Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.246 – 256

RESEARCH ARTICLE

SEAD AND ARIANE Routing Protocol: Comparative Study

Ankita, Vikram Nandal

M.Tech Student, Department of CSE, R.N. College of Engineering & Management

Assistant Professor, Department of CSE, R.N. College of Engineering & Management

Sindhwaniankita@gmail.com, vikramcse@live.com

Abstract: The latest advancement in wireless technology and its applications received a lot of attention. An ad hoc network is one such recent technology, which gives a new paradigm for wireless self-organised networks. Ad hoc networks are simple peer-to peer networks, self-organized and with no fixed infrastructure. Ad-hoc network is a concept in computer communication which means that user wanting to communicate with each other forms a temporary network, without use of centralized administration. Each node in the network acts both as host and router and must therefore willing to forward packet for other node. For this purpose routing protocol is needed. A Mobile Ad-hoc Network (MANET) is a temporary wireless network composed of mobile nodes without any permanent infrastructure. Each node not only operates as an end system, it also acts as a router to forward packets on behalf of other nodes. Ad hoc networks are basically peer-to-peer, multihop mobile wireless networks in which information packets are transmitted in a store-and –forward manner from a source to an arbitrary destination, via intermediate nodes.

Keywords: MANET, Doppler shift, signal attenuation, DOS, SEAD, ARAN

I. INTRODUCTION

- **SEAD** is designed based on the DSDV (Destination Sequenced Distance Vector) protocol. SEAD was proposed by Yih-Chun Hu, David B. Johnson and Adrian Perrig, [3].

DSDV: Destination Sequenced Distance Vector[10] routing protocol is one of the first protocol proposed for ad hoc wireless networks. It was developed based on the distributed Bellman Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. It's a table driven routing protocol. Routes to all destinations are readily available at every node at all times. The tables are exchanged between neighbours at regular intervals to keep an up-to-date view of the network topology. Whenever there is a change in the network topology, the table entries are updated. It provides loop free single path to the destination. DSDV sends two types of packets "*full dump" and "incremental"*. SEAD was developed based on DSDV working principle [4], [5]. SEAD incorporates One- Way Hash function [4] to authenticate in the routing update mechanism to enhance the routing security. Let us consider a One-Way Hash function 'H' and see how the hash property is used in SEAD node authentication. The hash function H generates a one way hash chain of values (h0, h1, h2, h3, h4,…….hn). The initial has chain value h0 is created using a random initial number x. At any stage 'h(i)' can be calculated using h(i-1) using the hash function H. i.e. h(i) = H(h(i-1).

Let us consider 'm' is the no of nodes in the network, so the upper bound for the hop counts is < m-1. Let the hash chain values calculated using H be (h1,h2...hn), where 'n' is divisible by m, then for a routing table entry with sequence number 'i', let k = ((n/m)-i). If the metric 'j'(distance) is used to authenticate the routing update entry, then h(km+j) is used to authenticate the table update entry for that sequence number 'i' and distance 'j'. A malicious node can modify h(km+j) only if it knows the value of h(km+j-1), which is impossible to calculate. So the hashing technique is used to authenticate the nodes participating in the ad hoc network.

- **Ariadne** is a secure routing protocol developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig [3], based on the Dynamic Source Routing protocol (DSR). [4][5][7].

DSR: DSR is an on-demand routing protocol, which finds the route as and when required, dynamically. DSR routing protocol manage the network without any centralized administrator or infrastructure. In route discovery this protocol discovers for the routes from source node to destination. In DSR, data packets stored the routing information of all intermediate nodes in its header to reach at a particular destination. Routing information for every source node can be change at any time in the network and DSR updates it after each change occur [7]. Intermediate routers don´t need to have routing information to route the passing traffic, but they save routing information for their future use. Basic purpose to develop DSR was to reduce the overhead on the network and designing self-organizing and self-configuring protocol to support MANET. The DSR protocol contains two phases in its routing mechanism:

a) **Route discovery:** In the route discovery phase the source node establishes a route by flooding route request packets (RREQ). The RREQ contains the source IP address and destination IP address. The neighbour nodes accumulate the traversed path into the RREQ and broadcast to its next neighbour if the current node is not the destination node. Once the destination node receives the RREQ it concatenates the source route in a Route Reply packet (RREP) and replies on the same path as in RREQ. In the RREQ unicast process, intermediate nodes update their routing tables to each of the nodes along the source route.

