STUDY OF SECURITY ENHANCEMENT IN AODV ROUTING PROTOCOL IN AD HOC NETWORKS

Jayashree Agarkhed
Professor, Department of Computer Science & Engineering, P.D.A College of Engineering, Kalaburagi, India

ABSTRACT

Ad hoc network is a dynamically formed network by collection of movable nodes with changing topology, due to nodes mobility and without having centralized administration. Nodes communicate by exchanging data with another node, establishing multi hop network. This type of communication needs vigilant design of routing protocols to satisfy various Quality of Service (QoS) parameters. There is a need to satisfy request of finding a route that utilizes sufficient available resources to meet the QoS constraints in order to achieve low cost or most stable route in real time and military applications. The study of Ad hoc On Demand Distance Vector (AODV) routing protocol has been presented along with security enhancement to AODV routing protocols.

Key word: AODV, Routing, Security attack, Black hole, Sink hole.


1. INTRODUCTION

Mobile Ad hoc networks (MANET) consist of nodes with mobility and get interconnect by multi hop communication. Nodes in an ad hoc network communicate directly with each other in a peer to peer manner due to lack of fixed infrastructure. The intermediate nodes act as router to provide communication between source and destination node. Each node to identify itself, broadcast periodically a beacon packet. MANET has wide range of applications such as commercial, health and industrial applications with cooperative huge mobile data exchange.

There is a demand for existing and future application in military networking for robust, IP-compliant data services within these wireless mobile networks [1]. These networks consist of dynamic autonomous topology. Wearable computing provides wide applications for MANET technology. MANET technology when combined properly with satellite information system, provide a method for flexible communications establishment to assure safety operations with efficient, survivable, dynamic networking. Most of the applications of
MANET find ad hoc on demand distance vector AODV as attractive routing protocol. It combines features of DSR for route discovery and route maintenance with appropriate mechanism and use sequence numbers and periodically updates packets as supported by DSDV. The main benefit of AODV over DSR is the source route does not need to be included with each packet. This results in a reduction of routing protocol overhead.

Due to some of stringent characteristics such as mobility, openness and dynamic topology, Ad hoc networks are prone to be vulnerable and unstable. Thus providing security has became one of the biggest issue as it is more difficult to design and implement various security solutions for Ad hoc networks than for any wired networks. This motivates to enhance security using AODV routing protocol.

The paper has been organized as follows. Section II specifies about related work being done. Section III describes about the working of AODV. Section IV presents types of attack detection and attack prevention in AODV. Section V highlights the conclusion.

2. RELATED WORK
As routing is an important component in MANET and numerous routing protocols have been presented in MANET for different application, which are affected from different attacks. In military applications, the motes in WSNs and MANET are dispersed into a unsafe adversary’s territory for detecting and tracking the enemy and their vehicles. In some indoor environments, these sensor networks are spatially deployed to detect intruders by means of a wireless security system. WSNs and MANET are networks that are most unattended and reachable physically from the outside world, and are likely vulnerable to many security threats and attacks. Thus there is need to be protect node from an intruder and also to provide secured delivery of real time data. AODV is one of the most suitable routing protocols for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. In [2], the author analyzed and improved the security of AODV routing protocol and presented the effects of black hole attack in MANET

In [3] author analyzed sinkhole problem, its effect on AODV protocol & prove that performance of AODV is improved after applying the proposed mechanism which is deteriorated due to attack. Also presented observation variation in the values of various performance metrics such as packet drop ratio (PDR), end to end delay, throughput and packet loss, by varying number of nodes from 10 to 50 and found that the performance of AODV is degraded heavily specially for 40 and 50 nodes under attack.

In [4] author specified that the AODV protocol does not incorporate any specific security mechanism and strong authentication mechanism. There is no obvious way to prevent mischievous behavior such as medium access control (MAC) spoofing, IP spoofing, dropping packets, or altering the contents of control packets. The author has proposed the tool that monitors network packets to detect local and distributed attacks within its radio range.

In [5] author shown that technique proposed by Security Enhancement in AODV protocol works better than the existing AODV technique by detection of black hole nodes. The results analyzed based on parameters detection and the results are recorded considering based on packet drop rate and packet delivery ratio.

Security issue has to be considered when MANET is employed into aerospace fields and military application. The author in [6] has designed a secure routing protocol Trusted AODV (TAODV) for MANET that extends the basic routing protocol AODV. In TAODV nodes use the trust relationships among themselves does not perform request and certificates...
verification every time. This helps to reduce large the computation overheads. The other neighbor nodes trust the relationship and make judgment about other node’s trustworthiness to maintain the whole system at a certain security level.

