Analysis of Security Attacks In AODV

Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim
Networks and Systems Laboratory
University of Badji Mokhtar
Annaba, Algeria

***Abstract*— An ad hoc network is a collection of mobile devices that communicate in a self-organized way using wireless network interfaces without neither centralized administration nor fixed infrastructure. In such a network, nodes must cooperate with each other so as to extend their transmission range to reach distant nodes. This cooperation requires a specific ad hoc routing protocol to establish and maintain routes between nodes. Ad hoc routing protocols are based on mutual trust between collaborating nodes and suppose a correct behavior. As a result, these networks are particularly vulnerable to various security threats. , and therefore, security is a more significant issue than infrastructure-based wireless networks. In this paper, we present security analysis of the Ad hoc On-demand Distance Vector (AODV) routing protocol to identify all possible security threats that can target its algorithm, such as resources depletion, blackhole, wormhole and rushing attacks.**

Keywords—MANET; AODV; security attacks; malicious node;

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are wireless multi-hop networks dynamically constructed by autonomous mobile nodes without the support of any infrastructure or centralized administration. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. This new paradigm of wireless communications aims to make communication possible in some situations where the services offered by both wired networks and WLAN are unavailable. MANETs are mainly useful in military and other tactical applications such as emergency rescues. Moreover, we can set up an ad hoc network at a conference to distribute files and discuss talks without using any wireless infrastructure that would have to be paid. Unlike the conventional network, a MANET is characterized by the following features:

II. AODV OVERVIEW

The AODV [1] protocol is an on-demand routing protocol, developed as amelioration to the Destination-Sequenced Distance-Vector (DSDV) routing algorithm [2]. AODV initiates a route discovery process only when there is data to be transmitted, to reduce the number of broadcast messages forwarded throughout the network. When an originator node desires to transmit a data packet to a destination node, it checks its routing table to see if it has a valid route to the destination node. If it finds an available route in its routing table, it simply forwards the packets to the next hop along the path to the destination. Otherwise, if there is no route in the routing table, the source node initiates a route discovery process. It broadcasts a Route Request (RREQ) message to its neighbors and those nodes broadcast further to their neighbors if they do not have a fresh enough route to the destination node. This process pursues until the RREQ packet either reaches an intermediate node with a route to the destination or the destination node itself. AODV uses sequence numbers to ensure that all routes are fresh and loop-free. Fig. 1 illustrates the forward and reverse path formation in the AODV protocol.

An intermediate node can reply to the RREQ packet only if it has a destination sequence number higher than or equal to the one contained in the RREQ packet. The destination or an intermediate node record in its routing table the address of the neighbor from which the first copy of the RREQ packet has been received. This recorded information is subsequently used to establish the reverse route that will be used to send the corresponding Route Reply (RREP) message to the originator node. The destination node or an intermediate node only processes the first copy of a RREQ packet, and discards the duplicated copies of the same RREQ message.

When the RREP packet arrives to the originator or an intermediate node, it records or updates the forward route to the destination node in its routing table, and forwards the RREP packet along the established reverse route. AODV uses hello message to maintain local connectivity of a node, Route Reply Acknowledgment (RREP-ACK) message to acknowledge receipt of a RREP message, and RERR message to alert link break and maintain routes [1].

III. SECURITY ATTACKS

AODV does not specify any special security measures and is vulnerable to many types of attacks that manipulate its routing control mechanisms. Malicious node can disrupt network operations by not following the AODV routing protocol specifications.

A. Modification

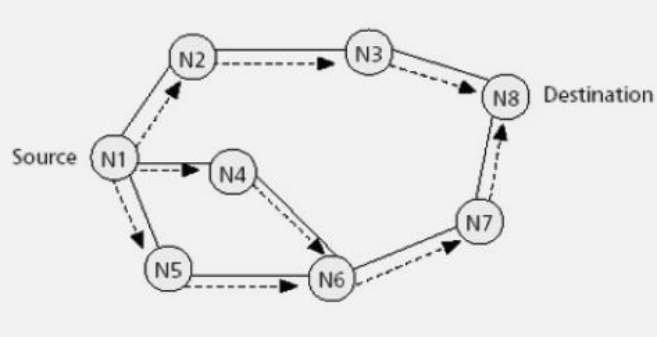

Fig. 1. AODV route discovery

Malicious node may illegally modify the routing information of the received messages before forwarding them, it can alter one or several fields in the message, depends on the goals that it may want to achieve. Such attack compromises the integrity of route discovery. By altering routing information, a malicious node can take control of a route, can cause network traffic to be dropped or redirected, or take a long route to the destination increasing communication delays [4]. Malicious node may increase the destination sequence number to make route appear fresher , decrease the hop count to make it appear shortest or even replace the source (destination) IP address in the IP header with another IP address to impersonate another node. RREQ, RREP and RERR messages can be modified in the following ways:

