# The Impact of Black-Hole Attack on AODV Protocol

FIHRI Mohammed
Mathematics and Computer Science
Dept, LAVETE Laboratory
Faculty of Sciences and Technical
Settat, Morocco

OTMANI Mohamed
Mathematics and Computer Science
Dept, LAVETE Laboratory
Faculty of Sciences and Technical
Settat, Morocco

EZZATI Abdellah
Mathematics and Computer Science
Dept, LAVETE Laboratory
Faculty of Sciences and Technical
Settat, Morocco

***Abstract*—In mobile Ad-Hoc networks, each node of the network must contribute in the process of communication and routing. However this contribution can expose the network to several types of attackers. In this paper, we study the impact of one attack called BLACK-HOLE, on Ad hoc On-Demand Distance Vector routing protocol. In this attack a malicious node can be placed between two or several nodes, and begin dropping all packets from a source and breaking communications between nodes. The vulnerability of the route discovery packets is exploited by the attacker with a simple modification in the routing protocol, in order to control all the traffic between nodes. In this study we simulate the attack with NS2, taking into account the mobility of the network and the attacker, the position of the attacker and finally the number of the attackers. We will also see the impact of this attack in a higher number of loss packet compared with AODV in normal situation.**

***Keywords—Black-Hole; AODV; Attack***

## I. Introduction

Mobile ad hoc network (MANET) is the network of mobile nodes that requires no infrastructure or centralized management in order to communicate. The nodes can join or leave the network any time thus have a dynamic approach of network topology. Here nodes carry the responsibility of router and host both. It does not have any preexistent infrastructure or centralized controller, and the nodes in it rely on each other in order to communicate. This type of network allows to create and deploy a wide field of communication quickly, and that's what we need in several cases such as a natural disaster or battlefield surveillance where there is no centralized infrastructure and all nodes are capable of movement and must be connected to each other dynamically and arbitrary. It offers better coverage and higher throughput with lower operating cost. However, due to distributed nature of the wireless nodes they are several vulnerabilities and the Black hole is one of the most known.

In this paper we will focus on the performance of AODV (Ad hoc On-Demand Distance Vector) protocol under Black hole attack. we did our simulation with ns2 by implementing a new protocol that adopts the algorithm of AODV and the behavior of a Black hole attacker.

## II. Overview of AODV Routing Protocol

Ad-hoc routing protocols determine the appropriate path from the source to destination and efficiently notify the network with link failure, if it occurs. These protocols are broadly divided into two categories.

- Table-driven routing protocols.
- Source-initiated on-demand driven routing protocols.

Table-driven routing protocols are also known as proactive routing protocols. These protocols desire to maintain consistent and up-to-date routing information in the network. The nodes exchange the routing information periodically and also when there is even a minor change in the network topology and thus, every node maintains one or more routing table to store routing information about every other node in the network.

As a result, these protocols are not preferred in large network. The highly dynamic network also avoids it, as there is lot of message exchanges and it will create congestion and delay in the network. The protocol evolves periodic exchanges even when there is no change in topology and this is simply the wastage of network resources. The mobile devices may also drain out their battery power sooner in such cases. In spite of several drawbacks, these protocols also have the advantage that there is no initial delay as routing information is always available.

AODV is a reactive routing protocol used to find a route between a source and a destination, and allows mobile nodes to obtain new routes for new destinations in order to establish an ad hoc network. In this order several messages are exchanged, different types of link are established, and many information can be shared between the participants nodes. In AODV protocol we find hello message and three others significant type of messages, route request RREQ, route reply RREP and route error RERR. The Hello messages are used to monitor and detect links to neighbours, every node send periodically a broadcast to neighbours advertising it existent ,if a node fails to receive an hello message from neighbour a link down is declared. In order to communicate every node must create routes to the destinations, to achieve that the source node send a request message RREQ to collect information about the route state; if the source receives the RREP message the route up is declared and data can be sent and if many RREP are received by the source the shortest route will be chosen . Any nodes have a routing table so if a route is not used for some period of time the node drop the route from its routing table and if data is sent and a the route down is detected another message (Route Error RERR) will be sent to the source to inform that data not received.

### A. *Route Request (RREQ) Message*

This type of message is used by AODV at first in order to locate a destination, this message contains identification of request, sequence number, destination address and also a count of hop initialled by zero.

