ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

An Analysis of Performance and Security of the Routing Protocols for Mobile Ad Hoc Networks

M. Jayabharathy
Research Scholar
Department of Computer Science
Prist University, India

Abstract:
In recent years mobile ad hoc networks have become very popular and lots of research is being done on different aspects of MANET. Mobile Ad Hoc Networks (MANET)-a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points, bridges, etc.). There are different aspects which are taken for research like routing, synchronization, power consumption, bandwidth considerations etc. This paper mainly focuses on two important issues in mobile Adhoc network-Performance and security. There are some of the general routing issues in MANETs and classifies the routing protocols. The working description consists of Destination Sequence Distance Vector/Proactive Protocol and Adhoc on Demand Distance Vetcor/Reactive protocol. Adhoc network have some security issues such as routing disruption and resource consumption. The working mechanism of four of the state-of-the-art routing protocols SEAD, ARIADNE, ARAN and SRP. It also compares these routing protocols with respect to their features. A study of certificate-based authentication mechanisms is also follows. A comparison of the mechanisms is done with respect to these requirements.

Keywords: Destination Sequence Distance Vector, Adhoc on Demand Distance Vetcor, routing disruption, resource consumption, certificate-based authentication.

I. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium. For example, consider communication amongst soldiers in a battlefield, involving troops spread out over a large area. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring down the whole network. This problem has led to a growing interest among the research community in mobile ad hoc networks, wireless networks comprised of mobile computing devices communicating without any fixed infrastructure.

II. EXISTING SYSTEM

Problem occurs in networks using contention based protocols such as ALOHA, CSMA/CD, etc. When two nodes which are out of range of each other send data frames to a node which is within their respective radio ranges, a collision of data frames occurs.

III. PROSPOSED SYSTEM

Several routing protocols have been proposed for ad hoc networks. In this section a broad classification of these routing protocols is given. At one end are the table-driven or proactive routing protocols such as the Destination Sequenced Distance Vector (DSDV) routing protocol, Wireless Routing Protocol (WRP), etc. At the other end, are the on-demand or reactive protocols such as Dynamic Source Routing (DSR) protocol and the Ad hoc On-demand Distance Vector (AODV) routing protocols. The primary goals of a secure protocol – confidentiality, integrity and availability, authenticity and non-repudiation. The working of a few secure routing protocols which address these threats such as SEAD, ARIADNE, ARAN and SRP is then described. The next section discusses another important issue in MANETs- certificate-based authentication

IV. ROUTING IN MANET

TABLE- DRIVEN /PROACTIVE ROUTING PROTOCOLS

In table-driven or proactive protocols, the nodes maintain an active list of routes to every other node in the network in a routing table. The tables are periodically updated by broadcasting information to other nodes in the network. Thus, they are an extension to the wired network routing protocols such as the Routing Internet Protocol (RIP). Any node wishing to communicate with another node has to obtain the next hop neighbor on the route to the destination from its routing table.

DESTINATION SEQUENCED DISTANCE VECTOR (DSDV) ROUTING PROTOCOL

The Destination Sequenced Distance Vector (DSDV) protocol is a proactive routing protocol based upon the distributed Bellman Ford algorithm. In this routing protocol, each mobile host maintains a table consisting of the next-hop neighbor and the distance to the destination in terms of number of hops. It uses sequence numbers for the destination nodes to determine “freshness” of a particular route, in order to avoid any short or long-lived routing loops. If two routes have the same sequence number, the one with smaller distance metric is advertised. The sequence number is incremented upon every update sent by the host. All the hosts periodically broadcast their tables to their neighboring nodes in order to maintain an updated view of the network. The tables can be updated in two ways – either incrementally or through a full dump. Let us consider an example to understand the routing mechanism better. Consider the network topology shown in figure 1.1. The routing table for this network is shown in table 1.1. As shown in the table, each node maintains a route to every other node in the network during the route establishment phase. Whenever there is a link break in the network, the end node of the broken link propagates a routing table update message with the broken link’s weight assigned to infinity. This message is broadcasted by every node to its neighbors. A broken link is denoted by an odd sequence number and an ordinary link by an even sequence number. When node 1 wants to send data to node 7, it checks the next hop neighbor for node 7, which is 2 and passes the data packet to it.

