**Alekha Kumar Mishra, Bibhu Dutta Sahoo, “ANALYSIS OF SECURITY ATTACKS FOR AODV PROTOCOL IN MANET”, Proceedings of National Conference on Modern Trends of Operating Systems, MTOS-2009, page 54-57**

# ANALYSIS OF SECURITY ATTACKS FOR AODV PROTOCOL IN MANET

**Alekha Kumar Mishra[1] , Bibhu Dutta Sahoo[2]**
Department of Computer Science and Engg.
National Institute of Technology, Rourkela, Orissa
[1]alekha@gmail.com
[2]bdsahu@nitrkl.ac.in

## ABSTRACT

There are various challenges that are faced in the Ad-hoc environment. These are mostly due to the resource poorness of these networks. They are usually set up in situations of emergency, for temporary operations or simply if there are no resources to set up elaborate networks. The solutions for conventional networks are usually not sufficient to provide efficient Ad-hoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. In this paper we attempt to analyze various kinds of security threats that may be imposed on an ad hoc network. We also discussed the nature and the serious ness of the various attacks on the popular protocols like AODV and DSR.

## 1. INTRODUCTION

These days’ small computers with storage capacity of Gigabytes, high resolution color display and pointing devices and wireless communication adapters can be operated with the power of battery helping the user to adopt ad hoc network with respect to traditional wired network. In a wireless ad hoc network [1], the devices communicate with each other using a wireless physical medium without relying on pre-existing wired infrastructure. That’s why ad hoc network is also known as infrastructure less network. One of the most exciting features of ad hoc network is, two nodes not in the communication range of each other can still send and receive data from each other with the help of intermediate nodes which can act as routers and is known as “multi-hop wireless network”.

Since the advent of Defense Advanced Research Project Agency (DARPA) packet radio network in the early 1970s, a number of protocols have been developed for ad hoc mobile networks.

The existing protocols can be broadly categorized into 2 types; Table-driven (proactive) and Demand-driven (reactive). Some examples of table-driven protocols are DSDV (Destination-Sequenced Distance-Vector Routing), CGSR (Cluster-head Gateway Switch Routing), WRP (Wireless routing protocol).Two most popular demand-driven routing protocols of this type are DSR (Dynamic Source Routing) and AODV (Ad Hoc On-demand Distance Vector) protocols. None of these protocols has any security mechanism for protecting an attacker to include himself in the routing operation. However, many proposals can be found to add security features to the existing protocol which are aimed either guaranteeing authenticity and integrity or monitoring the behaviour of other nodes. Still most of them fail to find a proper trade-off between security and performance with respect to limited resources of a participating node. In this article first we briefly discuss the AODV protocol in section-2. Section 3 and 4 will explain and analyze various attacks on AODV and categorized the on different basis.

## 2. AD HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

AODV [2, 3] is the most popular reactive routing protocol in MANET. The reactive implies that a node exchange routing information only when it need to transfer some data and keep the routing information updated as long as the communication with the node exists. When a source node need to send some data to another node and it doesn’t have or have invalid path to the same, then it starts a route discovery process in order to establish a route towards destination node by sending route request message (RREQ) to all its neighbours. Neighbouring nodes receive the request, increment the hop count and forward the message to their neighbours. This broadcasting of RREQ message is known as flooding. The objective of RREQ message is not only to find a path to destination but also making other nodes learn about a route toward source node (reverse route). When an intermediate node receives a RREQ message from a node A for S, then it has a reverse route to node S through a with path length equals to hop count field of RREQ. Finally, when RREQ message reaches destination node, it response by initiating a route reply message (RREP). The RREP is sent as a unicast, using the path towards the source node established by the RREQ. Similarly, the RREP message allows intermediate nodwes to learn a route towards the destination node. Hence, the end of the route discovery process, packets can be delivered from the source to the destination nod eand vice versa. A third kind of routing message, called route error(RERR), allows nodes to notify breakage of link between any two node or information about those nodes which are unreachable at present.

In AODV it is not necessary that always a RREQ should reach the destination node. Any intermediate node already has a valid route towards destination, can generate a RREP message and does not forward the RREQ any further. This enables quicker replies and limits the flooding of RREQS. AODV uses a sequence number to identify the freshness of routing information. Each node maintains its own sequence number and increments it before sending any new RREQ or RREP message. These sequence numbers are included in the routing messages and also stored in routing tables. AODV always give preferences to fresh or new information, thus node updates its routing table if they receive a message with a sequence number higher than the last recorded one for the destination. Reader can go through AODV links for more detailed information.

