IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 5 (Sep. - Oct. 2013), PP 127-134
www.iosrjournals.org

Review on security issues of AODV routing protocol for MANETs

Miss Morli Pandya[1], Associate Prof. Ashish Kr. Shrivastava[2]
[1](*M. Tech Scholar, Dept. of Computer Science Engineering, NIIST, Bhopal, India)*
[2](*Head PG Dept. of Computer Science Engineering, NIIST, Bhopal, India)*

Abstract: *Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure, Instead, hosts rely on each other to keep the network connected. One main challenge in the design of these networks is their vulnerability to security attacks. In this Survey, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. Routing protocols, which act as the binding force in these networks, are a common target of these nodes. Ad-hoc On Demand Distance Vector (AODV) is one of the widely used routing protocols that is currently undergoing extensive research and development. AODV is based on distance vector routing, but the updates are shared not on a periodic basis but on an as per requirement basis. The control packets contain a hop count and sequence number field that identifies the freshness of routing updates. As these fields are mutable, it creates a potential vulnerability that is frequently exploited by malicious nodes to advertise better routes. Similarly, transmission of routing updates in clear text also discloses vital information about the network topology, which is again a potential security hazard. This research addresses the problem of securing Mobile Ad Hoc Networks routing protocols. In this survey we examine different routing protocols and various types of routing security attacks. We also perform a survey in search for different routing security schemes that have been proposed to prevent and/or detect these attacks, and point out their advantages and drawbacks.*

Keywords: *Ad-hoc Network, (AODV) Ad-hoc On Demand Distance Vector, ARN (Authenticated Routing for Ad-hoc Networks).*

I. Introduction

In Latin, 'ad hoc' phrase means 'for this', meaning 'for this special purpose only', by expansion it is a special network for a particular application. An Ad-hoc wire-less network consists of a set of mobile nodes (hosts) that are connected through the wireless links. In Ad-hoc wireless network, communication is based on the principle of broadcast radio channel and reception of electromagnetic waves. The varied characteristics of wireless networks as compared to their wired counterparts addresses various issues such as mobility of nodes, limited bandwidth, error prone broadcast channels, hidden and exposed terminal problems and power constraints.

Mobile Ad hoc Network is an autonomous system of mobile nodes connected by wireless channel. Each node operates as an end system and a router for all other nodes in the network. A mobile Ad hoc Network is a self configuring network of mobile routers connected by wireless links –the union of which forms an arbitrary topology. An Ad hoc network is often defined as an "infrastructure less" network means that a network without the usual routing infrastructure, link fixed routers and routing backbones.

A MANET is a network that does not require centralized control, and every node works not only as a source and a sink but also as a router. This type of dynamic network is especially useful for military communications or emergency search and rescue operations, where an infrastructure cannot be supported. The nodes that make up a network at any given time communicate with and through each other. In this way every node can establish a connection to every other node that is included in the MANET.

Mobile ad hoc networks (MANETs) have become a Main research area over the last couple of years. Many research teams develop new ideas for protocols, services, and security applicable for these type of networks. Therefore, mechanisms and protocols have to be developed to secure MANETs. This especially becomes relevant for a commercial use of this technology, since customers expect a high quality service which is trustworthy and reliable. Because of the changing topology special routing protocols have been proposed to face the routing problem in MANETs. A secure routing protocol has to be able to identify trustworthy nodes and find a reliable and trustworthy route from sender to destination node. This has to be realized within a few second or better tenths of seconds, depending on the mobility of the nodes and the number of hops in the route. We briefly describe the AODV protocol, the attacks to which it is subject, and well known security extension proposal. Then, we present our prototype implementation and some tuning strategies.

