ANALYSIS OF SECURE ROUTING SCHEME FOR MANET

a thesis report submitted in partial fulfillment of the requirement
for the award of degree of

MASTER OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

BY
ALEKHA KUMAR MISHRA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY ROURKELA
ROURKELA-769008 (ORISSA), INDIA
2009

ANALYSIS OF SECURE ROUTING SCHEME FOR MANET

a thesis report submitted in partial fulfillment of the requirement
for the award of degree of

MASTER OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

BY

ALEKHA KUMAR MISHRA

Under the guidance of
Prof. BIBHUDUTTA SAHOO

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY ROURKELA
ROURKELA-769008 (ORISSA), INDIA

2009

NATIONAL INSTITUTE OF TECHNOLOGY

ROURKELA

CERTIFICATE

This is to certify that the thesis entitled, "**Analysis of Secure Routing Scheme for MANET**", is a bona fide work done by **Mr. Alekha Kumar Mishra** in partial fulfillment of requirements for the award of Master of Technology Degree in Computer Science and Engineering with specialization in information security at National Institute of Technology, Rourkela (Deemed University) is an authentic work carried out by him under my supervision and guidance.

The matter embodied in the thesis has not been submitted to any other University / Institute for the award of any Degree or Diploma to the best of my knowledge.

Prof. B. D. Sahoo

Date:

Dept. of Computer Science and Engg.

National Institute of Technology

Rourkela -769008

ACKNOWLEDGMENT

I am presenting my work on "**Analysis of Secure Routing Scheme for MANET**" with a lot of pleasure and satisfaction. I take this opportunity to thank my supervisor, **Prof. B.D. Sahoo**, for guiding me and providing me with all the facilities, which paved way to the successful completion of this work. This thesis work was enabled and sustained by his vision and ideas. His scholarly guidance and invaluable suggestions motivated me to complete my thesis work successfully.

I owe a lot to Professor B. Majhi, Head of the Department of Computer Science & Engg for his valuable suggestions and cooperation at various stages. I would like to thank Prof. A. K. Turuk, Asst. Professor, Department of Computer Science for his support and showing me right track whenever I seek his help. I am also thankful to all the faculty members, Department of Computer Science and Engg. who gave all possible help to bring my thesis work to the present shape. I would like to express my deep gratitude to my parents. Their continuous love and support gave me strength for pursuing my dream.

Last but not the least; I am thankful to my friends who have been a source of encouragement and inspiration throughout the duration of this thesis.

CONTENTS

ABSTRACT

Mobile ad hoc networks pose various kinds of security problems, caused by their nature of collaborative and open systems and by limited availability of resources. In our work we look at AODV in detail, study and analyses various attacks that can be possible on it. Then we look into some existing mechanism for securing AODV protocol. Our proposed work is an extension to Adaptive-SAODV of the secure AODV protocol extension, which includes tuning strategies aimed at improving its performance. In A-SAODV an intermediate node makes an adaptive reply decision for an incoming request that helps to balance its load that is over-burdened by signing and verification task of incoming messages. Namely, we propose a modification to adaptive mechanism that tunes SAODV behavior. In our paper we have proposed an extension to Adaptive-SAODV of the secure AODV protocol extension, which includes further filtering strategies aimed at further improving its network performance. We have analyzed the how our proposed algorithm can help in further improvement of performance in adaptive SAODV and also compared its performance with existing mechanisms using simulation.

LIST OF FIGURES

LIST OF TABLES

I

INTRODUCTION

1.1 ADHOC NETWORK

Recently laptop computers have replaced desktops with all respect as they continue to show improvements in convenience, mobility, capacity and availability of disk storage. Now small computers can be equipped with storage capacity of Gigabytes, high resolution color display, pointing devices and wireless communication adapters. Since, these small computer can be operated with the power of battery, the user are free to move as per their convenience without bothering about constraints with respect to wired devices.

In a wireless ad hoc network [3,20], the devices communicate with each other using a wireless physical medium without relying on pre-existing wired infrastructure. That's why ad hoc network is also known as infrastructure less network. These networks are also known as mobile ad hoc networks (MANETs), can form stand-alone groups of wireless terminals, but some of these may be connected to some fixed network. A very fundamental characteristic of ad hoc networks is that they are able to configure themselves on-the-fly without intervention of a centralized administration. The terminals in the ad hoc network can not only act as end-system but also as an intermediate system (routers). It is possible for two nodes which are not in the communication range of each other, but still can send and receive data from each other with the help of intermediate nodes which can act as routers. This functionality gives another name to ad hoc network as "multi-hop wireless network".

The major characteristics which distinguish an ad hoc network from a cellular network is the adaptability to changing traffic demand and physical conditions. Also since the attenuation characteristics of wireless media are nonlinear, energy efficiency will be potentially superior and the increased spatial reuse will yield superior capacity and thus

spectral efficiency. These characteristics make ad hoc networks attractive for pervasive communications, a concept that is tightly linked to heterogeneous networks and 4G architectures.

Depending on their communication range, wireless ad hoc networks can be classified into Body (BAN), Personal (PAN) and Wireless Local (WLAN) Area Networks. A Ban is a set of wearable devices that have a communication range of about 2 m. The second type, PANs, refers to the communication between different BANs and between BAN and its immediate surroundings (within approximately 10 m). WLANs have communication ranges of the other of hundreds of meters. The main existing technology for implementing BANs and PANs is Bluetooth, while for WLANs the main option is the family of standards IEEE 802.11. Although adhoc networks are not restricted to these technologies, most of the current research assumes Bluetooth or IEEE 802.11 to be the underlying technologies. For more features authors are requested to refer article [2] in detail.

The most active area of concern and research field in ad hoc networking is routing. In recent works the objective of routing algorithm to minimizing the number of hops has been taken over by the optimization of multiple parameters, such as packet error rate over the route, energy consumption, network survivability, routing overhead, route setup and repair speed, possibility of establishing parallel routes, etc.

Since the advent of Defense Advanced Research Project Agency (DARPA) packet radio network in the early 1970s, a number of protocols have been developed for ad hoc mobile networks. The proposed protocols are intended to deal with the typical limitation of ad hoc networks like high power consumption, low bandwidth and high error rates. The existing protocols can be broadly categorized into 2 types; Table-driven (proactive) and Demand-driven (reactive).

Table-driven routing protocols attempted to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more table to store their routing information, and they respond to changes in network topology by propagating updates throughout the network

in order to main a consistent network view. The areas in which they differ are the number of necessary routing tables and the method by which changes in the network structure are broadcast. Some examples are DSDV (Destination-Sequenced Distance-Vector Routing), CGSR (Cluster-head Gateway Switch Routing), WRP (Wireless routing protocol), etc.

On the other hand, the table-driven routing protocols have different approach by creating routes only when desired by the source node. When a node required sending some data to a desired destination, it initiates a route discovery process within the network. This process is terminated once a route is found or all possible routes are examined. Once a route has been established, it is maintained by a route maintenance procedure until destination becomes inaccessible or route is no longer desired. Two most popular routing protocols of this type are DSR (Dynamic Source Routing) and AODV (Ad Hoc On-demand Distance Vector) protocols.

1.2 SECURITY ISSUES OF EXISTING ROUTING PROTOCOLS

Among all the research issues of ad hoc network, security is particularly more challenging due to the nature of communication and lack of infrastructure support. A number of security mechanisms has been developed and proposed, but still it is still difficult to ensure that whole network is free from any malicious attack.

The insecurity of the wireless links, energy constraints, poor physical protection of nodes in a hostile environment compare to wired network and vulnerability of statically configured security scheme has been identified in article [4], [5], [6] and [16] as challenges. No part of the network is dedicated to support any specific functionality individually, with routing being the most vulnerable. The characteristics of ad hoc can not rely on a specific centralized certification authority (CA) to issue certificates and for other administrative works due to the dynamically changing topology.

The absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a line of defense, separating nodes into trusted and not-trusted. Such a distinction would have been based on a security policy, the possession of the necessary credentials and the ability for nodes to validate them. In

MANET, there may be no ground for an a priori classification, since all nodes are required to cooperate in supporting the network operation, while no prior security association can be assumed for all the network nodes. Moreover, freely roaming nodes in MANET form transient associations with their neighbors join and leave sub-domain independently and without notice. Thus it may be difficult in most cases to have a clear picture of the ad hoc network membership.

In our work we have concentrated on the security issues associated with the existing routing protocol AODV [1,2], which is also one of the most popular reactive routing protocols. Moreover any mechanism applied to AODV can be adopted by other routing protocols of ad hoc network with few changes.

1.3 OVERVIEW OF PROPOSED WORK

Considering various security issues of AODV routing protocol several secure AODV routing protocol has been proposed featuring variety of advanced mechanism for securing data and control information. SAODV[7,8] (secured Ad hoc On Demand Vector routing) is one of the popular existing secured mechanism which takes help of digital signature and hash chain techniques to secured AODV packets. SAODV enables each node to sign an outgoing message with its own secret key and verify all incoming message with the public key shared by other nodes. Since, digital signature technique is based on asymmetric key cryptographic method, heavy amount of computational time is required for signature and verification mechanism, and hence it affects the performance of SAODV protocol.

