Performance Comparison of Secure Routing Protocols in Mobile Ad-Hoc Networks

Ashwani Garg
Research Scholar, Department of
Computer Science & Engineering
N C College of Engineering, Israna, Panipat

Vikas Beniwal
Assistant Professor, Department of
Computer Science & Engineering
N C College of Engineering, Israna, Panipat

ABSTRACT

A mobile Ad-Hoc network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Each node operates not only as an end system but, also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These nodes change position frequently. A node can get compromised during the route discovery process. Attackers from inside or outside can easily exploit the network. Several secure routing protocols are proposed for MANETs by researchers. In this paper, an attempt has been made to compare the performance of two prominent secure routing protocols for MANETs: Secure Efficient Ad-Hoc Distance Vector Protocol i.e. SEAD (a proactive or table driven protocol) and Ariadne (a reactive or on demand protocol).Compared to the proactive routing protocols, less control overhead is a distinct advantage of the reactive protocols. Thus, reactive routing protocols have better scalability than proactive routing protocols. However, when using reactive routing protocols, source nodes may suffer from long delays for route searching before they can forward data packets. Hence these protocols are not suitable for real-time applications. As per our findings the difference in the protocols mechanics leads to significant performance differentials for both of these protocols. The performance differentials are analyzed using varying simulation time. These simulations are carried out using the NS-2 network simulator. The results presented in this work illustrate the importance in carefully evaluating and implementing routing protocols in an ad hoc environment.

Keywords

MANETs, Routing Protocols, SEAD, Ariadne

1. INTRODUCTION

A MANET is an autonomous group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly and unpredictably over time, because the nodes are mobile. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes. Most of the MANET routing protocols can be classified into two: Proactive routing protocols and reactive routing protocols. The problem of security in MANETs [1-2] represents a serious challenge. Confidentiality, integrity, availability, authentication, non-repudiation, are the basic requirements of information security. Ad hoc network's dynamic topology with no centralized administration makes it highly vulnerable for its security breach, particularly secure routing in ad hoc networks has been a challenging task for researchers. Therefore the traditional security mechanisms and protocols, including those for the wired networks are not directly applicable and require a careful relook [3]. We attempt revisiting the secure routing protocols applicable in MANETs and investigate the performance of some of the secure Ad-Hoc routing protocols.

2. RELATED WORK

A MANET is a kind of wireless Ad-Hoc network and it is a Self-configuring network of mobile routers connected by wireless links, the union of which forms an arbitrary Topology. Thus the network's wireless topology may change rapidly and unpredictably to a volatile topology which would make it hard to detect malicious nodes or selfish nodes. A selfish node refuses to share its own resources and attempts to benefit from other nodes. These selfish nodes may severely affect the performance of network [4-5]. In order to maintain connectivity in a mobile Ad-Hoc network is participating nodes have to perform routing of network traffic. So, to avoid the misbehaviour of selfish nodes and thus for improving the performance of mobile Ad-Hoc network's, we studied two protocols i.e. SEAD and Ariadne. SEAD is a proactive protocol which incorporates one way hash function to authenticate in the routing update mechanism. Ariadne is a reactive protocol which has MAC and shared keys between nodes to authenticate between nodes and use tome stamps for packet lifetime.

Both the protocols are good in their place but they cannot be used together so in our project we will be comparing the protocols on the basis of the amount of packets received and the packets lost i.e. performance and reliability, thus evaluating the correct use of protocol at right places. For analyzing it we examine the evaluation on NS2 simulator tool.

3. SECURE EFFICIENT AD-HOC DISTANCE VECTOR

The SEAD is a proactive routing protocol, designed based on the Destination Sequenced Distance Vector (DSDV) protocol. SEAD was proposed by Yih-Chun, David B. Johnson and Adrian Perrig [6]. SEAD incorporates One-Way Hash function [7] to authenticate on the routing update mechanism to enhance the routing security. Let us consider One-Way Hash function 'H' and see how the hash chain of values (h0, h1, h2, h3,

h4,…..,hn).The initial has chain value h0is 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 number of nodes in the network , so the upper bound for the hop counts is less than m-1.Let the hash chain values calculated using H be (h1,h2,h3,……,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 (k m + j) is used to authenticate the table update entry for that sequence number ‘i’ and distance ‘j’ .A malicious node can modify h (k m + j) , which is impossible to calculate. So, the hashing technique is used to authenticate the nodes participating in the ad hoc network.

