IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP1 01-107
www.iosrjournals.org

Effects Of Wormhole Attack On AODV And DSR Routing Protocol Through The Using NS2 Simulator

Mohamed Otmani[1], Dr. Abdellah Ezzati [2]
[1](Department of Computer Science and Engineering/ University Hassan 1 Settat, Morocco)
[2](Department of Computer Science and Engineering/ University Hassan 1 Settat, Morocco)

Abstract : *Mobile Adhoc Networks (MANET) are self organizing, decentralized networks and possess dynamic topology, which make them attractive for routing attacks. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. The security of the AODV and DSR protocol is compromised by a particular type of attack called 'Worm hole attack'. Wormhole attack is a network layer attack observed in MANET, which completely disrupts the communication channel. In This paper we analyses the performance of AODV and DSR routing protocols with and without wormhole attack using Network Simulator 2. For analyzing the performance we considered total packets received, total bytes received, first packet received, last packet received, average end-to-end delay and throughput as measures.*

Keywords: *AODV, DSR, MANET, Wormehole, Security*

I. Introduction

Ad-hoc networks are a collection of mobile devices that can dynamically exchange information between them without using a pre-existing infrastructure or centralized administration. Each unit of this type of network communicates directly with other devices that are within range of communication (radio range) .However, due to their inborn characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

✓ integrity

The role of integrity is to ensure the protection of messages or information exchanged in the network against any modification or alteration by an unauthorized person. In Ad-Hoc networks, network operation is based mainly on the exchange of control messages providing information for routing. In this context, it is important, first, to ensure the integrity of routing and control messages against all unauthorized changes.

✓ Confidentiality

The purpose of confidentiality is to ensure access to information only to authorized users or systems. In the context of Ad-Hoc networks, privacy is to deny access to information exchanged between two nodes in the network by any malicious or not desired node. However, the Ad-Hoc networks are characterized by the general dissemination of information, which constitutes a real challenge for confidentiality.

✓ Availability

Availability ensures continuous operation of services and guarantees user access to these services. Availability is difficult to apply in Ad-Hoc networks. Indeed, because of the mobility of nodes, a routing protocol could not maintain all the routes to all nodes and above nodes leaving the network. But some types of attacks could affect the availability of nodes participating in the network or the availability of certain services (attacks that deplete the batteries of nodes, attacks denial of service, etc.).

✓ Non-repudiation

Ensures that sending and receiving parties can never deny ever sending or receiving the message.

✓ Authentication

Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

Most previous ad hoc networking research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing. Applications that may require secure communications include

emergency response operations, military or police networks, and safety-critical business operations such as oil drilling platforms or mining operations.

Routing is the act of moving information from a source to a destination in an Ad hoc network.During this process, at least one intermediate node within the Ad-hoc network is encountered. The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups through an Ad hoc network.

In wormhole attack , an attacker redirect traffic between two geographically remote areas and have a good geographical position to control the traffic that passes through it. Section 2 of this paper discusses the routing protocols in ad hoc networks, section 3 discusses types of security attacks in MANETS, section 4 discusses wormhole attack. In Section 5, we present our simulation environment and results. Finally section 6 concludes our work.

Routing Protocols in MANETS

Routing protocols of MANETs can be classified into three categories:

- Proactive protocols:

In this type of routing protocol, each node in a network maintains one or more routing tables which are updated regularly. Each node sends a broadcast message to the entire network if there is a change in the network topology. However, it incurs additional overhead cost due to maintaining up-to-date information and as a result; throughput of the network may be affected but it provides the actual information to the availability of the network. Distance vector (DV) protocol, Destination Sequenced Distance Vector (DSDV) protocol, Optimized link state routing protocol (OLSR) protocol are the examples of Proactive protocols.

- Reactive Protocols:

In this type of routing protocol, each node in a network discovers or maintains a route based on-demand. It floods a control message by global broadcast during discovering a route and when route is discovered then bandwidth is used for data transmission. The main advantage is that this protocol needs less touting information but the disadvantages are that it produces huge control packets due to route discovery during topology changes which occurs frequently in MANETs and it incurs higher latency. The examples of this type of protocol are Dynamic Source Routing (DSR), Ad-hoc On Demand Routing (AODV) and Associativity Based Routing (ABR) protocols.

- Hybrid Protocols:

It is a combination of proactive and reactive protocols taking the best features from both worlds.