Since SAODV has been proved to be free of most of the security issues of AODV protocol, our objective is to propose some changes in routing behaviour of SAODV which in turn will improve its performance in term of performance metrics [12,13]. In a recent work called A-SAODV[12] (Adaptive SAODV), an adaptive mechanism that tunes the behaviour of SAODV to improve its performance. It makes an adaptive decision whether to reply an incoming request based on the load threshold value of the current node provided it has a valid and fresh route to the requested destination. This

decision helps to balance the load of intermediate nodes which are over-burdened by signing and verification task of incoming messages. In our paper we have proposed an extension to Adaptive-SAODV of the secure AODV protocol extension, which includes further filtering strategies aimed at further improving its network performance. We have analyzed the how our proposed algorithm can help in further improvement of performance in adaptive SAODV and also compared its performance with existing mechanisms using simulation.

1.4 OUTLINE OF THE REPORT

Chapter-2 describes AODV protocol in detail, which covers its basic elements of routing and parameters. We have discussed how AODV protocol has been designed to exchange routing information which makes it more reactive and popular among other existing protocol. We have also gone through the different message format of AODV mentioning the purpose of all the fields in it. The reason behind choosing AODV for studying is that any security mechanism that can be implemented on AODV also can be applicable on other reactive protocols with few changes.

Security concerns and attack classification in ad hoc routing mostly of AODV protocol has been discussed in detail in chapter-3. This chapter explains the weak points of AODV routing which a malicious node can use as an advantage for it and launch attack in the network.

Chapter-4 is a quick look on all existing security mechanisms securing AODV. It includes Secure AODV protocol with its message extension format and securing mechanisms like digital signature and hash chain. This chapter also describes the flaws of existing mechanisms along with proposed solutions for them. The performance issue of SAODV is also described in chapter-4 along with the adaptive mechanism used in Adaptive SAODV to tune its performance in detail featuring its decision algorithm.

Our proposed work has been discussed in chapter-5. It includes the algorithm and mechanism of proposed modification followed by analysis and simulation results in Chapter-6.

II

AD HOC ON-DEMAND DISTANCE VECTOR ROUTING

2.1 OVERVIEW

Ad Hoc On-Demand Distance Vector Routing protocol [1,2] is a pure on-demand route acquisition system, since nodes that do not lie on active paths (selected path for communication between two arbitrary nodes) neither maintain any routing information nor participate in any periodic routing table exchanges. Moreover, a node does not have to discover and maintain a route to another node until the two need to communicate, unless the former node is offering its services as an intermediate forwarding station to maintain connectivity between two other nodes.

When the local connectivity of the mobile node is of interest, each mobile node can become aware of the other nodes in its neighborhood by the use of several techniques, including local broadcasts known as hello messages. The routing tables of the nodes within the neighborhood are organized to optimize response time to local movements and provide quick response time for requests for establishment for new routes. The primary objectives of AODV are:

a) To perform path discovery process when necessary. AODV uses broadcast route discovery mechanism.

b) To distinguish between local connectivity management (neighborhood detection) and general topology maintenance

c) To broadcast information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information.

The AODV algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network.

The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity "problem offers a quick convergence when the ad hoc network topology changes. When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.

One distinguishing feature of AODV is its use of a destination sequence number of each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination a requesting node select the route with greatest sequence number. The route discovery and maintenance procedure has been discussed in the following section in detail.

2.2 PATH DISCOVERY

The Path Discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in the routing table or the route entry has been expired. Every node maintains two separate counters: a node sequence number and a request broadcast id. The sequence number is incremented every time before a node sends a RREQ or RREP message. The request broadcast id is incremented before a new request is disseminated. The RREQ format is shown in the figure 2.1.

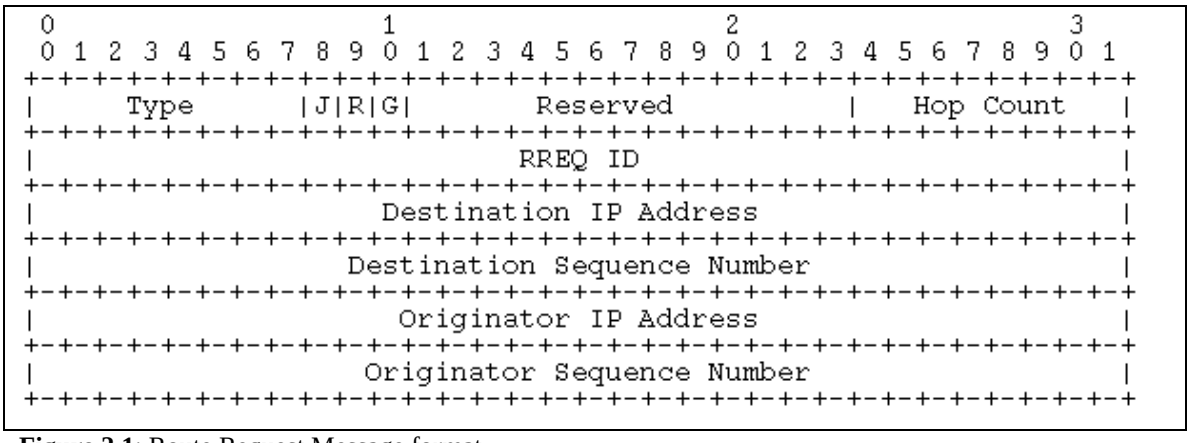

Figure 2.1: Route Request Message format.

The sequence number and request broadcast id uniquely identifies a RREQ. Each neighbor either satisfies the RREQ by sending a route reply (RREP) back to the source, or re-broadcasts the RREQ to its own neighbors after increasing the Hop Count. Notice that a node may receive multiple copies of the same route broadcast packet from various neighbors. When an intermediate node receives a RREQ, if it has already received a RREQ with the same broadcast id and source address, it drops the redundant RREQ and does not rebroadcast it. If a node cannot satisfy the RREQ, it keeps track of necessary routing information in order to implement the reverse path setup, as well as the forward path setup that will accompany the transmission of the eventual RREP.

When RREQ arrives at a node that possesses the current to the destination, it determines whether it has a valid route entry for the desired destination. If finds the freshness of the route by comparing sequence numbers. After ensuring that route is an updated route and valid one, the node unicast a route reply (RREP) message to the source using the reverse path that has been by the RREQ message. In some cases (for Gratuitous RREPs) the intermediate node has to unicast a gratuitous RREP to the destination node. If the node can not satisfies the RREQ, it re-broadcast it after incrementing Hop Count field to its neighbors. Finally, the request reaches the destination node if no intermediate node can satisfy the RREQ and destination ultimately sends RREP using reverse path back to the originator. The RREP format is shown in the figure 2.2 and 2.3.

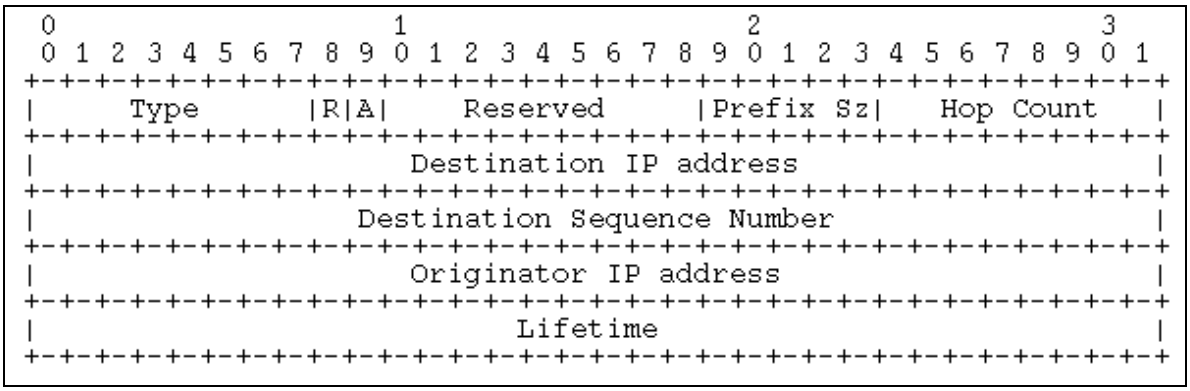

Figure 2.2: Route Reply Message Format

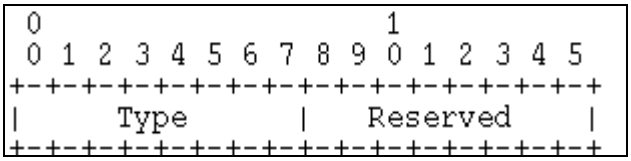

Figure 2.3: Route-Reply Acknowledgement format

2.3 HELLO MESSGES AND ROUTE TABLE INFORMATION

A node may offer connectivity information by broadcasting local Hellos messages. A node should only use hello messages if it is part of an active route. In every hello message interval, the node checks whether is has sent a broadcast with in last hello message interval. If it has not, it may broadcast a RREP with TTL field equal to 1 called a Hello message.