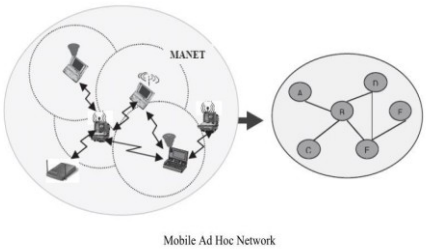

Figure 1. Basic of Mobile Ad-hoc networks and its communication topology

II. Protocol Techniques For Manet

Portable devices have limited capacity (battery power consumptions, computing power, available memory, movable nodes) that further complicates the protocol design. Several protocols for ad hoc networks have been developed. The protocols can perform well under certain situations that they are designed to solve, but they fail completely in other situations that can occur in the network.

Ad Hoc routing protocols can be classified based on different criteria [1]; however, the different classes of protocols are not mutually exclusive. So that, depending on the routing mechanisms employed by a given protocol, it may fall under more than one class.

2.1 Reactive (On-demand)

In this type of protocol maintain or constantly update their route tables with the latest route topology. Instead, when a source node ants to transmit a message, it floods a query into the network to discover the route to the destination. The discovered route is maintained until the destination node becomes inaccessible or until the route is no longer desired. Reactive protocols are generally considered efficient when the route discovery is employed rather infrequently in comparison to the data transfer. Although the network topology changes dynamically, the network traffic caused by the route discovery step is low compared to the total communication bandwidth. e.g. Dynamic Source Routing Protocol (DSR) [3] , Ad hoc On-Demand Distance Vector routing protocol (AODV).

2.2 Proactive (table driven)

In next proactive routing, each node/host has one or more tables that manage the latest information of the routes to any node in the network. Each row has the next hop for reaching to a node/subnet and the cost of this route. The two kinds of table updating in proactive protocols are the periodic update and the triggered update. Proactive routing tends to waste bandwidth and power in the network because of the need to broadcast the routing tables/updates. Furthermore, as the number of nodes in the MANET increases, the size of the table will increase; this can become a problem in and of itself. e.g. Destination Sequenced Distance Vector (DSDV) [3].

2.3 Hybrid

Both the proactive and reactive protocols work good for networks with a small number of nodes. As the number of nodes increases, hybrid reactive/proactive protocols are used to achieve higher performance. Hybrid protocols attempt to assimilate the advantages of proactive and reactive protocols. The key idea is to use a reactive routing procedure at the global network level while employing a proactive routing procedure in a node's local neighborhood. e.g. Zone Routing Protocol (ZRP) [3], Hybrid Ad hoc Routing Protocol (HARP).

2.4 Characteristics of Ad hoc Networks

The adhoc networks comprise of free to move mobile nodes. These nodes may be of same or variable type devices like laptops, PDAs, palmtops etc. These nodes operate in wireless modes thus inherit all the characteristics and limitations of wireless networks. The nodes in an adhoc network share a common bandwidth. The mobile nodes in adhoc networks also have dual tasks to perform(routing and own independent functions). These requirements have forced certain peculiarities on adhoc networks, they are:

- They have limited power (battery packs) and varied processing capability.
- High degree of security/ trust mechanism is required as the mobile nodes are free to join and leave the network without any laid down policy/ rule.

These peculiarities identify that any protocol / techniques designed for mobile adhoc networks must obey certain characteristics which include:

- Minimal processing to be involved (encryption/ decryption at source and destination only) to conserve processing and power requirements.
- Ensuring security requirements related to wireless communication, routing and exchange of data.

III. Security Issues

3.1 Attacks at Layers

The Basic target of securing a communication between two parties has propagated to the different layers that constitute the TCP/IP protocol Model. Over the time pass away, several security mechanisms have been proposed and implemented at different layers, trying to address specific security issues and acquiring the flavor of the layer at which they were implemented. For instance a security Method implemented at the TCP layer will naturally try to provide end-to-end security, while another, implemented at layer 3, would be specialized in routing security, and so on. In our survey, we identified three types of security protocols:

- Application Layer Protocols: e.g. Authentication mechanisms and key establishment and management strategies.
- Internet Layer Protocols: e.g. IPSec which tries to secure routing packets and all its related issues.