In [7] author considered a slight improvement for the routing table and the routing messages of ADOV by adding trust information. This information is updated by monitoring the neighborhood. When performing trusted routing discovery, unlike those cryptographic schemes that perform signature generation or verification at every routing packet, this method just combine the recommended opinions together and make a routing judgment based on each element of the new opinion. This helps to reduce computation overhead and provide guaranteed trustworthiness of the routing procedure. The security and selfishness issues of wireless networks are implemented either in non-cooperative form or in cooperative form which resulted in increase of cumulative utilities of cooperative nodes.

For the design of efficient routing protocol, different design issues, characteristics and QoS requirements [8] are to be considered as discussed in next section.

3. WORKING PRINCIPLE OF AODV

AODV routing protocol provides efficient communication among node in Ad hoc network. The routing protocol is subject to some the issues and challenges due to wireless mode of transmission. For efficient design of routing protocol one has to consider design issues as discussed below.

3.1. Design Issues

- Resource estimation: During route establishment, estimation of available bandwidth to a node or link and delay must be done. Bandwidth available to a link or node dynamically vary which in turn affects by the traffic of its neighboring nodes.

- Route discovery: Route discovery is based on choice of routing. Proactive routing leads to increase overhead with less delay. Reactive routing at the expense of more delay reduces routing overhead. To support QoS aware routing it is desirable to achieve routing with less overhead and latency. This is achieved by AODV reactive routing protocol.

- Resource reservation: The fair distribution of resources among hosts in Ad hoc networks is one of the challenging issue. To overcome this problem resource reservation scheme can be used to set and maintain QoS-aware routing.

- Route maintenance: In MANETs, mobility of nodes causes topology to change frequently, making it difficult to meet the QoS constraints. Biggest design issue is incorporating fast route maintenance scheme which discover a route break up.

- Route selection: As topology change causes route failures and affects the end-to-end QoS, there is need to avoid route failure. For efficient design of QoS aware routing the route with maximum available bandwidth has to be considered

- Route failure notification: Routing protocol must provide information about remaining bandwidth or estimation of route delay through feedback to the application.

3.2. Working of AODV

Only when a mobile terminal has packets to send to a destination does it need to discover and maintain a route to that destination terminal. In AODV, each terminal contains a route table for a destination. A route table stores the following information: destination address and its sequence number, active neighbors for the route, hop count to the destination, and expiration
time for the table. The expiration time is updated each time the route is used. If this route has not been used for a specified period of time, it is discarded.

3.3. Working Principle
When a source node desires a route to a destination, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node in its table and set up backwards pointers to the source node in the route tables. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. It unicast a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ’s source IP address and broadcast ID [9]. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As soon as RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

To transmit packet to destination, node first, checks its routing table in order to determine presence of a route to the destination. If route to destination is present, it forwards data packet to its neighbor. If route not present, broadcast RREQ (route request) to initiate route discovery. The format of RREQ is as shown in figure 1. [10].

![Figure 1 RREQ format](image)

During route discovery process, it broadcasts RREQ to all its neighbors for specified destination. The RREQ is then flooded throughout the network at once. An intermediate node on receiving a RREQ, checks its routing table, to find route to destination. If destination is found then it sends RREP to source by setting up a reverse route path to source node in its route table. If not found, intermediate node rebroadcast RREQ to its neighbor nodes. The intermediate node ignores RREQ if it has processed already [11]. The process is repeated till destination node is found and on reaching destination node with RREQ, the destination node unicast RREP (route reply) to source node. For unicast it uses reverse route to reach source node. The format of RREP is as shown in figure 2.

![Figure 2 RREP format](image)

Nodes also carry out route maintenance phase in which the active nodes periodically broadcast hello message. If not got hello message from a neighbor, then the next upstream
node will inform the source with an RERR packet and entire routes based on the node is cancelled. Source node starts again initializing a new route discovery stage and then floods RREQ packet. The format of RERR is as shown in figure 3.

![Figure 3 REER format](image)

Considering these characteristic, the basic AODV based routing algorithm is explained as follows.

Algorithm: AODV routing algorithm

Step 1: Start

Step 2: Neighbor node identification

Step 3: Find route to destination
   - Step 3.1: Broadcast RREQ to neighbor nodes
   - Step 3.2: If route present, neighbor sends RREP to source
   - Step 3.3: If no route, neighbor initiates route discovery

Step 4: For route discovery by intermediate node, go to step 3.