1) Modification of RREQ

The freshness of a RREQ message is represented by the RREQ ID, and based on this field along with the originator IP address, the intermediate node accepts or refuses to forward the RREQ message. Therefore a malicious node may increase the RREQ ID to convince other nodes to accept the modified RREQ message. It may also increase the destination sequence number to make route appear fresher , decrease the hop count to make route appear shortest or even replace the source address in the IP header with non-existent IP address to cause loss of the RREP message [3] [15].

2) Modification of RREP

Nodes uses the destination sequence number to determine the freshness of the information contained from the originating node [2]. When several RREP messages are received by a source node, it chooses the one with a largest Destination Sequence value and accordingly constructs a route to a destination. Therefore, a malicious node may increase the Destination Sequence value of the RREP message to guarantee that its RREP message or the RREP message passing through it, will suppresses the other RREP messages. As a result malicious node invades the established route and can carry out other malicious actions [3] [15].

3) Modification of RERR

When a malicious node receives a RERR message, it can replace an unreachable destination IP address with another IP address, or append new unreachable destination IP addresses that, in fact, can be reached through the malicious node, it can send out a faked RERR message without being triggered by the receipt of any RERR message. The modified RERR message can be send to the neighbors in the precursor list, or even to those that are not in the precursor list of the malicious node, in order to disable active routes and disrupt the routing operation [3]. Tab.1. lists the fields in a RREQ, RREP, and RERR message that the malicious node may manipulate.

B. Fabrication attack

Fabrication refers to attack performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [5]. In AODV there are two kinds of fabrication:

1) Forge reply

The malicious node sends forged routing control message in response to legitimate routing message. Forge Reply is mainly related to the generation of faked RREP and RREP-ACK messages, trigged respectively by the receipt of legitimate RREQ and RREP messages. Malicious node impersonates destination address in the received RREQ, sends a forge RREP message, and establishes a route with a source node, in order to intercept or to drop data packets [3].

2) Active forge

In this attack the malicious node sends a forged routing control message without prior reception of any routing message, to achieve malicious purpose such as; break route or delete route, by using respectively a forge RREQ or forged

Tab. 1. Possible modifications of fields in a AODV messages

fields	Message	Modifications
Type	All	Change the message type
Flags	All	Reverse the setting
Hop count	RREQ, RREP	Decrease it to update other nodes reverse route tables, or increase it to suppress its update
RREQ ID	RREQ	Increase it to make the faked RREQ message acceptable, or decrease it to make the RREQ message unacceptable
Dest_IP	RREQ, RREP	Replace it with another IP address
Dest_SEQ	RREQ, RREP	Increase it to update other nodes forward route tables, or decrease it to suppress its update
Orig_IP	RREQ, RREP	Replace it with another IP address
Orig_Seq	RREQ	Increase it to update other nodes reverse route tables, or decrease it to suppress its update
Prefix size	RREP	Increase/Decrease the size of the subnet prefix
Lifetime	RREP	Decrease/increase it to shorten/extend the lifetime of the route entry updated by this RREP message
Dest count	RERR	Modify it according to the number of unreachable destinations included in the RERR message
Un_Dest_IP	RERR	Replace it with another IP address
Un_Dest_SEQ	RERR	Increase it to update other nodes routing table, or decrease it to suppress this entry

RERR message. Malicious node may eventually Flood the network with RREQ messages to consume the network resources [3].

C. Dropping attack

In AODV protocol, dropping control packets might be the greatly benefit for both selfish and malicious nodes. Particularly, once dropping the RREQ packets, a selfish node prevents the established routes from passing through it and consequently it saves its energy for transmitting its own packets [7]. Likewise, a malicious node may directly disrupt the routing operation by dropping routing messages to prevent new route from being established, or isolate a node or a group of nodes from communicating with the rest of the network. Dropping RERR packets extends the duration of use of the broken routes and consequently the network bandwidth falls sharply since no packet reaches its destination. In some cases malicious node may carry out more sophisticated dropping to divert security mechanisms by performing periodic, selective or random dropping [6].