The Main goal of any security solution for AODV should be to provide security services, such as authentication, confidentiality, integrity and non repudiation [4]. In order to achieve these goals, the security solution must give complete protection against the attacks designed for each layer. Table identifies some security attacks [6].

Layer	Attacks
Application Layer	Repudiation, data Corruption
Transport Layer	Session hijacking
Network Layer	Wormhole, location Disclosure attacks.
Data link Layer	Traffic analysis, Eavesdropping
Physical Layer	Jamming, interception
Multi-Layer attacks	DoS, man in middle attacks

Table 1: Attack At different Layer

3.2 Attacks on ad hoc networks

Attacks on ad hoc network routing protocols generally divided into one of main two categories:

- Routing-disruption attacks: In this, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways.
- Resource-consumption attacks: In this, the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth or to consume node resources such as memory (storage) or computation power.

3.3 Protect Network from Attacks

To protect an ad-hoc network from various attacks a routing protocol must fulfill a set of some requirements [4] to ensure that the discovered path from source to destination functions properly in the presence of malicious nodes. These are:

1) Minimal exposure of networks topology,
2) Detection of spoofed routing messages,
3) Detection of altered routing messages,

A number of secure routing protocols [6] have been recently developed that conform to most of the requirements at this stage. These protocols employ a variety of cryptographic tools for protecting the vulnerabilities in different routing protocols. However, these protocols have been developed as a practical response to specific problems that arose due to attacks on ad-hoc network routing protocols. Consequently, these protocols only cover a subset of all possible threats and are not flexible enough to be integrated with each other.

IV. Security Issues Of Aodv

AODV[7,4] is the most well-known routing protocol for a MANET. It is a reactive protocol: nodes in the network exchange routing information only when a communication must take place and keep this

information up-to-date only as long as the communication lasts.

When a node/hope must send a packet to another node, it works start a route discovery process in order to establish a route toward the destination node. There, it sends data to its neighbors a route request message RREQ). Neighboring nodes receive the request, increment the hop count, and forward the message to their neighbors, so that RREQs are actually broadcasted using a flooding approach. The goal of the RREQ message is to find the destination node, but it also has the side effect of making other nodes learn a route towards the source node (the reverse route): anode that has received a RREQ message, with source address S from its neighbor A, knows that it can reach S through A and records this information in its routing table along with the hop count (i.e., its distance from node S following that route). The RREQ message will eventually reach the destination node, which will react with a route reply message (RREP). The RREP is sent as a unicast, using the path towards the source node established by the RREQ. Similarly to what happens with RREQs, the RREP message allows intermediate nodes to learn a route toward the destination node (i.e., the originator of the RREP). Therefore, at the end of the route discovery process, packets can be delivered from the source to the destination node and vice versa. A third kind of routing message, called route error (RERR), allows nodes to notify errors, for example, because a previous neighbor has moved and is no longer reachable. If the route is not active (i.e., there is no data traffic flowing through it), all routing information expires after a timeout and is removed from the routing table.

4.1 The major Vulnerabilities present in the AODV protocol are

4.1.1 Deceptive incrementing of Sequence Numbers

Destination Sequence numbers determine the freshness of a route path. The destination sequence numbers maintained by different nodes are updated when a newer control packet is received with a higher sequence or larger number. The destination sequence numbers received via control packets cannot be greater than the previous value held by the node plus one [7]. However, malicious nodes may increase this number so as to advertise fresher routes towards a particular destination. If this difference is equal or larger than two then there is a high probability that the network may be under a modification attack.

4.1.2 Deceptive decrementing of Hop Count

AODV prefers route freshness over route length of path. In that, nodes prefers a control packet with a larger destination sequence and hop count over a control packet with a smaller destination sequence and hop count of node. However, if the destination sequence numbers are the same then the route with the least hop count is given preference. Malicious nodes frequently exploit this mechanism in order to generate fallacious routes that portray minimal hop counts.