## 3. ANALYSIS OF SECURITY ATTACKS

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. In order to protect against insider attacks, it is necessary to understand how an insider can attack a wireless ad-hoc network. Several attacks have been discussed in several literatures. However, the articles [ 4, 5, 6] adopted a systematic way to study the insider attacks against mobile ad-hoc routing protocols. In this chapter we have discussed different existing threats on AODV protocols with references to the above mention literatures. On the basis of actions performed by the interceptor they can be categorizes as follows.

### 3.1 ATTACKS USING MODIFICATION

Malicious nodes can cause redirection of network traffic and DoS(Denial of services) attacks by altering control message fields or by forwarding routing messages with falsified values. For example, in the network illustrated in Fig. 1, a malicious node M could keep traffic from reaching X by consistently advertising to B a shorter route to X than the route to X that C advertises. Below are detailed several of the attacks that can occur if particular fields of routing messages in specific routing protocols are altered or falsified.

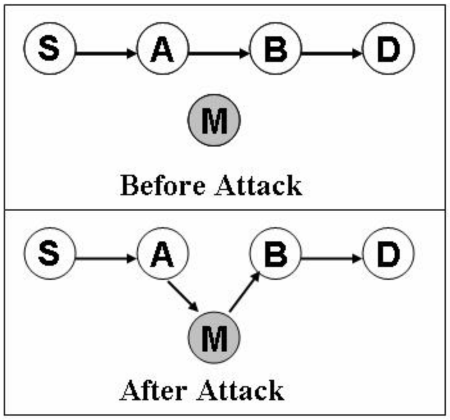

FIGURE 1: Attack using modification

#### 3.1.1 REDIRECTION BY MODIFIED ROUTE SEQUENCE NUMBERS

A malicious node M can redirects traffic toward itself by unicasting to A an RREP containing a much higher destination sequence num for D than the value last advertised by D. Subsequent traffic destined for D that travels through A will be directed toward M.

#### 3.1.2 REDIRECTION WITH MODIFIED HOP COUNTS

A redirection attack is possible by modification of the hop count field in route discovery messages. Malicious nodes can increase the chances they are included on a newly created route by resetting the hop count field of the RREQ to zero. Similarly, by setting the hop count field of the RREQ to infinity, created routes will tend to not include the malicious node. Such an attack is most threatening when combined with spoofing.

### 3.1.3 DENIAL-OF-SERVICE WITH MODIFIED SOURCE ROUTES

DSR utilizes source routes, thereby explicitly stating routes in data packets. So, when a malicious node M receives the packet, it can alter the source route in the packet's header, such as deleting an intermediate node from the source route. Consequently, when an authentic intermediate node receives the altered packet, it attempts to forward the packet to destination but fails because of altered route send by M. After retransmitting the packet a specified maximum number of attempts, the intermediate node should return a route error message to the source node. But the malicious node M which is sitting in between the path may continue the denial-of-service attack by dropping this route error message.

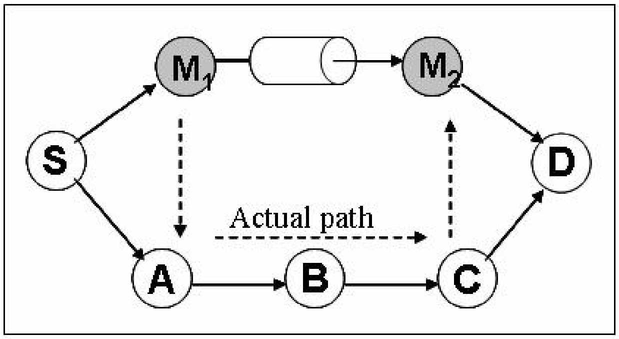

FIGURE 2: Tunneling

### 3.1.4 TUNNELING

Ad hoc networks have an implicit assumption that any node can be located adjacent to any other node. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. One vulnerability is that two such nodes may collaborate to falsely represent the length of available paths by encapsulating and tunneling between them legitimate routing messages generated by other nodes. In this case, tunneling prevents honest intermediate nodes from correctly incrementing the metric used to measure path lengths. Figure 2 illustrates such an attack where $M_1$ and $M_2$ are malicious nodes collaborating to misrepresent available path lengths by tunneling route request packets (e.g., an RREQ in AODV). Solid lines denote actual paths between nodes, the thin line denotes the tunnel, and the dotted line denotes the path that $M_1$ and $M_2$ falsely claim is between them. If route instantiation is determined by metrics that are governed solely by the operation of the routing protocol (such as a hop count metric), tunneling can cause routing metrics to be misrepresented. Only an unalterable physical metric such as time delay can provide a dependable measure of path length.

