Improving Throughput and Delay of Secure Ad hoc on-Demand Distance Vector Routing (SAODV)

Atul Garg
SRIT,Jabalpur

Prof. Nitin Shukla
SRIT,Jabalpur

Abstract: - Mobile ad-hoc networks operate in the absence of any supporting infrastructure. The absence of any fixed infrastructure in mobile ad-hoc networks makes it difficult to utilize the existing techniques for network services, and poses number of various challenges in the area. The discovery and maintenance of secure route is the most flinty challenge. In this thesis, we first deliberate and implement one secure routing protocol SAODV and study its performance under different scenarios. Then we carry out a number of experiments using NS-3 to compare the performance of AODV, SAODV in terms of security level and routing discovery time under different setups. From these experiments, we can see that performance of AODV and SAODV and Aridane.

Keywords:AODV,SAODV,NS-3

I. INTRODUCTION

The increased demands for mobility and flexibility in our daily life are demand that lead the development from wired LANs to wireless LANs (WLANs). Today a wired LAN can offer users high bit rates to meet the requirements of bandwidth consuming services like video conferences, streaming video etc.

With this in mind a user of a WLAN will have high demands on the system andwill not accept too much degradation in performance to achieve mobility and flexibility. This will in turn put high demands on the design of WLANs of the future infrastructure-less network mobile devices connected by wireless.

Adhoc is Latin and means"for this purpose".

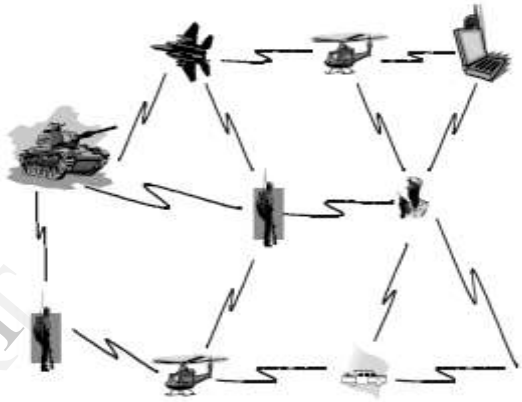


Figure 1 Overview of Mobile Ad hoc Network

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.Such networks may operate by themselves or may be connected to the larger Internet.

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still.

Therefore the network topology changes from time to time. Wireless ad-hoc network have many advantages:

- Low cost of deployment: Ad hoc networks can be deployed on the fly, hence no expensive infrastructure such as copper wires or data cables is required.
- Fast deployment: Ad hoc networks are very convenient and easy to deploy since there are no cables involved. Deployment time is shortened.
- Dynamic Configuration: Ad hoc network configuration can change dynamically over time. When compared to

configurability of LANs, it is very easy to change the network topology of a wireless network.

MANET has various potential applications. Some typical examples include emergency search-rescue operations,meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

Current Challenges

In a mobile ad hoc network, all the nodes cooperate with each other to forward the packets in the network, and hence each node is effectively a router. Thus one of the most important issues is routing. This thesis focuses mainly on routing issues in ad hoc networks. In this section, some of the other issues in ad hoc networks are described:

- Distributed network: A MANET is a distributed wireless network without any fixed infrastructure. That means no centralized server is required to maintain the state of the clients.
- Dynamic topology: The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time. Consequently, the routing protocols designed for such networks must also be adaptive to the topology changes.
- Power awareness: Since the nodes in an ad hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements. This implies that the underlying protocols must be designed to conserve battery life.
- Addressing scheme: The network topology keeps changing dynamically and hence the
- addressing scheme used is quite significant. A dynamic network topology requires a ubiquitous addressing scheme, which avoids any duplicate addresses. In wireless WAN environments, Mobile IP [10] is being used. Because the static home agents and foreign agents are needed, hence, this solution is not suitable for ad hoc network.

Network size: The ability to enable commercial applications such as voice transmission in conference halls, meetings, etc., is an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.

Security: Security in an ad hoc network is extremely important in scenarios such as a battlefield. The five goals of security availability, confidentiality, integrity authenticity and non-repudiation are difficult to achieve in MANET, mainly because every node in the network participates equally in routing packets. Security issues in MANETs

II. RELATED WORK

MANETs have certain unique characteristics that make them vulnerable to several types of attacks. Since they are deployed in an open environment where all nodes co-operate in forwarding the packets in the network, malicious nodes are difficult to detect. Hence, it is relatively difficult to design a secure protocol for MANET, when compared to wired or infrastructure-based wireless networks. This section discusses the security goals for an ad hoc network. Sample attacks and threats against existing MANET routing protocols are then discussed. I then discuss the working of two secure routing protocols to address these threats, ARIADNE [1] and SAODV [2].

