Security Enhancements in AODV Routing Protocol

[1]Preeti Bathla, [2]Bhawna Gupta
[1,2]N.C. College of Engineering, Israna (Panipat)

Abstract
An ad hoc network is a collection of wireless nodes communicating among themselves over possibly multi-hop paths, without the help of any infrastructure. The nature of ad hoc networks is dynamically changing and they have a fully decentralized topology. Hence, security is hard to achieve due to the dynamic nature of the relationships between the participating nodes as well as the vulnerabilities and limitations of the wireless transmissions medium 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. In our work we look at AODV in detail, study and analyses various attacks that can be possible on it. Then we look into some existing mechanism for securing AODV protocol.

Keywords
Ad Hoc; AODV; Security, SAODV

I. Introduction

Mobile ad hoc networks (MANETs) have become a prevalent research area over the last couple of years. MANETs consist of mobile nodes which can act as sender, receiver, and forwarder for messages. They communicate using a wireless communication link. These networks are subject to frequent link breaks which also lead to a constantly changing network topology. Due to the specific characteristics of the wireless channel, the network capacity is relatively small.

These networks are built, operated and maintained by its constituent wireless nodes. These nodes generally have a limited transmission range and so each node seeks the assistance of its neighbouring nodes in forwarding packets. In order, to establish routes between nodes, which are farther than a single hop, specially conFig.d routing protocols are engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology. Two kinds of attacks can be launched against ad-hoc networks, Passive and Active. In passive attacks the attacker does not disturb the routing protocol. It only eavesdrops upon the routing traffic and endeavours to extract valuable information like node hierarchy and network topology from it. In active attacks, malicious nodes can disturb the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information, and by impersonating other nodes.

Security in mobile ad-hoc wireless networks is a two-fold problem. One is the security of the routing protocols that enable the nodes to communicate with each other and the second is the protection of the data that traverses the network on routes established by the routing protocols.

II. Motivation

The nature of ad hoc networks make them vulnerable to various forms of attacks such as passive eavesdropping, active interfering, leakage of secret information, data tampering, impersonation and denial of service. Detecting the compromised node in a large scale Ad hoc network is severely challenged due to:

1. The nodes are constantly mobile.
2. The protocols implemented are co-operative in nature.
3. There is lack of a fixed infrastructure and a central concentration point where intrusion detection system can collect audit data.
4. There is no clear distinction between normal and anomaly in wireless networks.

The node after being part of the network could be compromised in such a way that the incorrect and malicious behaviour cannot be directly noted at all. Although the compromised nodes may appear to operate correctly, they may make use of the flaws and inconsistencies in the routing protocol. Malicious nodes can also create new routing messages and advertise nonexistent links, provide incorrect link state information and flood other nodes with routing traffic. Such failures are severe especially because they may come from seemingly trusted nodes, whose malicious intentions have not yet been noted. Hence the attacks to routing protocol can be further classified into two types. They are:

A. External Attack: An attack caused by nodes that do not belong to the network.
B. Internal Attack: An attack from nodes that belong to the network due to them getting compromised or captured [4].

III. AODV

AODV is perhaps 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 must send a packet to another node, it starts a route discovery process in order to establish a route toward the destination node. Therefore, it sends its neighbours a route request message (RREQ). Neighbouring nodes receive the request, increment the hop count, and forward the message to their neighbours, 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): a node that has received a RREQ message, with source address S from its neighbour 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 neighbour 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 [5].

IV. Security Threats in AODV

In this section, the security threats are illustrated and analysed for AODV routing protocol. A node is malicious if it is an attacker that cannot identify itself as a legitimate node due to the lack of valid cryptographic information. A node is compromised if it is an inside attacker who is behaving maliciously but can be identified

by the network as a legitimate node and is trusted by other nodes. A node is called selfish when it tends to deny its own resources for the benefits of other nodes in order to save its own resources. Since AODV has no security mechanisms several attacks can be launched against the AODV routing protocol:

A. Message tampering attack

An attacker can alter the content of routing messages and forward them with falsified information. for example, when forwarding a RREQ generated by a source node to discover a route to the destination node, an attacker can reduce the hop count field to increase the chances of being in the route path between source and destination so it can analyze the communication between them. A variant of this is to increment the destination sequence number to make the other nodes believe that this is a 'fresher' route.