D. Invisible node

A malicious node B situated at the same time within the transmission range of two legitimate nodes A and C (Fig. 2), knowing that A and C are not directly reachable by each other. By relaying the control messages from N1 to N2 and vice versa,
without carrying out any modification, the malicious node creates a fictitious link between A and C, which can fully control and can break at any time it want [8].

E. Black hole attack

In this attack a malicious node exploits the AODV vulnerabilities, by disseminating fake routing Information and announcing better routes to the requested destinations, to attract traffic through itself. Black hole attack is performed on two stages:
First the malicious node invades route at the discovery phase by advertising itself as having the freshness or the shortest routes to nodes whose packets it wants to intercept [5]. To achieve this goal, the malicious node applies the strategies illustrated below:

1. A malicious intermediate node may claim that it has the shortest route to the destination by resetting the hop count field of the RREP to zero, or the freshest route by increasing the destination sequence number. Consequently, if the RREP packet sent by the destination

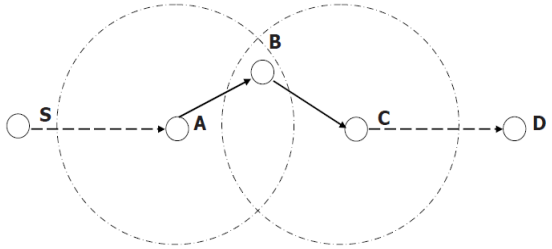

Fig. 2. Invisible node attack

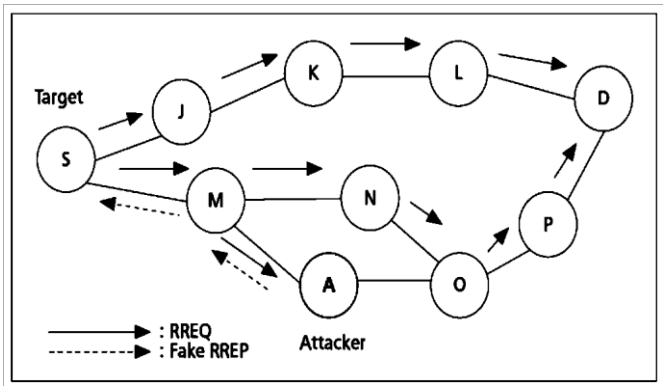

Fig. 3. Black hole attack

or any honest intermediate node, which has a fresh route to the destination, reaches the source node before the C's RREP then everything works well. Otherwise, the source node S deems that the route passing through the malicious node is the shortest path, and thus it starts transmitting data packets towards the malicious node [10]. Fig. 3. shows an instance of a blackhole attack, where a malicious node A sends a fake RREP packet to the source node S, pretending that it has a fresher route to the destination D. Since the malicious node's advertised destination sequence number is higher than other nodes' destination sequence numbers, the source node S will select the route containing the malicious node A [9].

2. A malicious node in the transmission range of the source node , may invade route by modifying the RREQ packet as follow ; increasing the originator sequence number and the destination sequence number by at least one and incrementing the RREQ ID . This strategy does not work if the malicious node is located out of the source transmission range, because of the resulting routing loops [3].
3. When the malicious node receives a RREQ packet, it impersonates the destination and transmits a RREP packet to reply back the source node claiming that it is the intended destination. Moreover, malicious node increases the destination sequence number received in RREQ packet by a value larger than one to guarantee that the source node chooses it as the actual destination [3].

Afterward, the malicious node simply drops all the data or control packets passing through it without any forwarding, however it runs the risk that neighboring nodes will monitor and expose the ongoing attack. The black hole can have more important impact when it is combined with other attacks such as wormhole and rushing attack [11].

F. Gray hole attack

This attack is more sophisticated than the black hole attack, instead of dropping all data packets a malicious node selectively drops packets. It may drop packets originating from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes, which limits the suspicion of its wrongdoing. It can also alternate by

interval of time between malicious behavior (dropping packets) and honest behavior (forwarding packets). To render the attack more difficult to detect malicious node can combines selective drop, and periodic or random dropping [10] [11].