## 3.2 ATTACKS USING IMPERSONATION

Spoofing occurs when a node misrepresents its identity in the network, such as by altering its MAC or IP address in outgoing packets, and is readily combined with modification attacks. The following example illustrates how an impersonation attack can work in AODV.

### 3.2.1 FORMING LOOPS BY SPOOFING

Assume a path exists between the five nodes illustrated in Figure. 3a toward some remote destination, X, as would follow after an AODV RREQ/RREP exchange. A malicious node can intentionally come close to the nodes each node and behave as other valid node by modifying its MAC address to their address and can send false routing message to divert the route towards it. The attacker can perform this attack in such a way that all neighbouring node may fall in a loop link and isolated from all other node of the network.

## 3.3 ATTACKS USING FABRICATION

The generation of false routing messages can be classified as fabrication attacks. Such attacks can be difficult to verify as invalid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted.

### 3.3.1 FALSIFYING ROUTE ERRORS IN AODV AND DSR

This kind of routing attacks can be launched by sending false route error messages. A malicious node M can launch a denial-of-service attack against a destination node D which has only link to M by continually sending route error messages to its neighbouring nodes, indicating a broken link between nodes M and D. Any node receives the spoofed route error message thinking that it came from a valid node deletes its routing table entry for D and forwards the route error message on to its neighbours.

### 3.3.2 ROUTING TABLE OVERFLOW ATTACK

In routing table overflow attack, the attacker attempts to create route to non-existent nodes. The goal of the attacker is to create enough routers to prevent new routes from being created or overwhelm the protocol. Implementation and flush out legitimate routes from routing tables. Proactive routing algorithms attempt to discover routing information even before they are needed, while reactive algorithms create only when they are needed. This makes proactive algorithms more vulnerable to table overflow attacks.

## 4. ATOMIC AND COMPOUND MISUSES

Based on the composition of operations for performing attack as mentioned in [3], misuses of AODV have been classified into two categories: atomic misuses and compound misuses. Intuitively, atomic misuses are performed by manipulating a single routing message, which cannot be further divided. In contrast, compound misuses are composed of multiple atomic misuses, and possibly normal uses of the routing protocol.

First, it is necessary to identify a number of misuse goals that an inside attacker may want to achieve, and then study how these goals may be achieved through misuses of the routing messages. The misuse goals that we have considered are listed as follows.

Route Disruption (RD):- Route Disruption means either breaking down an existing route or preventing a new route from being established.

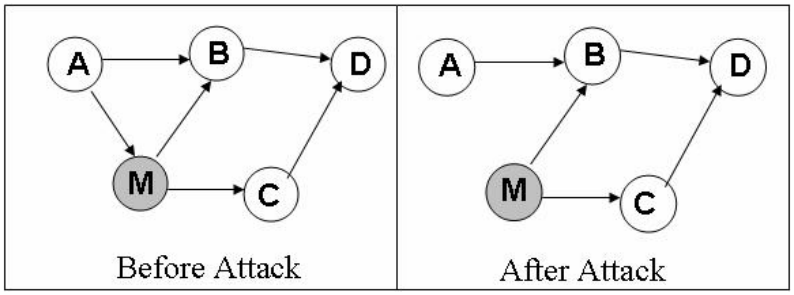

Figure 3: The malicious node M performs route disruption by breaking the existing route between A and C

Route Invasion (RI):- Route invasion means that an inside attacker adds itself into a route between two endpoints of a communication channel.