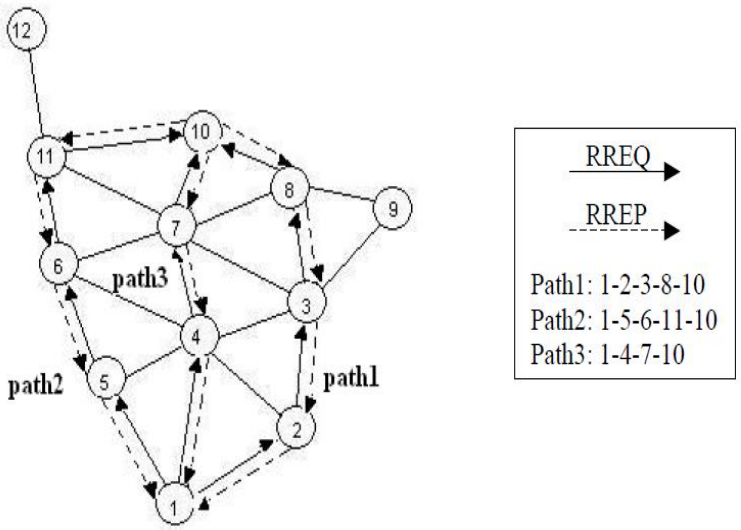


Fig1: route discovery

b) **Route maintenance:** Route maintenance is carried whenever there is a broken link observed in the specific route to the destination. When the packets are forwarded through a specific route, each node sends the packet to the next node in the route and the next node acknowledges the packet received. When a broken link is observed in the destination path the broken link will not acknowledge to the packet transmitted by the neighbour node, and the node send a route error message (RERR) to the source node. The source then responds to this RERR and stops sending the next packets and will look in its route cache for alternative routes and follow the next available path.

- **Secure Routing Protocol (SRP)**

Secure Routing Protocol (SRP), was proposed by Papadimitratos and Hass [8]. SRP is implemented over DSR [4], [5], with an underlying Security Association (SA) between the source and destination nodes. The trust relation is maintained with a public key infrastructure and a shared key K(sd), was maintained between the source and destination nodes using the security association. In SRP the route request (RREQ) contains six fields and a MAC value to initiate the discovery process. The RREQ is signed with the shared key K(sd) between the source and destination. The intermediate nodes participating in the route discovery measures the frequency of queries received from their neighbours and maintains a priority ranking inversely proportional to the query rate. So if a malicious node participates in the network with malicious RREQ‘s will be dealt last in the priority list. When the RREQ reaches the destination node, it verifies the integrity and authentication with the MAC value and shared key between the source and destination. Once the integrity and authentication is checked for the received RREQ, the Destination node responds with a Route Reply packet (RREP).

II. Protocol Evaluation

Case study against identified attack patterns

In ad hoc networks, attacks can be classified into active and passive attacks. In passive attacks, attackers don’t disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. An active attacker injects packets into the network, eavesdrops and also tries to compromise the network with denial of service. In the active attacks, the malicious nodes introduce false information to confuse the network topology. They can either attract traffic to them and

then drop or compromise the packets. They can also send false information and lead packets to the wrong node and cause congestion in one area. The attacks can either target at the routing procedure or try to flood the networks.

Most common attack patterns identified in ad hoc network environment

Denial-of-service with modified source route

- Tunnelling
- Spoofing
- Black hole attack
- Wormhole attack
- Routing table overflow attack

Denial-of-service with modified source route:

A denial of service attack in general could be launched at any layer of an ad hoc network.
On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could break down high-level services. In the routing mechanism a source node sends route request messages to all neighbours to find a route to the destination node. In the denial-of-service case a malicious node in between can successful send an erroneous route message to the source route to disrupt the service.

