International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Analysis of Black-Hole Attack in MANET using AODV Routing Protocol

Ms Neha Choudhary
Electronics and Communication
Truba College of Engineering, Indore
India

Dr Sudhir Agrawal
Electronics and Communication
Truba College of Engineering, Indore
India

Abstract: **MANET is an infrastructure less, dynamic, decentralised network. Any node can join the network and leave the network at any point of time. Due to dynamic infrastructure-less nature and lack of centralized monitoring points, the ad hoc networks are vulnerable to attacks. The network performance and reliability is break by attacks on ad hoc network routing protocols. AODV is a important on-demand reactive routing protocol for mobile ad hoc networks. There is no any security provision against a "Black Hole" attacks in existing AODV protocol. Black hole nodes are those malicious nodes that conform to forward packet to destination. But they do not forward packet intentionally to the destination node. The black hole nodes degrade the performance of the severe attacks of MANET. This paper discusses some of the techniques put forwarded by researchers to detect and prevent Black hole attack in MANET using AODV protocol .**

Keywords: ***MANET, AODV, adhoc, Black hole attack, Malicious Node.***

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) is formed by some wireless nodes communicating each other without having any central coordinator to control their function. Such a network is helpful in creating communication between nodes that may not be in line-of-sight and outside wireless transmission range of each other. Similar wireless networks have important applications in a wide range of areas covering from health, environmental control to military systems. In MANET, as the nodes are utilizing open air medium to communicate, they face acute security problems compared to the wired medium. A black hole attack is referred to as a node dropping all packets and sending forged routing packets to route packets over itself. A malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped [1]..

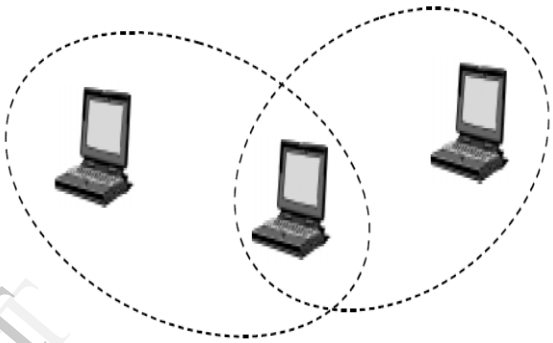

Figure 1.1: A simple ad-hoc network with three participating nodes.

2. ROUTING PROTOCOL

Routing is the process of discovering a suitable route for sending packets from a source to a destination. Routing is to produce reliable and efficient routes between pair of nodes for data transmission. To transmit a packet from source to destination it may be necessary to hop several hops (multi-hop) before a packet reaches the destination. To facilitate the communication within network, routing protocol is needed. The routing protocol has two main functions, selection of routes for various source-destination pairs and the maintenance of routes for delivery of messages to their correct destination. The route to be followed by the packets is determined by the network layer. The algorithms used to calculate these routes are known as routing algorithms. Routing protocols can be classified as:

- Proactive Protocols
- Reactive Protocols
- Hybrid Protocols
-

2.1.Proactive Protocols:

Proactive routing protocols also known as table driven routing protocols monitor the topology of the network at all times and continuously evaluate the routes within the network for all destinations. Routes are maintained for all nodes by periodically exchanging routing tables throughout the network, similar to wired networks. An advantage of this routing protocol is that when a packet needs to be

forwarded, the route is already known and can be immediately used. Obtaining the required route information and establishing a session is not time-consuming. A disadvantage of this routing protocol is that it reacts to topology changes even when no traffic is affected by that change, resulting in the unnecessary usage of bandwidth even when no data is transferred. Also proactive schemes needs time to converge to a steady state which is a problem if the topology is changing frequently. Typical routing protocols in this category are optimized link state routing (OLSR) and destination-sequenced distance-vector (DSDV).