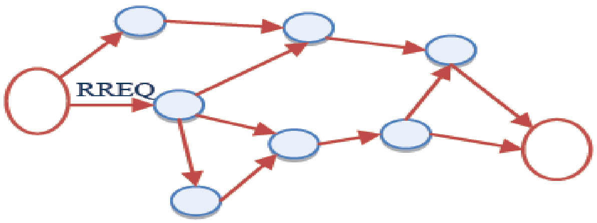


Fig. 1. Route Request (RREQ) Message

### B. *Route Reply (RREP) Message First*

This type of message contains the same fields like Route Request (RREQ) Message, and it sent in the same route of reception of RREQ message. When the source received this message it mean that the destination is ready to accept information and the rout is working correctly.

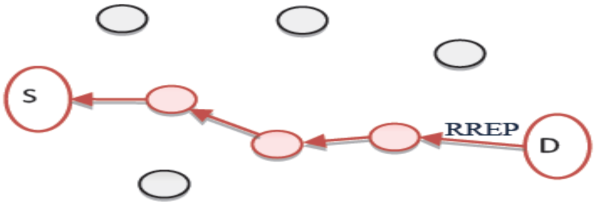


Fig. 2. Route Reply (RREP) Message

### C. *Route Error (RERR) Message*

Sometimes a node detect a destination node that not exists in network, in this scenario another message (Route Error RERR) is sent to the source informing that the data is not received. RERR is like an alert message used to secure table of routing.

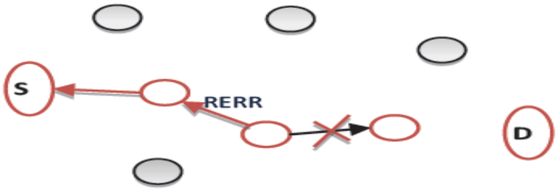


Fig. 3. Route Error (RERR) Message

## III. Ad Hoc Network and Security Issues

With the help of routing protocols, nodes in a MANET exchange the information organizing the topology accordingly. This information can be sensitive and targeted by malicious adversaries with an objective to intercept and harm the network or applications. There are two types of security attacks active and passive. In passive attack, the attacker does not affect the functionality of routers or we can say does not inject any kind of disturbance. It just spies on or monitors the routing. While in active attack, the attacker intercepts the routing by several means that can be done by impersonating the newly launched node, repeating the old data packets, disturbing the correct routing by faulty information etc. There are mainly two kinds of sources of MANET threats:

- There can be attackers who attack from outside of the MANET, that is external attacks on a mobile ad hoc network by distortion, overload, redundancy and injecting false routing information.
- In second type of approach, sources of attacks are internal that means the compromised nodes can affect the data adversely to cause failure and can misuse the information of routing to other nodes . There are many drawbacks of MANET that make it vulnerable to various malicious attacks. It doesn’t have any fixed infrastructure, nodes can leave and join the network anytime, dynamic topology, limited physical security, frequent routing updates and many other attributes are there due to which MANET often suffers with security attacks.

Some main security issues are briefly described here.

### A. *Security Issues in MANET*

*1) Decentralized Connection:* Unlike the traditional approach of networks having a fixed infrastructure and central points (access points), MANET is connected in a decentralized manner. It works without a pre-existent infrastructure. The nodes in it work as routers and host, forwarding and receiving the data packets. Due to this absence of a central management, detecting the attacks or monitoring the traffic is very difficult in large scale or highly dynamic MANETs.

*2) Uncertain Boundaries:* Mobile Ad Hoc Networks do not have any clear or secure boundary. As the nodes can leave or join the network anytime and can communicate with other nodes in the network, it is not possible for a MANET to have certain boundaries. If a node is in the radio range of a MANET, it automatically joins it. This characteristic makes a MANET more susceptible to security threats. Network or the applications running in it can be disturbed through redundancy, distortion, leakage and injection of false information .

*3) Dynamic Topology:* In MANET, nodes are free to frequently leave and join the network and move arbitrarily. Thus the routes change very often, changing the topology dynamically. These changes in nodes, routes and topologies are very frequent and unpredictable. This results as partitioning of network and cause loss of data packets affecting the integrity of information.