4. ARIADNE

The Ariadne is a reactive routing protocol based on Dynamic Source Routing (DSR) protocol [8]. Ariadne uses the basic routing mechanism of DSR and uses TESLA [9] broadcasting authentication protocol. Ariadne provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the pair of communicating nodes. In Ariadne a route request packet (RREQ) contains eight fields: RREQ, initiator, target, id, time interval, hash chain, node list, and MAC list. The initiator and target values are set to the source and destination addresses as like in DSR. The source also assigns an identifier (id) value, which is not recently used in a route discovery. When one node in the network receives a RREQ for the target node, the node checks its local table for the entries already available with the source id and identifier value. If it finds one it discards the packet, if not it will check for the validity of the time interval of d initiator, id values from recent RREQ it has received, to determine if it already seen a RREQ. If the time interval is not valid, the node discards the packet, if the time interval is in limit, it appends its own address in the RREQ and replaces the hash chain, MAC entries computed with the new entries. The node uses the TESLA key. Finally the node rebroadcasts the RREQ. When the target node receives the RREQ, it checks the validity of the RREQ by determining that the keys from the time interval specified have not been disclosed yet, and that the hash chain field is equal to [ηn, H[η(n-1), H[…, H[η1, MAC(Ksd)(initiator, target, id, time interval]…]]]. Where ηi is the node address at position ‘s’ of the node in the request, and where n is the number of nodes in the node list. If the target node determines that the RREQ is valid, it returns a RREP to the initiator, containing eight fields: ROUTE REPLY, target, initiator, time interval, node list, MAC list, target MAC, key list. The target, initiator, time interval, node list, and MAC list fields are set to the corresponding values from the RREQ, the target MAC is set to a MAC computed on the preceding fields in the reply with the key (ds) and the key list is initialized to the empty list. The RREP is the initiator of the request along the source route obtained by reversing the sequence of hopes in the node list of the request. RREP was prepared by the destination node when it is able to disclose its key from the time interval specified; it then appends its key from that time interval to the key list field in the RREP and forwards the packet according to the source route indicated in the packet. When the initiator receives a RREQ, it verifies that each key in the key list is valid the target MAC is valid, and that each MAC in the MAC list is valid. If all of these tests succeed, the node accepts the RREP, otherwise it discards it.

5. EXPERIMENTAL RESULTS

In this research paper, the comparisons of two routing protocols have been measured between SEAD and Ariadne to study the performance of each routing protocols in a free attack simulation environment using different performance metrics.

5.1 Scenario and Environment Settings

The scenario and the environment settings are fixed. It is purposely done to see the fair results between the routing protocols SEAD and Ariadne. Here are some of the details on the setup:

Number of Nodes	: 20
Maximum Connections	: 20 traffic sources
Mobility Pattern	: Uniform
Link Bandwidth	: 2 mbps
Mobility Speed	: 20 m/s
Network Density	: 1000 m * 1000 m
Simulation Time	: 800 sec

5.2 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. This 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.

It describes the loss rate that will be seen by the transport protocols which in turn, affect the maximum throughput that the network can support.

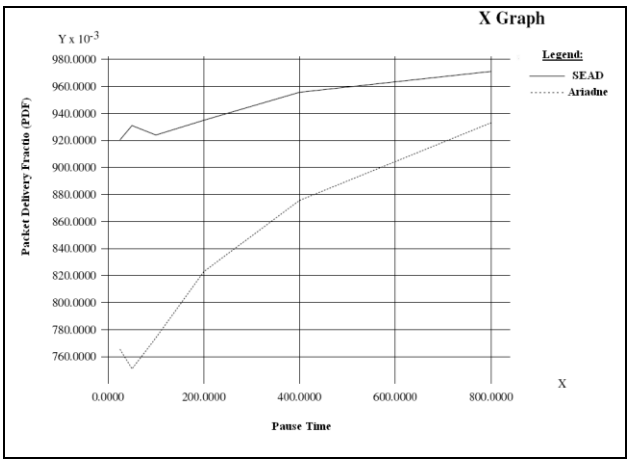

Figure 1: Packet Delivery Fraction Vs Pause Time

Figure 1 shows that 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. So at lower pause time SEAD contains more up to date routing information than Ariadne. At higher pause time 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.

5.3 Median Latency (ML)

The time taken by the route discovery 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.

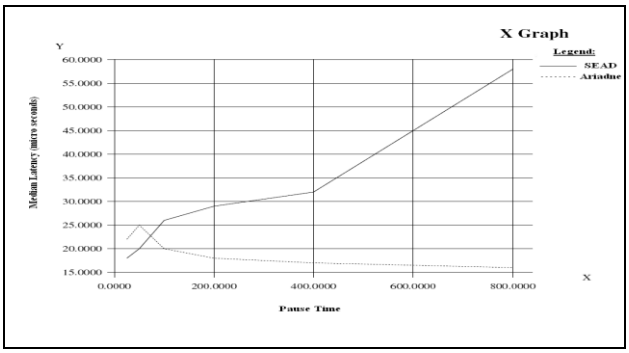

Figure 2: Median Latency Vs Pause Time

Figure 2 shows that time taken by the route discovery packet to reach from the source destination is known and median latency. The less time to discover the route to the destination indicates the higher performance of the protocol. Ariadne graph shows lower medial latency graph, which means it takes less time in the route discovery process when compared to SEAD, where as SEAD ML graph increases as the simulation time increases, indicating the congestion in the route discovery as the simulation time increases.

5.4 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.