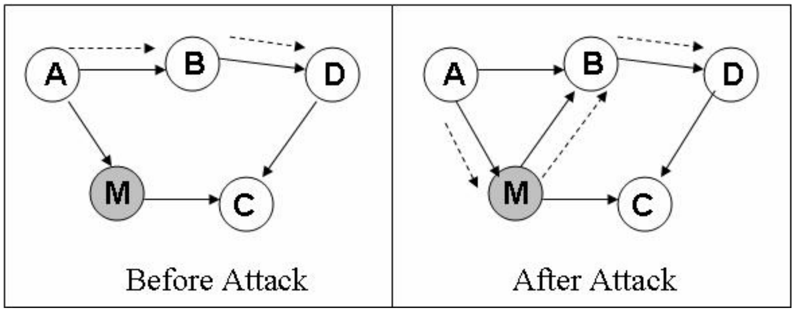

Figure 2: Malicious node achieves route invasion by adding itself to the route between A to D

Node Isolation (NI):- Node isolation refers to preventing a given node from communicating with any other node in the network. It differs from Route Disruption in that Route Disruption is targeting at a route with two given endpoints, while node isolation is aiming at all possible routes.

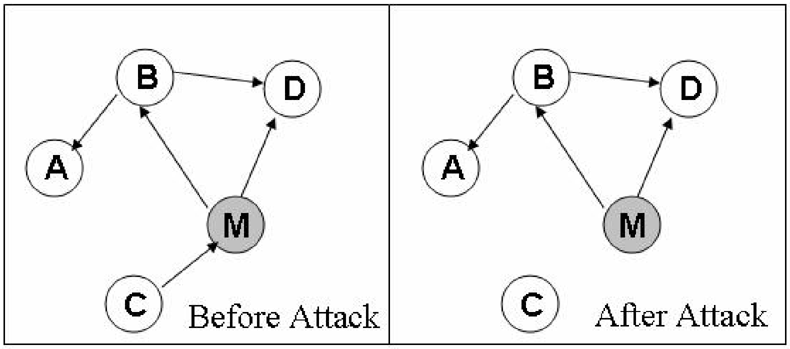

Figure 3: Node C has been isolated by the attacker M from rest of the nodes in the network.

Resource Consumption (RC):- Resource consumption refers to consuming the communication bandwidth in the network or storage space at individual nodes. For example, an inside attacker may consume the network bandwidth by either forming a loop in the network.

As an example, Route Disruption, route, Invasion and Route Isolation has been shown diagrammatically using figure 1, 2 and 3 respectively. Analysis of atomic misuses can be done in an effective way through understanding the effects of possible atomic misuse actions. Each atomic misuse action is an indivisible manipulation of one routing message. Specifically, the atomic misuse actions in AODV have been divided into the following four categories:

Drop (DR): Here, the attacker simply drops the received routing message.

Modify and Forward (MF): After receiving a routing message, the attacker modifies one or several fields in the message and then forwards the message to its neighbor(s) (via unicast or broadcast).

Forge Reply (FR): The attacker sends a faked message in response to the received routing message. Forge Reply is mainly related to the misuse of RREP messages, which are in response of RREQ messages.

Active Forge (AF): The attacker sends a faked routing message without receiving any related message.

As already mentioned that compound misuse can be performed by combining atomic misuses, one category of compound misuse is to simply repeating the same type of atomic misuses. The more interesting and complex one is that an attacker can combine several atomic misuses in a planned way and launch them. For example, an attacker may repeatedly launch the same type of atomic misuses to make the impact persistent. Another way, an attacker may launch some early atomic or compound misuses to prepare for some later ones. A crucial issue here is to understand the compound misuses that can be used as “building blocks” of more complex attacks, interested reader can refer the proceedings of Sun et al[4].

## 5. CONCLUSION

Developing an efficient security mechanism for protocols like AODV is still an open are for research as can be seen with the problems that exist in these networks and the emerging solutions. In this paper we have presented and analysed various security threat that can be possible on AODV. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. It is a difficult goal to achieve security goals in the resource deficient Ad-hoc environment. But the flexibility, ease and speed with which these networks can be set up imply they will gain wider application.

## REFERENCES:

[1] D. Remondo , "Tutorial of Wireless Ad Hoc Networks", HET-NETs 2004.

[2] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Wksp. Mobile comp. Sys. And Apps. Feb,1999, page 90-100

[3] C.E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad Hoc On-Demand Distance Vector Routing", IETF RFC 3561, July 2003

[4] P.Ning, K. Sun, "How to misuse AODV: A Case Study of Insider Attacks Against Mobile Adhoc Routing Protocols", Info Assurance Wksp, IEEE sys, Man and Cybernetics Soc, june 2003, page 60-67

[5] Weichao Wang, Yi Lu, Bharat K. Bhargava, "On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol", IEEE Proceedings, 2003, page 375-382

[6] Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the 10th IEEE International Conference on Network Protocols, 2002,