*4) Scalability issues:* Mobile Ad Hoc Networks are quite different from the traditional approach of fixed networks, where the network is created by connecting the devices through wires so that one can define the network during the initial phase of design and it does not changes during the use. On the other hand, in MANETs nodes are free to move in and out of the network. Nobody can predict the number of nodes a MANET had in past or can have in future.

*5) Compromised Node:* Compromised node is a node in MANET, on which the attackers get the control through unfair means with the intentions of performing malicious activities. The nodes in MANET are free to move and autonomous in nature. They cannot prevent the malicious activities they are communicating with. As the nodes can join and leave the network anytime, it becomes very difficult to track or monitor the malicious activity because the compromised node changes its position too frequently.

*6) Physical Security Limitations:* MANET often suffers with security attacks. Mobility of nodes increases this possibility and makes it more susceptible to malicious activities. These attacks include monitoring of traffic with unfair intentions, denial of service attack in which a malicious node claims to be a different node to get the sensitive information, masquerading, spoofing etc.

*7) Limited resources:* The nodes in a MANET rely only on battery power for energy means, as they do not have any centralized management. Bandwidth constraint also affects as they have lower capacity than that of the infrastructure based networks. MANETs have variable capacity links. Along with limited power, the storage capacity of a MANET is also limited.

### B. Security Issues in AODV

AODV protocol is exposed to a variety of attacks, the impact of these attacks on AODV protocol are not the same. Some of these attacks can cause a breakdown of the network connectivity, increasing the end-to-end delay, increasing the number of the loss packets, or shutting down some nodes by consuming all the energy left in there batteries.

*1) Black hole attack*

*2) In black hole attack:* A malicious node must be placed between two or more nodes and begin dropping all the traffic. This attack exploits the vulnerability of the route discovery packets of the routing protocol by modifying this last one in order to control all traffic that circulates between nodes.

*3) Wormhole attack:* In this type of attack, an attacker saves the packets generated in one location of the network and redirects it to another and replays it. This type of attack can be performed by several malicious nodes in same time.

*4) Byzantine attack:* In this type of attack, individually or cooperatively a malicious nodes carry out attacks such as creating routing loops and forwarding packets through non-optimal paths.

*5) Rushing attack:* Rushing attacker forwards data and messages very quickly by skipping some of the routing processes. So, in on-demand routing protocol such as AODV, the route between source and destination include rushing nodes.

*6) Resource consumption attack:* In this type of attack, an attacker attempts to consume battery life of other nodes to take it down.

*7) Location disclosure attack:* In this type of attack, the related information to the structure of network is revealed by attacker nodes.

## IV. Black Hole Attack

Due to these above mentioned issues, MANET is susceptible to many security attacks. Black Hole Attack is one of these attacks. It is a simple but certainly effective Denial of Service attack in which a malicious node, through its routing protocol, advertises itself for having the shortest path to the destination node or to the node whose packets it wants to intercept. It pretends to have enough of fresh routes for a certain destination. The source node assumes it to be true and the data packets are forwarded to a node which actually does not exist, causing the data packets to be lost. When a source node wants to initiate the communication, it broadcasts a RREQ message for route discovery. As soon as the malicious node receives this RREQ packet, it immediately responds with a false RREP message to the respective node advertising itself as the destination or having the shortest path for that destination. Since the malicious node needs not to check its routing table before responding to a routing request, it is often the first one to reply compared to other nodes. When the requesting node receives this RREP, it terminates its routing discovery process and ignores all other RREP messages coming from other nodes. Thus the data packets are sent to such a “hole” from where they are not sent anywhere and absorbed by the malicious node. Often many nodes send RREQ simultaneously; the attacker node is still able to respond immediately with false RREP to all requesting nodes and thus easily takes access to all the routes. In this way source nodes are bluffed by malicious node which gulps a lot of network traffic to itself resulting severe loss of data. Black Hole nodes may also work as a group in a network. This kind of attack is called Collaborative Black Hole attack or Black Hole Attack with multiple malicious nodes.

The main objective of black hole attack is to drape packets and break communications between nodes, all the network's traffic is redirected to a specific node which does not exist at all. Black hole node work with two scenarios, in the first one the node exploits all the vulnerability that exists in an ad hoc network such as announcing itself having a valid route to a destination node; the Second one, the node drupes and controls all the intercepted packets. The Black hole attack in AODV protocol can be classified into two categories: black hole attack caused by RREP and black hole attack caused by RREQ.