Tunnelling:

Ad hoc networks have an implicit assumption that any node can be located adjacent to any other node. A tunnelin*g* attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. One vulnerability is that two such nodes may collaborate to falsely represent the length of available paths by encapsulating and tunnelling the routing message between them.

Spoofing:

A single malicious node in the ad hoc network can spoof the nodes identity in order to forward packets through it. Later the information can be used to create DoS attacks.

Blackhole:

In Black hole attack a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept and in this way it can compromise the service.

Warmhole:

In Wormhole an attacker records packet at one location in the network, tunnels them to another location, and retransmits them back into the network. This attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

III. Mappings between Attacks Pattern and Protocol

SEAD:

SEAD was developed based on DSDV and incorporates One-Way Hash function to authenticate in the routing update mechanism in order to enhance the routing security. Securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. Distance vector protocols encapsulate the route information into a hop count value and a next hop. An attacker cannot create a valid route with a larger sequence number that it received due to the properties of hash function. As SEAD incorporates neighbour authentication through Hash functions, an attacker cannot compromise any node. SEAD is prone through warmhole attack. Even if authentication is provided using hash functions, a warmhole attack is possible through tunnelling the packets from one location and retransmitting them from other location into the network. All packets in the wormhole attack flow in a circle around instead of reaching the destination.

Ariadne:

Ariadne was developed based on an on demand protocol, Destination Source Routing (DSR). Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. Warmhole attacks are possible in Aridane through two compromised nodes. Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps.

SRP:

Secure routing protocol (SRP) was developed based on Destination Source Routing (DSR). The intermediate nodes participating in the route discovery measure the frequency of queries received from their neighbours and maintain a priority ranking inversely proportional to the query rate. So the malicious compromised nodes participating in the network are given least priority to deal with. The security analysis is similar to Ariadne as it is based on DSR protocol.

ARAN:

Aran uses public key cryptography and a central certification authority server for node authentication and neighbour node authentication in route discovery. Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbour node authentication through certificates. Participating nodes broadcast unnecessary route requests across the network. An attacker can cause congestion in the network, there by compromising the functionality of the network.

SAODV:

SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts. Tunnelling attacks are possible through two compromised nodes. Warmhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible reply attacks.

SAR:

SAR was developed using a trust-based framework. Each node in the network is assigned with a trust level. So the attacks on this framework can be analyzed based on trust level and message integrity. As show below the author [Seung, Prasad, Robin] evaluated the security of SAR in terms of trust level and message integrity.

Trust Level: SAR routing mechanism is based on the behaviour associated with the trust level of a user. It is a binding between the identity of the user and the associated trust level. To follow the trust-based hierarchy, cryptographic techniques like: encryption, public key certificates, shared secrets, etc. are employed.

Message integrity: The compromised nodes can utilize the information flow in between nodes and reading of packets to launch attacks. It results in corruption of information, confidentiality of the information, and in denial of network services.

Ad hoc security ▶ protocols / Attack patterns ▼	SEAD	Ariadne	SRP	ARAN	SAODV	SAR
DOS	Y	Y	Y	Y	Y	Y
Tunneling	Y	Y	Y	Y	Y	Y
Spoofing	Y	N	N	N	N	N
Blackhole	Y	N	N	N	N	N
Warmhole	Y	Y	Y	Y	Y	Y
Routing tables overflow attacks:	Y	N	N	N	N	N

Table 3.1

Y = Attack Possible N = Attack not possible

IV. SIMULATION AND EVALUATION

No. of nodes used for simulation	20
Maximum No. of connection	20
Network Density dimensions	1000 x 1000 meters
Mobility pattern	Uniform
Link Bandwidth	2 mbps
Traffic pattern	CBR
Simulation time	800 seconds
Maximum node Speed	20meters/sec

Table 3.2

Metrices used:

Packet Delivery Fraction (PDF):

This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes.

$$PDF = \frac{No\ of\ Packets\ Received\ by\ destination}{No\ of\ Packets\ Sent\ by\ Source}$$

This estimate gives us an idea of how successful the protocol is in delivering packets to the application layer. A high value of PDF indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance.

