A Method for Security Enhancements in AODV Protocol

Xinjun Du Ying Wang Jianhua Ge Yumin Wang
ISN NK Laboratory, XiDian University
dxjwy2002@hotmail.com, dxjwy@163.net

Abstract

An ad hoc network is a collection of wireless computers(nodes), communicating among themselves over possibly multi-hop paths, without the help of any infrastructure. Although many ad hoc network routing protocols have been proposed(DSR, AODV, ZRP etc), none of them considers the security problems. In this paper we put forward an efficient security mechanism based on the AODV routing protocol. In this security mechanism the double Hash authentications are adopted to protect routing information.

1. Introduction

Although many ad hoc network routing protocols(DSR[1], AODV[2], ZRP[3], LAR[4] etc.) have been proposed, they have generally assumed a trusted environment and no security mechanism has been considered. But in a hostile network environment (e.g., a battlefield), none but a secure ad hoc routing protocol can be used. Routing security was first studied in the seminal work of Perlman[5], who studied the security of the flooding and shortest-path routing algorithms and proposed the solution based on PKI. In this solution the digital signature technique is used to protect routing information.

Using the digital signature technique to protect routing packets in intuitive, but not efficient especially in a mobile wireless ad hoc network. nodes cooperate to forward packets for each other, due to the limited wireless transmission range of each individual node. On the other hand, the resources of an ad hoc network are limited, including network bandwidth and the CPU processing capacity, memory, and battery power(energy) of each individual node in the network. Expensive and cumbersome security mechanisms, like the digital signature technique, can delay or prevent exchanges of routing information, leading to reduced routing effectiveness, and may consume excessive network or node resource, leading to many new opportunities for possible Denial-of-Service(DoS) attacks through the routing protocol[8].

Based on the AODV protocol we propose a new security mechanism. In this scheme, we improve the flooding algorithm, and adopt the fast cryptographic tools, hashing, to protect routing information.

2. AODV protocol

Ad hoc On-demand Distance Vector Routing protocol is a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchange.

When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to located the other node. It broadcasts a route request(RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. Figure1(a) illustrates the propagation of the broadcast RREQs across the network. AODV utilizes destination sequence number to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies a RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ.

During the process of forwarding the RREQ, intermediate nodes recode in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by unicasting a route reply(RREP) packet back to the neighbor from which it first

Proceedings of the17 th International Conference on Advanced Information Networking and Applications (AINA'03)
0-7695-1906-7/03 $17.00 © 2003 IEEE

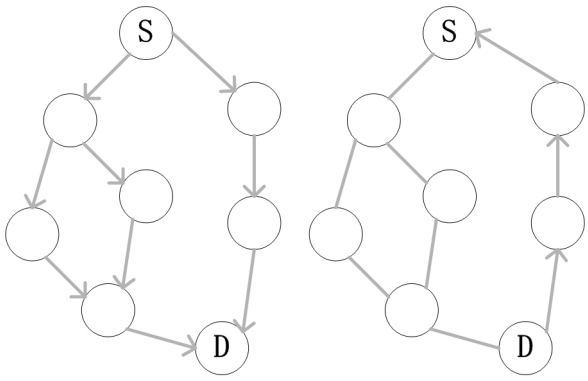

Figure 1. Figure1 AODV route discovery

received the RREQ(Figure1(b)). As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route table which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forward along the path established by the RREQ, AODV only supports the use of symmetric links.

Based on the AODV protocol we improve the flooding algorithm to make it more efficient and use efficient one-way Hash functions to protect routing information. Before describing the scheme, we first introduce the management of the local node groups, for it is the base of the scheme.

3. The management of the local node groups

Each node in a wireless ad hoc network maintains two local node groups: one group includes the nodes within its one-hop range, this could be done by sending the beacons periodically, the other group includes the nodes within its two-hop range, but not within its one-hop range, this can be achieved through the flowing processes. The neighboring node(within each other's radio range) exchange their one-hop node group each other, then each node can learn the nodes within its two-hop range. For example, in Figure2, node $S's$ one-hop node group is $O_s = \{A, B, C, D, E\}$. Though exchanging one-hop node group with its neighboring nodes, S can learn $O_A = \{S, E, F, G\}$, $O_B = \{S, C, H, I, J\}$, $O_C = \{S, B, D, J, K\}$, $O_D = \{S, C, E, L\}$, $O_E = \{S, A, M\}$. Then S can get its two-hop node group:

$T_S = (O_A \bigcup O_B \bigcup O_C \bigcup O_D \bigcup O_E) - O_S - \{S\}$
$= \{F, G, H, I, J, K, LM\}$