2.1 Security Goals

To secure the routing protocols in MANETs, researchers have considered the following security services: availability, confidentiality, integrity, authentication and non-repudiation [3][10][15].

Availability guarantees the survivability of the network services despite attacks. A Denial-of-Service (DoS) is a potential threat at any layer of an ad hoc network. On the media access control layer, an adversary could jam the physical communication channels. On the network layer disruption of the routing operation may result in a partition of the network,

rendering certain nodes inaccessible. On higher levels, an attacker could bring down high-level services like key management service.

Confidentiality ensures that certain information be never disclosed to unauthorized entities.

It is of paramount importance to strategic or tactical military communications. Routing information must also remain confidential in some cases, because the information might be valuable for enemies to locate their targets in a battlefield.

Integrity ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information.

Non-repudiation ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

The networking environment in wireless schemes makes the routing protocols vulnerable to attacks ranging from passive eavesdropping to active attacks such as impersonation, message replay, message littering, network partitioning, etc. Eavesdropping is a threat to confidentiality and active attacks are threats to availability, integrity, authentication and non-repudiation.

Nodes roaming in an ad hoc environment with poor physical protection are quite vulnerable and they may be compromised.

Once the nodes are compromised, they can be used as starting points to launch attacks against the routing protocols.

2.1 Attacks and exploits on the existing protocols

In general, the attacks on routing protocols can generally be classified as routing disruption attacks [16][19] and resource consumption attacks [16][19].

In routing disruption attacks, the attacker tries to disrupt the routing mechanism by routing packets in wrong paths; in resource consumption attacks, some non-cooperative or selfish nodes may try to inject false packets in order to consume network bandwidth. Both of these attacks are examples of Denial of Service (DoS) attacks. Figure 2 depicts a broader classification of the possible attacks in MANETs.

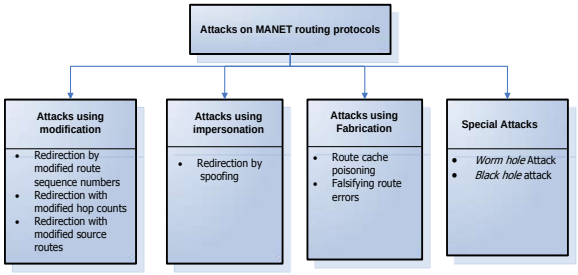


Figure 2: Classification of attacks on MANET routing protocols

Attacks using Modification

In this type of attacks, some of the protocol fields of the messages passed among the nodes are modified, thereby resulting in traffic subversion, redirection or Denial of Service (DoS) attacks. The following sections discuss some of these attacks.

- Modification of route sequence numbers: This attack is possible against the AODV protocol. The malicious node can change the sequence number in the route request packets or route reply packets in order to make the route fresh. In Figure 3.2, malicious node M receives a route request RREQ from node B that originates from node S and is destined for node X.
- M unicasts a RREP to B with a higher destination sequence number for X than the value last advertised by X. The node S accepts the RREP and then sends the data to X through M. When the legitimate RREP from X gets to S, if the destination number is less than the one advertised by M, then it will be discarded as a stale route. The situation will not be corrected until a valid RREP with higher sequence number than that of M gets to S.

- Modification of hop count: This type of attacks is possible against the AODV protocol in which a malicious node can increase the chance that they are included in a newly created route by resetting the hop count field of a RREQ packet to a lower number or even zero. Similar to route modification attack with sequence number, the hop count field in the routing packets is modified to attract data traffic.
- Modification of source route: This attack is possible against DSR which uses source routes and works as follows. In Figure 3, it is assumed that the shortest path exists from S to X. It is also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to X with the source route S-A-B-C-D-X. If M intercepts this packet, it removes D from the list and forwards it to C.
- C will attempt to forward this packet to X which is not possible since C cannot hear X. Thus M has successfully launched a DoS attack on X.