Byte Overhead (BO):

The total number of routing bytes transmitted during the simulation. For packets sent over multiple hops, each transmission of the byte at each hop counts as one transmission.

Packets Overhead(PO):

The total number of routing packets transmitted during the simulation. For packets (512 kbps) sent over multiple hops, each transmission of the packet at each hop counts as one transmission.

Median Latency(ML):

The time taken by the route discovery packet to reach from the source to destination is known and Median latency. The less time to discover the route to the destination indicates the high performance of the protocol.

Average end-to-end delay (AED):

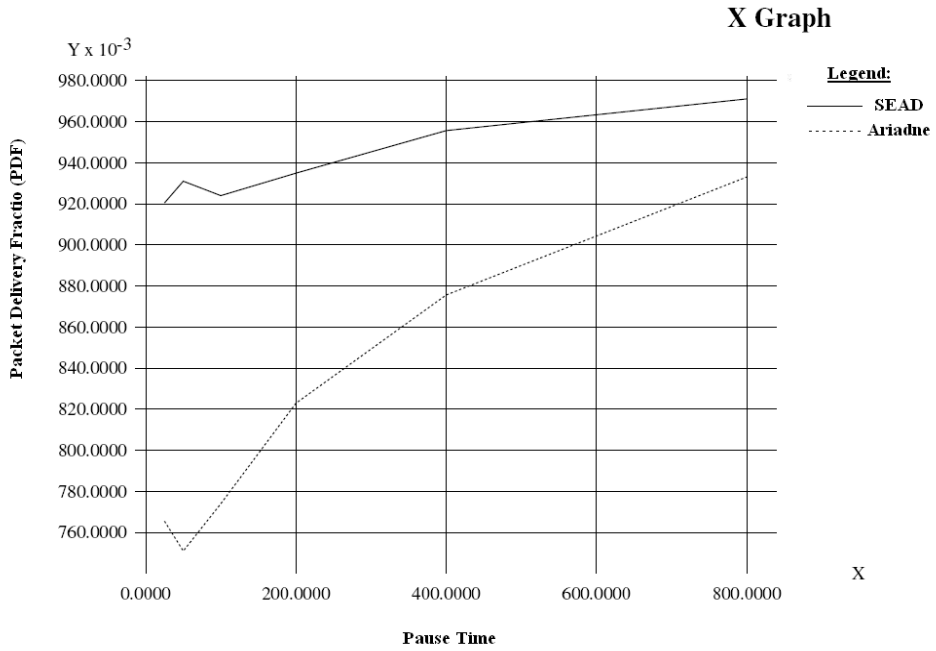
This is the average delay between, sending the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, and retransmission delays at the MAC layer.

$$AED = \frac{\sum_{i=0}^{n} Time\ Packet\ Received_i - Time\ packet\ sent_i}{Total\ Numbe\ of\ Packets\ Received}$$

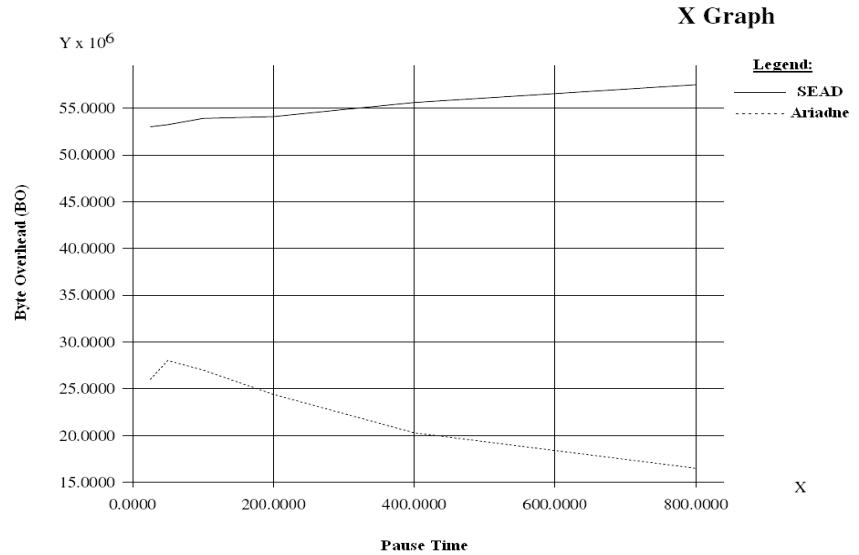
Where ‘n’ is the total number of packets. A higher value of end-to-end delay means that the network is congested and hence the routing protocol doesn’t perform well.

