SECURE ROUTING IN ADHOC NETWORKS USING ARAN

Yadu Kishore*

V. Venkata Ramana**

Dr. P. Chenna Reddy***

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 adhoc fashion, as on demand routing protocol often have low overhead and faster reaction time than other type of routing based on periodic protocol. However varieties 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. Our project analyzes the security aspects of one commonly used secure routing protocol ARAN.

Keywords: Adhoc network ,Network traffic, ARAN.

* Department of Computer Science and Engineering, JNTUA College of Engineering Pulivendula Y.S.R (Dist)., A.P., India.

** Associate Professor, Department of Computer Science and Engineering, SSITS, Rayachoty Y.S.R. (Dist)., A.P., INDIA.

*** Associate Professor, Dept of CSE, JNTUACEPY.S.R (Dist)., A.P., India.

1. INTRODUCTION:

OVERVIEW OF MOBILE AD HOC NETWORKS

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[1]. Many of these protocols are not secure. The most common Routing protocol is Ad-hoc On Demand Distance Vector (AODV[2] 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.

1.1. BACKGROUND

An adhoc network forms by the collection of mobile nodes and create a network by agreeing to route messages for each other. There is no shared infrastructure in an ad hoc network, such as centralized routers or defined administrative policy. All proposed protocols have security vulnerabilities and exposures that easily allow for routing attacks. Vulnerabilities are common to many protocols[2]. Differences between ad hoc networks and standard IP networks necessitate the development of new security services. In particular, the measures proposed for IPSec help only in end-to-end authentication and security between two network entities that already have routing between them; IPSec does not secure the routing protocol.

1.2. MOTIVATION:

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[3]. 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. one of most common and most efficient algorithm is ARAN which uses of cryptographic certificates[3] to offer secure routing.

1.3. PROBLEM STATEMENT

ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to end authentication. The protocol is simple compared to most non-secured ad hoc routing protocols[4]. It should be noted that the exploits modification, impersonation, and fabrication against ad hoc routing protocols are primarily due to the optimizations that have been introduced into ad hoc routing protocols for route computation and creation. Route discovery in ARAN is accomplished by a broadcast route discovery message from a source node which is replied to unicast by the destination node, such that the routing messages are authenticated at each hop from source to destination, as well as on the reverse path from the destination to the source

2. EXPLOITS ALLOWED BY EXISTING PROTOCOLS

The current proposed routing protocols for ad hoc wireless networks allow for many different types of attacks. Analogous exploits exist in wired networks, but are more easily defended against by infrastructure present in a wired network. In this we classify *modification[4]*, *impersonation*, and *fabrication* exploits against ad hoc routing protocols[4].

2.1. Threats using modification

Currently existing routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Malicious nodes easily cause traffic subversion and denial of service (DoS) by simply altering these fields: such attacks compromise the *integrity* of routing computations. By modifying routing information an attacker can cause network traffic to be dropped, redirected to a different destination or take a longer route to the destination increasing communication delays.

2.2. Threats using impersonation

Since current ad hoc routing protocols do not *authenticate* routing packets a malicious node can launch many attacks in a network by masquerading as another node (*spoofing*)[5]. Spoofing

occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather. As an example, a spoofing attack allows to create loops in routing information collected by a node with the result of partitioning the network.

2.3. Threats using fabrication

The notation "fabrication" is used when referring to attacks performed by generating false routing messages[5]. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages claiming that a neighbour can no longer be contacted.

3. AUTHENTICATED ROUTING FOR AD HOC NETWORKS

ARAN makes use of cryptographic certificates to offer routing security. Such certificates are already seeing deployment as part of one-hop 802.11 networks[6]. ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. The protocol is simple compared to most non-secured ad hoc routing protocols. Route discovery in ARAN is accomplished by a broadcast route discovery message from a source node which is replied to unicast by the destination node, such that the routing messages are authenticated at each hop from source to destination, as well as on the reverse path from the destination to the source.

3.1. CERTIFICATION

ARAN requires the use of a trusted certificate server; whose public key is known to all valid nodes. Keys are a priori generated and exchanged through an existing, perhaps out of band, relationship between each node[6]. Before entering the ad hoc network, each node must request a certificate. Each node receives one certificate after securely authenticating their identity.