1.1 Dynamic Source Routing (DSR) Protocol:

It is a reactive protocol that creates a route on demand using source routing protocol i.e. it requires a full series of paths to be established between source and destination nodes to transmit packets and each packet follows the same path. The major motivations of this protocol are to limit the bandwidth by avoiding the periodic table updates and long convergence time. The underline fact to this protocol is that it floods a route request message in the network to establish a route and it consists of two procedures: Route Discovery and Route Maintenance.

✓ Route Discovery:

As it is an on-demand routing protocol, so it looks up the routing during transmission of a packet. At the first phase, the transmitting node search its route cache to see whether there is a valid destination exists and if so, then the node starts transmitting to the destination node and the route discovery process end here. If there is no destination address then the node broadcasts the route request packet to reach the destination. When the destination node gets this packet, it returns the learned path to the source node.

✓ Route Maintenance:

It is a process of broadcasting a message by a node to all other nodes informing the network or node failure in a network. It provides an early detection of node or link failure since wireless networks utilize hop-to-hop acknowledge.

1.2 Ad-hoc On-demand Distance Vector (AODV) Protocol:

It is a classical routing protocol for MANETs that compromise the trade-off problems like large packet header in reactive source protocol and large messaging overhead due to periodic updates in proactive protocols. It uses a

distributed approach i.e. it keeps track of the neighbor nodes only and it does not establish a series of paths to reach the destination. It also uses route discovery and route maintenance mechanism like DSR.

✓ Route Discovery:

A source node send a broadcast message to its neighboring nodes if no route is available for the desired destination containing source address, source sequence number, destination address, destination sequence number, broadcast ID and hop count. Two pointers such as forward pointer and backward pointer are used during route discovery. Forward pointers keep track of the intermediate nodes while message being forwarded to destination node. Eventually, when route request message reached the destination node, it then unicast the reply message to the source via the intermediate nodes and the backward pointer keeps track of the nodes. The major feature of AODV that distinguish it from DSR is the destination sequence number which is used to verify the up-to-date path to the destination.

✓ Route Maintenance:

Three types of messages exchanged between source and destination such as route error message, hello message and time out message. Route error message ensures that this message will be broadcasted to all nodes because when a node observes a failed link, it will propagate this message to its upstream nodes towards source node only. Hello message ensures the forward and backward pointers from expiration. Time out message guarantees the deletion of link when there is no activity for a certain amount of time between source and the destination node.

1.3 Analysis of AODV and DSR

Analysis of DSR and AODV , the two on-demand protocols share certain salient characteristics. However, there are several important differences in the dynamics of these two protocols, which may give rise to significant performance differentials. First, by feature of source routing, DSR has access to a significantly greater amount of routing information than AODV. Second, to make use of route caching aggressively, DSR replies to all requests reaching a destination from a single request cycle. Having access to many alternate routes saves route discovery floods, which is often a performance bottleneck. In AODV, on the other hand, the destination replies only once to the request arriving first and ignores the rest. The routing table maintains at most one entry per destination. Third, the current specification of DSR does not contain any explicit mechanism to expire musty routes in the cache, or prefer "fresher" routes when faced with multiple choices. In contrast, AODV has a much more conservative approach than DSR. Fourth, the route deletion activity using RERR is also conservative in AODV. In DSR, however a route error simply backtracks the data packet that meets a failed link. Packets and is maintained as a priority queue with two priorities each served in FIFO order. Routing packets get higher priority than data packets.

II. Types Of Security Attacks In MANETS

The wireless Channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic is monitoring or access control mechanism scan be deployed so the boundary that separates the inside network from the outside world becomes blurred. There are two types of security attacks in mobile ad hoc networks.

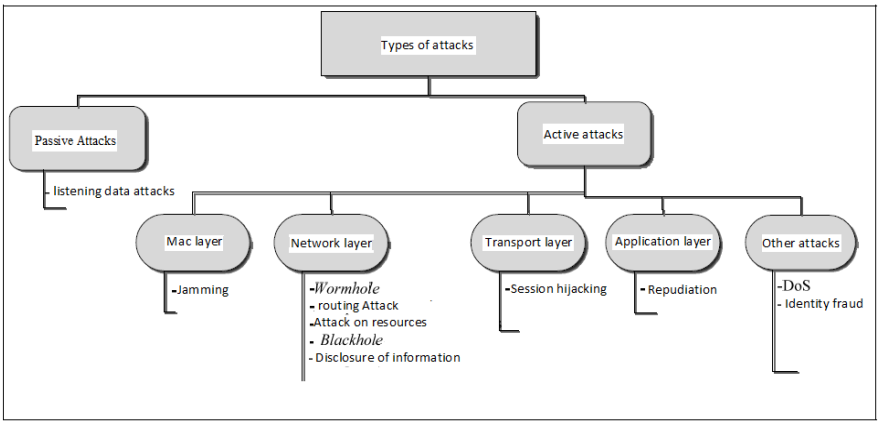

Fig 1: Types of attacks in Ad-Hoc networks

1.4 Passive Attacks

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overhead.