V. Results

Packet Delivery Fraction (PDF):



Byte Overload:



VI. Security and Performance Analysis Security Analysis

The security analysis of SEAD and Ariadne are done in this thesis. SEAD is a table driven protocol, and securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. From the table 3.1 we can see that all type of security attacks are possible in SEAD routing protocols with a compromised node. If no compromised malicious nodes exist in the network, SEAD is stable to all attack patterns through neighbour authentication. Routing loops can only be possible when there is more than one malicious node in the network. The confidentiality of the network topology with respect to participating nodes is maintained with neighbour authentication.
Ariadne uses MAC s and shared keys to authenticate between nodes and use time stamps for packet lifetime. Warmhole attacks are possible in Aridane through two compromised nodes. Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps.

Performance Analysis:

Packet Delivery Fraction (PDF):

Figure 3.1 shows the results of the performance metric, *packet delivery fraction.* A higher value of PDF indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance. SEAD consistently outperforms Ariadne in terms of packet delivery fraction at lower pause times in the simulation. This shows that the route discovery is faster in SEAD than in Ariadne and the number of routing advertisements sent by SEAD are more than Ariadne. So at lower pause time SEAD contains more up to date routing information than Ariadne. At higher pause times the PDF graph for Ariadne increases gradually. As Ariadne uses TESLA broadcast authentication with shared keys between nodes, at the lower pause times it takes more time for route discovery and once secure routes are discovered the PDF graph increases gradually because of the secure route.

Byte Overhead (BO):

Figure 3.2 shows the results of the performance metric, *byte overhead.* SEAD graph shows increased byte overhead than Ariadne, this is due to the increased number of routing advertisements in SEAD than Ariadne. Ariadne graph shows a decrease in byte overhead with increased simulation time. The increased overhead in SEAD causes some congestion in the network. As the simulation time increases Ariadne outperforms SEAD with decreased byte overhead.

VII. Conclusion and Future Work

Securing ad hoc environments is a challenging task. The main purpose of this thesis work was to acquire in-depth knowledge of ad hoc routing protocols and secures routing protocols. Security evaluation of some of the secure routing protocols are done using case study with the most commonly identified attack patterns in ad hoc networks. Performance evaluation of ad hoc secure routing protocols SEAD and Ariadne was done with most commonly identified performance metrics.
In the secure routing protocols most of the security attacks are possible with a compromised node. From the case study results, it concludes that table driven protocols are more prone to security attacks than on demand driven protocols. Protocols based on DSR and AODV are more stable to security attacks due to the strong cryptographic implementation.
The performance evaluation of SEAD and Ariadne shows that, Ariadne out performs SEAD in all the performance metrics. But it is important to see that at lower simulation pause times SEAD out performs

Ariadne. This is due to the routing mechanism involved in these protocols. SEAD encapsulates routing information in routing tables, so at lower pause time SEAD out performs Ariadne.

Future Work

Research in the area of ad hoc secure routing protocols is still actively done. Due to the time constraint and code limitations the current work was only focused on evaluating two secure routing protocols SEAD and Ariadne with some selected performance metrics. The evaluation of other ad hoc secure routing protocols discussed in this thesis work with some more performance metrics will be considered as future research work.

