SURVEY ON BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORK

S. ARUL JOTHI, Dr. M. LALLI
Research Scholar, Assistant Professor
School of Computer Science and Engineering,
Bharathidasan University, Trichy, India.

Abstract: Mobile ad-hoc network is a decentralized communication network. For a certain period of time, each node in a MANET acts as a server, client or router. It does not need any infrastructure such as a base station so that MANET becomes vulnerable to network attacks. In this, the malicious nodes act like a black hole node. It indicates itself as the shortest path to a destination in a network by sending the fake route reply to the source node [5]. This paper investigates the methods that are used to detect and prevent the black hole attack in MANETs.

Keywords - MANET, Black hole attack, Techniques

I. Introduction
MANET is a combination of three words: Mobile refers to moving state, ad-hoc refers to temporary purpose and network refers to collection of interconnected computers. It consists of mobile nodes that form network without wire for temporary purpose [8]. Each device in a MANET is free to move independently in any direction, and change its links to other devices frequently.

II. TYPES OF ROUTING PROTOCOLS
There are different types of routing protocol in MANET. These are classified into three types:

2.1 Table Driven Routing Protocols
2.2 On-Demand Routing Protocols
2.3 Hybrid Routing Protocols

![Routing protocols of MANET](image)

2.1 Table Driven Routing Protocols
It is also referred to as proactive protocols. It maintains routes to the destination even if they are not needed. Some of the examples are Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Cluster-Head Gateway Switch Routing Protocol, Source-Tree Adaptive Routing Protocol (STAR), and Optimized Link State Routing (OLSR).

2.2 On-Demand Routing Protocols
It is also referred to as reactive protocols. It maintains routes to a destination only when they are needed. Examples are Dynamic Source Routing (DSR), Ad Hoc-On-Demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA), and Associativity-Based Routing (ABR).
2.3 Hybrid Protocol

It is a combination of both reactive and proactive protocols. It maintains routes to nearby nodes even if they are not needed and maintain routes to far away nodes only when needed. Example Zone Routing Protocol (ZRP). [10][11]

III. ATTACKS IN MANET

3.1 Based on the source of the attacks [8]

3.1.1. External Attack

In this type of attack, the malicious node does not belong to the network. It causes congestion due to a false/fake advertisement.

3.1.2 Internal Attack

This attack occurs only within the network.

3.2 Based on the behavior of the attacks

3.2.1 Passive Attack

When we exchange the data between the source and destination the data will not be modified just the data will be accessed by the malicious node.

3.2.2 Active Attack

When we exchange the data between the source and destination the data will be modified by the malicious node.

IV. BLACK HOLE ATTACK

Blackhole is one type of network traffic attack of MANET [7]. In this, the malicious nodes act like a black hole attack, indicating itself as the shortest path to the destination in a network by sending a fake route reply to the source node [5]. It gets all the data packets from the source node and then drops the packets. The black hole attack is classified into two types. They are

4.1 Single Black Hole Attack

In a single black hole attack, only a single node act as a fake node [7]. It obtains all data packets from the source without forwarding to the destination. From below fig.3. The source node S wants to send the data to destination D. So S starts the route searching process to the destination D by broadcasts the RREQ message to all its neighbor nodes. Then the neighbor node has also broadcast the message until to reach the destination D. After receiving the RREP message, the destination node D will reply to the source node via RREP message. The malicious node M also generate the fake RREP message to the source node S. It indicating itself as the shortest path, spoofed sequence number, and minimum hop count to reach the destination D. Then the source node S discards other RREP coming from other authorized node and starts transmitting all its data packets via malicious node. The malicious node (M) drop all data packets without forwarding to the destination node (D). It will crash all data packets. Then it will make the packet loss in the network.
4.2 Multiple Black Hole Attack

In multiple black hole attack, more than one node act as a malicious node. This will affect network performance than the single black hole attack. The multiple black hole attack is shown in fig.4

V. RELATED WORKS

Taku Noguchi et al [1] in this method to prevent the black hole attack using multiple RREPs forwarding and RREP filtering mechanisms. It proposes a new threshold-based black hole attack prevention method using multiple RREPs. It also shows the performance metrics in terms of packet delivery rate, throughput and routing overhead.

