International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 9 No. 1 Sep. 2014, pp. 156-166
© 2014 Innovative Space of Scientific Research Journals
http://www.ijisr.issr-journals.org/

Securing Ad Hoc Networks: Trust Systems and Replicas Detection

Brahim IDHAJOUB, Mohammed ERRITALI, and Mohammed Fakir

TIAD laboratory, Computer Sciences Department, Faculty of Sciences and Techniques,
Sultan Moulay Slimane University,
Beni-Mellal, BP: 523, 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. The security of mobile ad hoc networks is an open research topic and a major in terms of their vulnerability to various attacks, such as black hole, Sybil ... etc. In this article, we analyze the attack black hole (black hole) in ad hoc networks using as AODV routing protocol. In a black hole attack, a malicious node impersonates a legitimate node, manufactures forged responses with a number of high sequence and thus forces the victim node to select it as a relay.

We are interested in a first time to study the impact of dishonest nodes on the network, and then we will simulate black hole attack using two simulator NS2 and OPNET.

KEYWORDS: Ad Hoc networks, Black-Hole, Attack, AODV.

1 INTRODUCTION

An ad hoc network [1] is an autonomous and cooperative set of mobile nodes that move and communicate via a wireless transmission that does not assume pre-existing infrastructure. The ad hoc network [1] is formed spontaneously as soon as the provisional and more mobile nodes are within radio range of each other. The nodes communicate, depending on the distance between them, two modes of communication: mobile nodes can communicate directly (in ad hoc transmission) as either they are within range, or they must use other mobile nodes as relays to route packets to their destination. Thus, each node is the end user and router to relay packets to their final destination, due to the limited coverage of the radio field available for each node once. However, due to the distributed nature of wireless nodes, there are several vulnerabilities and the black hole is one of the best known.

In this paper, we will focus on the performance of AODV [3] (Ad hoc On-Demand Distance Vector) protocol under Black hole attack. We did our simulation with OPNET [5] and NS2 [4] by implementing a new protocol, that adopts the algorithm of AODV [3] and the behavior of a Black hole attacker.

2 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 [3] is used to find a route between source and destination as needed and this routing protocol uses three significant type of messages, route request (RREQ), route reply (RREP) and route error (RERR). The source S sends its neighbors a route request RREQ (Route reqest) which contains the address of S, the request identifier , a sequence counter , address D and the counter number of jumps with a initial value zero. The source RREP_WAIT_TIMEOUT waiting period , if a response is received then the operation of route discovery is completed, otherwise it rebroadcasts the RREQ and waits for a longer period if no response is received, it will continue the replay RREQ up a maximum number of attempts RREQ_RRTRIE S (03 attempts) , if after RREQ_RETRIE S attempts to establish road, there is no response then the process is aborted and an error message is reported to the application. After a waiting period (10s), the application requests the route and consequently the route discovery process is initiated [6]. Each node that receives the RREQ checks its local routing table if a route to node D if the node that processes the request RREQ increments the hop count and diffuse again. When the request reaches the destination D or a node that has a route to the destination, a reply RREP (Route REPly) broadcasts on the same road of receipt of RREQ (reverse path). Reply RREP contains the source address, destination address, hop count , a destination sequence number and the life of the package. Reply RREP through the reverse route to the source node S. Thus each node on the route, writes an entry in the local routing table to the destination node before sending the packet. Once the source S receives the message, it starts to send data to D.

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 initialized by zero.(Fig.1) [9]

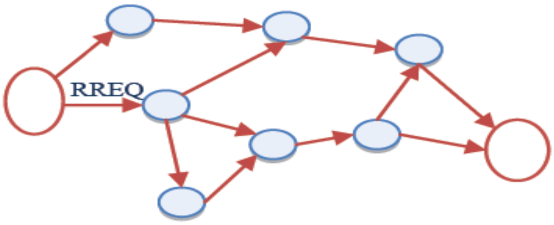

Fig. 1. Route Request (RREQ) Message

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) [9]