G. Wormhole

Also called tunneling attack, is composed of two (or group of) colluding malicious nodes directly linked to each other through wormhole tunnel established by means of a wired link, a high quality wireless out-of-band link or a logical link via packet encapsulation [10] . One malicious node forwards received RREQ control messages from one point in the network to the second malicious node in another point many hops away in the network through the wormhole tunnel. When the second node receives these tunneled packets it replays them in its neighborhood [13].

Fig. 4. shows an example of wormhole attack in AODV. In the figure we assume that M1 and M2 are two colluding malicious node linked through a tunnel. M1 sends a received RREQ packet through a high-speed channel to M2, so the tunneled RREQ packet arrives to destination D before the packets through other routes because the tunnel is faster than links between legitimate nodes. The destination replies with a RREP packet and discards all later RREQ packets received from legitimate routes. Therefore the malicious nodes are included in the established route and may now intercept or drop data packets instead of forwarding. Wormhole attack is difficult to detect, and can be launched even against communications that provide authenticity and confidentiality [12].

H. Rushing

In AODV route discovery process each node typically forwards only the first-received RREQ packet from any route discovery to prevent broadcast storms. An insider malicious node may exploit this property to invade any route of two or more hops, by broadcasting RREQ packets faster than honest nodes, delivering them to their destinations before legitimate RREQ packets, those will be discard when they arrive later to their destinations. Consequently, the source node will be incapable to discover any route longer than two hops that does not contain the malicious node. This attack can be easily carried out by a single malicious node for the reason that

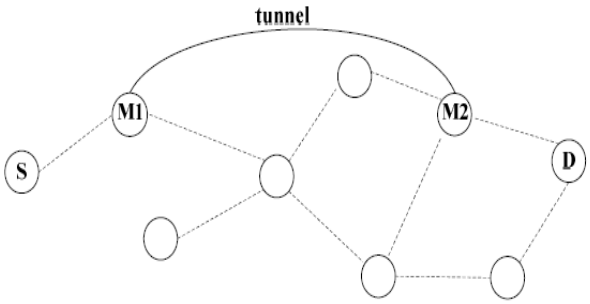

Fig. 4 wormhole attack

RREQ packets are delayed either by MAC layer or routing layer protocol. IEEE 802.11 [14] MAC layer protocol assumed by AODV protocol, delays packets using exponential backoff and interframe spacings [10].

To send out its packets as fast as possible, the malicious node may reduce or ignore delays imposed by the MAC layer protocol. It can for example select a smaller number to run the backoff mechanism after collision or ignore inter frame spacing time before transmission actually begins. Likewise malicious node can reduce processing time of the RREQ packet within the routing protocol [18].

Another method used by malicious node in protocols employing public key techniques and using inefficient RREQ authentication mechanism, is to keep other nodes busy authenticating RREQ packets containing bogus authentication to slow their ability to forward legitimate RREQ packets.

A malicious node can also achieve faster transit of its RREQ packets by transmitting them at a higher wireless transmission power level, over a longer distance and overtaking hops to increase the probability of its RREQ reaching the destination first, however this method do not allow him to insert itself on the discovered route. A more powerful rushing attacker may employ a wormhole to rush packets, in this case malicious node simply broadcasts RREQ packets through the tunnel [12].

I. Resource depletion

Also known as the sleep deprivation attack, it can be achieved by constantly generating fake routing packets and flooding it through the whole network, creating routing loops or injecting unnecessary data flows in some parts of the network. Hence, the malicious node may effectively consume the network bandwidth, power energy, and the processing time of the legitimate nodes. To achieve this end, the malicious node applies the strategies illustrated below:

1) RREQ flooding

The malicious node floods the network either by modify incoming RREQ messages to make them appear fresh by increasing their RREQ ID or by continuously fabricate a large number of fake RREQ packets. In both cases the fake RREQ packets will be rebroadcast by the malicious node's neighbors and propagated to the rest of the network [3].

2) Routing loop

The malicious node creates a loop(s) between forwarding nodes within a real route by sending a fake RREP, therefore the nodes involved in the loop(s) consume about 10 times more energy than the normal cases. Furthermore, the data packets transmitted in the loop will be dropped in the end and some nodes will be isolating from the rest of the network [3].