Because of the mobility of wireless ad hoc networks,

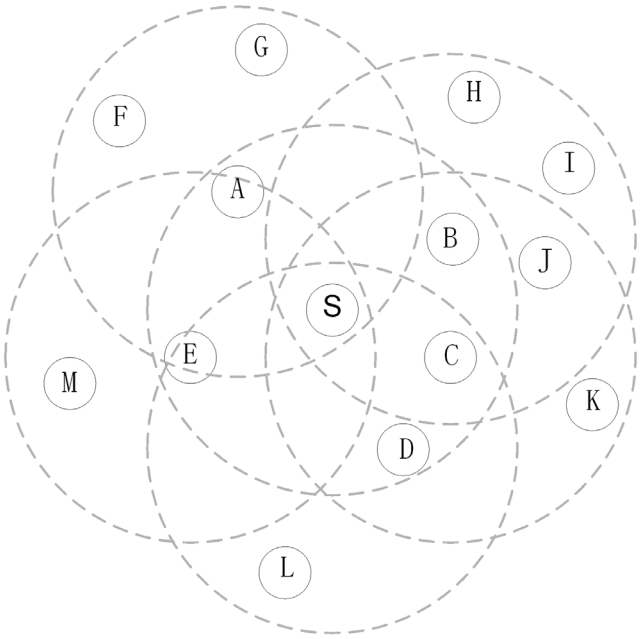

Figure 2. Figure2 The management of the local node groups

each node must maintain its local node groups timely. Certainly we should apply some security mechanisms, e.g. digital certificates, in this process to authenticate the nodes' identity.

4. Improving the flooding algorithm

The flooding algorithm is the important component in many routing protocols. In the original AODV protocol, the flooding algorithm is realized by using the broadcast. However, in the worst case, all the nodes in the network could take part in the route computation. At the same time, related work[6,7] has shown that the capacity utilization in ad hoc networks decreases significantly when broadcast relays or "broadcast storms" are performed frequently.

Based on the management of the local node groups, the multicast is used to realize the flooding algorithm. The source node and the intermediate nodes forwarding the RREQ need to calculate their multicast groups to which the RREQ is to be sent.

In Figure2, the source node S calculates its multicast group Z_S as follows:

$Z_S = O_S$;
for each node x and y in $Z - S$ do
    if $O_x \subseteq O_y$
        $Z_S = Z_S - \{x\}$

of course we suppose that the destination node does not include in O_S or T_S.

Proceedings of the17 th International Conference on Advanced Information Networking and Applications (AINA'03)
0-7695-1906-7/03 $17.00 © 2003 IEEE

When an intermediate node x receives a copy of RREQ from the node y, x can calculate its multicast group $Z_x = O_x - (O_y \bigcap O_x) - \{y\}$.

For a wireless ad hoc network using the multicast to realize the flooding algorithm can reduce the redundancy and overhead produced by the broadcast to some extent.

5. The security mechanism

The fast and efficient Hash function is adopted to authenticate routing information instead of the digital signature technique in this mechanism. Under the reasonable assumption that no two compromised nodes are colluding and are within two hops of each other, we adopt the double Hash authentications, one of which is used to authenticate the received routing packets and the other is used to prevent the current nodes modify the routing information themselves. If some compromised node modified the routing information, its neighboring nodes can detect this misbehavior immediately.

In an initialization phase, each node makes use of the management of the local node group to distribute the common secret with its two-hop node group.

5.1. Distribution of the common secret

In this scheme, each node needs to distribute a common secret shared by its two-hop node group. For example, node S needs to distribute a secret key K_S to its two-hop node group T_S. Because this secret key is kept secret against its one-hop node group O_S, the distribution can be based on PKI. Each node in the ad hoc network has a digital certificate signed by CA, i.e. each node has a pair(public key, private key), and the public key is widely known. Node S generates a random secret key K_S, and encrypts it with the public key of the nodes within T_S. Then, S seperately sends these encrypted keys to be nodes within T_S. On receiving the encrypted key each node decrypts it with the corresponding private key and gets the common secret K_S.

Because the mobility of the ad hoc network can result in the change of the local node groups, the distribution of the common secrets should be adjusted timely. First, when some new nodes join is two-hop node group T_S, S needs distributing K_S to these new nodes, second, if some nodes within T_S become the members of its one-hop node group O_S because of roaming, S needs refreshing and redistributing K_S.

5.2. Securing the flooding algorithm

A Public one-way Hash function $H(\cdot)$ is used to authentication RREQ twice, so a routing packet includes not only RREQ but also two Hash values (H_1, H_2), where H_2 is used to check whether the received routing packet has been modified and H_1 is used to prevent the current node modifying the packet.