Ankit Singh et al [2] the purpose of this paper is to analyze the performance of various routing protocols like AODV, DSR, OLSR, DSDV, ZRP during the black hole attack in MANET. From the results, the ZRP routing protocol shows better performance than all other routing protocols in terms of packet delivery ratio, average throughput, packet-drop-ratio, average end-to-end delay.

Mangesh A.Suryawanshi et al [3] the purpose of this paper is to prevent the black hole attack in AODV routing protocol by Diffie-Hellman key exchange and advanced encryption standards[AES] algorithm. This method isolates the malignant node on the selective path in AODV routing protocol and secures the channel by utilizing two algorithms such as D-H exchange and AES algorithm.

Helmi Hartadi et al [4] the purpose of this paper is to analyze the performance of two routing protocols such as AODV and DSR during a black hole attack in MANET. From the results, the AODV routing protocol shows better performance than DSR routing protocols in terms of throughput, delay, and packet loss.

A. A Chavan et al [5] this paper analysis the performance of AODV and DSDV routing protocols in terms of routing overhead, packet delivery ratio, throughput, and end-to-end delay. The performance of modified AODV is better than DSDV in terms of throughput, packet delivery ratio and routing overhead. This paper did some modifications in AODV to improve the performance of AODV in the presence of a black hole attack.

Jyoti Prabha et al [6] have proposed from this method conjunct blackhole attack eliminate from the DSR routing protocol using the RSA algorithm. It also shows the performance metrics in terms of delay and throughput of the network in the ad hoc network environment.
Table. 6.1: comparative analysis of black hole attack detection and prevention techniques

<table>
<thead>
<tr>
<th>S.No</th>
<th>Title of Paper</th>
<th>Authors</th>
<th>Year &amp; Publication</th>
<th>Technique Used</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Comparative study of OLSR, DSDV, AODV, DSR, and ZRP routing protocols Under Black hole attack in mobile ad hoc Network.</td>
<td>Ankit Singh et al.[2]</td>
<td>2018 Springer</td>
<td>-</td>
<td>1. ZRP had given better result in terms of packet drop ratio, Average throughput.</td>
<td>1. Increases avg.end-to-end delay. 2. Did not find a solution for a collaborative black hole attack.</td>
</tr>
</tbody>
</table>

Table 6.1 shows the black hole attack detection and prevention techniques, metrics, advantages, and disadvantages. Column 5 in table 6.1 shows that the technique is used to detect and prevent the black hole attack. in column 7 shows that some parameters are not concluded with any solution in the existing work (1-6).

In the above table following metrics are used: [4] [13]

**Throughput**
The rate of successfully transmitted data per second in the network during the simulation.

**Packet Delivery Ratio**
The ratio of the number of packets received by the receiver to the number of packets sent out by the sender.
PDR = \frac{\text{Data sent out by the sender}}{\text{Data received by the receiver}}

End To End Delay
The total time it takes data packets to reach the destination from the source across the network. It calculates as

\text{Dend-to-end} = \text{transmission} + \text{propagation} + \text{processing}

Packet Drop Ratio
The ratio of the total number of lost packets and the total number of received packets.

\text{PDR} = \frac{\text{Total number of lost packets}}{\text{Total number of received packets}}

Routing Overhead (RO)
The ratio of the total number of routing packets (RREQ, RREP, and RERR) and the total number of data delivered packets.