In addition to the source and destination sequence numbers, other useful information is also stored in the route table entries. Associated with reverse path routing entries is a timer, called the route request expiration timer. The purpose of this timer is to purge reverse path routing entries from those nodes that do not lie on the path from the source to the destination. The expiration time depends upon the size of the ad hoc network. Another important parameter associated with routing entries is the route caching timeout, or the time after which the route is considered to be invalid. In each routing table entry, the address of active neighbors through which packets for the given destination are received is also maintained. A neighbor is considered active (for that destination) if it originates or relays at least one packet for that destination within the most recent active timeout period. This information is maintained so that all active source nodes can be notified when a link along a path to the destination breaks. A route entry is considered active if it is in use by any active neighbors. The path from a source to a destination, which is followed by packets along active route entries, is called an active path.

A mobile node maintains a route table entry for each destination of interest. Each route table entry contains the following information

- Destination IP Address
- Destination Sequence Number

- Valid Destination Sequence Number flag
- Other state and routing flags
- Network interface
- Hop Count
- List of Precursors (see section 2.4)
- Lifetime (expiration or deletion time of the route)

2.4 ROUTE ERROR MESSAGE AND ROUTE EXPIRATION

When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates those destinations which are no longer reachable by way of the broken link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbors that are likely to user it as a next hop towards each destination. The information the precursor lists is most easily acquired during the processing for generation of a RREP message, which by definition has to be sent to anode in a precursor list.

Generally, route error and link breakage processing requires the following steps

- Invalidating existing routes
- Listing affected destinations
- Determination which, if any, neighbors may be affected
- Delivering an appropriate RERR to such neighbors

A Route error (RERR) message may be broadcast, unicast, or iteratively unicast to all precursors. Even when the RERR message is iteratively unicast to several precursors, it is considered to be single control message for the purposes of the description in the text that follows. With that understanding, a node should not generate more that a RERR rate limit message per unit time. The RERR message format has been shown in the figure 2.4.

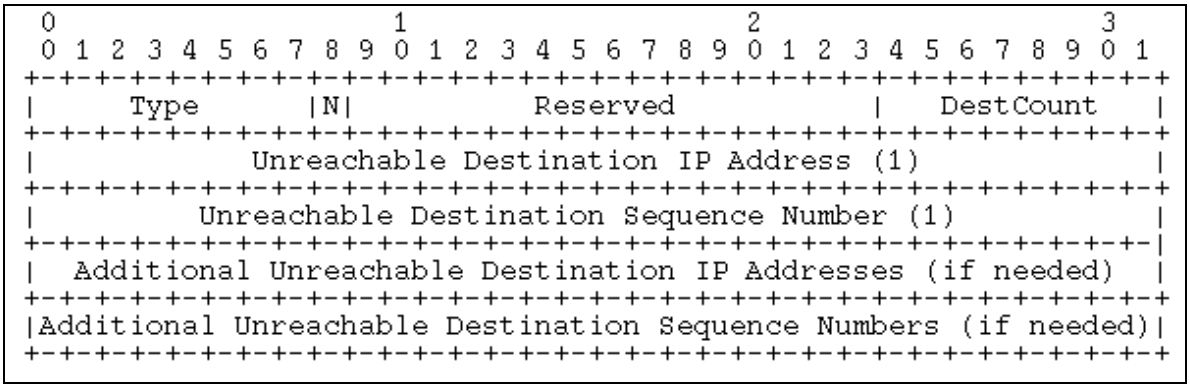

Figure 2.4: Route Error Message Format

Within the limits imposed by worst-case route establishment latency as determined by the network diameter, AODV is an excellent choice for ad-hoc network establishment. It is useful in applications for emergency services, conferencing, battlefield communications, and community-based networking.

AODV reduces memory requirements and needless duplications. It also has quick response to link breakage in active routes. The most important feature it has is loop-free routes maintained by use of destination sequence numbers and most important scalable to large populations of nodes.

III

SECURITY ISSUES OF AODV

3.1 ANALYSIS OF SECURITY ATTACK

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. In order to protect against insider attacks, it is necessary to understand how an insider can attack a wireless ad-hoc network. Several attacks have been discussed in several literatures. However, the articles [4], [5] and [6] adopted a systematic way to study the insider attacks against AODV routing protocols. In this chapter we have discussed different existing threats on AODV protocols with references to the above mention literatures.

On the basis of actions performed by the interceptor they can be categorizes as follows.

3.1.1 ATTACKS USING MODIFICATION

Malicious nodes can cause redirection of network traffic and DoS(Denial of services) attacks by altering control message fields or by forwarding routing messages with falsified values. For example, in the network illustrated in Figure 3.1, a malicious node M could keep traffic from reaching X by consistently advertising to B a shorter route to X than the route to X that C advertises. Attacks like redirection by modified route sequence numbers, redirection with modified hop counts, denial-of-service with modified source routes and tunneling are under this category.

3.1.2 ATTACKS USING IMPERSONATION

Spoofing occurs when a node misrepresents its identity in the network, such as by altering its MAC or IP address in outgoing packets, and is readily combined with

modification attacks. Forming loops by spoofing is an example of attack using impersonation

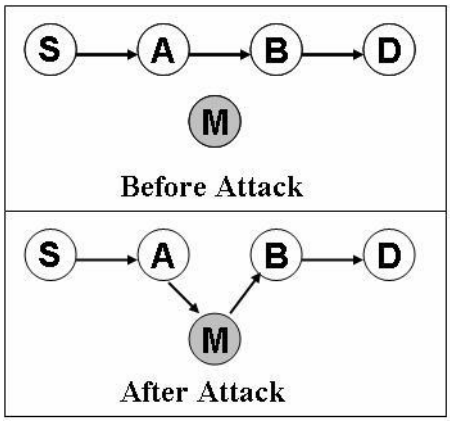

Figure 3.1: Attack using modification

3.1.3 ATTACKS USING FABRICATION

The generation of false routing messages can be classified as fabrication attacks. Such attacks can be difficult to verify as invalid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted.

Falsifying route errors in aodv and dsr, routing table overflow attack are of this category

3.2. ATOMIC AND COMPOUND MISUSES

Based on the composition of operations for performing attack as mentioned in [4], misuses of AODV have been classified into two categories: atomic misuses and compound misuses. Intuitively, atomic misuses are performed by manipulating a single routing message, which cannot be further divided. In contrast, compound misuses are composed of multiple atomic misuses, and possibly normal uses of the routing protocol.

First, it is necessary to identify a number of misuse goals that an inside attacker may want to achieve, and then study how these goals may be achieved through misuses of the routing messages. The misuse goals that we have considered are listed as follows.

Route Disruption (RD):- Route Disruption means either breaking down an existing route or preventing a new route from being established. Figure 3.2 shows an example of this.

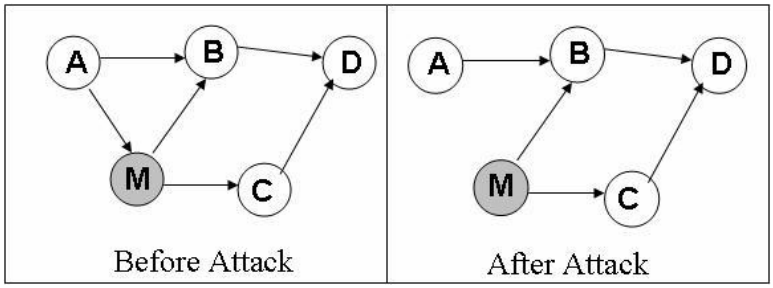

Figure 3.2: The malicious node M performs route disruption by breaking the existing route between A and C

Route Invasion (RI):- Route invasion means that an inside attacker adds itself into a route between two endpoints of a communication channel and figure 3.3 illustrates this.

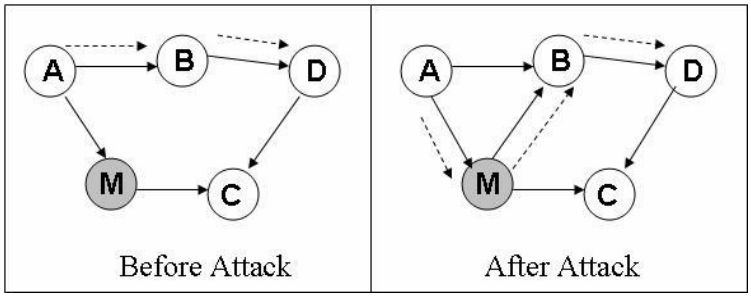

Figure 3.3: Malicious node achieves route invasion by adding itself to the route between A to D

Node Isolation (NI):- Node isolation (Figure 3.4) refers to preventing a given node from communicating with any other node in the network. It differs from Route Disruption in that Route Disruption is targeting at a route with two given endpoints, while node isolation is aiming at all possible routes.

Resource Consumption (RC):- Resource consumption refers to consuming the communication bandwidth in the network or storage space at individual nodes. For example, an inside attacker may consume the network bandwidth by either forming a loop in the network.

Analysis of atomic misuses can be done in an effective way through understanding the effects of possible atomic misuse actions.

