TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

PULCHOWK CAMPUS

THESIS NO: 068/MSI/616

An Approach for Performance Enhancement of Secure Routing Protocols in Mobile Ad Hoc Networks

by

Santosh Raj Timilsena

A THESIS
SUBMITTED TO THE DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION AND COMMUNICATION ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

LALITPUR, NEPAL

NOVEMBER, 2015

COPYRIGHT ©

The author has agreed that the library, Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk Campus, may make this thesis freely available for inspection. Moreover the author has agreed that the permission for extensive copying of this thesis work for scholarly purpose may be granted by the professors, who supervised the thesis work recorded herein or, in their absence, by the Head of the Department, wherein this thesis was done. It is understood that the recognition will be given to the author of this thesis and to the Department of Electronics and Computer Engineering, Pulchowk Campus in any use of the material of this thesis. Copying of publication or other use of this thesis for financial gain without approval of the Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk Campus and author's written permission is prohibited.

Request for permission to copy or to make any use of the material in this thesis in whole or part should be addressed to:

Head
Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk Campus
Lalitpur, Nepal

TRIBHUVAN UNIVERSITY INSTITUTE OF ENGINEERING

PULCHOWK CAMPUS

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

APPROVAL PAGE

The undersigned certify that it has been read and recommended to the Institute of Engineering for acceptance, a thesis entitled **"An Approach for Performance Enhancement of Secure Routing Protocols in Mobile Ad Hoc Networks"**, submitted by **Mr. Santosh Raj Timilsena** in partial fulfillment of the requirements for the award of the degree of **"Master of Science in Information and Communication Engineering"**.

Supervisor: Dr. Arun Kumar Timalsina
Assistant Professor
Department of Electronics and Computer Engineering
Pulchowk Campus, Institute of Engineering, TU

External Examiner: Mr. Krishna Prasad Bhandari
Deputy Manager, IT Directorate
Nepal Telecom, Jawalkhel, Lalitpur

Committee Chairperson: Dr. Dibakar Raj Pant
Head of the Department
Department of Electronics and Computer Engineering
Pulchowk Campus, Institute of Engineering, TU

Date: November 4th, 2015

DEPARTMENTAL ACCEPTANCE

The thesis entitled **“An Approach for Performance Enhancement of Secure Routing Protocols in Mobile Ad Hoc Networks”**, submitted by **Mr. Santosh Raj Timilsena** in partial fulfillment of the requirements for the award of the degree of **“Master of Science in Information and Communication Engineering”** has been accepted as a bonafide record of work independently carried out by him in the department.

Dr. Dibakar Raj Pant
Head of the Department
Department of Electronics and Computer Engineering,
Pulchowk Campus, Institute of Engineering
Tribhuvan University
Nepal

ACKNOWLEDGEMENTS

First and foremost, I would like to offer my sincerest gratitude to my supervisor Dr. Arun Kumar Timalsina for his precious guidance, support and constant encouragement throughout the thesis work. I am greatly indebted to him for reviewing, analyzing the thesis structure and giving me valuable recommendations. His support and motivation is highly acknowledged.

I am highly thankful to the Department of Electronics and Computer Engineering, Pulchowk Campus, for providing the platform to me to initiate and successfully complete master's thesis work. I am also indebted to Prof. Dr. Shashidhar Ram Joshi, Prof. Dr. Dinesh Kumar Sharma, Dr. Surendra Shrestha, Dr. Nanda Bikram Adhikari, Mr. Sharad Kumar Ghimire and all my teachers from MSc. in Information and Communication Engineering program at Pulchowk Campus. I would also like to express my gratitude to Mr. Shiv Raj Baral for his valuable feedback and suggestions.

Finally, I would like to express my gratitude to my brother Binod Raj Timilsena, all my friends, especially Niranjan Baral and family members for the motivation and moral support right through the master's degree course.