3.2. Authenticated Route Discovery

The goal of end-to-end authentication is for the source to verify that the intended destination was reached. In this process, the source trusts the destination to chose the return path. Source node starts route instantiation to destination by broadcasting to its neighbours a *route discovery packet* (RDP)[7].

3.3. Authenticated Route Setup

Eventually, the message is received by the destination, who replies to the first RDP that it receives for a source and a given nonce. There is no guarantee that the first RDP received

travelled along the shortest path from the source. An RDP that travels along the shortest path may be prevented from reaching the destination first if it encounters congestion or network delay, either legitimately or maliciously manifested. In this case, however, a non-congested, non-shortest path is likely to be preferred to a congested shortest path because of the reduction in delay[7]. Because RDPs 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 with the exploits. 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 destination node be source node.

4. SECURITY & NETWORK PERFORMANCE ANALYSES

In this section, we provide a security analysis of ARAN by evaluating its robustness in the presence of the attacks[7]. We also compare through simulation the performance of ARAN to the AODV routing protocol.

4.1. Unauthorized participation: ARAN accept only packets that have been signed with a certified key issued by the trusted authority. In practice, many single-hop 802.11 deployments are already using VPN certificates. Mechanisms for authenticating users to a trusted certificate authority are numerous[8]. The trusted authority is also a single point of failure and attack, however, multiple redundant authorities may be used.

4.2. Spoofed Route Signaling: Since only the source node can sign with its own private key, nodes cannot spoof other nodes in route instantiation. 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.

4.3. Fabricated Routing Messages: Messages can be fabricated only by nodes with certificates. In that case, ARAN does not prevent fabrication of routing messages, but it does offer a deterrent by ensuring non-repudiation[8]. A node that continues to inject false messages into the network, may be excluded from future route computation.

4.4. Alteration of Routing Messages: ARAN specifies that all fields of RDP and REP packets remain unchanged between source and destination. Since both packet types are signed by the initiating node, any alterations in transit would be immediately detected by intermediary nodes

along the path, 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.

4.5. Securing Shortest Paths: We believe there is no way to guarantee that one path is shorter than another in terms of hop count. Tunneling attacks, are possible in ARAN as they are in any secure routing protocol. Securing a shortest path cannot be done by any means except by physical metrics such as a timestamp in routing messages[9]. 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 do 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; clearly, a difficult task.

4.6. Replay Attacks: Replay attacks are prevented by including a nonce and a timestamp with routing messages.

5. NETWORK PERFORMANCE

We performed our evaluations using Global Mobile Information Systems Simulation Library (GloMoSim) [10]. We used a 802.11 mac layer and CBR traffic over UDP. We simulated field configuration: 20 nodes distributed over a 670m x 670m terrain.

The initial positions of the nodes were random. Node mobility was simulated according to the random

waypoint mobility model, in which each node travels to a randomly selected location at a configured speed and then pauses for a configured pause time, before choosing another random location and repeating the same steps. Node transmission range was 250m. We ran simulations for constant node speeds of 1, 5 and 10 m/s, with pause time fixed at 30 seconds. We simulated five CBR sessions in each run, with random

source and destination pairs. Each session generated 1000 data packets of 512 bytes each at the rate of 4 packets per second. ARAN was simulated using a 512 bit key and 16 byte signature. These values are reasonable to prevent compromise during the short time nodes spend away from the certificate authority and in the ad hoc network.

In order to compare the performance of ARAN and AODV, both protocols were run under identical mobility and traffic scenarios[10]. A basic version of AODV was used, which did not include optimizations such as the expanding ring search and local repair of routes. This enables a consistent comparison of results.

We evaluated six performance metrics[11]:

(1) **Packet Delivery Fraction:** This is the fraction of the data packets generated by the CBR sources that are delivered to the destination. This evaluates the ability of the protocol to discover routes.

(2) **Routing Load (bytes):** This is the ratio of overhead bytes to delivered data bytes. The transmission at each hop along the route was counted as one transmission in the calculation of this metric. ARAN suffers from larger control overhead due to certificates and signatures stored in packets.

(3) **Routing Load (packets):** Similar to the above metric, but a ratio of control packet overhead to data packet overhead.

(4) **Average Path Length:** This is the average length of the paths discovered by the protocol. It was calculated by averaging the number of hops taken by each data packet to reach the destination.

(5) **Average Route Acquisition Latency:** This is the average delay between the sending of a route request/discovery packet by a source for discovering a route to a destination and the receipt of the first corresponding route reply. If a route request timed out and needed to be retransmitted, the sending time of the first transmission was used for calculating the latency.

