Information Technology Journal 3 (2): 142-145, 2004
ISSN 1682-6027

Secure Route Path Formation in Ad hoc On-demand Distance Vector Routing Protocol

Muhammad Asfand-e-Yar and Muhammad Sher
Department of Computer Science, International Islamic University, Islamabad, Pakistan

Abstract: This study describes the secure route path formation in the Ad hoc On-demand Distance Vector routing protocol. For secure route path formation in Ad hoc On-demand Distance Vector Routing Protocol (RSA) for encryption is used. The Secure Ad hoc On-demand Distance Vector (SAODV) is an extension in Ad hoc On-demand Distance Vector routing protocol that is used to protect the route path from integrity and authentication attacks. Ad hoc network maintains a routing table giving distance from itself to all possible destinations. In Ad hoc On-demand Distance Vector routing protocol the route discovery is done by route request and reply packets. After establishing a route the communication between source and destination takes place. Ad hoc On-demand Distance Vector routing protocol solves the loop formation. It works on wired as well as on wireless networks.

Key words: Ad hoc On-demand distance vector algorithm, route discovery, secure route, security attacks

INTRODUCTION

Ad hoc wireless networks are self organizing multi hop wireless networks where all hosts take part in the process of forwarding packets. Ad hoc networks can easily be developed since they do not require any fixed infrastructure, such as base stations or routers[1]. Ad hoc network is a collection of mobile nodes that communicate with each other with out any centralized administration. Ad hoc networks use different types of protocols like Distance Vector (DV), Distance Sequence Distance Vector (DSDV), Dynamic Source Routing, On-demand Distance Vector Routing Protocols.

In DV routing, each router maintains a routing table giving the distance from itself to all possible destinations. In route path formation loops are formed between source and destination. RIP (Routing Information Protocol) handles these routing loops. DSDV solves the looping problem in DV routing by attaching Sequence number to routing entries. Node increments its current sequence number and includes it in the updates originated at that node. This method in DSDV increase routing overhead[2,3]. Ad hoc On-demand Distance Vector routing protocol (AODV) is introduced which solves the looping and routing overhead problems.

The AODV routing protocol provides quick and efficient route establishment between nodes desiring communication. AODV is designed specifically for ad hoc wireless networks; it provides communication between mobile nodes with minimal control overhead[4]. When a path is formed by the route request and route reply packets in AODV routing protocol, then the communication starts between source and destination. If any hacker is sitting in the network and wants to steal data from source and destination then it can easily change the route path, by adding its own address in the route and increasing the hop count. By this hacker can easily get information from source and destination. To get rid of this attack we make the route authentic and secure. For authentication we use the Secure Hash Algorithm (SHA), which help us to make check sum of packet header and for security we use the Revist Shamir and Adleman (RSA) algorithm which encrypt the source and destination address and make difficult for the hacker to know the source or destination node.

Ad hoc On-demand Distance Vector Algorithm: In AODV algorithm the nodes do not have to discover and maintain a route until the two nodes, need to communicate and the former node is offering its service as an intermediate forwarding station. The primary objectives of algorithm are:

- To broad cast discovery packets only when necessary.
- To distinguish between local connectivity management and general topology maintenance.
- To disseminate information about changes in local connectivity to those neighboring mobile nodes that is likely to need the information.

Corresponding Author: Muhammad Zaheer Aziz, Department of Computer Sciences, Faculty Block 2, International Islamic University, Islamabad, Sector H-10, Islamabad, Pakistan

Instead of source routing, AODV relies on dynamically establishing route table entries at intermediate nodes[5] .

Route discovery: In AODV the route discovery is purely on demand and follows a route request/reply discovery cycle. The route requests are sent using the Route Request message (RREQ) and the reply is sent back by the Route Reply message (RREP). When a node wants to make a route to destination then it sends packet. Before sending a packet it checks the Route table whether it has a current route to that node. If so, it forwards the packet else it initiates a route discovery process. This packet contains the following instructions (Fig. 1).

Type 8 bits	J 1 bit	R 1 bit	Reserved 14 bit	Hop Count 8 bits	Broad cast ID 32 bit
Destination IP address 32 bits		Destination sequence No. 32 bits		Source IP address 32 bits	Source sequence No 32 bits

Fig. 1: Route request packet

After receiving the packet then it sets the reverse route entry form the source node in its route table. The route reply packet contains the following information (Fig. 2).