Santosh Raj Timilsena
068/MSI/616

ABSTRACT

Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure. Although the principle of wireless, structure-less and dynamic networks is attractive, there are still some major flaws that prevent its commercial expansion. Security is one of these main barriers. The open and dynamic operational environment of MANET makes it vulnerable to various network attacks. The security goals can be achieved using secure routing protocols. Ad hoc On-demand Distance Vector (AODV) is one of the most widely used routing protocols that is currently undergoing extensive research. This thesis presents the AODV protocol and surveys security enhancements using both cryptographic and trust based approaches. The impact of security features on routing performance was analyzed. The addition of a trust based approach with cryptographic features reduces routing overheads significantly. The proposed mechanism offers more resilience to attack from malicious nodes, while also promotes collaboration among cooperative nodes and penalizes selfish nodes. The simulation results show that the proposed trust model increases routing efficiency and reliability at cost of delay.

Keywords: MANET, MANET routing, AODV, SAODV, TAODV

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AODV	Ad hoc On Demand Distance Vector
AED	Average End-to-End Delay
BAN	Body Area Network
CBR	Constant Bit Rate
DES	Data Encryption Standard
DSR	Dynamic Source Routing
LAN	Local Area Network
MANET	Mobile Ad hoc Network
NAM	Network Animinator
NRL	Normalized Routing Load
NS-2	Network Simulator 2
OPNET	Optimized Network Evaluation Tool
OTCL	Object Tool Command Language
PAN	Personal Area Network
PDF	Packet Delivery Fraction
RERR	Route Error Packets
RREP	Route Reply Packets
RREQ	Route Request Packets
RSA	Rivest-Shamir-Adleman
SAODV	Secure Ad Hoc On Demand Distance Vector
TAODV	Trusted Ad Hoc On Demand Distance Vector
TCL	Tool Command Language
TRREP	Trust Recommendation Reply
TRREQ	Trust Recommendation Request
TSAODV	Trusted Secure Ad Hoc On Demand Distance Vector

VBR	Variable Bit Rate
VINT	Virtual Internetwork Testbed
WLAN	Wireless Local Area Network

CHAPTER ONE: INTRODUCTION

1.1 Background

An ad hoc network is a network without any fixed communication infrastructures. The network is created in ad hoc fashion by the participating nodes without any central administration. There are no dedicated routers or network management centers, instead the participating nodes work in peer-to-peer fashion and act as both servers and routers [1]. The nodes are usually assumed to be independent and do not need to have any kind of affiliation from network, so both computational resources and link capacity might vary greatly from node to node. Nodes are not assumed to be static. They are allowed to move freely inside a network, as well as leave or enter the network at any time. Thus the network by definition is wireless.

Ad hoc networks are primarily meant for use by military forces [2] and emergency rescue situations. At the state of war an army cannot rely on fixed infrastructure, as it is an easy and attractive target for the enemy. Ad hoc networks are optimal solution in such cases. For civil use ad hoc networks are crucial if the fixed infrastructures have been torn down by some natural disaster, like flood or earthquake. Then rescue operations could in such a situation can be managed by utilizing ad hoc networks.

The mobile ad hoc network is a new model of wireless communication and has gained increasing attention. Implementing routing in an ad hoc network is a challenging task [3]. The distinctive features of the network make normal routing protocols nearly useless. Traditional routing protocols assume that the underlying network is stable and reliable. This is far from the truth in ad hoc networks. As in a general networking environment, mobile ad hoc networks have to deal with various security threats. Due to its nature of dynamic network topology, routing in mobile ad-hoc network plays a vital role for the performance of the networks. It is obvious that most security threats target routing protocols which is the weakest point of the mobile ad hoc network. There are various studies and many researches in this field trying to propose more secure protocols [4]. However, there is not a complete routing protocol that can secure the operation of an entire network in every situation. Typically a “secure” protocol is only good at protecting the network against one specific type of attacks. Protocols for secure routing usually apply cryptography and thus come with a significant increase in complexity and computational overhead. In order to achieve security requirements [5], complicated encryption techniques and additional information in the routing packets are used which reduces overall routing efficiency.

The adversary is usually not very clearly defined in researches [6]. On one hand an adversary might be a node behaving badly just because of a bug in the software. On the other hand the adversary could be a motivated enemy, which would want to either eavesdrop on communications, or possibly to make all normal communication impossible. The secure routing algorithms need to protect against all the different cases.