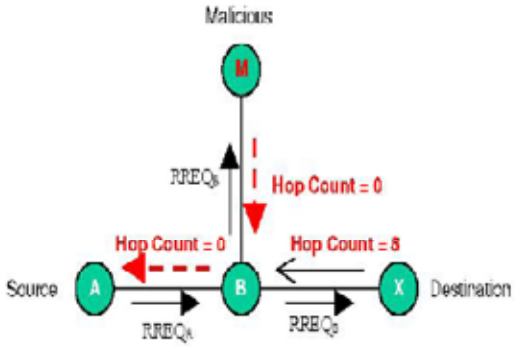


Fig. 1: Message tampering attack

B. Message dropping attack

Both attackers and selfish nodes can intentionally drop some (or all) routing and data messages. Since all the mobile nodes within a MANET function as both end hosts and router, this attack can paralyze the network completely as the number of message dropping increase.

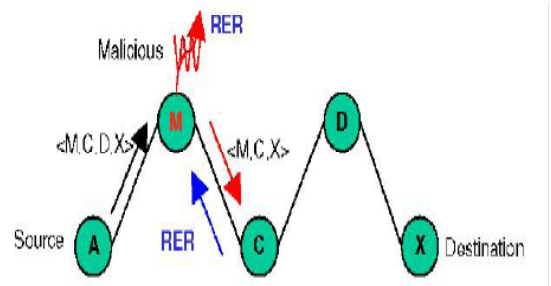


Fig. 2: Message dropping attack

C. Message reply attack

Attackers can retransmit eavesdropped messages again later in a different place. One type of reply attacks is the wormhole attack. A wormhole attacker can tunnel an RREQ directly to a destination node. Since a wormhole attacker may not increase the hop-count value, it prevents any other routes from being discovered. The wormhole attack can be combined with the message dropping attack to prevent the destination node from receiving packets.

The security requirements for AODV routing protocol include:

1. Source authentication: To be able to verify that the node is the one it claims to be.
2. Neighbour authentication: The Receiver should be able to confirm that the identity of the sender (i.e. one hop previous node) is indeed who or what it claims to be.
3. Message integrity: To be able to verify that the routing information that is being send, has arrived unaltered.
4. Access control: It is necessary to ensure that mobile nodes seeking to gain access to the network have the appropriate access rights.

V. Secure AODV Routing Protocol

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

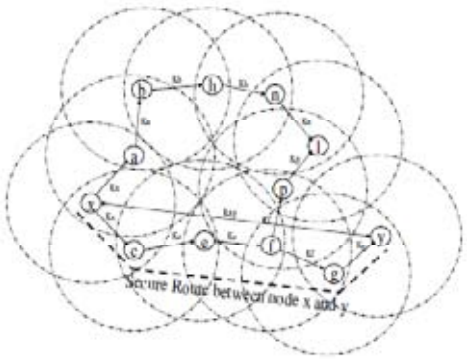
1) Key Exchange
2) Secure Routing
3) Data Protection

1) Key Exchange: Most of the current key exchange protocols are dependent upon a central trust authority for initial authentication. 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. After this, the nodes can negotiate session keys among each other, without any reliance on the CA, using any suitable key exchange protocol for ad-hoc networks. These session keys are used for securing the routing process and subsequently the data flow. To avoid multiple peer-to-peer encryptions during broadcast or multicast operations, a group session key may be established between immediate neighbours using a suitable Group Keying Protocol. This mechanism absolves the ad-hoc network of superfluous requirements and provides necessary elements to secure both routing and data in presence of malicious nodes by providing security services like authentication, confidentiality and integrity.