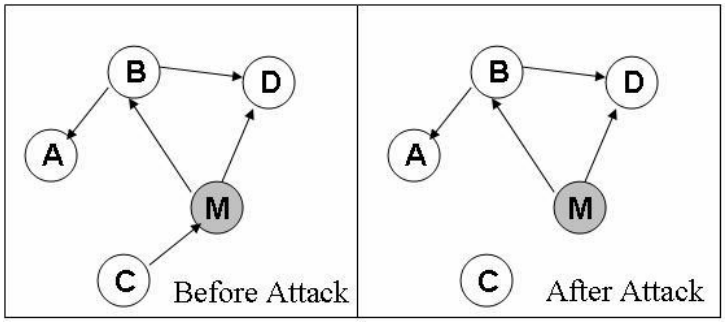

Figure 3.4: Node C has been isolated by the attacker M from rest of the nodes in the network.

Each atomic misuse action is an indivisible manipulation of one routing message. Specifically, the atomic misuse actions in AODV have been divided into the following four categories:

Drop (DR): Here, the attacker simply drops the received routing message.

Modify and Forward (MF): After receiving a routing message, the attacker modifies one or several fields in the message and then forwards the message to its neighbor(s) (via unicast or broadcast).

Forge Reply (FR): The attacker sends a faked message in response to the received routing message. Forge Reply is mainly related to the misuse of RREP messages, which are in response of RREQ messages.

Active Forge (AF): The attacker sends a faked routing message without receiving any related message.

As already mentioned that compound misuse can be performed by combining atomic misuses, one category of compound misuse is to simply repeating the same type of atomic misuses. The more interesting and complex one is that an attacker can combine several atomic misuses in a planned way and launch them. For example, an attacker may repeatedly launch the same type of atomic misuses to make the impact persistent. Another way, an attacker may launch some early atomic or compound misuses to prepare for some later ones. A crucial issue here is to understand the compound misuses that can be used as "building blocks" of more complex attacks, interested reader can refer the proceedings of Sun et al[4].

IV

EXISTING SECURE MECHANISMS FOR AODV

4.1 SECURE AD HOC ON DEMAND VECTOR ROUTING

One of the most popular existing security mechanism for AODV is secured AODV [7,8], that uses per-hop hashing technique to protect mutable fields has been proposed by Zapata and Asokan in 2002. Secured AODV (SAODV) which is based on public key cryptography extends the AODV message format to include security parameter for security the routing messages.

Considering RREQ and RREP message in SAODV protocol there are two alternatives for ensuring secured route discovery; first, the basic one where only destination is allowed to reply a RREP and the second, any intermediate node which has valid routing information allowed to reply a RREP. Two mechanisms are used to secure the message. Digital Signature is used to authenticate and preserve integrity of non-mutable fields' data in RREQ and RREP messages. For non-mutable field the authentication is done in an end-to-end manner. Hash chain to secure mutable field like hop count information. The two mechanisms have been discussed in brief in following sections.

4.1.1 HASH CHAIN

The hash chain mechanism helps any intermediate node to verify that the hop count has not been decreased by any malicious node. A hash chain is formed by applying a one-way hash function repeatedly to a seed (random number). Every time a node originates a RREQ or RREP message, the following operation are performed on hash chain

i. A random number 's is generated called seed
ii. The MAX_HOP_COUNT field is set equal to time to leave value from IP header

iii. The value of s is stored in HASH field.

iv. Hash function is chosen and assigned to the field HASH_FUNCTION

v. TOP_HASH field is calculated as

$$TOP\_HASH = HASH\_FUNCTION^{MAX\_HOP\_COUNT}(s)$$

i.e., the hash function is applied to s exactly MAX_HOP_COUNT times.

Every time a node receive a RREQ or RREP from its neighbor node, it verify by performing the operation

$TOP\text{-}HASH = = HASH\_FUCTION^{MAX\_HOP\_COUNT - HOP\_COUNT}$ (HASH), which is true if both are equal.

Before re-broadcasting a RREQ or forwarding a RREP message, a node apply hash function to the HASH value i.e. HASH = HASH_FUNCTION (HASH). The HASH_FUNCTION, MAX_HOP_COUNT, TOP_HASH and HASH field are transmitted with the AODV messages in the signature extension so that intermediate node can verify the message using them.

4.1.2 SAODV DIGITAL SIGNATURE

As mentioned earlier that SAODV use two way for performing verifying authentication of message. Therefore, signing and verifying mechanism by sender and receiver also differ up to some extent.

In the first one, where only destination is allowed to reply, every time a RREQ is sent, the sender signs the message with its private key. An intermediate node verifies the signature before creating or updating the reverse path to the source and stores it only if verification is successful. For RREP message the final destination node sign the message using its private key. Intermediate and final node again verifies the signature before creating a route to that host.

In the second method the signing and verifying process is almost similar to first one i.e. the sender signs the message with its private key and an intermediate node verifies the signature before creating or updating the reverse path to the source and stores it only if verification is successful. But the difference is that the RREQ message also has a second

signature that is always stored with the reverse path route. The second signature is needed to be added in the gratuitous reply (see AODV message format) of that RREQ and in regular RREPs to future RREQs that node might reply as an intermediate node. An intermediate node that wants to reply a RREP needs not only the correct route, but also the signature corresponding to that route to add in the RREP and the lifetime and the originator IP address fields that work with that signature. All the nodes that receive the RREP and those update the route; store the signature, the lifetime and originator IP address with that route. Route discovery mechanism of SAODV has been described concisely in Figure 4.1.

```
1) Sender Generates RREQ packet;
2) Sender signs all non-mutable fields (except hop count and hash chain fields) with its private key;
Apply Hash to a seed to generate hash chain field;
if (intermediate node can reply){
        Clear destination only tag;
        Include second signature in the signature extension;
}
Append signature extension to RREQ packet;
3) Broadcast RREQ to all neighbour nodes;
4) Intermediate node receives RREQ packet;
5) Node Verifies signature with public key of source (from RREQ packet);
        if (valid packet)
        then update routing information of source in any (establishment of reverse path);
6) if (destination I.P == node I.P){
        Generate RREP;
        Sign all the signs all non-mutable fields (except hop count and hash chain fields) with its
        private key;
        Apply Hash to a seed to generate hash chain field;
        Append signature extension to RREP packet;
        Unicast RREP to the neighbor which is in the reverse path for the source node;
}
else if ( Node has valid route for destination && !(Destination only tag)){
        Generate RREP;
        Copy the signature and other necessary field of source to the signature extension;
        Sign all the signs all non-mutable fields (except hop count and hash chain fields) with its
        private key;
        Apply Hash to a seed to generate hash chain field;
        Append signature extension to RREP packet;
        Unicast RREP to the neighbor which is in the reverse path for the source node;
}
else
        Forward RREQ to all its neighbouring node;
```

Figure 4.1: SAODV Route Discovery algorithm

If a node want to have the feature of replying as an intermediate node for a route, it has to store the 'RREQ Destination' or 'RREP Originator' IP address, the lifetime and the signature. Since Hello messages of AODV are nothing but a reply messages, so they are signed and verified the same as mentioned above. Also every node generating or forwarding a RERR message uses digital signature to sign the whole message and is verified by the neighbour who receives it. The packet format of secure AODV extension for all message formats has been shown in the figure 4.2-4.6.