For example, the source node S generates a $RREQ = \{s, j+1, h, M\}$, s is the identity of S, $j+1$ is the sequence number of this RREQ, h is the hop counter and M is the other routing information, then S multicasts $\{s, j+1, h, M, H_1, 0\}$ to its multicast group Z_S, any node x within Z_S can immediately verify the authenticity of the packet, for this packet is coming to x along the direct connection from S, so $H_2 = 0$. $H_1 = H(s|j+1|h|M|K_S)$ is to be used by the nodes within $x's$ multicast group Z_x to authenticate the packet, where K_S is the secret key share by S and its two-hop node group $T - S$.

Before the intermediate node x forwards the routing packet, it increases the hop count of RREQ by one and copy H_2 form H_1 and calculates the new hash value H_1. That is, $H_1 = H(s|j+1|h+1|M|K_x)$ and $H_2 = H(s|j+1|h|M|K_S)$, where K_x is the common secret key between node x and its two-hop node group T_x. Then node x forwards the routing packet $\{s, j+1, h+1, M, H_1, H_2\}$ to its multicast group Z_x.

On receiving $\{s, j+1, h+1, M, H_1, H_2\}$ the nodes within Z_x which belongs to T_S can use $\{s, j+1, h+1, M\}$ and the puclic Hssh function $H(\cdot)$ to calculate $H(S|j+1|h|M|K_S)$ and compare this value with H_2, accordingly validate whether the routing packet was modified by the node x.

If x want to modify the routing packet, it has to forge H_2 before forwarding the packet. However x belongs to the one-hop node group S, O_S, and do not know K_S shared by S and T_S, under the assumption that the Hash function is cryptographically secure, $x's$ misbehavior can be detect by the nodes within Z_x with high probability.

5.3. Securing the route reply

In order to secure the route reply, we apply some thoughts of DSR protocol to our scheme. In DSR protocol, the full path information is included in the RREP packet. Here we only include the next hop node in the RREP rather than the full path. Then the route reply packet can be expressed as $\{RREP, next_hop\}$. Then double Hash authentications also can be used to protect the route reply packets. After receiving the route reply packet, the source node needs to save the Hash value H_1 for this path.

If the RREP packet is generated by the destination node d, it is $\{RREP, next_{hop}, H_1, 0\}$, where $H_1 = H(RREP|next_{hop}|K_d)$. Because this packet can be immediately verified, $H_2 = 0$.

If the RREP packet is generated by an intermediate node i with a fresh enough route, it is $\{RREP, next_{hop}, H_1, H_2\}$, where $H_1 =$

$H(RREP|next_{hop}|K_i)$, H_2 is the hash value which the node i saved for this path. If a malicious intermediate node advertises itself as having the shortest path to the destination node and wants to generate a route reply packet, it has to forge a hash value for this virtual path, but this behavior can be detected with high probability by its neighboring node.

6. Conclusion

The security mechanism based on the digital signature is sufficient only for outside attacks, because the compromised inside node can easily generate a digital signature on a wrong routing packet. On the other hand, the digital signature technique is expensive and can produce huge overhead. Under the reasonable assumption that no two compromised inside node are colluding and are within two hops of each other, the security mechanism of double hash authentications is sufficient and efficient. At the same time each node can detect its neighboring node's malicious behavior immediately.

References

[1] D.B. Johnson and D.A. Maltz,"Dynamic source routing in ad hoc wireless networks", *Mobile Computing vol 353*, 1996.

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

[3] Z.J. Hass and M.R. Pearlman, "the Zone Routing Protocol(ZRP) for Ad Hoc Networks", *Intermet Draft, Mobile Ad-Hoc Network(MANET) Working Group, IETF* , Springer, August 1998.

[4] Y. Ko and H. Vaidva, "Location-Aided Routing(LAR) in Mobile Ad Hoc Network",*In Proc. MobiCom'98*, Dallas TX, October 1998, pp. 66-75.

[5] R. Perlman, "Network Layer Protocol with Byzantine Agreement", *PhD thesis*, The MIT Press, Oct 1988.

[6] J.Broch, D.A. Maltz, D.B. Johnson, Y.G. Hu and J. Jetcheva, "A Performance Comparision of Multi-Hop wireless Ad Hoc Network Rouring Protocols", *In Proc. IEEE MOBICOM*, Dallas TX, Oct, 1998.

[7] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek and M. Degermark, "Scenario-based Performance Analysis of Routing Protocols for Mobile Adhoc networks", *In Proc. IEEE MOBICOM*, Seattle, Aug 1999, pp. 195-206.

[8] Yih-Chun Hu and D. Johnson, "SEAD: Secue Efficient Vector Routing for Mobile Wireless Ad Hoc network".