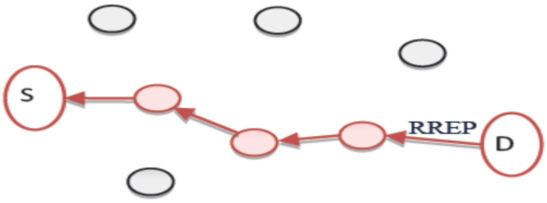

Fig. 2. Route Reply (RREP) Message

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) [9]

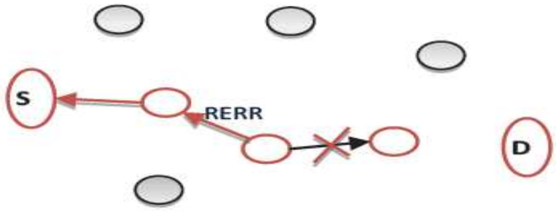

Fig. 3. Route Error (RERR) Message

3 AD HOC NETWORK AND SECURITY ISSUES

In a MANET [2], all entities can participate in routing, so there are no barriers for a malicious node to cause disturbances in the circulating traffic. The interest of the attacker is essentially to compromise the confidentiality and integrity of information in transit, or more generally to disrupt the proper functioning of the routing process to dominate the network.

In MANET [2], depending on the level of intrusion actions by an attacker, there are generally two types of attacks: passive attacks and active attacks.

❖ Attack passive

The adversary only monitors the communication channels. Listening occurs when an attacker captures a node and studied traffic that passes through without altering the operation. The analyzed data help the intruder to act later. A passive adversary that threaten privacy.

❖ Active Attack

An attack is active when a node unauthorized alter routing information in transit through actions modification, deletion, or manufacturing, which leads to disturbances in the functioning of the network.

In addition, by field of membership of a node, active attacks can themselves be divided into two categories, namely internal and external attacks. While external attacks are carried out by nodes that do not belong to the network domain, internal attacks are carried out by compromised nodes that are allowed to participate in the network operation. Because attackers are already part of the network of nodes allowed, internal attacks are generally more harmful and difficult to detect than external 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 [2] 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 [1] 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 [2] to have certain boundaries. If a node is in the radio range of a MANET, it automatically joins it. This characteristic makes a MANET [2] 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 [2], 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 [2] 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 [2] nodes are free to move in and out of the network. Nobody can predict the number of nodes a MANET [2] had in past or can have in future.

5) Compromised Node: Compromised node is a node in MANET [2], on which the attackers get the control through unfair means with the intentions of performing malicious activities. The nodes in MANET [2] 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 [2] 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 [2] 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 [2] have variable capacity links. Along with limited power, the storage capacity of a MANET [2] is also limited.

B. Security Issues in AODV

AODV [3] protocol is exposed to a variety of attacks, the impact of these attacks on AODV [3] 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) Wormhole attack

In this attack, an attacker records a packet, at one location in the network, tunnels the packet to another location and replays it there [8].

2) Byzantine attack

In this attack, malicious nodes individually or cooperatively carry out attacks such as creating routing loops and forwarding packets through non-optimal paths.

3) Rushing attack

Rushing attacker forwards packets quickly by skipping some of the routing processes. So, in on-demand routing protocol such as AODV [3], the route between source and destination include rushing nodes.

4) Resource consumption attack

In this attack, an attacker attempts to consume battery life of other nodes.

5) Location disclosure attack

In this attack, information relating to structure of network is revealed by attacker nodes.

6) Black hole attack

In the Black hole attack : A malicious node must be placed between two or more nodes start dropping all traffic.

This attack exploits the vulnerability of route discovery packet routing protocol by modifying the latter to control all traffic flowing between the nodes.

4 Black Hole Attack

Due to these above-mentioned issues, MANET [2] 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 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 [3] 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

With sending fake RREQ messages, an attacker can form black hole attack as follows:

a) Set the originator IP address in RREQ to the originating node's IP address.

b) Set the destination IP address in RREQ to the destination node's IP address.

c) Set the source IP address of IP header to its own IP address.

d) Set the destination IP address of IP header to broadcast address.

e) Choose high sequence number and low hop count and put them in related fields in RREQ.