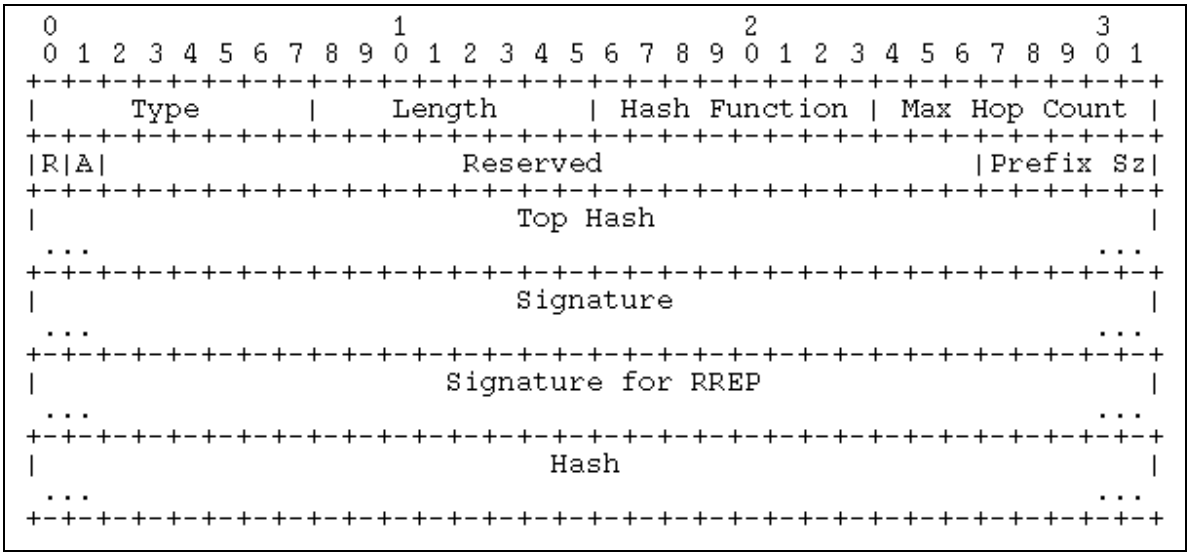

Figure 4.2: RREQ (double) signature extension

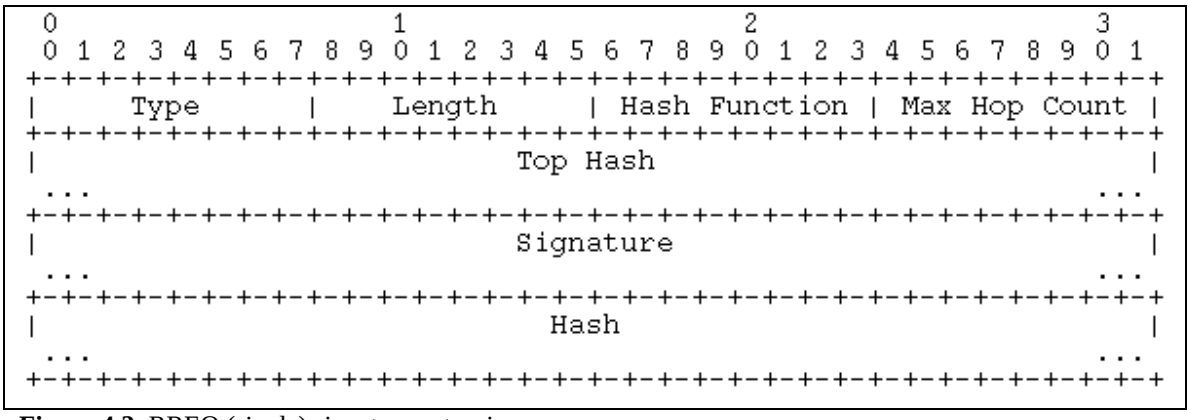

Figure 4.3: RREQ (single) signature extension

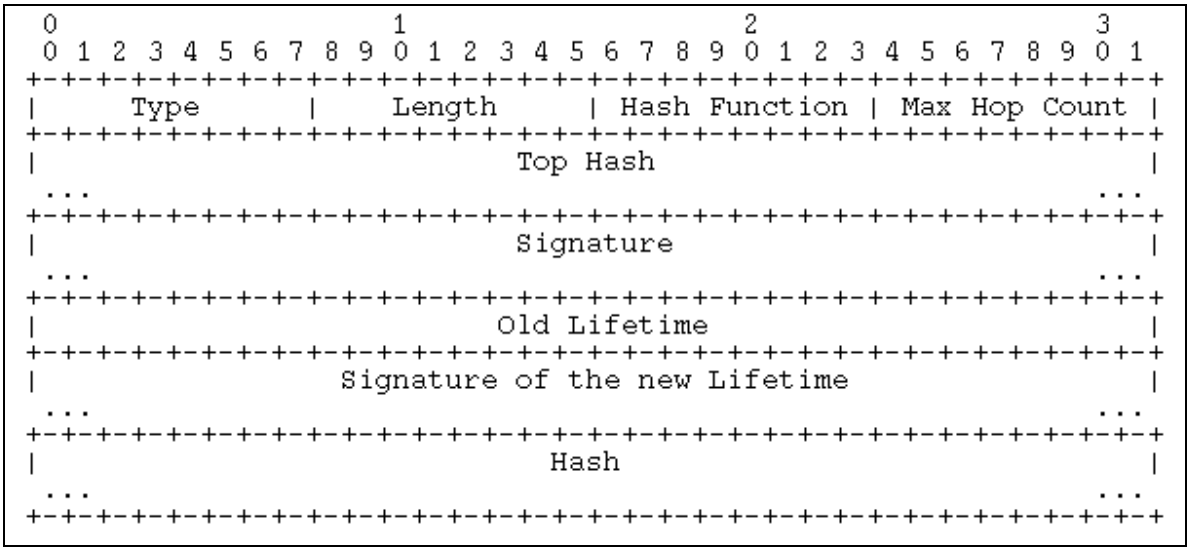

Figure 4.4: RREP (double) signature extension

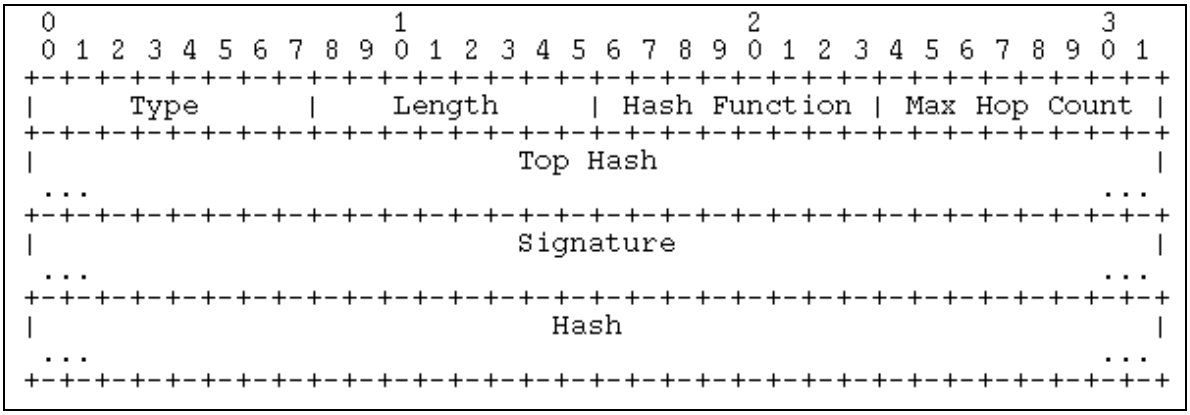

Figure 4.5: RRP (single) signature extension

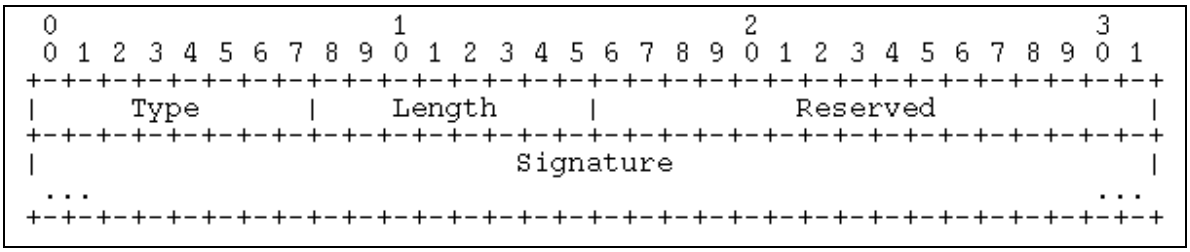

Figure 4.6: RERR signature extension

SAODV does not take help of any extra message for security operations. Since a digital signature of x can be created only by x using its private key, the SAODV mechanism

prevents attacks like active forge, forged reply etc. using digital signature and prohibits malicious node from illegally modifying mutable fields like hop count. However, SAODV also has some issues like it cannot detect tunnel attack and cannot do much about denial of service attack. In our work we are more concerned about the performance of SAODV rather about securing mechanism. SAODV messages are significantly larger and require heavy computation time because of digital signatures especially for double signature mechanism.

4.2 OTHER WORKS

In a work related to securing AODV protocol, Pirzada and McDonald [9] proposed a symmetric-key based secured mechanism for exchanging routing messages. In their work they have stressed on exchanging encrypted message using group session key that has been generated using a group session key exchange protocol. Before initiating a new connection with any immediate neighbour, a node first establish a group session key K with its neighbours. Then, the routing message exchange is performed using this group session key. If any intermediate node moves out of the wireless range a new group session key is established. To avoid synchronization problem the author has recommended that each node maintain a table of session key along with its other primary key associated with group members. This scheme is based upon point-to-point and end-to-end encryption using symmetric key based mechanism

Siva kumar and Ram kumar has also presented their work[10] regarding the security of mutable fields (hop count) in AODV route discovery process. They investigated the shortcomings of SAODV and proposed some modification to overcome the same. They used recently proposed Broadcast Encryption scheme (BE) for providing efficient authentication strategy. They relies on two-hop authentication mechanism for providing security to mutable fields where the use of BE can ensure that a node securely recognizes its two hop neighbours, without having to trust the one-hop neighbours in between the two nodes. Using this authentication mechanism they have overcome some of the pitfalls of SAODV protocols.

Li et. al [11] present a secured efficient Ad Hoc Routing Protocol (SEAR) that emphasizes the uses symmetric cryptography while asymmetric cryptography is used only for the distribution of initial key commitments. Their protocol SEAR uses one-way hash functions to provide authenticity by generating a set of hash values called authenticators associated with each node. SEAR takes the help of two hash chains. First hash chain is to protect the sequence numbers and hop counts for routing packets associated with routes to the node. This hash chain values are generated by recursively applying a hash function. Second one is a TESLA key chain for authenticating RERR messages. Performance analysis shows that SEAR has been proven better than SAODV with respect to all performance metrics [13] used to evaluate AODV protocol. Other related works has been cited at [17], [18] and [19]. Interested reader can go through these links for detail.