1.2 Problem Statement

The real-world network does not operate in an ideal working environment; there are always threats and malicious actions affecting the performance of the network. Thus, studying the performance of secure routing protocols in malicious environments is needed in order to effectively evaluate the performance of those routing protocols. A central vulnerability of MANET comes from peer-to-peer architecture in which each node acts like a router to forward packets to other nodes. Moreover, these nodes on network share the same open environment that gives opportunity for malicious attackers. The challenges for MANET security are lacking of central points, mobility, wireless link, limited resources and cooperativeness [4, 6]. The Protocols in MANET are vulnerable to many different types of attacks. Attacks Using Modification, Attacks Using Impersonation, Attacks Using Fabrication, Black Hole, Gray Hole, Replay, Wormhole, Blackmail and Denial of Service attack are some of the common threats in MANET. One of the reasons to explore security attributes at the routing level is to prevent attacks on the routing protocol itself, and thereby secure a fundamental building block of the ad hoc network infrastructure.

Securing the routing protocols for ad hoc networks is a very challenging task due to its unique characteristics. Shared radio channel, insecure environment, limited resources and lack of central authority and association of rules in MANET argues necessity of secure routing protocols and their performance analysis.

1.3 Research Objectives

The overheads associated with secure routing protocols are vital for better performance of routing protocol. It is important to know the overheads and performance implications associated with secure routing so that appropriate protocols are implemented in the network. The main objective of this thesis is to find out how routing overhead and performance metric gets affected if we add security features to a routing protocol. In this research AODV is chosen and a secured version of AODV (SAODV) [9] has been implemented. These two protocols are discussed in detail and their performance is evaluated to propose a secured version of AODV with trust parameter.

The performance of AODV and SAODV were evaluated under normal circumstances where there are no malicious nodes in the network and also under attack conditions where the network contains malicious nodes. The protocols performance is measured using the performance metrics including packet delivery fraction, normalized routing overhead and average end to end delay of packets and routing overhead. The use of a type of cryptographic approach makes the routing protocols immune to only specific type of attack. Modification of secured routing protocols to make them more robust and increase their routing efficiency is the main target of the thesis. To achieve this, the following objectives were identified:

i. To develop and implement the SAODV routing protocol and compare its performance with AODV.

ii. To identify the critical measures to improvise the performance of secure routing protocols.

1.4 Scope and Application

MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural disasters, military conflicts, emergency services and the regular mobile communication.

The purpose of this research is to compare AODV and its security enhanced versions based on their performance under various network conditions. The proposed solution is focused on the enhancement of security measures along with the routing performance. The actual need of security depends on the type of application and the value of the information that travels in the network. Secure routing protocols have different applications ranging from low to extremely high security needs. The research involves use of cryptographic measures and trust based models to enhance security. The implementation of the research the focuses on the AODV as the best overall performing ad hoc routing protocol. The routing protocols are simulated in different network scenarios using NS-2.

1.5 Thesis Outline

The remainder of this thesis is organized as follows:

In Chapter 2, literature review is discussed. It gives the over view of the ad hoc networks, AODV routing protocols, its security issues and available solutions.

Chapter 3 is about the description of the research methodology. It describes the development of system model. Different models for security implementation are discussed in this chapter.

Chapter 4 presents the experimental implementation of the research.

In chapter 5, simulation results obtained from the designed system level simulation model are discussed. The performance of the AODV and its secured versions in both malicious and non-malicious environment are compared in different network scenarios.

Chapter 6 states the conclusion of the obtained results. The possible enhancements in the research are also discussed in this chapter.

CHAPTER TWO: LITRATURE SURVEY

2.1 AD Hoc 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, the devices communicate with each other using a wireless physical medium without relying on pre-existing wired infrastructure [3]. That is why ad hoc network is also known as infrastructure less network. These networks known as 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 [7]. The terminals in the ad hoc network can not only act as end-system but also as an intermediate system (routers). In MANETs 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 [10].