So, false information about source node is inserted to the routing table of nodes that get fake RREQ. Hence, 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

With sending fake RREP messages, an attacker can form black hole attack. After receiving RREQ from source node, a malicious node can generate black hole attack by sending RREP as follow:

a) Set the originator IP address in RREP to the originating node's IP address.

b) Set the destination IP address in RREP to the destination node's IP address.

c) Set the source IP address of IP header to its own IP address.

d) Set the destination IP address of IP header to the IP address of node that RREQ has been received from it.

5 Simulation Of Black Hole Attack On AODV Protocol

Ad hoc networks [1] are a typical example of systems that require the cooperation of all participants for their good work. Any deviation from a participating authorized by the policy implemented in the system behavior negatively affect the proper functioning of the network. For example, the function of routing in ad hoc networks or sensor networks. As there is no infrastructure routing, a node is free on his handling of the packets it receives. It may decide to behave in accordance with routing rules (to properly address these packets) or to adopt a behavior contrary to the rules defined in the network. Indeed, the node may decide not to route messages from its neighbors (node adopts selfish behavior), which is the opposite of the spirit of cooperation of ad hoc networks. The node can go even further and question the integrity of the data it receives (modify packets received special control packets which are in most cases not encrypted). The node can also inject false routing information that will result in corrupting the routing tables of some nodes of the network and thereby distort the routing function.

In our simulation of the Black hole attack, we used two simulators: the first one is OPNET [5] and the second is NS2 [4].We fixed some cases where we study the impact of the crisis on the AODV [3] protocol and the entire network without knowing. The contested node or how the traffic is generated. We try to determine the number of packet loss in the network with the most real scenarios in terms of mobility and traffic generation.

A. Simulation in OPNET

To study the impact of the black hole attack on mobile networks MANET [2], we will create two scenarios on OPNET [5] in the first we will simulate the network without attack and in the second we will implement the attack, then we will compare the results.

Simulation parameters	
Simulateur	OPNET 14.5
Routing Protocol	AODV
Number of nodes	5
Field simulation	1000x1000
MAC (wireless protocol)	802.11

To observe the effect of the attack of the black hole more clearly the following metrics are added :

- Traffic received.
- Traffic sent.

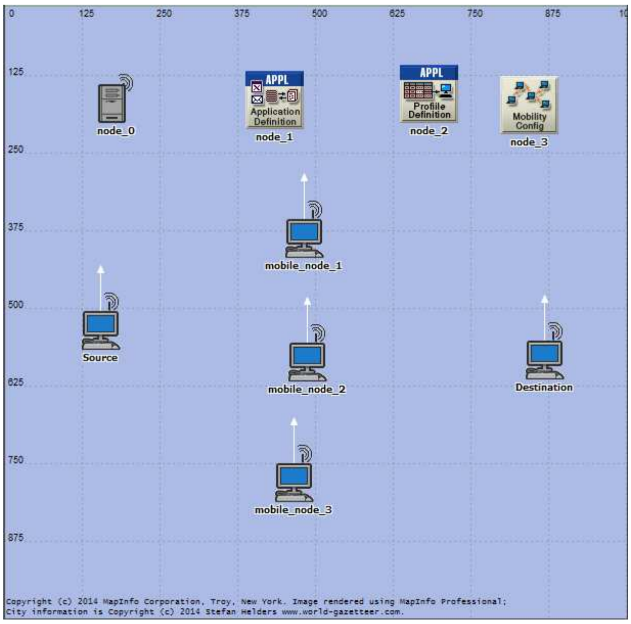

Figure 4 : Simulation environment.