### A. Black hole attack caused by RREQ

This attack work by sending fakes RREQ messages, an attacker can form a black hole attack as follows:

- Set the originator IP address in RREQ.
- Set the destination IP address in RREQ.
- Set the source IP address of the IP header to its own IP address.
- Set the destination IP address of the IP header to broadcast address or to a nonexistent IP address.
- Increase the sequence number and declaring a low hop count and put them in the related fields in RREQ.

False information about source node is inserted to the routing table of nodes that get the fake RREQ, if these nodes want to send data to the source, at first step they send it to the malicious node.

### *B. Black hole attack caused by RREP*

This attack work by sending fakes RREP messages after receiving RREQ from source node, a malicious node can generate black hole attack by sending RREP as follow:

- Set the originator IP address in RREP to the originator node's IP address.
- Set the destination IP address in RREP to the destination node's IP address.
- Set the source IP address of the IP header to its own IP address.
- Set the destination IP address of the IP header to the IP address of the node that RREQ has been received from it.

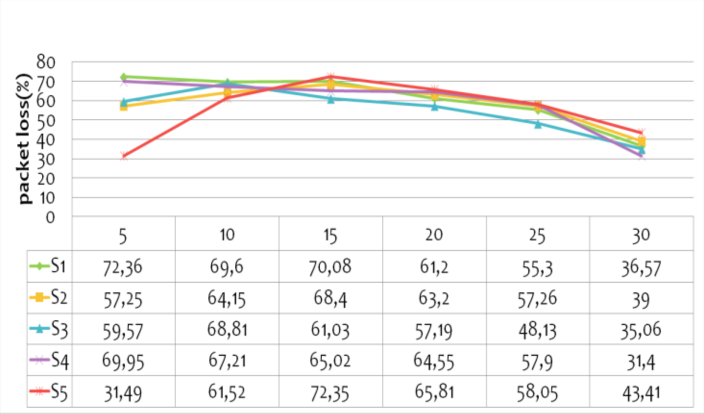
## V. Simulation of Black Hole Attack On AODV Protocol

In our simulation of the Black hole attack, we did use Ns2 as a simulator and We fixed some cases where we will study the impact of the attack on AODV protocol and the hole network without knowing the attacked node or the way the traffic is generated. We try to determine the of the attack on the network with the most real way possible,

In order to simulate a Black hole behavior we did integrate a new protocol in NS2 using the source code of AODV protocol and adding the black hole algorithm in it by modifying the AODV functions.

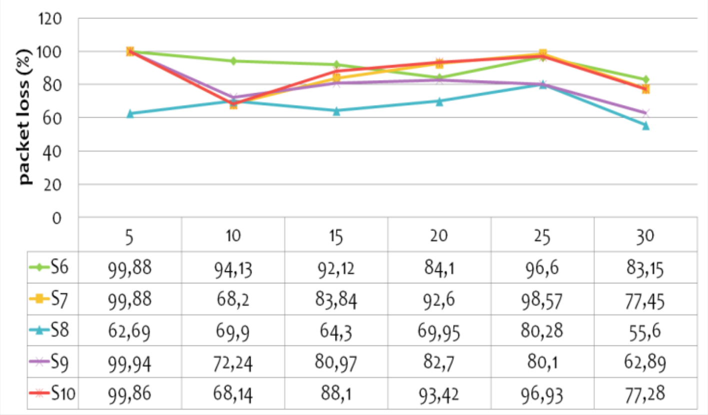
| Simulator | Ns2.34 |
|---|---|
| Time | 500s |
| TRAFFIC | CBR |
| Pause Time | 1.0 |
| Max speed | 20 m/s |
| Number of nodes | 5 , 10 , 15 , 20 , 25 , 30 |
| Flat space | 750 * 750 m |