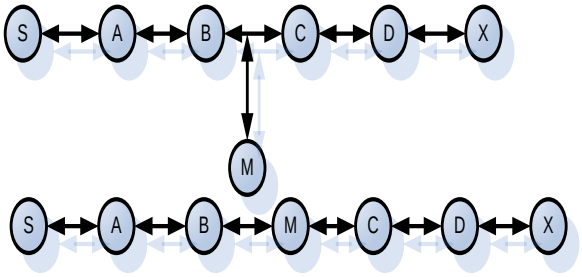


Figure 3: An example of route modification attack

Attacks using Impersonation

This type of attacks violates authenticity and confidentiality in a network. A malicious node can impersonate or spoof the address of another node in order to alter the vision of the network topology as perceived by another node. Such attacks can be described as follows in Figure 4

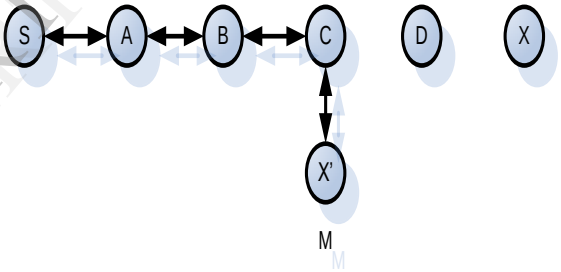


Figure 4: An example of impersonation attack

Node S wants to send data to node X and initiates a Route Discovery process. The malicious node M, closer to node S than node X, impersonates node X as X'. It sends a route reply (RREP) to node S. Without checking the authenticity of the RREP, node S accepts the route in the RREP and starts to send data to the malicious node. This type of attacks can cause a routing loop within the network.

II. PROPOSED WORK AND IMPLEMENTATION

A mobile ad hoc network (MANET) is a set of mobile wireless nodes that can communicate with each other without need the any fixed networking infrastructure. Thus, set up the ad-hoc network is fast and quite inexpensive. Such characteristics of MANETs have been easily applied in military field, disaster relief, the organization of conferences and so on.

MANETs are characterized by self-organized, dynamic changes of network topology, limited bandwidth, and instability of link capacity, etc, the reliability of data transmission in the network is uncertain. In some special application conditions with harsh requirements on PDR and

link quality, higher criteria for routing protocol will have been laid out [1].

Due to its infrastructure less architecture, cooperation among nodes is the key point for efficient transmission of data. For fast and reliable communication there will be a need of set path to deliver the packet from source to destination. For achieving such task every network requires a route finding mechanism do discover the available path to send the data i.e. routing mechanism.

In MANET, various routing mechanism has been applied, there fundamentally classified into two: static or table driven (also called proactive) and dynamic or on demand (also called reactive) routing. The table driven routing protocols, find out the available routes from all set nodes proactively i.e. before actual data transmission and periodically update them, the well known proactive protocols are OLSR (based on link state information), DSDV (based on distance vector). While in case of reactive routing, route discovery has been initiated when any one wants to send the data i.e. reactively, in other words discover routes when needed, the well known reactive routing protocols are DSR (based on link state information), AODV, TORA and ABR (all 3 are based on distance vector) . As shown in figure 1.

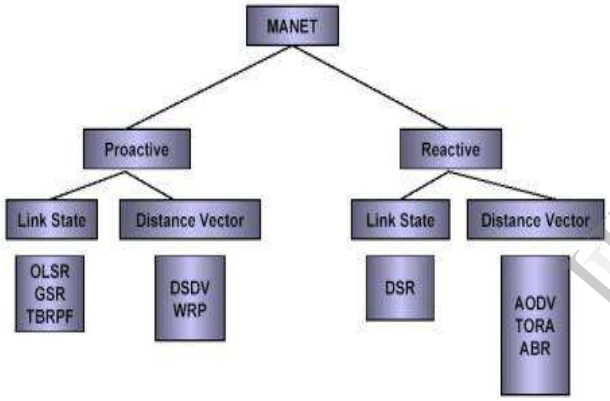


Figure 5. Classification of MANET Routing Protocol

Problem Domain

Author [2], has evaluated the routing protocols in this article, Author has found that with the ongoing progress of Telecommunication has increased the want of mobility, wireless or mobile networks and this desire has already swapped the wired networks. The upcoming networks has totally different infrastructure and has different protocols and devices. These networks are infrastructure less and no dedicated protocols or devices are required to deploy such networks. The theme of author [2] article is to evaluate the two secure routing protocols Ariadne and SAODV in the performance aspects instead of security aspects under Random Way Point and Manhattan Grid mobility models. Author used and implement the extension of AODV that is Secure Ad-hoc on-Demand Distance Vector routing protocol (SAODV) and the extension of DSR that is Ariadne in the NetworkSimulator2 (NS-2). In this paper author has compared these protocol on basis of following quality of service (QoS) parameters like delay, jitter, routing overhead, route acquisition time, throughput, hop count, packet delivery ratio using Manhattan grid and random waypoint mobility models.