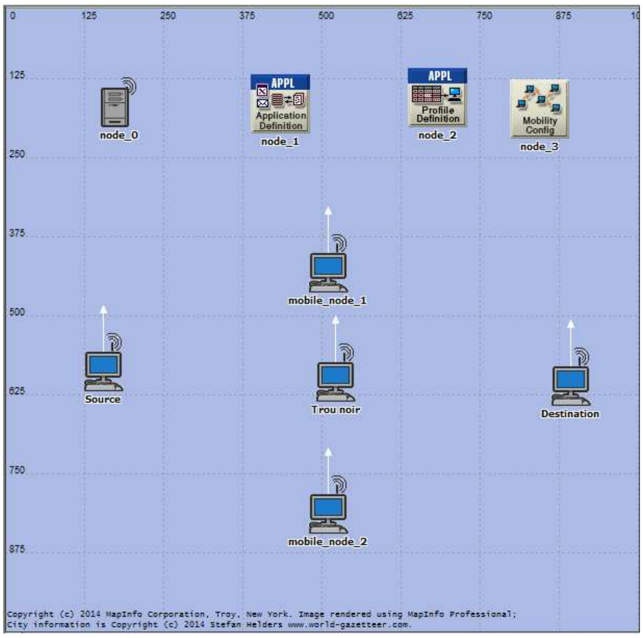

Figure 5 : Simulation environment with black hole.

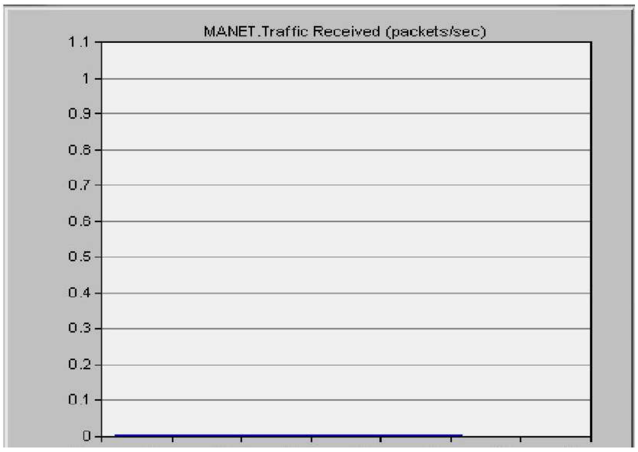

Figure 6 : Traffic received by the destination.

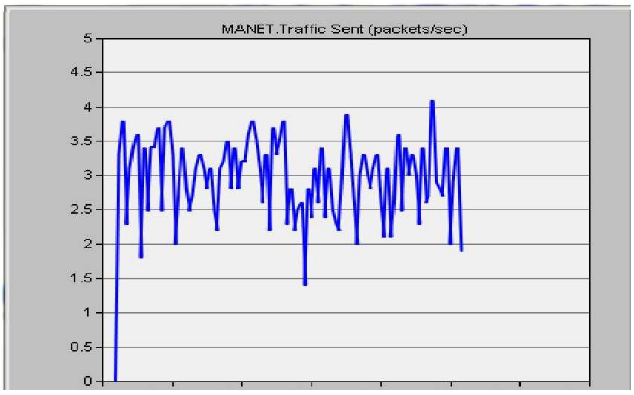

Figure 7 : Traffic received by the black hole.

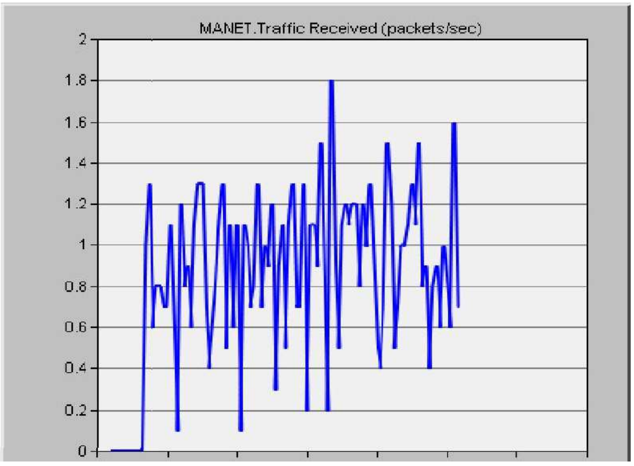

Figure 8 : Traffic sent by the source.