4.2 Secure AODV Routing Protocol

Securing the AODV protocol can be divided into the following three major categories:

1) Key Exchange
2) Secure Routing
3) Data Protection

1) Key Exchange: Most of the current key exchange protocols are dependent upon a central trust authority for initial authentication. A variant of the central trust authority is the Distributed Public-Key Model [10] that makes use of threshold cryptography to distribute the private key of the Certification Authority (CA) over a number of servers. Whatever the case may be, the requirement of a central trust authority in such a dynamic environment is considered both impractical and unsafe, as such an entity may not always be accessible and it also creates a single point of failure. Similarly, key exchange using a Key Distribution Server [7] creates a similar set of problems. We suggest that all nodes, before entering a network, procure a one-time public and private key pair from the CA along with the CA's public key. without any reliance on the CA, using any suitable key exchange protocol for ad-hoc networks [8].

2) Secure Routing: Ad-hoc On-Demand Distance Vector routing protocol operates at the third layer of the TCP/IP protocol suite using UDP port 654. The source node that requires a route to a destination broadcasts arouse REQUEST packet, each intermediate recipient node retransmits the packet, if not a duplicate, and the final destination uncast arouse REPLY packet back to the original sender. For route maintenance it uses ROUTE ERROR packets that inform active users of route failures.

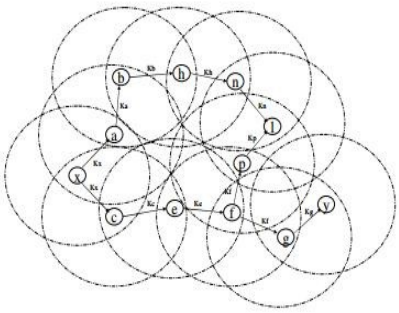

Figure 2: Point-to-Point Establishment of Secure Routes

The core security related problems linked to ad-hoc networks originate due to the route development by the intermediate nodes. It is therefore, imperative that only authorized nodes are allowed to update routing packets and malicious nodes be avoided at all costs. To restrict modification of routing packets by intermediate nodes, we recommend peer-to-peer symmetric encryption of all routing information. All routing control packets between nodes are first encrypted and then transmitted. The sequence of steps, for route discovery and route maintenance, is as follows:

Route Request:

1) Any Node 'x' desiring to establish communication with another Node 'y' first establishes a group session key kx with its immediate neighbors (nodes that are a single hop away) as shown in Figure.
2) It then creates the ROUTE REQUEST packet as per the routing protocol specifications shown in Figure.
3) The ROUTE REQUEST packet is then encrypted using the group session key Kx and broadcasted.
4) All intermediate recipient nodes that share the same group session key decrypt the ROUTE REQUEST packet and, if required, modify it according to the routing protocol specifications.
5) After establishing the group session key, the intermediate nodes encrypt the ROUTE REQUEST packet using the new session key and rebroadcast the packet.
6) Steps 4 to 5 are followed until the final destination Node's' receives the packet.

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP address							
Originator sequence Number							

Figure 3: Route Request (RREQ) Message Format Route Reply

1) In response to the ROUTE REPLY packet Node 'y' creates a ROUTE REPLY packet as per the routing protocol specifications shown in Figure.
2) The ROUTE REPLY packet is encrypted using the last group session key (Kg in this case) that was used to decrypt the received ROUTE REQUEST packet and is uncast back to the original sender.
3) If any of the intermediate nodes has moved out of the wireless range a new group session key is established.
4) All recipient nodes that share the forward group session key decrypt the ROUTE REPLY packet and, if required, modify it according to the routing protocol specifications.
5) The ROUTE REPLY packet is then again encrypted using the backward group session key and uncast towards Node 'x'.
6) Steps 4 and 5 are repeated until the packet is received by Node 'x'.