1.5 Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication.

Table1: Types of attacks in Ad-Hoc networks

Attacks	Definition
Wormhole	An attacker could redirect traffic between two zones geographically isolated to create a vertex in the topology and have a good geographical position to monitor the traffic that passes through it.
Routing Attack	A malicious node can disrupt the operation of a routing protocol by modifying the routing information, making false routing information or usurp the identity of another node.
Jamming	This is a classic attack on the availability of the channel communication through the mass generation of a large amount of radio interference.
Backhole attack	The purpose of this attack is falsification of information routing or traffic diversion.
Attack on resources	The MANET resources are characterized by limited (battery and bandwidth). An attack on resources may affect availability.
Byzantine attack	Through this attack, a malicious node alters the messages and could create problems of routing loops, routing packets to non-optimal paths, selecting the packets to reject ... This type of attack is difficult to detect because the network seem to work properly.
DoS	This type of attack consists of sending deliberately messages to cause saturation of the bandwidth and paralyze the network.
Disclosure of information	Exchange of confidential information must be protected against listening or unauthorized access.
Repudiation	This type of attack has an impact on the integrity of communications between nodes in the network.
Identity fraud	Identity fraud is designed for falsifying information relating to identities. Which could lead to isolation of nodes sharing false information Routing and affect the confidentiality and integrity.

III. Wormhole Attack

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multihop route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole. If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways. The attack can also still be performed even if the network communication provides

confidentiality and authenticity, and even if the attacker has no cryptographic keys. Furthermore, the attacker is invisible at higher layers; unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route.The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. For example, when used against an on-demand routing protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then discard without processing all other received ROUTE REQUEST packets originating from this same Route Discovery. This attack thus prevents any routes other than through the wormhole from being discovered, and if the attacker is near the initiator of the Route Discovery, this attack can even prevent routes more than two hops long from being discovered. Possible ways for the attacker to then exploit the wormhole include discarding rather than forwarding all data packets, thereby creating a permanent Denial-of-Service attack (no other route to the destination can be discovered as long as the attacker maintains the wormhole for ROUTE REQUEST packets), or selectively discarding or modifying certain data packets.

IV. Simulation and Results

1.6 Simulation Environment

Network Simulator ns-2 is used to run MANET simulations.NS-2 is a simulation project developed by the University of California Berkley.It is one of the most widely used network simulators for wired and wireless networks. NS is an object – oriented, discrete event driven network simulator which is written in C++, with an OTcl interpreter as a frontend, and is available free. It follows the layered approach, and is accompanied by a rich set of protocols.

We run two simulations, one without the attacker node and other including the attacker node. The simulation parameters are shown in Table 2

Table2: Simulation Parameters

Parameter	Value
Area	1500 x1500
Simulation time	1000 s
Application	CBR(Constant Bit rate)
Network density	20 nodes
Network mobility	Random
Routing protocols	AODV/DSR
Malicious node	Worm hole