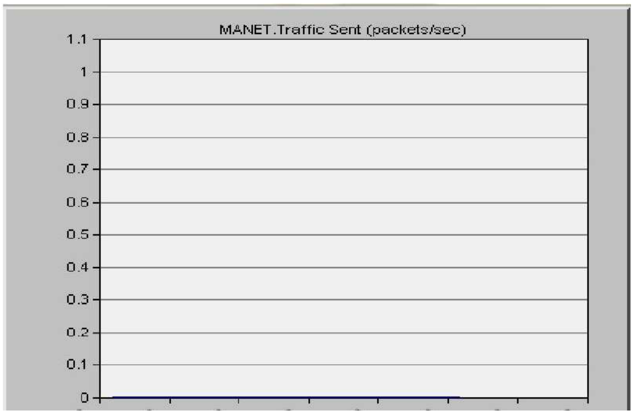

Figure 9 : Traffic sent by the black hole.

In Figure 8, the source node sends packets to the mobile node that sent the packet then the malicious node that keeps these packets as shown in Figure 9.

From the results, we can say that the corrupt node is its goal:

- Manage the flow of data over the network.
- Allow traffic flow itself.

B. Simulation in NS2

Various mobilities of nodes have been considered to measure the performance of network in presence of malicious nodes as attackers. Fig. 10 demonstrates the results in presence of only one malicious node. Fig. 11 demonstrates the results in presence of tow malicious nodes. Fig. 12 shows the results in the presence of malicious nodes to three. Fig. 13 shows the results in the presence of four malicious nodes.

Simulation parameters	
Simulator	Ns2.34
Routing Protocol	AODV
Nombre des nœuds totaux	20, 40, 70, 100, 120.
Number of total nodes	5, 10, 15, 20, 25.
Field simulation	750 * 750 m
Pause Time	1.0
Max speed	20 m/s
Time	500s
Trafic	CBR
MAC (wireless protocol)	802.11