2.2.Reactive Protocols

Reactive routing protocols also known as on demand routing protocols invoke a route determination procedure on demand only. Reactive protocols find a route only at the beginning of a connection when there is a demand for data transmission. This is done by initiating a route discovery within the network by flooding the entire network with route request (RREQ) packets. Once a route is established, it is maintained in the routing table until the destination is out of reach or the route expires. As the routing information is not updated periodically, the routing overhead is significantly reduced during topology changes. One disadvantage of these protocols is the latency occurred during route discovery. However, for highly mobile networks, these protocols show better performance for MANETs. Typical routing protocols in this category are ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR).

2.3.Hybrid Protocols

Hybrid routing protocols combines the merits of both proactive and reactive routing protocols. On-demand routing has relatively less routing overhead, but it suffers from routing delay. Table-driven routing ensures high quality in static topologies but cannot be extended to mobile networks. Combining the advantages of both, a few hybrid routing protocols have been designed, in which the routing is first initiated with some proactive routes and then serves the demand from other nodes through reactive flooding. The hybrid protocols exploit hierarchical network architectures. Typical routing protocols in this category are as follows: zone routing protocol (ZRP) and temporally ordered routing algorithm (TORA).

3.AODV

AODV is a source initiated on-demand routing protocol. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand [7]. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself.

AODV is a reactive routing protocol designed for ad hoc wireless networks. In AODV routes to connect two nodes are obtained only when it is required i.e. on demand. AODV routing algorithm is specially suited for dynamic self-configured networks like MANET. AODV provides loop free routes along with route management for broken links. Bandwidth requirement of mobile nodes in AODV is comparatively less than other protocols as AODV does not require periodic route advertisements [1].

AODV uses symmetric links between communicating nodes. Nodes which are communicating or intermediate nodes on active route only maintain routing information. Nodes which do lie on active path need not maintain routing information and does not exchange routing table periodically. Furthermore, routes are discovered and maintained between two nodes only when they need to communicate or if they are acting as the intermediate node supporting in communication. For route discovery AODV uses broadcast mechanism . Instead of using source routing, routing strategy used in AODV is to establish route entries dynamically at intermediate nodes. This kind of routing serves networks with large number of nodes by saving overhead required by source routes in each data packet.

4.Security Issues In Manet: Due to self-organize, rapidly deploy capability and many other features discussed earlier, MANET is preferable for different applications like battlefield communications, emergency disaster relief, public conferences and other security-sensitive computing environments. Security is a major concern in network design especially in hostile environments where ad hoc networks are readily used. This characteristic makes MANET more susceptible to security attacks from inside the network.

5. Black Hole Attack: A black hole attack is referred to as a node dropping all packets and sending forged routing packets to route packets over itself. A malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination [1].

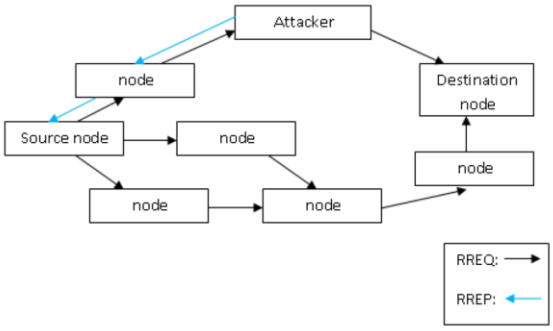

Figure 1.2: Black Hole Attack in MANET

Intrusion Detection Technique- IDS can be classified as Network-based and Host-based. Network-based IDS can be installed on data concentration points of a network such as switches and routers. Where as Host-based IDS are installed on hosts that can supervise the activities of other hosts. The proposed technique (IDS-AODV) uses Host-based IDS scheme as a Network-based IDS scheme require central device to monitor traffic flow in MANETs. IDS-AODV assumes every activities of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Intrusion detection can also be classified into three broad categories:

- Anomaly detection
- Misuse (signature) detection,
- Specification-based detection.