(6) **Average End-to-End Delay of Data Packets:** This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc.

6. RESULTS AND ANALYSIS

1. Avg Packet Delivery

Node speed	1	5	10
AODV	0.78	0.8982	0.9458

ARAN	0.9998	0.9988	0.9980

Table 1(a): Avg Packet Delivery

Node speed	1	5	10
AODV	0.8303	0.8326	0.9138
ARAN	1	0.999	0.995

Table 1(b): Avg Packet Delivery fraction with 10 malicious nodes

2. Avg end-end delivery

Node speed	1	5	10
AODV	0.02000	0.02020	0.02050
ARAN	0.01739	0.01767	0.01775

Table 2(a): Avg end-end delivery

Node speed	1	5	10
AODV	0.0134	0.0160	0.0202
ARAN	0.0183	0.0184	0.0195

Table 2(b): Average End-to-End Delay of Data Packets with 10 malicious nodes

3. Routing Load (bytes)

Node speed	1	5	10
AODV	0.0170	0.0489	0.0980
ARAN	0.0672	0.1260	0.2390

Table 3(a): Routing Load in bytes

Node	1	5	10

speed			
AODV	0.0092	0.0292	0.0698
ARAN	0.0623	0.1198	0.2320

Table 3(b): Routing Load in bytes with 10 malicious nodes

4. Routing Load (packets)

Node speed	1	5	10
AODV	0.1820	0.3232	0.5980
ARAN	0.1730	0.3012	0.5720

Table 4(a): Routing Load in packets

Node speed	1	5	10
AODV	0.1000	0.1998	0.3214
ARAN	0.1710	0.2989	0.5230

Table 4(b): Routing Load in packets with 10 malicious nodes

5. Average Path Length

Node speed	1	5	10
AODV	2.2732	2.2798	2.4746
ARAN	2.2500	2.2567	2.4652

Table 5(a): Average Path Length

Node speed	1	5	10
AODV	2.098	2.1076	2.2672

ARAN	2.2498	2.2521	2.4542

Table 5(b): Average Path Length with 10 malicious nodes

6. Average Route Acquisition Latency

Node speed	1	5	10
AODV	25	25.92	27.20
ARAN	24.89	25.94	28.32

Table 6(a): Average Route Acquisition Latency

Node speed	1	5	10
AODV	19.9	20.02	22.32
ARAN	24.28	25.45	27.98

Table 6(b): Average Route Acquisition Latency with 10 malicious nodes

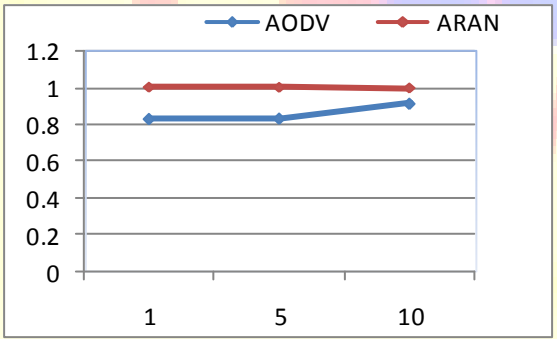

Fig 1:Avg Packet Delivery fraction with 10 malicious nodes

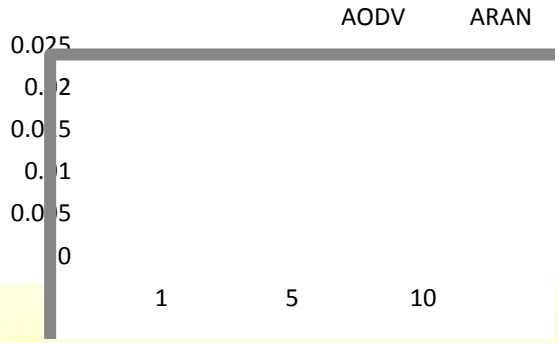

Fig 2:Average End-to-End Delay of Data Packets with 10 malicious nodes

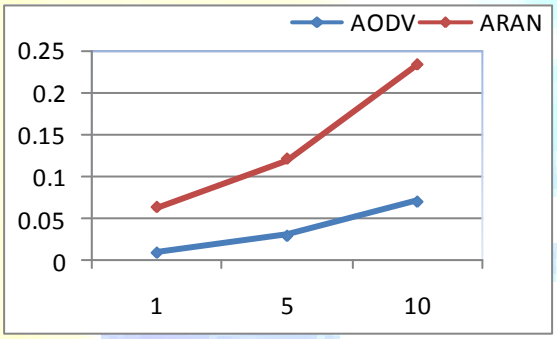

Fig 3:Routing Load in bytes with 10 malicious nodes

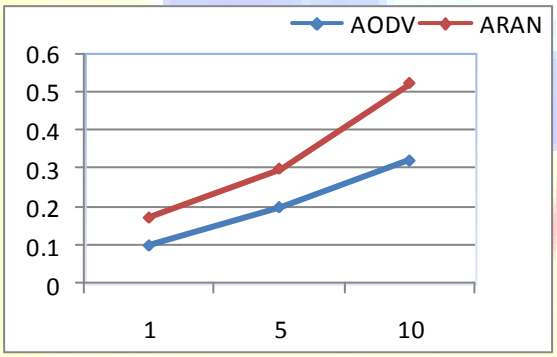

Fig 4:Routing Load in packets with 10 malicious nodes

Fig 5:Average Path Length with 10 malicious nodes

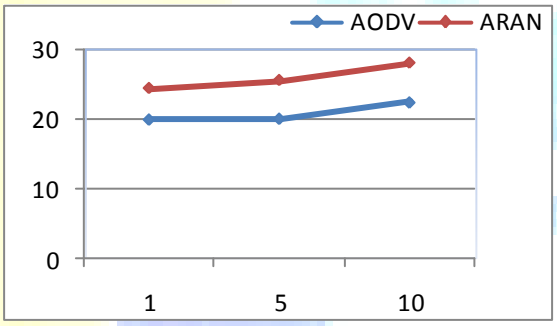

Fig 6:Average Route Acquisition Latency with 10 malicious node

7. CONCLUSION