Type 8 bits	R 1 bit	Reserved 10 bit	Ptx length 5 bits	Hop Count 8 bits	Destination IP address 32 bits
Destination Sequence No 32 bits		Source IP Address 32 bits		Source sequence No 32 bits	Life Time 32 bits

Fig. 2: Route reply packet

To response the RREQ, the node must have the unexpired entry for the destination in its route table. Also the sequence number associated with that destination must be latest that indicated in the RREQ packet. This prevents the formation of routing loops. It must be also sure that the route returned is never old enough that points to a previous intermediate node. If the node is able to satisfy these two conditions then it responds by unicasting a route reply RREP back to the source, otherwise the RREQ hop count is incremented and broadcast the packet to its neighbor[4].

Loop freedom: AODV play a key role in ensuring loop freedom. Every node maintains a single increase sequence number for itself and also maintains highest sequence number for each destination in routing table (i.e. "destination sequence number"). This increase of sequence number along a valid route prevents routing loops.

If (($seqnum^d_i$<$seqnum^d_j$) or
  (($seqnum^d_i$=$seqnum^d_j$) and
  ($hopcount^d_i$>$hopcount^d_j$))
then
    $seqnum^d_i$:= $seqnum^d_j$;
    $hopcount^d_i$:= $hopcount^d_j$ +1;
    $nexthop^d_i$:= j;
endif.

Fig. 3: AODV route update rule

A node can receive a routing update via a RREQ or RREP packet either forming or updating a reverse or forward path. The update rule (Fig. 3) is invoked upon receiving a route request or reply packet. It is easy to see why loops cannot be formed if this rule is followed. Consider the tuple (-$seqnum^d_i$, $hopcount^d_i$) where $seqnum^d_i$ represent the sequence number at node i for the destination d. Similarly, $hopcount^d_i$ represents the hopcount to the destination d from node i. For any two successive nodes i and j on a valid path to the destination, j being the next hop from i to d, the route update rule (Fig. 3) on forces that

(-$seqnum^d_i$, $hopcount^d_i$) >
(-$seqnum^d_j$, $hopcount^d_j$)

where the comparison is in the lexicographic sense. Thus, the tuples (-$seqnum^d_i$, $hopcount^d_i$) along any valid route are in a lexicographic total order, which in turn implies loop freedom[6].

Secure routing: In Ad hoc networks there must be two security systems, one to protect the data transmission and other to make the routing secure[7]. Here we are concerned with the secure route communication not with the protection of data transmission. First it should be described that what security measures are needed for AODV routing protocol. It is needed to have the authentic route. It is also desired to avoid tampering attacks like reusing of packet; this can be solved by using the sequence number in AODV. In the Ad hoc network it is impossible to prevent denial of service attacks[8].

AODV protocol is under consideration of Internet Engineering Task Force (IETF), therefore it is not standardized for the internet or intranet communication[6]. We made changes in the routing packet header of AODV for secure route communication. In the request and reply

packets we introduced the authentication and encryption algorithm.

In SAODV protocol the route is made on-demand of source node. Therefore, the RREQ packet is send to the neighboring node with Source Address, Destination Address and with other instruction to the neighboring node (Fig. 1). Neighboring node transmits the RREQ packet to other nodes, till the destination is reached. Then the destination replies to source by route reply packet (Fig. 2). The source node discards all other entries of neighboring node when the destination reply is reached. After defining route path the source node encrypts the source address, destination address and hop count by RSA algorithm[9] and then embed the public key and encrypted data with in the packet header. This security is done so, that any other node may not easily configure the source address, destination address and the hop counts to the destination node. The secure request packet (SREQ) (Fig. 4):

Type 8 bits	J 1 bit	R 1 bit	Reserved 14 bit	Offset Hop Count 8 bits	Broad cast ID 32 bit
Destination IP address 32 bits		Destination sequence No. 32 bits		Get Source IP address 32 bits	Source sequence No. 32 bits
Signature (Encrypted source add and Hop count) 80 bits				Public Key 8 bits	

Fig. 4: Secure request packet

Then source node transmit SREQ packet to destination. When SREQ packet is received by the destination it performs the check sum of packet and then decrypts the packet by public key sent by source node. On second time when the source packet needs to transmit SREQ packet it done not need to attach the public key of RSA algorithm (Fig. 5). This will make less load on routing traffic. When the destination receives the SREQ packet it replies to source by the following secure reply packet (SREP) (Fig. 6).