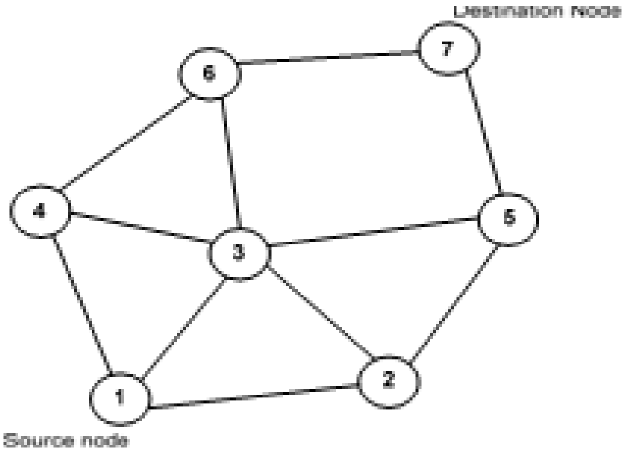

Figure.1.Topology graph of the network

Table.1. Routing table for node 1

Destination	Next hop	Metric	Sequence number
1	-	0	S40_1
2	2	1	S340_2
3	3	1	S22_3
4	4	1	S334_4
5	2	2	S76_5
6	3	2	S84_6
7	2	3	S94_7

ON- DEMAND/ REACTIVE ROUTING PROTOCOLS

In contrast to table driven routing protocols, on-demand routing protocols find route to a destination only when it is required. The on-demand protocols have two phases in common – route discovery and route maintenance. In the route discovery procedure, a node wishing to communicate with another node initiates a discovery mechanism if it doesn’t have the route already in its cache. The route maintenance phase involves checking for broken links in the network and updating the routing tables. The working of a few reactive routing protocols is now described.

AD HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

The Ad hoc on-demand Distance Vector routing protocol inherits the good features of both DSDV and DSR. The AODV routing protocol uses a reactive approach to finding routes and a proactive approach for identifying the most recent path. More specifically, it finds routes using the route discovery process similar to DSR and uses destination sequence numbers to compute fresh routes.

ROUTE DISCOVERY

During the route discovery process, the source node broadcasts RREQ packets similar to DSR. The RREQ packet contains the source identifier (SId), the destination identifier (DId), the source sequence numbers (SSeq), the destination sequence number (DSeq), the broadcast identifier (BId) and TTL fields. When an intermediate node receives a RREQ packet, it either forwards it or prepares a Route Reply (RREP) packet if it has a valid route to the destination in its cache. Figure 1.2 shows an example of route discovery mechanism in AODV. Let us suppose that node 1 wants to send a data packet to node 7 but it doesn’t have a route in its cache. Then it initiates a route discovery process by broadcasting a RREQ packet to all its neighboring nodes.