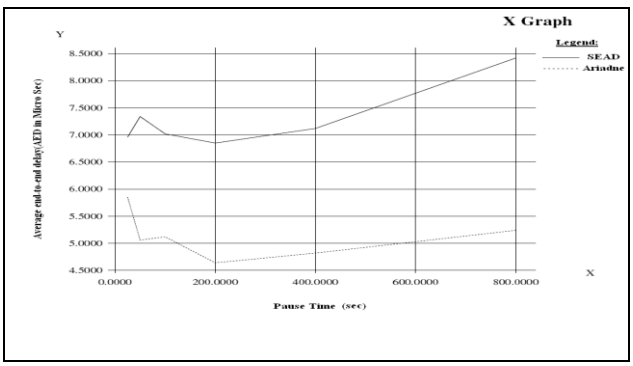

Figure 3: Average End to End Delay Vs Pause Time

Figure 3 shows the simulation results of the performance metric, average end-to-end delay. A higher valve of end-to-end delay means that the network is congested and hence the routing protocol doesn't perform well. SEAD graph for AED shows that at lower simulation time AED values are lesser and it increases with increase in simulation pause time. Ariadne graph for AED shows decreased values for lower pause time and increases slowly. Ariadne outperforms SEAD with lower AED values.

5.5 Packet 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.

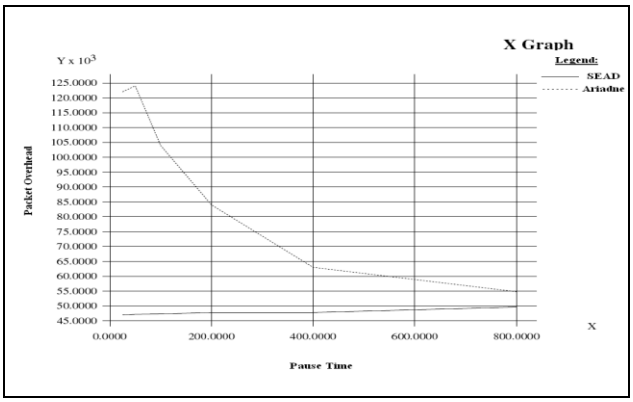

Figure 4: Packet Overhead Vs Pause Time

Figure 4 shows that Packet overhead graph for SEAD is lower than in Ariadne. PDF graph for Ariadne decreases gradually and reaches SEAD as the simulation time increases. The increased packet overhead in Ariadne at the lower pause time is due to the route discovery packet flooding. After discovering the secure routes, the packet overhead decreases gradually.

6. CONCLUSION AND FUTURE USES

Some analysis and performance comparisons of SEAD and Ariadne routing protocols in MANETs have been done in this research paper, based on the performance metrics rather than security metrics. 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.

Compared to SEAD, less control overhead is a distinct advantage of Ariadne. Thus Ariadne has better scalability than SEAD. However, Ariadne may suffer from long delays for route searching before they can forward data packets. Hence cannot be suitable for relative application.

The two protocols SEAD and Ariadne have been compared using simulation, it would be interesting to note the behaviour of these protocols on a real life bed that depends on the requirements of the routing environment of systems.

7. REFERENCES

[1] Hongmei Deng, Wei Li, Dharma, P. Agarwal,"Routing security in wireless Ad-Hoc networks", IEEE Communications Magazine, October 2002.

[2] Lidong Zhou, Zygmunt J. Haas, "Securing Ad-Hoc networks", IEEE Network, 1999

[3] Ebrahim Mohammad, Louis Dargin, "Routing Protocols Security in Ad-Hoc Networks", a Thesis at Oakland University School of Computer Science and Engineering.

[4] M. Aziz, M. Al-Akaidi, "Security issue in wireless Ad- Hoc Networks and the application to the telecare project", Proceedings of the 15 international Conference on Digital Signal Processing, DSP2007,pp. 491-494.

[5] Jane Zhen, Sampalli Srinivas,"Preventing Replay attacks for Secure Routing in Ad-Hoc Networks", Dalhousie University, Halifax, NS. Canada, Springer- Verlag Berlin Heidelberg 2003, Ad-Hoc- NOV 2003, LNCS 2865, pp.140-150, 2003.

[6] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02).

[7] Basagni, S. Conti, M. Giordano, S.Stojmenovi & cacute 2004. Mobile Ad-Hoc Networking: September 2004 Wiley –IEEE Press (pp. 1-33,275-300,330-354)

[8] David B.Johnson, David A. Maltz and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad-Hoc Networks in Ad-Hoc Networking, Editor: Charles E.Perkins, Chapter 5, pp.139-172, Addison-Wilsey, 2001

[9]Adrian Perrig, Ran Canetti, Dawn Songand J.D Tygar."Efficient and Secure Source Authentication for Multicast" in Network and Distributed System Security Symposium, NDSS '01, pages 35-46, February 2001.

[10]C.E. Perkins and E.M. Royer, - Adhoc On Demand Distance Vector Routing, University of California, Santa Barbar.