Type	R	A	Reserved	Prefix size	Hop Count
Destination IP Address					
Destination Sequence Number					
Originator IP address					
Life Time					

Figure 4: Route Reply (RREP) Message Format

4.4 Attacking Aodv

AODV messages are neither encrypted, authenticated, or integrity protected and basically are always assumed as trusted protocol. Many different kinds of attacks are possible, based on the possibility to forge packets and on the distributed and uncontrolled nature of the network. A malicious node could impersonate a

source node by creating RREQ messages with its victim's address as originator and by using a sequence number higher than its victim's (similarly, the attacker can impersonate a destination node by creating fake RREPs). The attacker also can generate false error messages, spreading fake information in the network, for example, to announce that a certain destination is not reachable any more. This kind of false information could be spread around as the first stage of a more complex attack, aimed at excluding a target node from the network before fake RREQs or RREPs are sent to other nodes. Spoofed RREQ and RREP messages can be used to redirect some traffic through alternative routes, create loops in the network, segment the network, or perpetrate a denial of service attack. A systematic analysis of AODV security is proposed in [4], where misuse goals that an inside attacker may want to achieve are analyzed and classified.

4.5 Identification of Attack

- Route Invasion: In this means that an inside attacker can add itself or own to a route between two endpoints of a communication channel between each other.
- Node Isolation: this refers to preventing a node from communicating with any node in the network. It differs from route disruption in that node isolation is aimed at all possible routes, instead of targeting two specific endpoints.
- Resource Consumption: this refers to consuming the communication bandwidth in the network or memory space at individual nodes

V. Analysis Of Current Security Techniques

5.1 SAODV

The SAODV routing protocol proposed in [5] is used to protect the routing messages of the original AODV. SAODV uses digital signatures [8] to authenticate non-mutable fields and hash chains [8] to authenticate the hop-count field (only mutable field) in both RREQ and RREP messages. The SAODV uses cryptographic extensions [8] to provide authenticity and integrity of routing messages and prevent the manipulation of the hop count information.

5.2 SAR

SAR protocol integrates the trust level of a node and the security attributes of a route to provide the integrated security metric for the requested route. A Quality of Protection (QoP) vector used is a combination of security level and available cryptographic techniques. It uses the timestamps and sequence numbers to stop the replay attacks. Interception and subversion threats can be prevented by trust level key authentication. Attacks like modification and fabrication can be stopped by verifying the digital signatures of the transmitted packet. The main drawbacks of using SAR are that it required excessive encrypting and decrypting at each hop during the path discovery. The discovered route may not be the shortest route in the terms of hop-count, but it is secure [7] and [11].

5.3 Trusted Ad-hoc On-demand distance vector Routing (TAODV)

TAODV is secure routing protocol which uses cryptography technologies recommended to take effect before nodes in the establish trust relationships among one another. The main salient feature of TAODV is that using trust relationships among nodes, there is no need for a node to request and verify certificates all the time.

TAODV (Trusted AODV) has several salient features:
(1) The performance of the System is improved by avoiding requesting and verifying certificates at every routing step.
(2) A node that performs malicious behaviors will eventually be detected and denied to the whole network.

That protocol greatly reduces the computation overheads. Assume that the keys and certificates needed by these cryptographic technologies have been obtained through some key management procedures before the node performs routing behaviors. Some extra new fields are added into a node's routing table to store its opinion about other nodes' trustworthiness and to record the positive and negative evidences when it performs routing with others. The main advantages of embedding trust model into the routing layer of MANET, save the consuming time without the trouble of maintaining g expire time, valid state, etc. which is important in the situation of high node mobility and invalidity. Trusted AODV are mainly three modules in the whole TAODV system: basic AODV routing protocol, trust model, and trusted AODV routing protocol. Based on trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating [3]

