Analyzing security of Authenticated Routing Protocol (ARAN)

Seema Mehla
Computer Department
N.C.College of Engineering
Panipat, India

Bhawna Gupta
Computer Department
N.C.College of Engineering
Panipat, India

Preeti Nagrath
Computer Department
Bharti VidyapeethCollege of Engineering
Delhi, India

ABSTRACT

Ad hoc network allow nodes to communicate beyond their direct wireless transmission range by introducing cooperation in mobile computer (nodes). Many proposed routing protocol for ad hoc network operate in an ad hoc fashion, as on demand routing protocol often have low overhead and faster reaction time than other type of routing based on periodic protocol. However variety of attacks targeting routing protocol have been identified. By attacking the routing protocol attacker can absorb network traffic, inject them in the path between source and destination and can thus control network traffic. So many secure routing protocols have been developed that deals with these attacks. This paper analyzes the security aspects of one commonly used secure routing protocol ARAN

KEYWORDS : AODV, ARAN, RREQ, RREP, Black hole, Gray Hole, Denial of Service

INTRODUCTION

MANET are the mobile network that do not have any infrastructure involved in it i.e they have no fixed routers and all nodes are capable of movement and can be connected dynamically in an arbitrary manner. There are many routing protocols that are in use or have been proposed for use in MANET. Many of these protocols are not secure. The most common Routing protocol is Ad-hoc On Demand Distance Vector (AODV)[1] that handles the dynamically changing network well but only performs very basic security functions. With MANET being used for applications like on-line banking, business sensitive applications, and transfers of military information, security is much more important. From the viewpoint of security any routing protocol must satisfy the following criteria

Certain discovery. If a route between two points in a network exists, it should always be possible to find it. Also, the node, which requested the route, should be able to be sure it has found a route to the correct node.

Isolation. The protocol should be able to identify misbehaving nodes and make them unable to interfere with routing. Alternatively, the routing protocol should be designed to be immune to malicious nodes.

Lightweight computations. Many devices connected to an ad hoc network are assumed to be battery powered with limited computational abilities. Such a node cannot be expected to be able to carry out expensive computations. If operations such as public key cryptography or shortest path algorithms for large networks prove necessary, they should be confined to the least possible number of nodes; preferably only the route endpoints at route creation time.

Location privacy. Often, the information carried in message headers is just as valuable as the message itself. The routing protocol should protect information about the location of nodes in a network and the network structure.**Self-stabilization.** The self-stabilization property requires that a routing protocol should be able to automatically recover from any problem in a finite amount of time without human intervention. That is, it must not be possible to permanently disable a network by injecting a small number of malformed packets. If the routing protocol is self-stabilizing, an attacker who wishes to inflict continuous damage must remain in the network and continue sending malicious data to the nodes, which makes the attacker easier to locate.

Byzantine robustness. A routing protocol should be able to function correctly even if some of the nodes participating in routing are intentionally disrupting its operation. Byzantine robustness can be seen as a stricter version of the self-stabilization property: the routing protocol must not only automatically recover from an attack; it should not cease from functioning even during the attack.

Security also implies identification of threats, attacks and vulnerability of a certain system. A variety of attacks targeting routing in network layer have been identified. Attacks on any routing protocol can be divided into two categories: passive and active. In passive attack, the attacker goal is just to obtain information. This means that the attacker does nor modify or harm the system. However active attacks are those in which attacker may modify or harm the system. Therefore from integrity and authentication point of view active attacks are more dangerous. Some common types of active attacks are:

a) Attacks by dropping the packet
   - I) Black hole attack: Here the attacker drops all type of packet both control as well as data. As any intermediate node responds to the RREQ message if it has a fresh enough route, the malicious node easily disrupts the correct functioning of the routing protocol and make at least part of the network crash. Gray holes: Here the attacker is selective in dropping packets (drops data packets but not control message

b) Attacks using Modification of Protocol message: malicious nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication. Malicious nodes can easily cause redirection of network traffic and DOS simply altering these fields [2].
   - I) Redirection with modified Hop count: malicious node can succeed in diverting all the traffic to a particular destination through itself by advertising a shortest route (very low hop count) to that destination. Once the malicious node has been able to insert itself between two communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop packets to perform a denial of service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.
   - II) Denial of service: A malicious node might generate frequent unnecessary route requests to make the network resources unavailable to other nodes

c) Attacks using Impersonation: A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table

d) Attacks using Fabrication: These attacks are classified into two types:
   - I) Falsifying route error message: A malicious node can succeed in launching a denial of service attack against a benign node by sending false route error messages against this benign node.
   - II) Routing table overflow: The attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed. AODV is less vulnerable to this attack being reactive rather than proactive

e) Worm Hole Attack: In wormhole attacks [3], the attacker receives packets at one point in the network and tunnels them to another part of the network and replays them into the network from that point onwards. This form of attack does not require the attacker to have any knowledge of the cryptographic keys.