Proposed Strategy for Blackhole Detection and Prevention

In the proposed work, every AODV node executes an IDS mechanism, i.e. each node in the network has an IDS agent in-built in the form of module with AODV routing protocol. IDS module estimates the suspicious value called count of a node according to the numbers of RREQ and RREP packets transmitted or forwarded from the node. 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 Proposed Algorithm

In this section the proposed mechanism for defending against black hole attack is presented. The mechanism modifies the AODV protocol by introducing three concepts,

i. Broadcast RREP packet,
ii. Data Routing Information, count
iii. Reliability checking of a route

6.SIMULATION RESULTS AND DISCUSSION

The simulation results of AODV, wormhole AODV and MAODV routing protocols and their comparisons are shown in the following section 9.2 in the form of graphs. Also the simulation results of AODV, blackhole AODV and IDSAODV routing protocols and their comparisons are shown in the section 7.3 in the form of graphs. The simulation analysis of three routing protocols primarily focuses on a few performance metrics discussed in next section.

6.1 Performance Metrics

The following metrics are used in this work for comparing the performance of AODV, AODV under attacks and Modified AODV routing protocols.

6.1.1.Packet Delivery Ratio (PDR)

It is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source node. It can be calculated in terms of percentage (%) [25]. Packet delivery ratio shows total number of data packets that reach destination successfully. The reason for packet drops may arise due to congestion, faulty hardware and queue overflow etc. Packet drop affects the network performance by consuming time and more bandwidth to resend a packet. Higher packet delivery ratio shows higher protocol performance.

6.1.2.End to end Delay

It can be defined as the time a packet takes to travel from source to destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

6.1.3.Throughput

Throughput is the amount of data transferred successfully on a communication network or network link over the period of time. Throughput is calculated in bytes/sec or bits/second (bps).

These metrics are not completely independent. For example, lower packet delivery fraction means that the delay metric is evaluated with fewer samples. Path lengths play a vital role, the longer the path lengths, the higher the probability of a packet drop. Thus, with a lower delivery fraction, samples are usually biased in favour of smaller path lengths and therefore have less delay.

6.2.PERFORMANCE COMPARISON FOR SEVERAL NODES

6.2.1 Packet Delivery Ratio Comparison

This subsection shows the packet delivery ratio of the three routing protocols, calculated for different number of nodes. The variation of packet delivery ratio with the number of nodes is shown in figure1.3 .

Packet Delivery Ratio (PDR)

Nodes	AODV	BLACKHOLE AODV	IDS AODV
5	99.4%	1.13%	49.2%
10	98.54%	1.46%	62.9%
15	98.66%	0.89%	45.1%
20	87.85%	1.21%	38.87%
25	86.97%	0.85%	49.01%

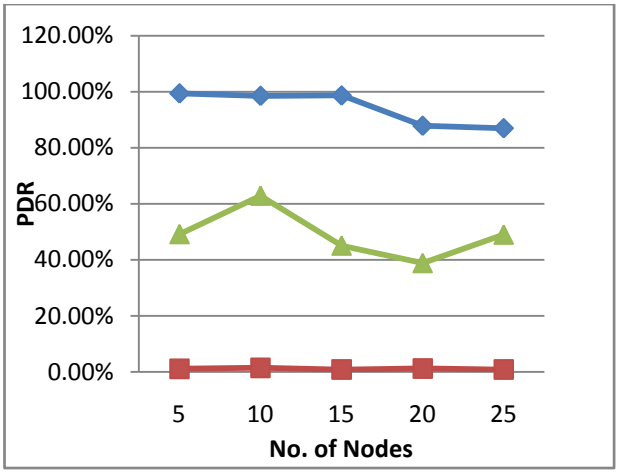

Figure 1.3 PDR Comparisons for AODV, Blackhole AODV and IDS AODV

AODV routing protocol shows higher PDR than the AODV under blackhole attack and IDS-AODV for any number of nodes. However, under blackhole attack IDS-AODV shows performance improvement with increase in PDR whereas AODV delivers only about 1% of the packets.

6.2.2 Average End-to-End Delay Comparison

End-to-end delay for all the received packets is calculated and averaged. In this subsection, average end-to-end delay for the three routing protocols is calculated for different number of nodes. The variation of delay with the number of nodes is shown in figure 1.4.