Though the above works has proposed various ways of securing different fields of routing messages using most advanced cryptographic techniques but they lacks mechanism which emphasizes the trade-off between security and performance of a secure routing protocol.

4.3 PERFORMANCE ISSUE OF SAODV

As we mentioned earlier that SAODV extension protocol is the most successful secured protocol extension for AODV and already it has been proven better than AODV by [13] experimentally. It has been found that all securing proposal including SAODV consists of two kinds of techniques; one emphasizing on guaranteeing authenticity and integrity of routing messages and other to monitor the behaviour of other nodes in routing operation. Both this techniques results in consumption of some additional resources of mobile ad hoc network like bandwidth, processing power etc. Considering constraints on limited resources of a mobile node in MANET the main issue of our concern is the trade-off between security and performance of secure AODV protocol. Though SAODV mechanism does not require any additional message in addition to routing messages of AODV, SAODV messages are significantly larger and require heavy computation time

because of digital signatures especially for double signature mechanism. So, its performance may degrade significantly in heavy traffic scenarios of MANEt.

4.4 ADAPTIVE-SAODV PROTOTYPE

In a recent work, Cerri and Ghioni [12] proposed an adaptive mechanism that tunes its behaviour for optimizing the performance of routing operation. They developed a prototype called Adaptive SAODV (A-SAODV) which is a multithreaded application. Cryptographic operations are performed by a dedicated thread to avoid blocking the processing of other message and other thread to all other functions.

The promising feature of A-SAODV which is called adaptive reply decision is to optimize SAODV performance with respect to double signature option. Allowing intermediate node to reply on behalf of destination node in AODV has a positive impact on its performance it do not require any additional computation. But, the case is different in SAODV as node may spend much time in computing these signatures and becomes overloaded. If only destinations are allowed reply then the performance becomes even worse than SAODV. This tends to make double signature mechanism adaptive i.e. the intermediate nodes are allow to reply only if they are not overloaded.

Each node has a queue of routing messages to be signed or verified, and the length of this queue is used to check the current load state of the routing operations. When a node receives a RREQ message and has the information to generate a RREP on behalf of the destination, it checks the queue length and compares it with a threshold. If the queue length is lower than the threshold, the node generates a RREP; otherwise it forwards the RREQ without replying. Figure 4.7 shows this adaptive behaviour of an intermediate node in A-SAODV. The same mechanism can be applied when generating a RREQ message in order to decide between a single signature and a double signature. In the simplest case, the threshold can be a fixed value; however, this value may be adjusted taking some external factors into account. An additional external parameter may be used to take into account the previously mentioned external factors (how much a node is willing to collaborate, e.g., depending on its battery state).

```
1) Intermediate node receives RREQ packet;
2) if ( Node has valid route for destination && !(Destination only tag)){
        L=length(routing packet queue to be signed or verified);
        if( L >= queue_threshold )
                simply forward the packet to its neighbouring nodes;
        else
                reply to source node using the procedure involved in SAODV;
```

Figure 4.7: A-SAODV algorithm

Experiments and simulation shows that Adaptive-SAODV is better than both variations (single and double signature) of SAODV with respect to performance metrics like first data packet delay, number of successful connection etc. In our proposed work we have tried to further modify the adaptive ness of an intermediate node to enhance its performance. The following chapter discusses our proposed work in detail.

V

PROPOSED WORK

Our objective is to extend adaptive-SAODV with a modification in the behaviour of an intermediate node using double signature mechanism. The proposed prototype intend to relax the overloading of a node with heavy cryptographic computations like signing signing and verifying routing packet up to a possible extent. The adaptive reply decision in A-SAODV depends mostly on the routing queue length of the current node which it uses to determine its load state. Our work further look for the load state of immediate neighbour of a current node which has fresh route to destination so that if it is found that the neighbour node is not overloaded then the replying job is left to it. Successive sections discuss the modification in detail.

5.1 MODIFIED ADAPTIVE REPLY DECISION

As we have discussed earlier that in A-SAODV, each node has a queue of routing messages to be signed or verified, and the length of this queue is used to check the current load state of the routing operations. When a node receives a RREQ message and has the information to generate a RREP on behalf of the destination, it checks the queue length and compares it with a threshold. If the queue length is lower than the threshold, the node generates a RREP; otherwise it forwards the RREQ without replying.

In our proposed work, when an intermediate node that receives RREQ, finds that it has a fresh enough route to the destination and it is allowed to reply if it has them same, first it checks time to leave field (TTL) field of the packet, if its below some predefined time to leave threshold then the packet is simply forwarded to its neighbour nodes assuming that either the packet is going to be dropped after TTL hops or the packet going reach its destination with in this number of hops. When the above condition is not true then the node follows the steps of A-SAODV i.e. if the node has fresh route to destination and

queue length is lower than the threshold, the node generates a RREP on behalf of destination node. If it is already over loaded with the job of singing or verifying of routing messages then the node do not simply forward as mentioned in A-SAODV rather it looks for its immediate neighbour that has a fresh route to destination. This can be easily found by looking at the next hop field of the fresh route entry to the destination in the routing table. Now the node checks for the load state of its neighbour in the path to the destination and if finds that the next hop neighbour node's routing packet queue length is less than the threshold value then it simply forward RREQ only to this neighbouring node, otherwise, it again broadcast the route request message to all its neighbour since this condition shows that both the current node and the neighbouring node in the path to destination are overloaded. Figure 5.1 shows the modification to behaviour of an intermediate node in A-SAODV.

```
/*Each node exchange their routing packet queue size
 (route load) periodically with the help of Hello message.*/
1) Intermediate node receives RREQ packet;
2) if ( Node has valid route for destination && !(Destination only tag)){
        node_L = length(routing packet queue to be signed or verified);
        if(RREQ.TTL <=TTL_threshold)
            forward the packet to all neighbours;
        else if( node_L >= queue_threshold ){
            nbd_to_dest = the neighbour node which is equal to the next hop in
            the route entry to the destination;
            nbd_L= length(routing packet queue of the nbd_to_dest);
            if ( nbd_L < queue_threshold )
                  simply forward the packet to nbd_to_dest;
            else
                  forward the packet to all the neighbouring nodes;
        }
        else
            reply to source node using the procedure involved in SAODV ;
```

Figure 5.1: Extension to A-SAODV

This modified adaptive reply mechanism not only helps to relax the load of a node in term of signing and verifying task but also reduces the traffic of the network by simply avoiding flooding when it is found that a node in the path to destination has load state less then the threshold value.

5.2 NEIGHBOUR LOAD STATE MAINTENANCE

Since our algorithm takes help of the load state of immediate neighbourhood node for adaptive reply decision so it is necessary for a node to maintain the load state all the current immediate neighbours so that it can take the decision based on this. According to our proposed modification each node maintains an additional queue length field apart from its common routing information for all neighbouring node. This field is associated with the information of each neighbours of a node in the routing table. One issue arises with this field is that how often we should update this load state field? The longer is update interval the lesser is freshness of the load state and this may lead to make an incorrect decision by an intermediate node when it receives a route request packet. On the other part shorter update interval may help each node to have fresh load status of each neighbour but more frequent information sharing may lead to increase in traffic overhead of the network. So to obtain a trade-off between these to extremes we have proposed to utilize the hello packet broadcast interval as the update interval for load state of neibours. Each node may update and exchange their load state with their neighbours using hello message periodically. Since this information can be sent along with the hello messages, our modified prototype do not requires an additional message for this purpose.

5.3 ANALYSIS OF PROPOSED ALGORITHM

As we know that the time to leave (TTL) field is the number of hops to be traveled by the packet before being discarded by an arbitrary router. A small value of TTL say ‘t’, implies that either the packet going to reach its destination within t hops or going to be discarded after t hops. So, choosing a sufficiently small TTL value as TTL threshold field, any intermediate node is allow to reply a route request only if TTL field of the RREQ packet is larger than the TTL threshold value. Otherwise, the request packet is simply forwarded to all neibouring nodes assuming that either destination is within TTL threshold hop neibourhood of it or packet is to be dropped after TTL hops. This may significantly reduce the queue length of any intermediate node in the path to destination.

Secondly, in A-SAODV an intermediate node having a route to destination simply forward a route request for same without sending reply if it founds that its current routing message queue length is more than threshold queue length. If an intermediate node has a valid path to destination then among all the copy of forwarded packets to all neighhouring nodes, the packet which has been forwarded to the next hop node of route entry for destination will follow the optimal path to destination. Our proposed modification is an additional checking to see that the whether next hop to the destination's load factor is less than the threshold level. If yes, then the request packet is simply forwarded to next hop node instead of forwarding to all neibouring nodes. This may in turn relax the load of all neighbouring nodes which are not an active member of the optimal path to the destination.

The objective behind our modification and adaptive-SAODV is to reduce the number of reply routing message generated by an intermediate node that uses double signature scheme when its queue is overloaded. Reducing the number of replies to arrived requests by an intermediate node in turns helps to decrease the load of the routing message queue. This has been proved mathematically as follows.