5.4 ARAN (Authenticated Routing for Ad-hoc Networks)

ARAN provides authentication, message integrity and non-repudiation in ad-hoc networks by using a preliminary certification process which is followed by a route instantiation process that ensures end-to-end security services. But it needs the use of trusted certification server.As a consequence, ARAN is capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. However, erratic behavior can come from a malicious node, which will be defended against successfully by existing ARAN protocol, and can also come from an authenticated node. The currently existing ARAN secure routing protocol does not account for attacks that are conducted by authenticated selfish nodes as these nodes trust each other to cooperate in providing network functionalities. This results in that ARAN fails to detect and defend against an authenticated selfish node participating in the mobile ad hoc network. Thus, if an authenticated selfish node does not forward or intentionally drop control or data packets, the current specification of ARAN routing protocol cannot detect or defend against such authenticated selfish nodes. This weakness in ARAN specification will result in the disturbance of the ad hoc network and the waste of the network bandwidth [3]

5.5 AODV and other Secure AODVs.

- Increased overheads due to AODV based routing path and subsequently applying SSL/ IPSec technique for data protection.
- Increased complexity and processing time as Secure AODV routing path techniques have their inbuilt cryptographic parameters/ mechanisms. Any subsequent implementation of conventional security protocols for data security may duplicate the desired authentication and integrity checks

VI. Exploits Allowed By Existing Protocols

The current proposed routing protocols for ad hoc wireless networks allow for many different types of attacks at different Layer. Analogous exploits exist in wired networks [8], but are more easily defended against by infrastructure present in a wired network. In this section, we classify modification, impersonation ,and fabrication exploits against ad hoc routing protocols. In Section 5,we propose a protocol not exploitable in these ways. Our focus is on vulnerabilities and exposures that result from the specification of the ad hoc routing protocol, and not from problems with IEEE 802.11 [8]. Additionally, trivial denial-of-service attacks based on interception and noncooperation are possible in all ad hoc routing protocols. While these attacks are possible, they are not achieved through subversion of the routing protocol.

6.1 Attacks Using Modification

Malicious nodes can cause redirection of network traffic and DoS attacks by altering control message fields or by forwarding routing messages with falsified other values. For example, in the network illustrated in Fig. , a malicious node 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.

6.1.1 Redirection by modified route sequence numbers

In AODV, node may divert traffic through itself by advertising a route or path to a node with a destination sequence num greater than the authentic value. Fig. 5 illustrates an example ad hoc network.

Suppose an any malicious node, M, receives the RREQ that originated from S for destination X after it is re-broadcast by B during route discovery. M redirects traffic toward itself by uncasing to B an RREP containing a much higher destination sequence num for X than the value last advertised by X. Eventually, the RREQ broadcast by B will reach a node with a valid route to X and a valid RREP will be uncast back toward S. However, at that point B will have already received the false RREP from M. If the destination sequence num for X that Mused in the false RREP is higher than the destination sequence num for X in the valid RREP, B will drop the valid RREP, thinking that the valid route is stale. All subsequent traffic destined for X that travels through B will be directed toward M. The situation will not be corrected until either a legitimate RREQ or a legitimate RREP with a destination sequence num for X higher than that of M's false RREP enters the network.

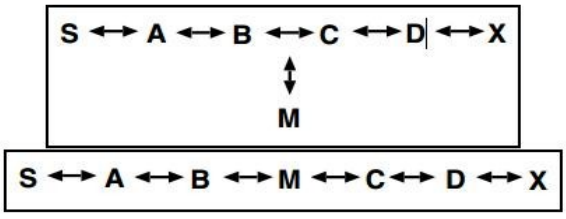

Figure 5. (A) A simple ad hoc network. (B) Another example ad hoc network.

6.1.2 Denial-of-service with modified source routes

DSR utilizes source routes, therefore explicitly stating routes in data packets. These routes lack any integrity checks and a simple denial-of-service attack can be launched in DSR by altering the source routes in packet headers. Assume a shortest path exists from S to X as in Fig.6. Also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S wishes to communicate with X and that S has an unexpired route to X in its route cache. S transmits a data packet toward X, with the source route S A B M C D X contained in the packet's header.