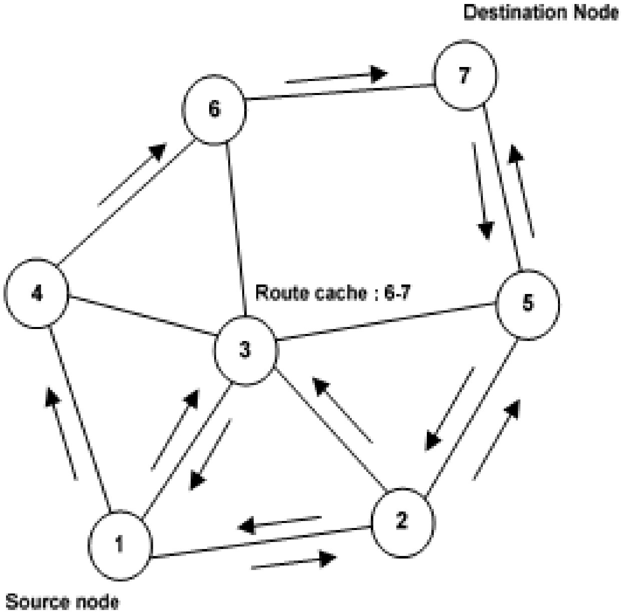

Figure.2. Route discovery in AODV

ROUTE MAINTENANCE

The route maintenance mechanism works as follows – Whenever a node detects a link break by link layer acknowledgements or HELLO beacons, the source and end nodes are notified by propagating an RERR packet similar to DSR. This is shown in Figure 1.3. If the link between nodes 3 and 5 breaks on the path 1-3-5-7, then both 5 and 3 will send RERR packets to notify the source and destination nodes.

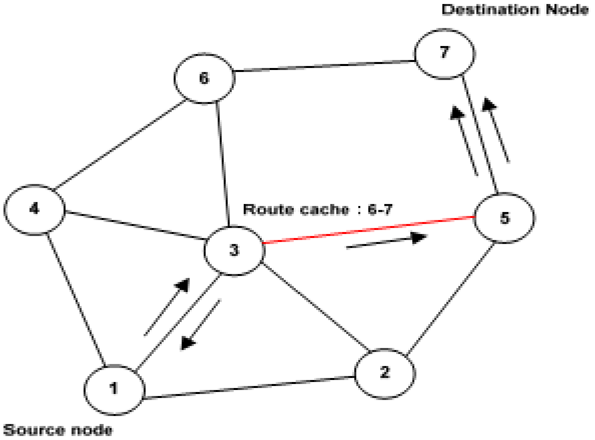

Figure .3. Route Maintenance in AODV

One optimization possible in AODV route maintenance is to use an expanding ring search to control the flood of RREQ and discover routes to unknown destinations. The main advantage of AODV is that it avoids source routing thereby reducing the routing overload in large networks. Further, it also provides destination sequence numbers which allows the nodes to have more up-to-date routes. However, AODV requires bidirectional links and periodic link layer acknowledgements to detect broken links. Further, it has to maintain routing tables for route maintenance unlike DSR.

V. SECURITY IN MANET

SECURE AND EFFICIENT AD HOC DISTANCE VECTOR (SEAD) ROUTING PROTOCOL

The *Secure and Efficient Ad hoc Distance vector routing protocol* (SEAD) is based upon the *DSDV-SQ* routing protocol (which is a modified version of *DSDV* routing protocol). It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and sequence number in the routing table. More specifically, for authenticating a particular sequence number and metric, the node generates a random initial value x Є $(0,1)^{\rho}$ where ρ is the length in bits of the output of the hash function, and computes the list of values $h_0,h_1,h_2,h_3,\ldots,h_n$, where $h_0=x$, and h_i = H(h_i-1) for $0<i \leq n$, for some *n*. As an example, given an authenticated *hi* value, a node can authenticate $h_{i-3}$by computing H (H (H (h_i-3))) and verifying that the resulting value equals $h_{i.}$

Each node uses one authentic element of the hash chain in each routing update it sends about itself with metric 0. This enables the authentication for the lower bound of the metric in other routing updates for that node. The use of a hash value corresponding to sequence number and metric in a routing update entry prevents any node from advertising a route greater than the destination's own current sequence number. The receiving node authenticates the route update by applying the hash function according to the prior authentic hash value obtained and compares it with the hash value in the routing update message. The update message is authentic if both values match. The source must be authenticated using some kind of broadcast authentication mechanism such as TESLA. Apart from the hash functions used, SEAD doesn't use *average settling time* for sending triggered updates as in DSDV in order to prevent eavesdropping from neighboring nodes.