Let

n_a = number of routing messages enters the queue per unit time.

n_{rep} = number of reply messages generated by the node per unit time against arrival of its request message.

Let us also suppose that

t_f = time required to verify and forward a routing message by a node.

t_{rep} = time required by a node to verify a request and generate reply message for it using double signature scheme (provided it has fresh route entry to reply on behalf of destination node).

So, it's obvious that $t_{rep} > t_f$ since t_{rep} need relatively more time to generate or verify two signatures.

Now, the time required to verify and forward all the routing messages arrived per unit time = $t_f.(n_a - n_{rep})$

Similarly the time required to verify and generate reply message for arrived request messages per unit time = $t_{rep} \cdot n_{rep}$

Hence total time required to process all routing messages arrived per unit time

$$= t_f.(n_a - n_{rep}) + t_{rep} \cdot n_{rep} \quad (5.1)$$

In other word, number of packets leaves queue per unit time

$$= \frac{n_a}{t_f.(n_a - n_{rep}) + t_{rep} \cdot n_{rep}} \quad (5.2)$$

Hence, the length of the routing message queue per unit time

$$L_q = n_a - \frac{n_a}{t_f.(n_a - n_{rep}) + t_{rep} \cdot n_{rep}} \quad (5.3)$$

Or,

$$L_q = n_a - n_l \quad (5.4)$$

Where

$$n_l = \frac{n_a}{t_f.(n_a - n_{rep}) + t_{rep} \cdot n_{rep}}$$

This is the queue length of a node under the behaviour of SAODV protocol with out adopting adaptive reply decision i.e. the queue length of the node is same as given in eq-(5.3) under the condition that queue length is greater than a predefined threshold value. Now let us calculate the queue length of a node when a node adopts adaptive reply decision. Under this scenario all the request packets are verified and forwarded to the entire neighbour even if the node has a fresh and valid route to the requested destination. Then the time required to verify and generate reply message for arrived request messages (n_{rep}) per unit time becomes zero, i.e. $t_{rep} \cdot n_{rep} \cong 0$

$$\Rightarrow \qquad n'_l = \frac{n_a}{t_f \cdot n_a}$$

$$\Rightarrow \qquad n'_l = \frac{1}{t_f} > n_l$$

Because $t_{rep} > t_f \Rightarrow t_f < (t_{rep} \cdot n_{rep} + t_f \cdot (n_a - n_{rep})$ where $n_{rep} \geq 1$

Hence

$$\Rightarrow \qquad L'_q < L_q \qquad \text{Where } L'_q = n_a - n'_l$$

This proves that the routing message queue length reduces when a node adopts adaptive reply decision and in turns it relaxes the signing and verifying task of a node up to some extents. Next chapter comprises simulation and result analysis of the proposed modified prototype of A-SAODV.

VI

SIMULATION AND RESULTS

6.1 SIMULATION PARAMETERS

In order to validate our analysis results, we have implemented all the misuses and performed a series of experiments through simulation. We have used ns2[14,15] network simulator version 2.33. Table 1 show the parameters used in our experiments. Since the real performance of an intermediate node is more crucial in longer routes, we have tested the protocol under more critical conditions using a rectangular scenario of 1500 × 50 m, The network topology consists of 100 mobile nodes with each node establishing maximum 100 connections. Initially, the nodes are placed randomly in the grid. The random waypoint mobility model is used. The maximum node's speed is kept at 20 m/sec with 0 pause time. Simulation time for each test is 200 seconds. We have used Constant Bit Rate (CBR) to generate UDP packets. CBR transmission rate is 4 packets/sec. Our prototype is implemented by modifying the original AODV source code in ns-2.

Simulation area	1500 X50 m
No. of nodes	100
Communication Traffic	CBR
Simulation duration	200 seconds
Max. no. of connections	100
Pause time	0
Max. Speed of a node	20 m/s
Packet rate	4 packets / sec

Table 6.1: simulation parameters

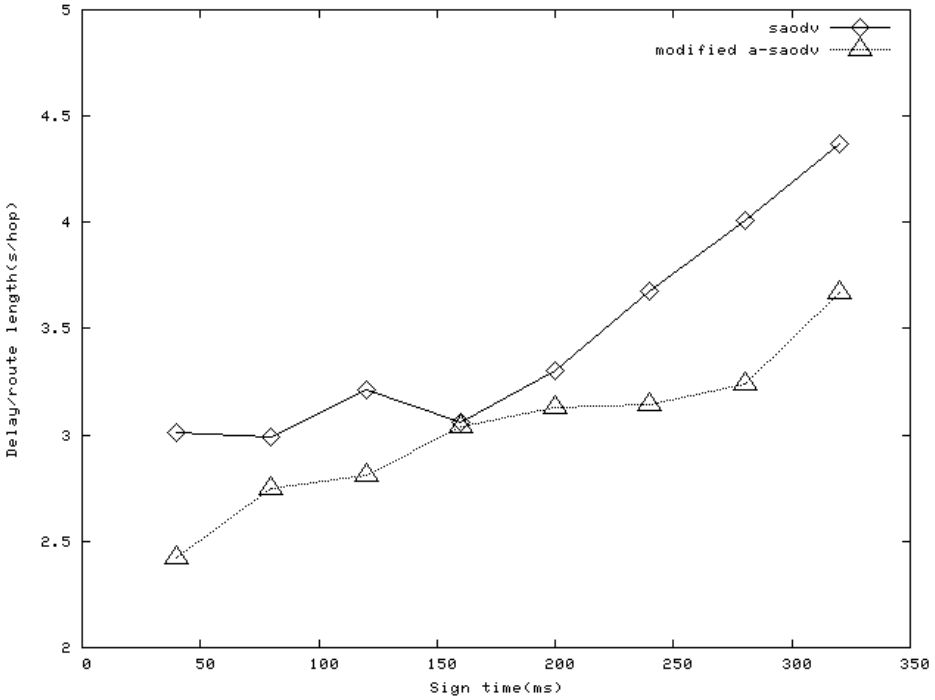

Figure 6.1: first data packet delay comparison between SAODV and modified A-SAODV.

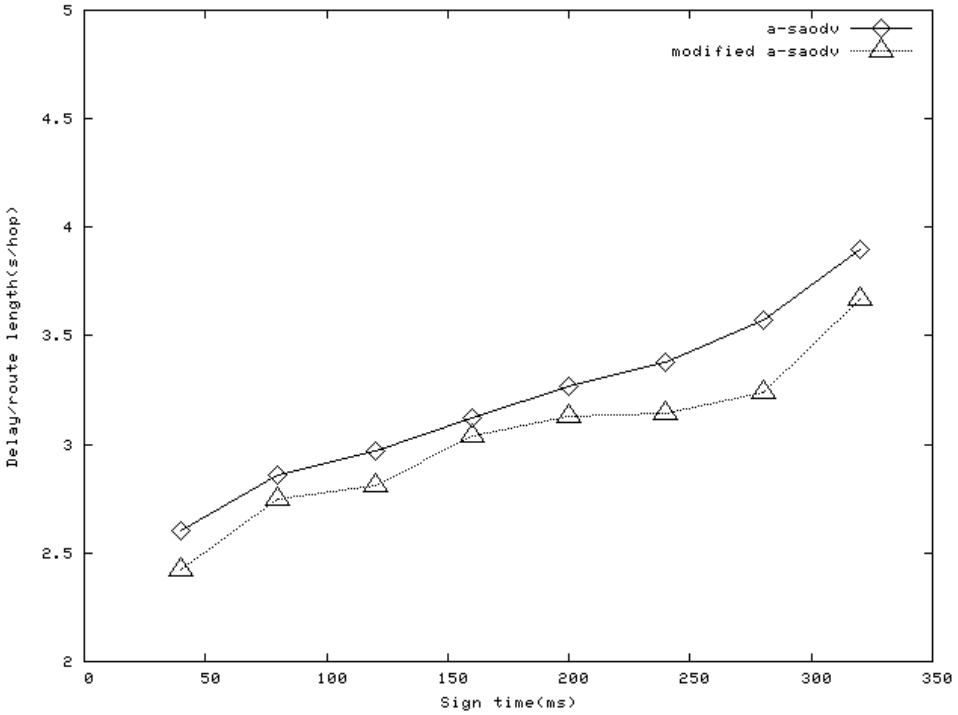

Figure 6.2: first data packet delay comparison between A-SAODV and modified A-SAODV.