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 a ROUTE REQUEST packet, each intermediate recipient node retransmits the packet, if not a duplicate, and the final destination unicasts a ROUTE REPLY packet back to the original sender. For route maintenance it uses ROUTE ERROR packets that inform active users of route failures. The ROUTE REQUEST and ROUTE REPLY packets are usually modified by the intermediate nodes so as to add necessary routing information to these packets. The core security related problems linked to ad-hoc network originate due to the route development by the intermediate nodes. It is therefore, imperative that only authorised 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.

3) Data Protection: Once protected routes have been established, secure data transfer is relatively straightforward. To ensure connection confidentiality a source node adopts the following steps:

1) Any Node 'x' desiring to establish an end-to-end secure data channel, first establishes a session key Kxy with the intended Node 'y' using the key exchange protocol.



"Fig. 3: Point-to point Establishment of Secure Routes"

2) It then symmetrically encrypts the data packet using the session key Kxy and transmits it over the secure route.
3) The intermediate nodes simply forward the packet in the intended direction.
4) When the encrypted data packet reaches the destination it is decrypted using the session key Kxy.
5) Steps 2 to 4 are followed for all further data communication. [2]

There are two options available for obtaining the session key for secure data exchange.

Following symbols will be used in the proposed options, source (S), destination (D), session key (KS), encrypted session key (KE). KAX public key of x, KBX private key of x, where X is either source or destination. EK encryption using key K, DK decryption using key K.

Option 1

A source generates RREQ, attaches its certificate and sends it for route discovery of destination. In addition source also requests for a session key from the destination node. The intermediate nodes rebroadcast the RREQ packet in accordance with the operation of AODV protocol. On receipt of RREQ, the destination node verifies the certificate of source and on confirmation generates a session key. The destination also encrypts the session key with the public key of the source (KE = EKAS (KS)). The destination finally sends RREP including encrypted session key to the source. On receipt source decrypts the encrypted session key by its private key and obtain the session key (KS = DKBS (KE)). The obtained session key will finally be used for secure data exchange (Fig. 4).

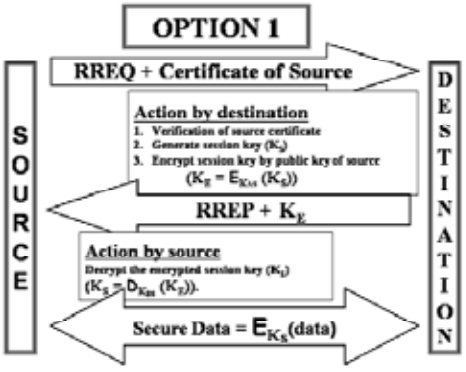


Fig. 4: Routing, generation of session key and encryption of session key in Option 1

Option 2

Source generates RREQ, attaches its certificate and sends it for route discovery of destination. Source also attaches a request for a session key from the destination node. The intermediate nodes rebroadcast the RREQ packet in accordance with the operation of AODV protocol. On receipt of RREQ, the destination node verifies the certificate of source and on confirmation generates a session key. Destination encrypts the session key with its private key as (KE1= EKBD (KS)) and further encrypts KE1 with the public key of the source as (KE = EKAS (KE1)). Destination respond with RREP attach its certificate and encrypted session key KE.
On receipt, source confirms the authenticity of destination from its certificate, decrypts the session key first through its private key and then through public key of destination as (KE1= DKBS (KE)) and (KS= DKAD (KE1) respectively. Finally session key is obtained that will subsequently be used for secure data exchange (Fig. 5 & 6).