Our proposed work is to test and evaluate the performance of NS-3 AODV centered as QoS and compare its performance and effectiveness with the outcome of authors [2] work.

The main motto of this work to carry out is the NS-3 AODV version is the latest and the simulator NS-3 has gain widest popularity among researches since its development. The reason behind is to its accuracy of evaluation found better than NS-2.

For this we have simulate NS-3 AODV protocol with the S-AODV and ARIADNE, for better evaluation, we have modified the NS-3 and tested AODV and compare its results with the protocols mentioned by the author.

Table I- Simulation Parameter

Simulation Parameter	Value
Simulator	NS-3 (VERSION 3. 18)
Operating System	Ubuntu 12.10
Simulation Time	50, 100, 150 sec
Simulation Area	1OOm x 100m
Number of Nodes	20,50,100,150,200
Transmission Range	50 meters
Movement Model	Random 2d-walk and random Waypoint
Speed of Mobile Nodes	I mlsec and 2 mlsec
Traffic Type	CBR
Data Payload	512 bytes
Packet Rate	20 p/sec- 80 p/sec
Mac Layer	802.11 DCF with RTS/CTS
Radio Frequency	2. 40Hz
Radio Channel Rate	2Mbps
Propagation Loss Model	Friis Propagation Loss Model
Propagation Delay	Constant Speed Propagation Delay

Evaluation Metric (QoS)

Following QoS has been consider for evaluation –

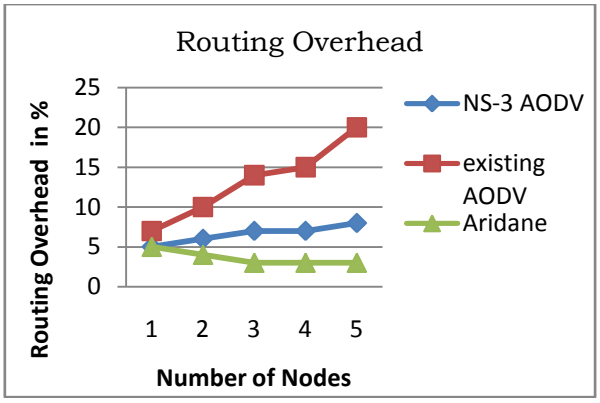
- Packet Delivery Ratio (PDR)
- Normalized Routing Overhead (NRO)
- Route Acquisition Time
- Jitter
- Average End to End Delay
- Throughput

IV. RESULTS

We have performed simulation of routing protocol on Network simulator NS-3.18 on Ubuntu 12.04 environment

A.Routing Overhead

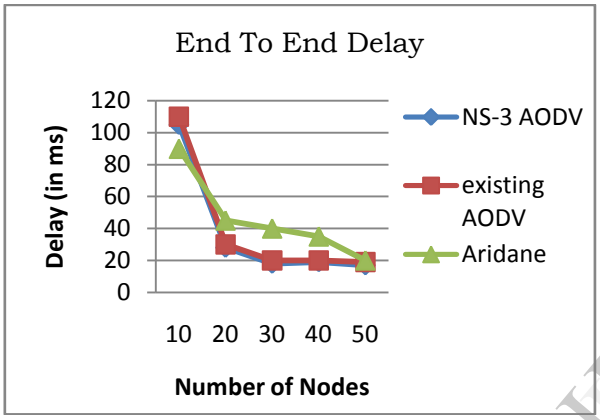
As we can see Routing overhead is less in case of ns-3 Aodv but slightly greater then with Aridane



(a)Routing over head on node in a nwetowrk

B. End To End Delay

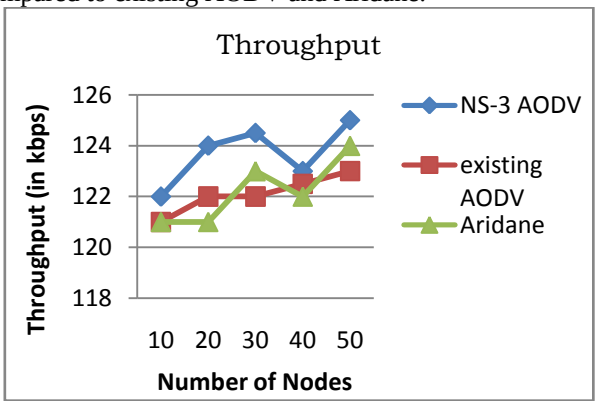
As we can see End to End slightly less then the existing Aridane and AODV