SECURE AD HOC ROUTING PROTOCOL

AODV does not satisfy the requirements of certain discovery, isolation or Byzantine robustness. So secure routing protocol for ad hoc networks were developed, in order to offer protection against the attacks. These proposed solutions are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing protocols (e.g. DSR and AODV). A common design principle in all the proposals is the performance-security trade-off balance. Since routing is an essential function of ad hoc networks, the integrated security procedures should not hinder its operation. Another important part of the analysis is the examination of the assumptions and the requirements on which each solution depends. Although a protocol might be able to satisfy certain security constraints, its operational requirements might thwart its successful employment. Five most common categories of secure routing protocol are: solutions based on asymmetric cryptography; solutions based on symmetric cryptography; hybrid solutions; reputation-based solutions; and a category of mechanisms that provide security for ad hoc routing. In this paper one of most common and most efficient algorithm that is ARAN is chosen for analysis with respect of security from asymmetric cryptographic solution. This paper firstly presents a short description of ARAN then it briefly describes the analysis of ARAN in presence of above discussed attacks

ASYMMETRIC CRYPTOGRAPHIC SOLUTIONS

Protocols that use asymmetric cryptography to secure routing in mobile ad hoc networks require the existence of a universally trusted third party (TTP).

ARAN

ARAN or authenticated routing protocol detects and protects against malicious actions by third party and peers in ad hoc network. Two distinct stages of ARAN consist of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. ARAN makes the use of cryptographic certificate to accomplish its task.

a) **Route Initiation Step**

Stage 1 each node, before attempting to connect to the ad hoc network, must contact the certification authority and request a certificate for its address and public key.

$T \rightarrow A$: cert $_{A}$= $[IP_A, K_{A+}, t, e]K_{T-}$

The certificate contains the IP address of A (IP_A), the public key of A (K_{A+}), a timestamp k of when the certificate was created, and a time e at which the certificate expires.. These variables are concatenated and signed by K_{T-}. The protocol assumes that each node knows a priori the public key of the certification authority.

Stage 2 The second operational stage of the protocol ensures that the intended destination was indeed reached. Each node must maintain a routing table with entries that correspond to the source-destination pairs that are currently active. The route discovery of the ARAN protocol begins with a node broadcasting a route discovery packet (RDP) to its neighbors.

A→ brdcst: [RDP, IP_X, N_A] K_{A-}, CertA

The RDP includes a packet type identifier ("RDP"), the IP address of the destination X (IP_X), A 's certificate (cert $_A$) and a nonce N_A , all signed with A 's private key. Note that the RDP is only signed by the source and not encrypted, so the contents can be viewed publicly. The purpose of the nonce is to uniquely identify an RDP coming from a source. Each time, A, performs route discovery it monotonically increases the nonce.

Each node validates the signature with the certificate, updates its routing table with the neighbor from which it received the RDP, signs it, and forwards it to its neighbors after removing the certificate and the signature of the previous node (but not the initiator's signature and certificate).

Let B be a neighbor that has received from A the RDP broadcast, which it subsequently rebroadcasts.

B → brdcst: [[RDP, IP_X, N_A] K_{A-}] K $_{B-}$, $Cert_A$, $Cert_B$

Upon receiving the RDP B's neighbor C validates the signatures for both the RDP initiator, and B, the neighbor it received the RDP from, using the certificates in the RDP. C then removes B's certificate and signature, records as its predecessor, signs the contents of the message originally broadcast by Y and appends its own certificate C then rebroadcasts the RDP.

C→ brdcst: [[RDP, IP_X, N_A] K_{A-}] $K_{C\_}$, $Cert_A$, $Cert_C$

Eventually, the message is received by the destination X, who replies to the first RDP that it receives for a source and a given nonce. This RDP need not have traveled along the path with the least number of hops; the least-hop path may have a higher delay, either legitimately or maliciously manifested. In this case, however, a non-congested, non-least-hop path is likely to be preferred to a congested least-hop path because of the reduction in delay. Because RDP's do not contain a hop count or specific recorded source route, and because messages are signed at each hop, malicious nodes have no opportunity to redirect traffic

After receiving the RDP, the destination unicasts a Reply (REP) packet back along the reverse path to the source. Let the first node that receives the REP sent by X be node D.

X→ D: [REP, IP_A, N_A] $K_{X-,}$ $cert_x$

The REP contains the address of the source node, the destination's certificate, a nonce, and the associated timestamp. The destination node signs the REP before transmitting it. The REP is forwarded back to the initiating node by a process similar to the process described for the route discovery, except that the REP is unicasted along the reverse path.

Let D's next hop to the source be node C .