3) Data flow injection

In this attack malicious node injects large volumes of data flows on the network to congest existing routes and set up unnecessarily data flows to any point in the network up to its extreme transmission bandwidth. This type of attack is difficult to defend against, because it is hard to differentiate between legitimate and malicious data flows. [10]

J. *Impersonation and Sybil*

Impersonation also known in the literature as spoofing or masquerading attack is launched by using other node's identity (IP address) in outgoing routing packets. The malicious node may impersonate source node to communicate with destination node, or the destination node to reply the source node, or even announce new route with high destination sequence number or reduced hop count to the others nodes. Therefore the attacker can read, alter the received packets or even totally (entirely) isolate the real (authentic node (the real owner of the address) from the network. Impersonation attack sometimes is the first step for more sophisticated attacks [17].

A Sybil attack is an improved version of impersonation, in which a single node pretends to be many different nodes at the same time, by using multiple distinct addresses while transmitting. An attacker can obtain (acquire) an address through two manners; it can usurp an existing address or forging (fabricate) one if the network has no restriction to the allowed [16].

IV. CONCLUSION

In this paper we analyzed security issues against AODV to illustrate the scope of security vulnerabilities in MANET routing protocols. We have examined all types of attacks that can target AODV protocol. Particularly, we have examined different routing attacks, such as flooding, black hole, wormhole, and rushing attacks. The presented analysis in this paper is potentially helpful for protocol designers to assess their designs, and for security researchers to validate their security mechanisms such as intrusion detection systems and trust management systems.

REFERENCES

[1] C. E Perkins, E. M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.

[2] C. Perkins, P. Bhagwat, Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, in: ACM SIGCOMM, August–September 1994, pp. 234–244.

[3] P. Ning, K. Sun, "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols," Ad Hoc Networks, vol 3, pp. 795–819, May 2004.

[4] G. Hernández, C. Felipe, V. Cruz, J. Alonso, "Security in AODV Protocol Routing for Mobile Ad Hoc Networks", IEEE ROC&C'2005, C-03, P-11, Acapulco Gro. México, 29/November-04/December 2005.

[5] A. Amara korba, M. Nafaa, S. Ghanemi, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", in Proceedings of the Uksim'2013, 2013, pp. 693-698.

[6] S. Şen, J.A. Clark, J.E. Tapiador, 2010."Security Threats in Mobile Ad Hoc Networks," in Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, Al-Sakib Khan Pathan, Ed. Boca Raton, Florida: Taylor & Francis, 2010, pp. 127-146.

[7] M.S. Alkatheiri, L. Jianwei, A.R. Sangi, "AODV routing protocol under several routing attacks in MANETs," Communication Technology (ICCT), 2011 IEEE 13th International Conference on , vol., no., pp.614,618, 25-28 Sept. 2011.

[8] A. Amara Korba, M. Nafaa, S. Ghanemi, " Security attacks in mobile ad hoc networks", in Proceedings of the 3th ICIST, 2013, pp. 70-75.

[9] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," Wireless Communications, vol.14, no.5, Oct. 2007, pp. 85-91,doi: 10.1109/MWC.2007.4396947.

[10] J.V. Mulert, I. Welch and K. G. W. Seah, "Review: Security threats and solutions in MANETs: A case study using AODV and SAODV," Journal of Network and Computer Applications, vol. 35, issue 4, pp. 1249-1259,July 2012.

[11] M.K. Rafsanjani, Z.Z. Anvari and S. Ghasemi, "Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET", IJCA Special Issue on Network Security and Cryptography NSC(5), pp. 11-17, December 2011.

[12] V. Kumar and A. Kush, "Worm_Secure Protocol for Wormhole Protection in AODV Routing Protocol", International Journal of Computer Applications 44(4):15-21, April 2012.

[13] H. Ehsan, F.A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on , vol., no., pp.1181,1187, 25-27 June 2012.

[14] ANSI/IEEE std 802.11-1999, IEEE 802.11 wireless lan media access control (mac) and physical layer (phy) specifications.

[15] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto and N. Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks," Vehicular Technology, IEEE Transactions on , vol.58, no.5, Jun. 2009, pp. 2471-2481.

[16] C. Piro, C. Shields, B.N. Levine, "Detecting the Sybil Attack in Mobile Ad hoc Networks," Secure comm and Workshops, 2006 , vol., no., pp.1,11, Aug. 28 2006-Sept. 1 2006.

[17] C. Castelluccia and G. Montenegro, "Protecting AODV against impersonation attacks. SIGMOBILE Mob. Comput. Commun. Rev. 6, 3 (June 2002), 108-109.

[18] Y.C. Hu, A. Perrig and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in Proceedings of the 2nd ACM workshop on Wireless security (WiSe '03), 2003, pp. 30-40.