Type 8 bits	J 1 bit	R 1 bit	Reserved 14 bit	Offset Hop Count 8 bits	Broad cast ID 32 bit
Destination IP address 32 bits		Destination sequence No. 32 bits		Get Source IP address 32 bits	Source sequence No 32 bits
Signature (Encrypted source add and Hop count) 80 bits					

Fig. 5: Secure request packet 2

Type 8 bits	R 1 bit	Reserved 10 bit	Pfx Length 5 bits	Offset Hop Count 8 bits	Destination IP address 32 bit
Destination sequence No 32 bits		Signature (Encrypted source add and Hop count) 80 bits		Source sequence No 32 bits	Life Time 32 bits

Fig. 6: Secure reply packet

The security can be increased by increasing the number of bits in RSA algorithm. This will make more difficult for the hacker to decrypt the signature field in the SREQ or SREP. The secure communication takes place between source and destination (Fig. 7), after the route establishment.

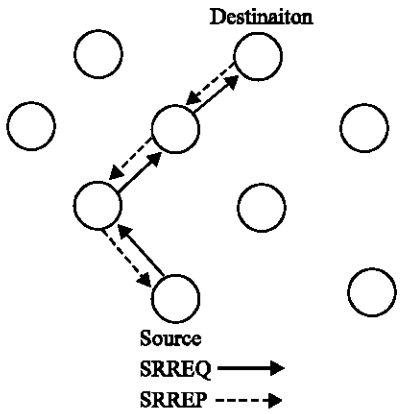

Fig. 7: Route path of SAODV

The route path is maintained by the hello packets. These hello packets will make the route active till the source needs. The hello packets and route error packets are same as the AODV routing protocol use. The only extension in the SAODV is the addition of signature field in the packet header. In SAODV routing communication the hacker can not get the source and destination addresses due to signatures and authentication make the route path authentic, by which any intruder can't enter in route path.

SAODV is a secure route path formation protocol, of AODV. It is used for the authentic route formation and signature prevents attacks of integrity and non-repudiation. Hacker can not easily get the source and destination address from SAODV packet header, which could be done in AODV routing packet.

SAODV routing protocol simulation works only on unicast routing path. This simulation is the secure route communication between the source and destination.

Further work is to done on the multicast routing path formation. In which one source or multi source nodes communicate with multi destination nodes.

REFERENCES

1. Baruch, A., C. N. Rotaru, D. Holmer and H. Rubens, 1998. An On Demand Secure Routing Protocol Resilient to Byzantine Failures. ACM Press. New York NY, USA.
2. Charles, E.P., E.M. Royer and S.R. Das, 2000. A Performance Comparision of Two On demand Routing Protocols for Ad Hoc Networks. In Proceeding of the IEEE Conference On Computer Communication (In Focom), Tel Aviv, Israel, pp: 3-12.
3. Rajendra, V.B. and S.P. Kondum, 2001. An Adaptive Distance Vector Routing Algorithm for Mobile, Ad Hoc Networks, IEEE Infocom.
4. Charles, E.P. and E.M. Royer, 1999. Ad Hoc Networking. Prentice Hall of India Private Limited New Delhi, pp: 173-219.
5. Charles, E.P. and E.M. Rouer, 1999. Ad hoc On-Demand Distance Vector Routing. In Proceeding of the 2nd IEEE workshop on Mobile Computing Systems and Applications, New or leans LA.
6. Mahesh, K.M. and S.R. Das, 2001. On demand Multipath Distance Vector Routing in Ad Hoc Networks. In Proceeding of IEEE International Conference on Network Protocols (ICNP), pp: 14-23.
7. Manel, G.Z., 2001. Secure Ad hoc On-demand Distance Vector Routing, IETF internet Draft draft-guerrero-manet-saodv-00.txt (work in progress).
8. Elizabeth, G.V., R.A. Kemmerer and S. Gwalani, 2000. AODVSTAT: Intrusion Detection in AODV, In Proceedings of the 23rd National Information System Security Conference.
9. Williani, S., 1993. Network and Internet work Security. The McGraw Hill Companies, Inc.