D→ C : [[REP, IP_A, N_A] K_{X-}] K_{D-} , cert $_X$, cert $_D$

C validates D 's signature on the received message, removes the signature and certificate, then signs the contents of the message and appends its own certificate before unicasting the REP to B

C → B : [[REP, IP $_A$, N_A] K_{X-}] K_{C-} ,$cert_x$, cert $_C$

Each node checks the nonce and signature of the previous hop as the REP is returned to the source. When the source receives the REP, it verifies the destination' s signature and the nonce returned by the destination.

b) Route maintenance

When no traffic has occurred on an existing route for that route' s lifetime, the route is simply de-activated in the route table. Data received on an inactive route causes nodes to generate an Error (ERR) message. Nodes also use ERR messages to report links in active routes that are broken due to node movement. All ERR messages must be signed. For a route between source A and destination X}, a node B generates the ERR message for its neighbor C as follows:

B → C : [ERR, IP_A, IP_X, N_b] K_{B-} , $cert_b$

This message is forwarded along the path toward the source without modification. A nonce ensures that the ERR message is fresh. It is extremely difficult to detect when ERR messages are fabricated for links that are truly active and not broken. However, the signature on the message prevents impersonation and enables non-repudiation. A node that transmits a large number of ERR messages, whether the ERR messages are valid or fabricated, should be avoided

Key Revocation

In the event that a certificate needs to be revoked, the trusted certificate server, T, sends a broadcast message to the ad hoc group that announces the revocation. Calling the revoked certificate cert $_X$, the transmission appears as:

T → brdcst : [revoke, $cert_T$] K $_{T-}$

Any node receiving this message re-broadcasts it to its neighbors. Revocation notices need to be stored until the revoked certificate would have expired normally. Any neighbor of the node with the revoked certificate needs to reform routing as necessary to avoid transmission through the now un trusted node.

SECURITY ANALYSIS

a) Attacks by dropping the packets: Nodes can drop the packets for no-reason, as there is no mechanism to prevent from this attack.

b) Attacks Using Modification of Protocol Message: ARAN specifies that all fields of RDP and REP packets remain unchanged between source and destination. Since the initiating node signs both packet types, any alterations in transit would be detected, and the altered packet would be subsequently discarded. Repeated instances of altering packets could cause other nodes to exclude the errant node from routing, though that possibility is not considered here. Thus, modification attacks are prevented. This prevents the attacks that alter routing messages while in transit or creates routing loops.

I) Redirection with Modified hop-count: ARAN packets contains only destination address, it do not contain field for hop-count, which prevents it from this attack.

II) Denial of service: Denial-of-service attacks can be conducted by nodes with or without valid ARAN certificates. In the certificate less case, all possible attacks are limited to the attacker' s immediate neighbors because unsigned route requests are dropped. There are more severe attacks available at the MAC and physical layer than ARAN provides. Nodes with valid certificates can conduct effective attacks, however, by sending many unnecessary route requests. Because these are broadcast and forwarded across the network, an attacker can cause widespread congestion and power-loss to all nodes in the network. Because it is difficult to infer the node' s intent at the network level, it can be hard to differentiate between legitimate and malicious RREQs.

c) Attacks using Impersonation: Route discovery packets contain the certificate of the source node and are signed with the source' s private key. Similarly, reply packets include the destination node' s certificate and signature, ensuring that only the destination can respond to route discovery. This prevents impersonation attacks where either the source or destination nodes is spoofed.

d) Attacks using Fabrication: Since all routing messages must include the sending node' s certificate and signature, ARAN ensures non-repudiation and prevents spoofing and unauthorized participation in routing. ARAN does not prevent fabrication of routing messages, but it does offer a deterrent by ensuring non-repudiation. A node that continues to inject false messages into the network may be excluded from future route computation.[4]

e) Securing Shortest Paths: Securing a shortest path cannot be done by any means except by physical metrics such as a timestamp in routing messages. Accordingly, ARAN does not guarantee a shortest path, but offers a *quickest* path, which is chosen by the RDP that reaches the destination first. Malicious nodes could save some processing time by not verifying the previous hop' s signature on the RDP packet, thus increasing their chances of being on the quickest route. However such an attack is likely to succeed only if it is executed by multiple malicious nodes on a route, or if a malicious node is already on one of many quick routes to the destination. Malicious nodes also have the opportunity in ARAN to lengthen the measured time of a path by delaying REPs as they propagate, in the worse case by dropping REPs, as well as delaying routing after path instantiation. Finally, malicious nodes using ARAN could also conspire to elongate all routes but one, forcing the source and destination to pick the unaltered route.[5]

CONCLUSION

This paper has presented the authenticated routing protocol for securing the routing protocols of wireless networks. The study has demonstrated that inherent characteristics of ad hoc network such as lack of infrastructure network, rapidly changing topology adds difficulties to already complicated problem of secure routing [6]. Additionally, the flexibility of ad hoc networks enables them to be deployed in diverse application scenarios. Each application has its own set of security requirements and places unique demands on the underlying routing protocol. Hence, an additional difficulty in designing a secure protocol lies in the application scenario that is going to be protected, and how well the protocol can handle scenarios different than the scenario for which it has been designed.