\text{RO} = \frac{\text{Total number of routing packets}}{\text{Total number of data delivered packets}}

Detection Time (DT)
It is measured by

\text{DT} = \text{the attack detection time - the traffic start time.}

VII. ANALYSIS ABOUT EXISTING BLACK HOLE ATTACK PREVENTION TECHNIQUES AND MEASURES

Table 7.1: Comparison of AODV, DSDV and modification AODV in terms of Packet Delivery Ration, Throughput

<table>
<thead>
<tr>
<th>Prevention Technique</th>
<th>No.of Nodes</th>
<th>Packet Delivery Ratio</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AODV</td>
<td>DSDV</td>
<td>Modifications in AODV</td>
</tr>
<tr>
<td>10</td>
<td>0.904966</td>
<td>0.99732</td>
<td>0.006668</td>
</tr>
<tr>
<td>30</td>
<td>0.980403</td>
<td>0.79651</td>
<td>0.999463</td>
</tr>
<tr>
<td>40</td>
<td>0.826577</td>
<td>0.999463</td>
<td>0.006668</td>
</tr>
<tr>
<td>50</td>
<td>0.914631</td>
<td>0.999463</td>
<td>0.006667</td>
</tr>
<tr>
<td>60</td>
<td>0.840805</td>
<td>0.999463</td>
<td>0.006668</td>
</tr>
<tr>
<td>70</td>
<td>0.99732</td>
<td>0.913557</td>
<td>0.006665</td>
</tr>
<tr>
<td>80</td>
<td>0.980403</td>
<td>0.914094</td>
<td>0.998658</td>
</tr>
<tr>
<td>90</td>
<td>0.914899</td>
<td>0.998389</td>
<td>0.006668</td>
</tr>
<tr>
<td>100</td>
<td>0.917584</td>
<td>0.999195</td>
<td>0.006668</td>
</tr>
</tbody>
</table>

Table 7.2: Comparison of AODV, DSDV and modification AODV in terms of End to End Delay, Routing Overhead

<table>
<thead>
<tr>
<th>Prevention Technique</th>
<th>No.of Nodes</th>
<th>End To End Delay</th>
<th>Routing Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AODV</td>
<td>DSDV</td>
<td>Modifications in AODV</td>
</tr>
<tr>
<td>10</td>
<td>0.027915</td>
<td>0.011007</td>
<td>0.01167</td>
</tr>
<tr>
<td>30</td>
<td>0.044079</td>
<td>0.010753</td>
<td>0.011668</td>
</tr>
<tr>
<td>40</td>
<td>0.011683</td>
<td>0.01068</td>
<td>0.011669</td>
</tr>
<tr>
<td>50</td>
<td>0.028415</td>
<td>0.01095</td>
<td>0.011671</td>
</tr>
<tr>
<td>60</td>
<td>0.011688</td>
<td>0.010876</td>
<td>0.011688</td>
</tr>
<tr>
<td>70</td>
<td>0.028964</td>
<td>0.011522</td>
<td>0.011669</td>
</tr>
<tr>
<td>80</td>
<td>0.043806</td>
<td>0.011748</td>
<td>0.011674</td>
</tr>
<tr>
<td>90</td>
<td>0.011703</td>
<td>0.012568</td>
<td>0.011672</td>
</tr>
<tr>
<td>100</td>
<td>0.011701</td>
<td>0.012614</td>
<td>0.011669</td>
</tr>
</tbody>
</table>

From the table 7.1 and table 7.2 comparative analysis this modifications in AODV shows better result in packet delivery ratio, throughput, end to end delay and routing overhead when compared with AODV and DSDV [5]. From Table 6.1 comparative analysis this multiple RREPs technique achieves the minimum routing overhead and increases the minimum routing overhead and increases the throughput and packet delivery ratio [1]. D-H key exchange and AES algorithm methods decrease the route discovery time and...
The RSA technique provides more security than other techniques. Because, this technique eliminate the conjunct black hole attack. It decreases the delay and increase the throughput.

VIII. CONCLUSION

From the performance analysis carried out in this paper, it is found that the RSA algorithm performs better than all other techniques. This method has some benefits such as, increase the throughput, decrease the delay, and also it prevents multiple black hole attack. All the above-mentioned methodologies have some drawback because it has packet losses and also it does not support the cooperative black hole attack. Further, the main aim of the RSA algorithm to improve security as well as the performance of the network. In future this RSA algorithm will continue with another routing protocol instead of DSR routing protocol.

REFERENCES