ARIADNE

The ARIADNE routing protocol proposed by Yi-Chun Hu, Adrian Perrig, etc. prevents against several types of *active* and *passive* attacks. Active attacks are those where a malicious node eavesdrops on a network and injects fake packets. On the other hand, passive attacks are threats against the confidentiality of the communication rather than the network's function. Active attacks can be of several types such as Active-0-1 (in which the attacker owns one node), Active-1-x (in which the attacker owns one compromised node and distributes the cryptographic keys to its x-1 other nodes), and Active-y-x. In addition, an attacker that has compromised nodes is called an Active VC attacker when it owns all nodes through a vertex cut in the network that partitions the good nodes into multiple sets, thereby forcing the good nodes to communicate through the attacker nodes. The wormhole attack is an example of this type of attack. It also prevents against the black hole attack by using per hop hashing mechanism and many kinds of Denial of Service (DoS) attacks due to flooding of route request packets in the network. Furthermore, it is also efficient since it is based on a reactive protocol which has a better performance than table-driven protocols, and symmetric key cryptography.

AUTHENTICATED ROUTING FOR AD HOC NETWORKS (ARAN)

Authenticated Routing for Ad hoc Networks (ARAN) is a secure routing protocol based on the AODV protocol. The assumption in ARAN is that every node has a certificate that is signed by a trusted authority. The route discovery and route maintenance mechanisms are based on AODV and elaborated as follows; Let us assume that a source node S wants to discover a route to destination node D. Also assume that A, B and C are three intermediate nodes on the path from S to D, that their certificates are cert$_{A,}$ cert$_B$ and cert$_C$ and their private keys are K$_{a,}$ K$_{b,}$ K$_c$ respectively. During the route discovery phase, a source node broadcasts a RREQ packet signed with its public key. The packet contains the destination node's address D, source node's certificate cert$_S$, a nonce N and a timestamp t. The nonce and timestamp ensure that the route is fresh. A sequence of route discovery messages is shown below:

S → * : (RREQ, D, cert$_S$, N, t) K$_s$
A → * : ((RREQ, D, cert$_S$, N, t) K$_s$) K$_a$,cert$_A$
B → * : ((RREQ, D, cert$_S$, N, t) K$_s$) K$_b$,cert$_B$
C → * : ((RREQ, D, cert$_S$, N, t) K$_s$) K$_c$,cert$_C$
(NOTE: * denotes a broadcast)

As shown, each intermediate node (such as A, B or C) that forwards the RREQ packet checks the signature(s) of the previous node on the packet by extracting the public key from the certificate. Further, it removes the previous node's signature, signs the RREQ packet with its own private key, adds the certificate to the header and broadcasts the packet to its neighboring nodes. This process continues until the packet reaches the destination D.

CERTIFICATE-BASED AUTHENTICATION

The certificate-based authentication is well studied in wired networks. However, adapting certificate-based authentication protocols to mobile ad hoc networks (MANETs) is a nontrivial task, mainly because, in a MANET, as opposed to conventional wired networks, typically no fixed infrastructure or centralized management exists. For example, a conventional certificate-based authentication system relies on a fixed trusted Certificate Authority (CA), which is responsible for the creation, distribution, renewing, and revocation of certificates. In a MANET, due to issues such as node mobility, limited wireless medium, and frequent link failures, it is typically not feasible to include such a fixed centralized CA in the network. Various approaches have been proposed to tackle the unique challenge of adapting certificate-based methods for distributed authentication in mobile ad hoc networks. The contribution of this thesis is twofold: first, an analysis of the requirements of a secure distributed authentication system for MANETs, and secondly a survey some of the existing certificate-based authentication mechanisms, their comparison including pros and cons; in the context of distributed authentication.

VI. METRICS FOR EVALUATION

The following metrics have been identified, based on which the authentication mechanisms can be evaluated. Some of the metrics have been adapted from.