Existing ad hoc routing protocols are subject to a variety of attacks that can allow attackers to influence a victim's selection of routes or enable denial-of-service attacks. We have shown a number of such attacks, and how they are easily exploited in two ad hoc routing protocols under consideration by the IETF[12]. In particular, we introduced the notion of a tunneling attack, in which collaborating malicious nodes can encapsulate messages between them to subvert routing metrics. ARAN provides a solution for secure routing in the managed-open environment. ARAN provides authentication and non-repudiation services by pre-determined cryptographic certificates that guarantees end-to-end authentication. In doing so, ARAN limits or prevents attacks that can afflict other insecure protocols. ARAN is a simple protocol that does not require significant additional work from nodes within the group. Our simulations show that ARAN is as efficient as AODV in discovering and maintaining routes, at the cost of using larger routing packets which result in a higher overall routing load, and at the cost of higher latency in route discovery because of the cryptographic computation that must occur.

8. REFERENCES

[1] The global mobile information systems simulation library (glomosim).http://pcs.cs.ucla.edu/projects/glomosim.

[2] C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. In *IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, Feb. 1999.

[3] B. Schneier. *Applied Cryptography: Protocols,Algorithms, and Source Code in C*. John Wiley & Sons, Inc., New York, 1996.

[4] J.-P. HuBaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proc. ACM MOBICOM*, Oct. 2001.

[5] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, Clay Shields, and Elizabeth M. Belding-Royer. "A Secure Routing Protocol for Ad Hoc Networks". In proceedings of IEEE ICNP, Paris, France, November 2002.

[6] I.D. Chakeres and E.M. Belding-Royer. A quantitative analysis of simulation and implementation performance for the aodv routing protocol. Submitted for publication.

[7] C. R. Davis. *IPSec: Securing VPNs*. McGraw-Hill, New York, 2000.

[8] J.-P. HuBaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proc. ACM MOBICOM*, Oct. 2001.

[9] D. Johnson, D. Maltz, Y.-C. Hu, and J. Jetcheva. The dynamic source routing protocol for mobile ad hoc networks. *IEEE Internet Draft*, March 2001. draft-ietf-manet-dsr-05.txt (work in progress).

[10] J. Kong et al. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Proc. IEEE ICNP*, pages 251–260, 2001.

[11] S.-J. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks.

[12] S. Murthy and J.J. Garcia-Lunca-Aceves. An efficient routing protocol for wireless networks. *ACM Mobile Networks and Applications Journal*, pages 183–197, Oct. 1996.