1.7 Results

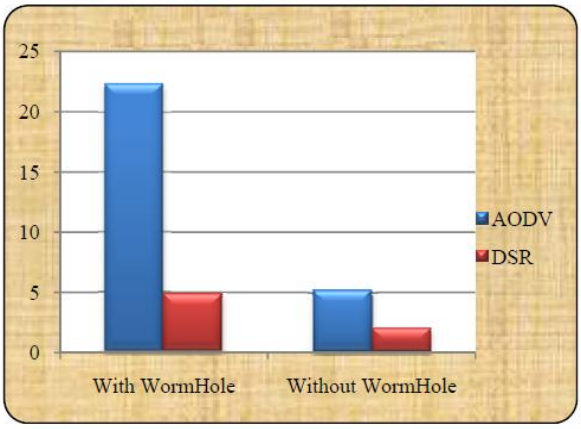

Fig 2: First Packet Received

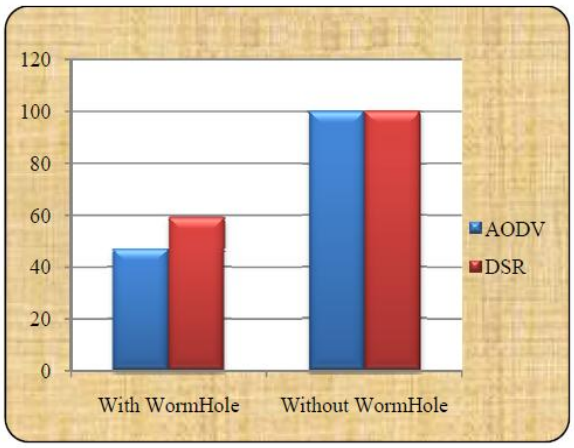

Fig 3: Last Packet Received

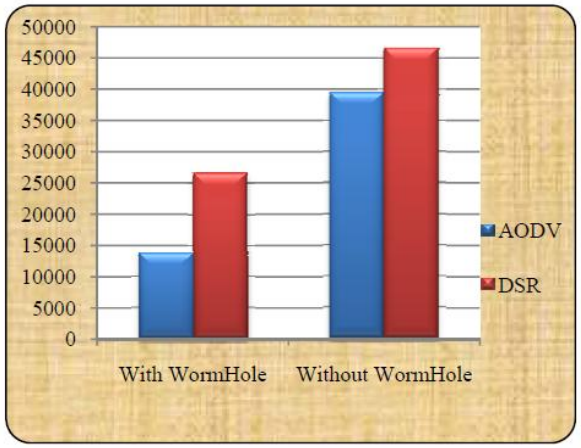

Fig 4: Total Bytes Received

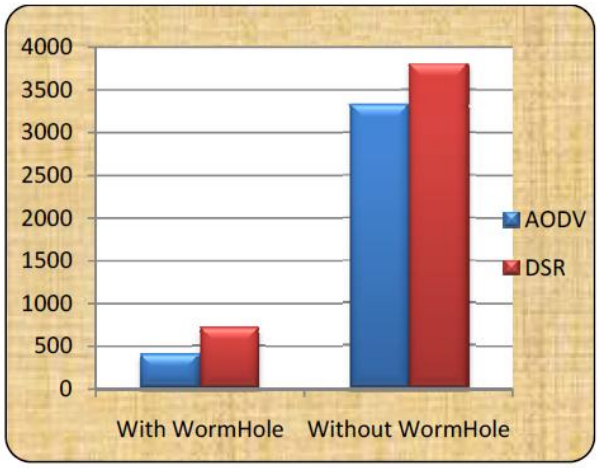

Fig 5: Throughput (bits/s)

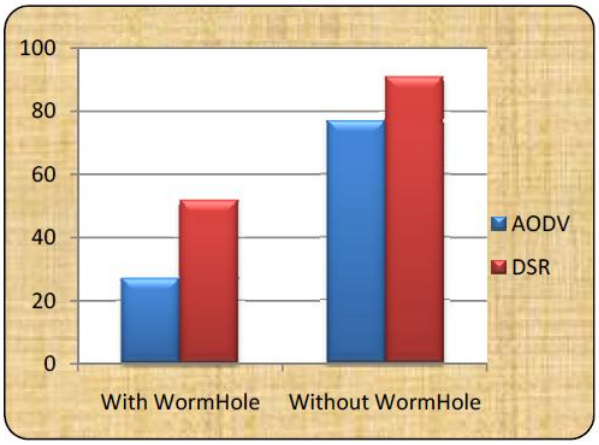

Fig 6: Total Packets Received

V. Conclusion

The security of the Ad Hoc network routing protocols is still an open problem and deserves more research work. In this paper, we analyzed effect of the Worm Hole attack in AODV and DSR routing. We have implemented Worm hole Attack against AODV and DSR routing protocol using Network Simulator 2, for analyzing the performance we considered total packets received, total bytes received, first packet received, last packet received, average end-to-end delay and throughput as measures. We presented the results of evaluation of both protocols. The results show that DSR performs better than AODV. Wormhole attack is a real threat against routing protocols in MANET .The detection and evasion of wormholes in an ad-hoc network is still considered as future challenging task.

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]. 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
[3]. 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
[4]. 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
[5]. Charles Perkins and Elizabeth Royer, " Ad hoc On-Demand Distance Vector (AODV) Routing ," RFC 3561, 2003, p. 1-37
[6]. Jhaveri, R.H., Parmar, J.D., Patel, A.D., and Shah, B.I,"MANET Routing Protocols and Wormhole Attack against AODV",International Journal of Computer Science and Network Security, 10 (4).
[7]. C. E. Perkins and E. M. Royer, "The ad hoc on-demand distance vector protocol", in Ad hoc Networking, Addison-Wesley, pp. 173–219, 2000.
[8]. Reshmi Maulik and Nabendu Chaki, "A Study on Wormhole Attacks in MANET",International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279