequence number, routing table sequence number and number of replies received during the time interval. Peak value is the maximum value of any RREP Sequence number. If the RREP sequence number is greater than peak value it is marked as malicious node. In this source node append the list of malicious node along with the RREQ packet so any node receiving RREQ packet mark the node as malicious in its routing table.

## 4. Comparsion of Different Studies for Blackhole Attack in AODV Based Manets

**Table 1**: Comparison between different methods.

| Research Paper | Method | Blackhole Nodes | Network Parameters (AODV vs Modified AODV) | Limitations | Future Scope |
|---|---|---|---|---|---|
| Prevention of Blackhole attack in MANET | Repeated next hop node | Detect single Blackhole node | Packet delivery ratio -increased, end to enddelay-increased (due to wait and check of replies) routing overhead-increased | Work same as AODV in absence of repeated next hop node, detect Blackhole attack only up to single level | Identification of Blackhole attack at multiple levels |
| Blackhole attack detection and prevention by real time monitoring | Real Time Monitoring of nodes | Detect single Blackhole node | Packet delivery ratio -increased, end to enddelay-slightlyincreased routing overhead-increased (depends on threshold,control packets sent to check the node reliability) | Identification depends upon the value of threshold | Detect a cooperative Blackhole node attack using real time monitoring |

| | | | | | |
|---|---|---|---|---|---|
| Detecting and overcoming Blackhole attack in AODV Protocol | Honesty of node by receiving opinion from other nodes | Detect Single Blackhole node | Packet Delivery Ratio: Increased, end to end delay: Increased (time in overcoming attack and resume) and Routing Overhead: increased (time to take opinion from neighbors) | The methods works well for Blackhole attack but unable to detect more than one Blackhole node | Algorithm can be implemented for other routing protocol attacks like grayhole, wormhole etc. |
| Prevention of Blackhole attack in MANET | Difference in Sequence number | Detect single Blackhole node | Packet delivery Ratio: increased, end to end delay: slightly increased( in comparing sequence number) | If sequence number is not extremely large I will not be able to detect Blackhole node. | Simulations to analyze performance based on other parameters like mean to mean delay time, mobility etc |
| Secure route discovery for preventing Blackhole attack on AODV – based ,manets | Defined threshold for maximum destination sequence number in different enviroments | Detect single Blackhole node | Packet delivery Ratio: increased, routing overhead increased in comparing the sequence number with threshold value | Routing overhead increases as source node and destination nodes both are comparing sequence number with | Security mechanism for data transmissions between the source node and destination node after a route has been established. |
| A method for detection of cooperative Blackhole attack in Mobile Adhoc network | Use Data Routing Information and Cross Checking for identification | Detect Cooperative Blackhole nodes | Packet delivery ratio: increased, routing overhead: increased largely additional efforts in detecting and overcoming cooperative attacks | One of the few methods of detecting cooperative Blackhole attack, wide area for researches t further improve the performance under cooperative Blackhole node. | Security mechanism can be extended so that it can defend against other attacks like packet dropping, resource consumption attack. |

| | | | | | |
|---|---|---|---|---|---|
| A novel Approach for gray hole and Blackhole attacks in mobile Ad-hoc Networks | Peak value is calculated to define the maximum value of sequence number | Detect single Blackhole node | Improves packet delivery ratio with negligible packet overview | Depends upon the destination sequence number. | Implementation of the method is yet to be done |

## 5. Conclusion

Blackhole Attack in Manet is a Denial of Service Attack which reduces the network performance. The study here shows different modified versions of AODV algorithms which have been proposed and implemented to prevent and detect Blackhole attack. A comparison table shows the performance of methods, their limitations and Future work.

## References

[1] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole attack in MANET", BSA Crescent Engineering college, 2007 IEEE

[2] Durgesh Kshirsagar and Ashwini Patil, "Blackhole attack prevention and detection by real tiem monitoring", 4th ICCCNT 2013

[3] Ms. Monika Y. Dangore and Mr. Santosh S. Sambare "Detecting and overcoming Blackhole attack in AODV protocol", Internation conference on cloud & ubiquitous computing, 2013 IEEE

[4] Pooja Jaiswal and Dr. Rakesh Kumar "Prevention of Blackhole attack in MANET", IRACST, October 2012

[5] Seryvuth Tan and Keecheon Kim "Secure route discovery for preventing Blackhole attacks on AODV-based MANET" 2013, IEEE

[6] Jaydip Sen, Sripad koilakonda, Arijit Ukil "A mechanism for detection of cooperative Blackhole attack in MANET, 2nd international conference on intelligent system, modeling and simulations

[7] Rutvij H. Jhaveri, Sankita J. Patil, Devesh C. Jinwala, "A novel approach for grayhole and Blackhole attacks in Mobile Adhoc networks", 2nd international conference on advanced computing & communication technologies

[8] Sarita mandala, abdul hanan Abdulla, "A review of Blackhole attack in mobile Adhoc network" 3rd international conference on instrumentation, communication, nformation technology and biomedical engineering, 2013.

[9] U. venkanna, R. Leela veludsmy," blackhole attack and their counter measure based on trust management in MANET, survey, Int. conf. on advances in recent technologies in communication and computing, 2011.

[10] Humaira ehsan, farrukh aslam khan, “malicious AODV” 11th Int. Conf. on trust, security and privacy in computing.
[11] Ming Yang Su, Kun-Lin Chiang, Wei-Cheng Liao,”mitigation of Blackhole nodes in MANET network,”, international symposium on parallel and distributed processing with applications.