- Scenario 1: we simulate with mobile nodes that use AODV as routing protocol and one non-mobile node with the behavior of a black hole attacker.
- Scenario 2: we simulate with mobile nodes that use AODV as routing protocol and one non-mobile node and another mobile node with the behavior of black hole attackers.
- Scenario 3: we simulate with mobile nodes that use AODV as routing protocol and one mobile node with the behavior of a black hole attacker.
- Scenario 4: we simulate with mobile nodes that use AODV as routing protocol and two mobile nodes with the behavior of black hole attackers.
- Scenario 5: we simulate with mobile nodes that use AODV as routing protocol and two non-mobile nodes with the behavior of black hole attackers.
- Scenario 6: we simulate with non-mobile nodes that use AODV as routing protocol and one non-mobile node with the behavior of a black hole attacker.
- Scenario 7: we simulate with non-mobile nodes that use AODV as routing protocol and two non-mobile nodes with the behavior of black hole attackers.
- Scenario 8: we simulate with non-mobile nodes that use AODV as routing protocol and one mobile node with the behavior of a black hole attacker.
- Scenario 9: we simulate with non-mobile nodes that use AODV as routing protocol and two mobile nodes with the behavior of black hole attackers.
- Scenario 10: we simulate with non-mobile nodes that use AODV as routing protocol, one non-mobile node and another mobile node with the behavior of black hole attackers.



| | 5 | 10 | 15 | 20 | 25 | 30 |
|---|---|---|---|---|---|---|
| S1 | 72,36 | 69,6 | 70,08 | 61,2 | 55,3 | 36,57 |
| S2 | 57,25 | 64,15 | 68,4 | 63,2 | 57,26 | 39 |
| S3 | 59,57 | 68,81 | 61,03 | 57,19 | 48,13 | 35,06 |
| S4 | 69,95 | 67,21 | 65,02 | 64,55 | 57,9 | 31,4 |
| S5 | 31,49 | 61,52 | 72,35 | 65,81 | 58,05 | 43,41 |

Fig. 4. Simulation results for the first five scenarios where the AODV nodes are mobile. X number of nodes, Y % of packet loss.



| | 5 | 10 | 15 | 20 | 25 | 30 |
|---|---|---|---|---|---|---|
| S6 | 99,88 | 94,13 | 92,12 | 84,1 | 96,6 | 83,15 |
| S7 | 99,88 | 68,2 | 83,84 | 92,6 | 98,57 | 77,45 |
| S8 | 62,69 | 69,9 | 64,3 | 69,95 | 80,28 | 55,6 |
| S9 | 99,94 | 72,24 | 80,97 | 82,7 | 80,1 | 62,89 |
| S10 | 99,86 | 68,14 | 88,1 | 93,42 | 96,93 | 77,28 |

Fig. 5. Simulation results for the last five scenarios where the AODV nodes are non-mobile. X number of nodes, Y % of packet loss.

## VI. Conclusion

Ad Hoc Network is independent of any fixed infrastructure or central management and have frequent routing updates which makes it easy to set up, low in cost, provides communication by wireless means with nodes working as routers as host.

But along with advantages these features of MANET make it vulnerable to many active and passive security attacks, which affects the confidentiality, integrity and availability of data being transmitted. Black Hole Attack is one of these The Black hole is one of the most powerful attacks on an Ad hoc network; it can cause a complete failure of the network by dropping all the traffic specially when the nodes are non-mobile. In some protocols where we use cluster heads an attacker can be placed between two cluster and cause isolation. In this study we implemented an new protocol that communicate like AODV but behaves like a Black hole and we did choose some study cases where we did use this new protocol to see how the Black hole attack can increase the packets loss.

## REFERENCES

[1] H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[2] M. Ghonge, S. U. Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANET,"International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 2, Feb 2012.

[3] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French

[4] H.A. Esmaili, M.R. Khalili Shoja, Hossein gharaee, "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT), Vol. 1, No. 2, 49-52, 2011.

[5] Jasvinder, M. Sachdeva, "Effects of Black Hole Attack on an AODV Routing Protocol Through the Using Opnet Simulator," International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 8, Aug 2013.

[6] Charles E. Perkins and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing ," 2nd IEEE workshop on mobile computing systems and applications, New Orleans, Louisiana, USAp. 90-100, Feb. 1999

[7] Seung Yi and Prasad Naldurg, "Security-aware ad hoc routing for wireless networks ," 2nd ACM international symposium on Mobile ad hoc networking & computing, MobiHoc'01, 2001,p. 299 - 302

[8] Charles Perkins and Elizabeth Royer, " Ad hoc On-Demand Distance Vector (AODV) Routing ," RFC 3561, 2003, p. 1-37