Successful Certification Ratio (μ) measures the ratio of the number of successful certification services (including issuance, NC_{ISS}, and renewal, NC_{REN}, respectively) to the total number of requests for such services ($NC_{TOT-ISS}$ and $NC_{TOT-REN}$, respectively). It gives an idea about the efficiency of the mechanism in providing successful certification services. If$\mu_{REN}$is the successful certification renewal ratio, and μ_{ISS} is the successful certificate issuance ratio, then their respective value can be calculated as follows:

$\mu REN = NCREN / NCTOT - REN$

$\mu ISS = NCISS / NCTOT - ISS$

Here, $NC_{REN}$and $NC_{ISS}$are the respective total number of certificate renewed and issued, and $NC_{TOT-REN}$ and $NC_{TOT-ISS}$the respective number of requests for certificate issuance and renewal.

Settling time (st) measures the initial time taken for all the nodes in the network to be issued valid certificates. The value of *st* can be calculated as the difference between the time when all the nodes are issued valid certificates and the starting time when the process of certificate issuance begins. The settling time taken will depend on factors such as the number of malicious or non-cooperative nodes, the algorithms used for key generation and distribution, etc. If the pre-authentication methods are efficient (R.5), the settling time will be less.

c)Frequency of Certification (f_{cert}) measures the number of certification services per time interval.

$f\,cert = N\,cert / T\,\mathrm{int}$

Here N_{cert} is the total number of certification services (issuance/renewal) by nodes in the network, and T_{int} is the simulation time.

VII. CONCLUSION AND FUTURE WORK

This thesis focuses on the two most important issues in mobile ad hoc networks – performance and security. Each mobile node in a MANET acts as a router by forwarding the packets in the network. Hence, one of the challenges in the design of routing protocols is that it must be tailored to suit the dynamic nature of the nodes. Some of the scenarios such as battlefield are quite demanding in terms of both throughput and security. For such scenarios, we require a combination of a reactive and proactive approach. As a continuation of this research, future work could involve the study of AODV and its secure version, the SAODV which was not studied in this thesis. The simulation study of attacks in a MANET and the resulting performance degradation is also an interesting area of research. Further, the key management issue is another area which needs further research. A deeper understanding of the authentication mechanisms such as the certificate-based approach and their related performance study will be very useful in designing secure applications for MANETs.

VIII. REFERENCES

[1]. C. Siva Ram Murthy, B.S. Manoj, "*Ad Hoc Wireless Networks: Architectures and Protocols*", Prentice Hall Publishers, May 2004, ISBN 013147023X

[2]. C.-K. Toh, "*Ad Hoc Mobile Wireless Networks: Protocols and Systems*", Prentice Hall publishers, December 2001, ISBN 0130078174

[3]. C. Perkins and P. Bhagwat, *Highly Dynamic Destination-Sequenced Distance-Vector Routing* (*DSDV*) for Mobile Computers. In Proc. of the ACM SIGCOMM, October 1994. http://www.cs.umass.edu/~mcorner/courses/691M/papers/perkins.pdf

[4]. Shree Murthy, J.J. Garcia-Luna-Aveces, "*A Routing Protocol for Packet Radio Networks*," Proc. ACM International Conference on Mobile Computing and Networking, pp. 86-95, November, 1995 http://www.pdos.lcs. mit.e du/decouto/ papers/dube97.pdf

[5]. C.-C. Chiang, "*Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel*," Proc. IEEE SICON '97, Apr. 1997, pp. 197–211. http://www.ics.uci.edu/~ atm/adhoc/paper-collection/gerla-routing-clustered-sicon97.pdf

[6]. [online] The Secan Lab, University of Luxembourg, Luxembourg. http://wiki.uni.lu/secan-lab/ Distributed+Bellman-Ford.html

[7]. [online] The Secan Lab, University of Luxembourg, Luxembourg. http://wiki.uni.lu/secan-lab/Count-To-Infinity+ Problem. html