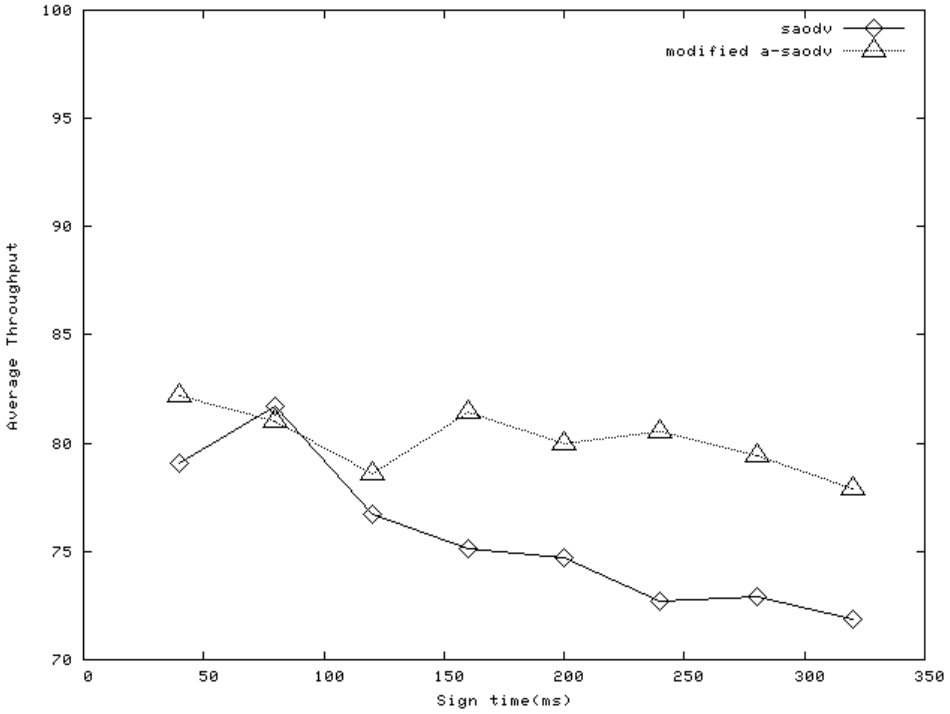

Figure 6.3: Average throughput comparison between SAODV and modified A-SAODV.

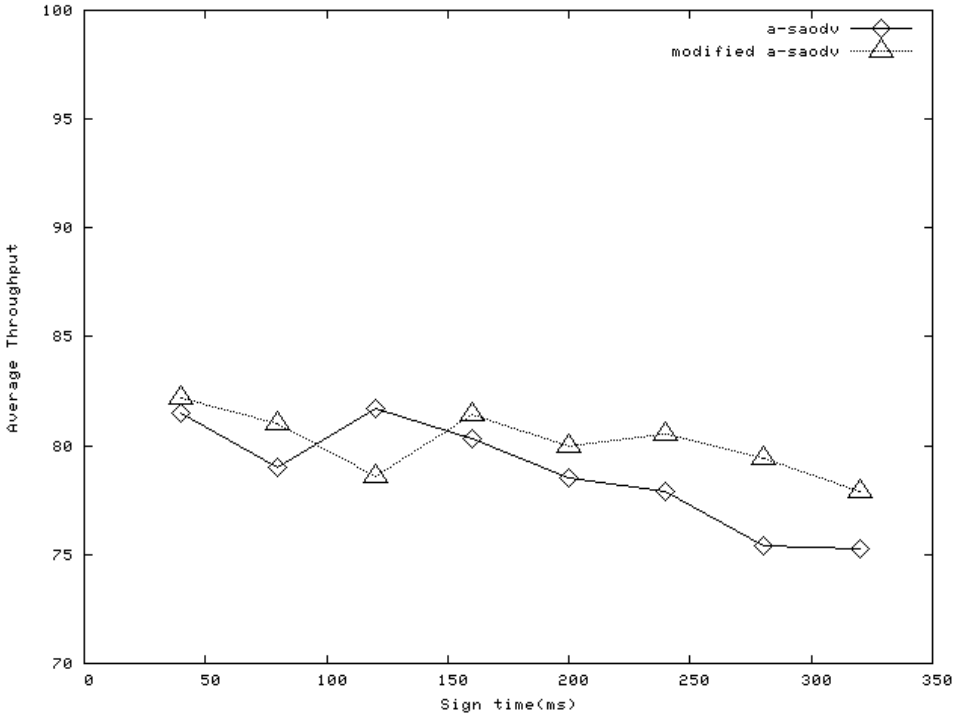

Figure 6.4: Average throughput comparison between A-SAODV and modified A-SAODV.

6.2 COMPARISON OF RESULTS

During each run we have taken first data packet delay and average throughput metrics to measure the performance of existing and proposed prototypes using different signing time. The figure 6.1 to 6.2 shows the comparison of our prototype with SAODV and Adaptive-SAODV protocols with respect to the first data packet delay metric. The average throughput of all three mechanisms has been shown in figure 6.3 and 6.4. Although the improvement of our prototype is not significant because of other mobile ad hoc network constraints, the modified prototype behaves better than the other two, having shorter delay and better throughput in the given scenario. From the simulation results we can say that our modification to adaptive reply decision of A-SAODV is contributing further improvement in the performance of SAODV. Other parameters, such as the number of generated routing packets and packet delivery fraction do not show significant differences between the three considered strategies.

VII

CONCLUSION AND FUTURE WORK

Securing AODV still an open area for research work. The existing mechanisms like SAODV able to secured the protocol with its signature extensions. But the overhead of cryptographic computation still persist in the SAODV mechanisms. A-SAODV is one of the steps towards optimizing the routing performance of secured protocols with help of a threshold mechanism. The adaptive reply decision by an intermediate node helps to balance the load of intermediate nodes which are over-burdened by signing and verification task of incoming messages. Our proposed extension to Adaptive-SAODV includes further filtering strategies aimed at further improving its network performance. We have analyzed and simulated our proposed algorithm to measure its ability in further improvement of performance in adaptive SAODV and also compared its performance with existing mechanisms using simulation. So, we can conclude that strength of a secured protocol for AODV not only depend on the strength of the cryptographic mechanism but also on the routing performance metrics.

The work is also open for a way to provide intermediate hop authenticity verification which still lack in existing literatures. To avoid the unnecessary flow of packet in the network one may also use selectively broadcasting instead of flooding. A mechanism for minimizing time involved in computation and verification of security fields will definitely boost the performance of AODV hence can be a nice work to proceed.

REFERENCES

[1] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Wksp. Mobile comp. Sys. And Apps. Feb,1999, pp. 90-100

[2] C.E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad Hoc On-Demand Distance Vector Routing", IETF RFC 3561, July 2003

[3] D. Remondo , "Tutorial of Wireless Ad Hoc Networks", HET-NETs 2004.

[4] P.Ning, K. Sun, "How to misuse AODV: A Case Study of Insider Attacks Against Mobile Adhoc Routing Protocols", Info Assurance Wksp, IEEE sys, Man and Cybernetics Soc, june 2003, pp. 60-67

[5] Weichao Wang, Yi Lu, Bharat K. Bhargava, "On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol", IEEE Proceedings, 2003, pp. 375-382

[6] Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the 10th IEEE International Conference on Network Protocols, 2002, pp.1-10

[7] M. Gurrero Zapata and N. Asokan, "Securing Adhoc Routing Protocols", Proceeding 1st ACM Workshop. Wireless Sec., 2002, pp. 1-10.

[8] M. Gurrero Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, IETF Internet draft, September 2006, pp-1-22

[9] Asad Amir Pirzada, Chris McDonald, "secure Routing with the AODV protocol", Asia-Pacific Conference on Communications, Perth, Western Australia, October 2005. pp. 57-61

[10] K. A. Sivakumar, M. Ramkumar, "Safeguarding Mutable fields in AODV Route Discovery Process", Proceedings of 16th International Conference on Computer Communications and Networks, 2007. pp. 645-651

[11] Qing Li, Meiyuan Zhao, Jesse Walker, Yih-Chun Hu, Adrian Perrig, Wade Trappe, "SEAR: A Secure Efficient Ad Hoc On Demand Routing Protocol for Wireless Networks", Proceedings of the 2008 ACM symposium on Information, computer and communications security**,** 2008, pp. 201-204

[12] Davide Cerri, Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE Communication Magazine, Volume 46, Issue 2, February 2008 pp.120 - 125

[13] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, Joo-Han Song, "Experimental Comparisons between SAODV and AODV Routing Protocols", Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling**,** 2005, pp. 113 - 122

[14] NS Manual, http://www.isi.edu/nsnam/ns/ns-documentation.html

[15] Altman, Jimenez, "NS Simulator for Beginners", http://www-sop.inria.fr/maestro/personnel/Eitan.Altman/COURS-NS/n3.pdf.

[16] M. Aziz, M. Al-Akaidi, "Security issues in wireless Ad Hoc Networks and the application to the telecare project", Proceedings of the 15th International Conference on Digital Signal Processing, DSP 2007, pp. 491-494

[17] Lindong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Network Magazine, 1999 pp. 1-12

[18] P. Papadimitratos, Z. Haas, "Secure Routing for Mobile Ad Hoc Network", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002 pp. 1-13

[19] Liu Jinghua, Geng Peng, Qiu Yingqiang, Feng Gui, "A Secure Routing Mechanism in AODV for Ad Hoc Networks", Proceedings of International Symposium on Intelligent Signal Prcessing and Communiction System, 2007 pp. 435-438

[20] Mohammad Ilyas, "The Hand Book of Ad Hoc Wireless Networks", CRC Press LLC.