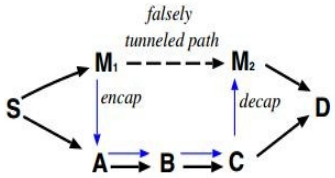

Figure 6. Path lengths spoofed by tunneling

When M receives the packet, it can alter the source route in the packet's header, such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to forward the packet to X. Since X cannot hear C, the transmission is unsuccessful. DSR provides a route maintenance mechanism such that a node forwarding a packet is responsible for confirming that the packet has been received by the next hop along the path. If no confirmation of receipt is received after retransmitting the packet a specified maximum number of attempts, this node should return a route error message to the source node. In this case ,C would send a route error message to S. Since M would be the first hop the route error takes on its path back to S, M can continue the denial-of-service attack by dropping this route error message.

6.2 Redirection with modified hop counts

A redirection attack is possible by modification of the hop count field in route discovery messages. When routing decisions cannot be made by other metrics, AODV uses the hop count field to determine a shortest path. In AODV, 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.

VII. Conclusion

The security of the ad hoc network routing protocols is still an open problem and deserves more research work. This paper studies the vulnerabilities of and attacks on two protocols – AODV. The analysis shows that as AODV provides fair performance with reasonable overhead and adaptability to both traffic load and host mobility, the on-demand property also introduces some security deficiencies. It allows the malicious host to attack the network in real time with flexibility. It is more difficult to locate the sources of the false information. The proactive property also has disadvantages. The routine exchange of routes enables the false routing information to propagate within a wider range. The malicious host can conduct multiple attacks in the same routing packet. Because both protocols prefer the fresh routes which are identified by large sequence numbers, the attacks on destination sequence have more severe impacts than the attacks on distance vector.

References

[1] Monis Akhlaq, M Noman Jafri, Muzammil A Khan, Baber Aslam, Addressing Security Concerns of Data Exchange in AODV Transactions on Engineering, Computing and Technology, Volume 16 November 2006 ISSN 1305-5313, pp. 29-33.

[2] Davide Cerri and Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype "IEEE Communications Magazine • February 2008.

[3] Durgesh Wadbude, Vineet Richariya, An Efficient Secure AODV Routing Protocol in MANET., International Journal of Engineering and Innovative Technology (IJEIT)Volume 1, Issue 4, April 2012 274

[4] Songbai Lu1, Longxuan Li and Kwok-Yan Lam, Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", IEEE 2009 International Conference on Computational Intelligence and Security, pp 421-425.

[5] Seung Yi, Prasad Naldrug, Robin Kravets, A Security Aware Routing Protocol for Wireless Ad hoc Networks, In the proceedings of 3rd ACM international of mobile ad hoc networking and computingpp 226-236, 2002.

[6] Yih-chunhu, Adrianperrig, "A Survey of Secure Wireless Ad Hoc Routing", PUBLISHED BY THE IEEE COMPUTER SOCIETY, 1540-7993/04.

[7] Asad Amir Pirzada and Chris McDonald "Secure Routing with the AODV Protocol" 2005 Asia-Pacific Conference on Communications, Perth, Western Australia, 3 - 5 October 2005

[8] Kimaya Sanzgiri, Bridget Dahilly, Brian Neil, Elizabeth m. Belding-royer "A Secure Routing Protocol For Adhoc Networks" Proceedings of the 10th IEEEInternational Conference on Network Protocols(ICNP'02).

[9] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE NetworkMagazine, vol. 13, no. 6, pp. 24–30, 1999.

[10] A. A. Pirzada and C. McDonald, "Kerberos assisted authenticationin mobile ad-hoc networks," Proceedings of the 27th Australasian Computer Science Conference (ACSC),vol.26,no.1,pp.41–46,2004.