Delay

Nodes	AODV	BLACKHOLE AODV	IDS AODV
5	62.67 ms	15.39 ms	6.88 ms
10	15.77 ms	14.25 ms	6.73 ms
15	12.55 ms	33.25 ms	23.33 ms
20	67.8 ms	53.51 ms	17.86 ms
25	252.78 ms	33.95 ms	26.27 ms

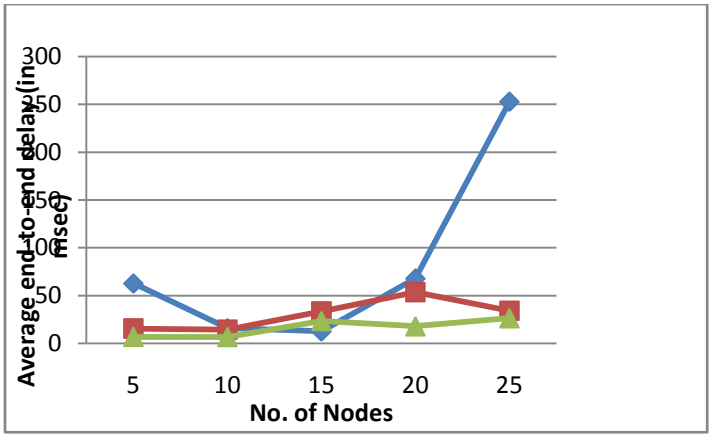

Figure 1.4 : Average End-to-End Delay Comparisons for AODV, Blackhole AODV and IDS AODV

The average end-to-end delay of AODV is higher as compared to blackhole AODV and IDS-AODV except for 15-nodes scenario. IDS-AODV has superior performance than AODV under blackhole attack as the average end-to-end delay for IDS-AODV is less than delay for AODV under attack for all cases except for 15-nodes scenario.

6.2.3 Throughput Comparison

The throughput is calculated at destination node during entire simulation period. In this subsection, throughput for the three routing protocols is calculated for different number of nodes. The variation of throughput with the number of nodes is shown in figure 1.4.

Throughput

Nodes	**AODV**	**BLACKHOLE AODV**	**IDS AODV**
5	88.27	80.16	91.06
10	146.71	83.14	97.51
15	131.28	100.55	106.03
20	182.74	132.61	146.09
25	252.98	219.46	243.52

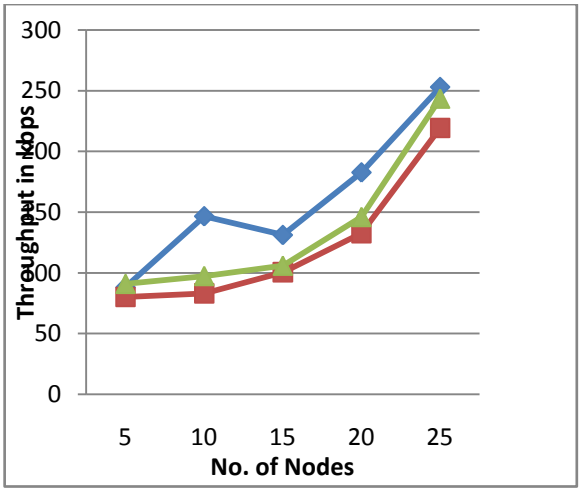

Figure 1.4 : Throughput comparisons for AODV,

Blackhole AODV and IDS AODV

From the comparison results it is clear that IDS-AODV has better performance than AODV, as throughput is always higher in all the topologies considered.

From all the results it is clear that IDS-AODV has superior performance over AODV under attacks. Also the performance of IDS-AODV improved with the increase in number of nodes and simulation time.

7.CONCLUSIONS

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in MANET theoretically and through simulation. . To evaluate the performance of proposed techniques, simulation of blackhole attack along with the simulation of proposed techniques had been done.

8.REFERENCES

[1]C. K. Toh, "Ad Hoc Wireless Networks",

[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.

[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, pp 30–40, 2003.

[4]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