Step 5: Data transmission phase
   - Step 5.1: Transmit data to next hop neighbor
   - Step 5.2: If route break identified
     - Step 5.2.1: Notify the source with an RERR.
     - Step 5.2.2: Go to step 3

Step 6: Performance evaluation

Step 7: End

**Advantages**

- Support unicast and multicast routing
- Uses sequence numbers to ensure the freshness of route
- It is loop-free, self-starting, and scales
- It maintains one entry per destination

**Limitations**

- Each intermediate device has to maintain route table

**4. TYPES OF DETECTION AND PREVENTION OF ATTACKS IN AODV**

AODV routing protocols in Ad hoc network needs to provide reliable communication is one of the issues to be considered. The various detection and prevention method in AODV are discussed next.
4.1. Sinkhole Attack Detection & its Prevention

Considering the behavior of sinkhole attack and working of AODV the mechanism for detection and prevention of sinkhole attack is specified. In [10] detection mechanism consists of four phases as Initialization, Storage, Investigation, and Resumption Phase. A sinkhole detection algorithm can be placed at source, intermediate and destination nodes in the network and performs detection in phases as explained step wise below.

- Initialization phase: It is first phase. In this phase AODV performs its route discovery phase by sending the RREQ to all its neighbors in order to find shortest and new path to destination.
- Storage phase: In this phase AODV stores information regarding each RREQ in the nodes routing table. Each entry mainly includes sequence number, hop count & node id. The routing table apart from this information also stores other information as destination sequence number, hop count, source and destination address.
- Investigation phase: This third phase begins as examination of source sequence number of current and previous request and then it considers difference between them. If it is found that source sequence number of current route request is too large compared to previous request then the node from which current route request has been received is assumed as malicious and the entry for this RREQ is not considered from routing table.
- Resumption Phase: This last phase of algorithm acts as final phase of algorithm. It is known as resumption phase and starts by calling send Request of default AODV and AODV starts performing its operation in normal way [12].

4.2. Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks

The State Transition Analysis Technique (STAT) designed to model host-based and network-based intrusions in a wired environment [13] is used as a basis for an intrusion detection tool, called AODV-STAT which detects attack against the AODV routing protocol in wireless ad hoc networks. A Subset of nodes have been deployed in the AODVSTAT sensors network. In AODVSTAT, events are either data packets or AODV control messages which are exchanged over a wireless network. An AODVSTAT sensor has two modes of operation. The first mode called stand-alone mode and second mode called distributed mode. In stand-alone mode, a sensor node identifies attacks within its immediate neighborhood.

The update messages consisting of details of the neighboring nodes of each sensor node are exchanged periodically in distributed mode. This update messages enclose the list of known MAC/IP pairs, the number of hops to required to known nodes, and information about local attacks that are detected. This information can then be used to detect attacks in a distributed fashion [4].

4.3. Blackhole Detection and Prevention

A Blackhole detection and prevention scheme proposed in [5] helps to detect and prevent the black hole attacks in the mobile ad hoc network. The source node requests one of the backbone nodes for a restricted IP address whenever the node wants to make a transmission. After confirmation of RIP (Restricted IP Address), the source node sends dummy packets to all the intermediate nodes and packet loss is checked. If it is greater than the threshold value then the node is added to the blacklist. The proposed scheme to detect the black hole nodes and prevents the packet dropping in the network. Here the specified method has helped to improve the number of packets received and the Packet Delivery Ratio.
4.4. Trust Based Secure Model (TAODV)
In MANET each relays on its neighbors for routing message. These nodes should cooperate with each other without centralized control. The nodes may be subjected to major vulnerability. To provide security, trust value plays a important role in all activities of the network and network known as trusted network. TAODV is modified version of AODV to support trusted node and trusted route. To calculate trust value node's performance and collection of neighbor node's opinion value are evaluated and used to identify the trust relationship of one node with other node. TAODV establish a perfect trust model to build secure route between source and destination that cannot be subjected to any intruder or malicious nodes [7].

5. CONCLUSIONS
In MANET, the mobile nodes communicate with other node in an infrastructure less environment. The communication among node should be trust worthy. Providing communication among nodes using standard routing protocols in Ad hoc network is challenging due to mobility of nodes. This can be achieved by AODV routing protocol as discussed in this paper highlighting security aspects to be considered in order to provide trusted and secure transmission among nodes in dynamically changing network environment.

REFERENCES