(b)End to End delay between nodes on network

C .Throughput

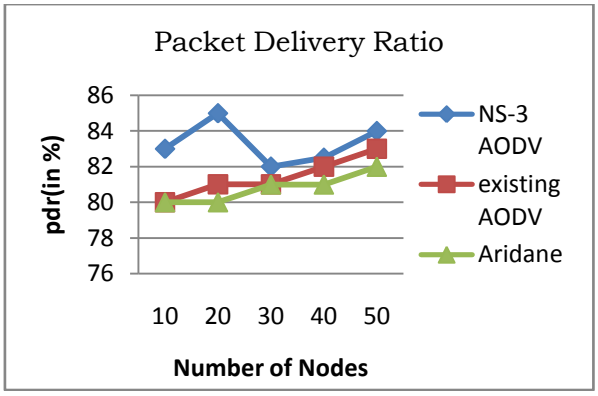
As we can in the graph Throughput is increased as compared to existing AODV and Aridane.



(b)Throughput of each node in a network

D. Packet Delivery Ratio

As we can see in the graph Packet Delivery Ratio has been increased.



(d)Packet delivery ratio of node in a network.

V. CONCLUSION

I have analyzed two secure routing protocols, ARIADNE and SAODV, based on their respective underlying protocols, DSR and AODV The ultimate goal of a routing protocol is to efficiently deliver the network data to the destinations; therefore, two metrics, Packet Delivery Fraction (PDF) and Normalized Routing Load (NRL),packet delivery ratio(PDR) and End to end delay are used to evaluate the protocols. In order to get the accurate experimental results, each scenario is run eleven times in order to calculate the average value for the two evaluation metrics. Through the collected evaluation metrics from the various scenarios, the impacts of attacks upon the routing protocols are then studied.

REFERENCES:

1) LIU Jian and LI Fang-min "An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad hoc Networks", IEEE Fifth International Conference on Information Assurance and Security, 2009.
2) Muhammad Naeem, Zahir Ahmed, Rashid Mahmood and Muhammad Ajmal Azad "QOS Based Performance Evaluation of Secure On-Demand Routing Protocols for MANET's", IEEE, 2010.
3) L. Kleinrock and F.A. Tobagi, "Packet Switching in Radio Channel," In proceeding of IEEE Trans on Comm., vo1.23, no.5, pp. 1400-1416,1990.
4) S.S. Lam, "A Carrier Sense Multiple Access Protocol for Local Networks," In proceedings ofComputer Networks, vol. 4, no. 16, pp.2132, 1991
5) M.M.A. Assaf, "Wireless Ad-Hoc Networks," In Department of EECS, Syracuse University, Syracuse, New York, November 2004.
6) Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad-Hoc Networks," Wireless Networks (WINET), vol. 11, no.I-2, pp. 21-38, January 2005.
7) T.H. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," IETF RFC3626 - Experimental Standard, October 2003.
8) M.G. Zapata and N. Asokan, "Secure Ad-Hoc On-Demand Distance Vector Routing," In proceeding of ACM Mobile Computing and Communications Review, vol. 3, no. 6, pp.l06-107, July 2002.
9) Y.C. Hu, A. Perrig and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad-Hoc Networks," In Proceeding of 8th ACM International Conference Mobile Computing and Networking (Mobicom '02), Atlanta, Georgia, pp. 12-23, September 2002.
10) A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and Secure Source Authentication for Multicast," In proceeding of Network and Distributed System Security Symposium (NDSS'Ol), San Diego, California, USA, February 2001.

11) R.J. Perlman, "Fault-Tolerant Broadcast of Routing Information," In proceeding of Computer Networks, North-Holland, vol. 7, no. 9, pp. 395- 405, 1983.
12) L. Zhou and Z. 1. Haas, "Securing Ad-Hoc networks," IEEE Network Magazine,pp.24-30, ovember/December 1999.
13) P. Papadimitratos and Z. 1. Haas, "Secure Routing for Mobile Ad-Hoc Networks," In Proceeding of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS '02),Texas, USA, January 2002.