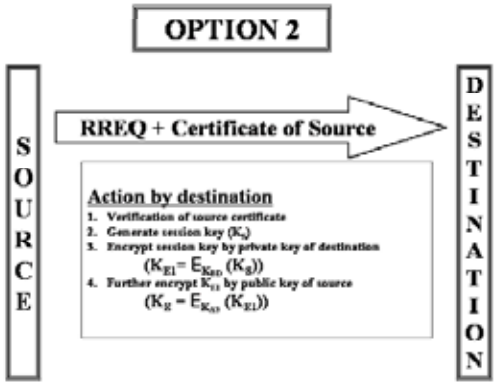


Fig.5: Generation of RREQ, session key and encryption of session key

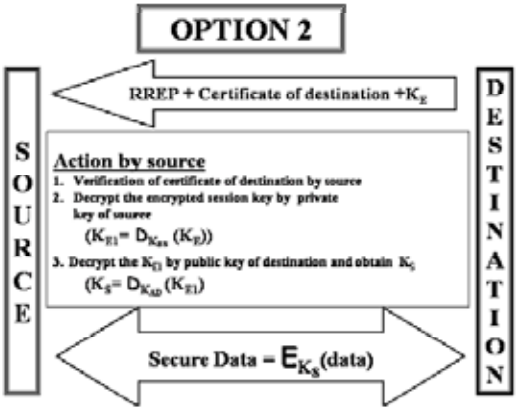


Fig.6: RREP, decryption of session key and exchange of secure data

VI. Conclusion

In this paper we have presented a scheme for securing the Ad-hoc On-Demand Distance Vector routing protocol used in mobile ad-hoc wireless networks. The secure AODV protocol provides requisite measures for protection of route discovery and transfer of data. These measures can be exercised independently without a central trust authority with nodes negotiating session keys independently. Nodes are, however, required to register themselves once with a Certification Authority, prior to joining a network. The scheme is based upon point-to-point and end-to-end encryption using symmetric key-based mechanisms. SAODV is effective in preventing control message tampering and adapt dropping attacks under TCP traffic.

References

[1] E. M. Royer, C. K. Toh, "A Review of current routing Protocols for ad hoc mobile wireless networks, IEEE Personal Communications Magazine ,vol. 6, no. 2, pp. 46 -55, 1999.

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

[3] Xinjun Du, Ying Wang, Jianhua Ge, Yumin Wang, "A Method for Security Enhancements in AODV Protocol", in Proceedings of the 17th International Conference on Advanced Information Networking and Applications, 2003

[4] Sonali Bhargava, Dharma P. Agrawal, "Security Enhancements in AODV protocol for Wireless Ad Hoc Networks", IEEE, 2001

[5] Davide Cerri, Alessandro Ghioni, CEFRIEL — Politecnico di Milano, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE Communications Magazine, February 2008

[6] Li pengwei, Xu zhenqiang, "Security Enhancement of AODV against Internal Attacks", Natural Science Foundation of He'nan Educational committee, 2010 IEEE

[7] N. Ch. Sriman Narayana Iyengar, "An Efficient and Secure Routing Protocol for Mobile AD-hoc Networks",in International Journal of Computer Networks and Communications,Vol 2, No.3, May 2010

[8] Y. C. Hu, A. Perrig, D. B. Johnson, "Ariadne: A secure ondemand routing protocol for ad hoc networks," Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 12–23, 2002.

[9] Charles E.Perkins, Samir R.Das, Elizabeth Royer, "Ad-hoc on demand distance vector (aodv) Routing", Internet Draft, IETF Mobile Ad Hoc Networking Woring Group, November 2001.

Preeti Bathla received her B.Tech degree in Computer Science and Engineering from N.C College of Engineering, Israna, Panipat in 2008, and pursuing M.Tech in Computer Science And Engineering from N.C College of Engineering, Israna, Panipat At present, She is Lecturer in Computer Science and Engineering Departmaent in N.C College of Engineering, Israna, Panipat.

Bhawna Gupta received her B.Tech degree in Computer Science and Engineering from N.C College of Engineering, Israna, Panipat in 2001, and M.Tech in Computer Science and Engineering from Vanasthali Vidhyapeth Rajasthan.At present,She is pursuing Ph.D. from Thapar University . She is A.P. in Computer Science and Engineering Departmaent in N.C College of Engineering, Israna, Panipat. University,