Authenticated routing protocol requires trusted third party for obtaining certificates. Therefore is preferable for applications where we can took help of some already existing infrastructure.

ARAN protocol is based on Ad hoc on demand distance vector routing so as to take benefit of high performance and low cost due to its on reactive nature.

In this paper, we have introduced active attacks on AODV. This paper then discusses 5 types of active attacks. Generally, active attacks can be avoided by this use of stringer authentication methods This paper firstly presents the complete working behind ARAN. As some limitations are also attached with every advantage, so is the case for ARAN. Apart from achieving so many security goals, it is also sufferer of weaknesses. For example ARAN does not have any mechanism that deals with black hole attack, wormhole attack, Denial of service attack.

FUTURE SCOPE

In this paper we identified different attacks on Authenticated Routing Protocol. ARAN has solution for some attacks but it is also silent about some attacks like black hole attack, denial of service attack etc. some research can be done to add functionality to ARAN that is also able to combat with above said attack.Areas in secure ad hoc network routing that have been explored are trust establishment [7, 8, 9, 11], key generation [10], nodes that maliciously do not forward packets [14], and security requirements for forwarding nodes [13]. These areas are beyond the scope of this paper. Routing protocol intrusion detection has been studied in wired networks as a mechanism for detecting misbehaving routers. Cheung and Levitt [15] and Bradley et al [16] propose intrusion detection techniques for detecting and identifying routers that send bogus routing update messages

REFERENCES

[1] Mobile Ad -hoc Networks (MANET). URL: http://www.ietf.org/html.charters/manet-charter.html.

[2] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, A secure routing protocol for ad hoc networks, in: Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November 2002.

[3] Y.-C. Hu, A. Perrig, D.B. Johnson, Wormhole detection in wireless ad hoc networks, A Technical Report TR01-384, Rice University Department of Computer Science.

[4] K. Sanzgiri *et al.*, “A Secure Routing Protocol for Ad hoc Networks,” *Proc. 10th IEEE Int’l. Conf. Network Protocols (ICNP’02)*, IEEE Press, 2002, pp. 78–87.

[5] S. Yi, P. Naldurg, and R. Kravets, “Security-Aware Ad hoc Routing for Wireless Networks,” *Proc. 2nd ACM Symp. Mobile Ad Hoc Net. and Comp. (Mobihoc’01)*, Long Beach, CA, Oct. 2001, pp. 299–302.

[6] E. M. Royer and C.-K. Toh, “A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks,” *IEEE Pers. Commun.*, vol. 2, no. 6, Apr. 1999, pp. 46–55.

[7] Dirk Balfanz, D. K. Smetters, Paul Stewart, and H. Chi Wong. Talking To Strangers: Authentication in Ad-Hoc Wireless Networks. In *Symposium on Network and Distributed Systems Security (NDSS 2002)*, February 2002.

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, pages 12–23, September 2002.

[9] Jean-Pierre Hubaux, Levente Butty´an, and Srdjan Cˇ apkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceedings of the Third ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001)*, Long Beach, CA, USA, October 2001

[10] Stefano Basagni, Kris Herrin, Emilia Rosti, and Danilo Bruschi. Secure Pebblenets. In *ACM International Symposium on Mobile Ad Hoc Networking andComputing (MobiHoc 2001)*, pages 156–163, Long Beach, California, USA, October 2001.

[11] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. In *Proceedings of the Sixth Annual InternationalConference on Mobile Computing and Networking (MobiCom 2000)*, pages 255–265, Boston MA, USA, August 2000.

[12] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Security Protocols, 7th International Workshop*, edited by B. Christianson, B. Crispo, and M. Roe. Springer Verlag Berlin Heidelberg, 1999.

[13] Seung Yi, Prasad Naldurg, and Robin Kravets. Security-Aware Ad-Hoc Routing for Wireless Networks. Technical Report UIUCDCS-R-2001-2241, Department of Computer Science, University of Illinois at Urbana-Champaign, August 2001.

[14] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. Secure Efficient Distance Vector Routing in MobileWireless Ad Hoc Networks. In *Fourth IEEEWorkshop on Mobile Computing Systems and Applications (WMCSA ’02)*, June 2002.

[15] Steven Cheung and Karl Levitt. Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection. In *The 1997 New SecurityParadigms Workshop*, September 1998.

[16] Kirk A. Bradley, Steven Cheung, Nick Puketza, Biswanath Mukherjee, and Ronald A. Olsson. Detecting Disruptive Routers: A Distributed Network Monitoring Approach. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 115–124, May 1998