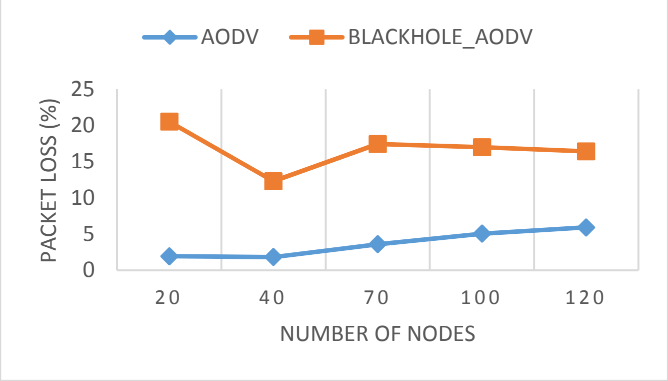

Figure 10 : Lost packets under the impact of a single malicious node in AODV

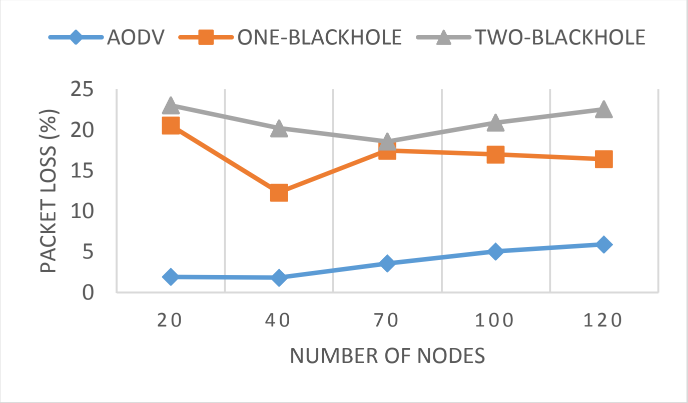

Figure 11 : Lost packets under the impact of two malicious nodes in AODV

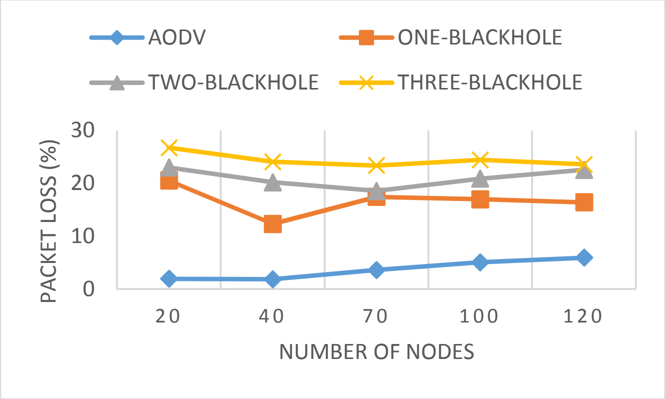

Figure 12 : Lost packets under the impact of three malicious nodes in AODV

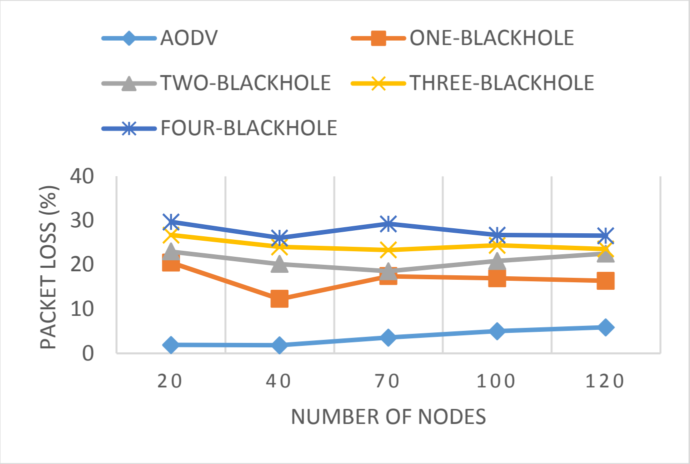

Figure 13 : Lost packets under the impact of four malicious nodes in AODV

From the results obtained, we can conclude that as the number of malicious nodes in the network increases more packet loss become important.

6 CONCLUSION

Ad Hoc Network [1] 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.. However, with these benefits MANET [2] characteristics make it vulnerable to many attacks of active and passive safety, 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 an isolation In this article we are interested in the analysis of the black hole attack, we propose a model to measure the effect of this attack on the operation of mobile ad hoc networks [2].

REFERENCES

[1] Van der Meerschen Jérome, Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wifi. Rapport de DEA, 2006.

[2] Performance Evaluation of Routing Protocols in Mobile Ad hoc Networks (MANETs),Bained Nyirenda,Jason Mwanza.

[3] C. Perkins, E. Belding-Royer, S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing”, IETF RFC 3561, 2003.

[4] 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.

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

[6] T. Issariyakul and E. Hossain. Introduction to Network Simulator NS2. Springer, De-cember 2008.

[7] Opnet, http://www.opnet.com/.

[8] N. Tebbane, S.Tebbane, A. Mehaoua, “Simulation et Mesure des performances du protocole de routage AODV,” JTEA'2004, Hamamet, Tunisia 2004.

[9] Abdellaoui Rachid and Jean-Marc Robert, “SU-OLSR: A NEW SOLUTION TO THWART ATTACKS AGAINST THE OLSR PROTOCOL”, Ecole de Technologie Supérieure, MONTRÉAL, 2009.

[10] Valérie Gayraud, Loutfi Nuaymi, Francis Dupont, Sylvain Gombault, and Bruno Tharon, « La Sécurité dans les Réseaux Sans Fil Ad Hoc ».

[11] FIHRI Mohammed, OTMANI Mohamed, EZZATI Abdellah, Mathematics and Computer Science Dept, LAVETE Laboratory, "The Impact of Black-Hole Attack on AODV Protocol", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. XXX, No. XXX, 2014.

[12] 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.

[13] 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.

[14] 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.