The major characteristics which distinguish an ad hoc network from a cellular network are 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 [4]. 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 BAN, PAN and WLAN [3]. 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 order 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 ad hoc networks are not restricted to these technologies, most of the current research assumes Bluetooth or IEEE 802.11[9] to be the underlying technologies. The most active area of concern and research field in ad hoc networking is routing.

2.2 Routing in Ad Hoc Network

Routing Protocols are used to discover and maintain routes between the source and destination nodes. For MANET, there are two main kinds of routing protocol: on-demand protocols (also called reactive protocols) and table-based protocols (also called proactive protocols) [7]. For reactive protocols, nodes only compute routes when they are needed. Usually, caches are used to reduce the effort of route discovery. For proactive protocols, each node maintains a routing table containing routes to all nodes in the network. Nodes must periodically exchange messages with routing information to keep routing tables up-to-date. Furthermore, there are also some hybrid protocols. Both proactive and reactive routing has specific advantages and disadvantages that make them suitable for certain kinds of scenarios. The hybrid methods try to take the advantages of those two and achieve better performance.

2.3 Reactive Routing Protocols

Reactive routing only finds a route when necessary. This makes it more scalable to dynamic, large networks. When a node needs a route to another node, then only it initiates a route discovery process to find a route. Generally, it consists of the two main phases: route discovery and route maintenance.

Route discovery is the process of finding a route between two nodes, whether directly reachable within wireless transmission range or reachable through one or more intermediate network hops through other hosts. When a node needs to communicate with another node a route discovery process is initiated.

Route maintenance is the process of repairing a broken route or finding a new route in the case of a route failure. Route maintenance procedure monitors the operation of the route and informs the sender if any routing errors occur. Two of the most widely used reactive routing protocols are DSR and ADOV.

2.4 AODV

AODV is a dynamic reactive routing protocol designed for larger ad hoc networks. AODV routing protocol is a pure on-demand route acquisition system. 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 needs 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 becomes aware of the other nodes in its neighborhood by the use of 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 features of AODV are:

i. It performs path discovery process when necessary. AODV uses broadcast route discovery mechanism.
ii. It distinguishes between local connectivity management (neighborhood detection) and general topology maintenance.
iii. It broadcasts information about changes in local connectivity to those neighboring mobile nodes which 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 [15]. The operation of AODV is loop-free, and by avoiding the Bellman-Ford “counting to infinity” [20] problem. It offers a quick convergence when the ad hoc network topology changes. In case of link failure, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes. Other 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. Use of destination sequence numbers ensures loop freedom [20] and is simple to program. Given the choice between two routes to a destination a requesting node select the route with greatest sequence number.

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.

2.4.1 Routing in AODV

The AODV routing protocol uses a reactive approach to finding routes and a proactive approach for identifying the most recent path [4]. It is typical Distance Vector routing protocol, so it uses Bellman-Ford algorithm [20] for route calculation. It has three main mechanisms: route discovery, maintenance of active routes and Hello messages, for up-keeping the neighborhood topology.

There are three main messages involved in AODV mechanisms are Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs). RREQ messages are broadcasted; RREP messages are unicasted back to the source. It supports unicast and multicast, as well as it can use bidirectional and unidirectional links [10]. On-demand nature of AODV allows for broadcasting discovery messages only when it is needed. The routes are maintained only when they are in active communication.

2.4.1.1 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 sequence number and request broadcast id uniquely identifies a RREQ. Each neighbor either responds the RREQ by sending a RREP back to the source, or re-broadcasts the RREQ to its own neighbors after increasing the Hop Count. A node may receive multiple copies of the same route broadcast packet from various neighbors. When an intermediate node receives a RREQ, it checks its broadcast id and source address. 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.

The RREQ packet travels across the network until it arrives at a node that possesses the current to the destination. The node determines whether it has a valid route entry for the desired destination. It 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 RREP message to the source using the reverse path that has been by the RREQ message. If the node cannot 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. Route discovery mechanism in AODV is shown in Figure 2.1 [15]. 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. Source inserts the source id, destination id, source sequence number, destination sequence number, broadcast id, and TTL fields in the RREQ packet. When nodes 4, 3 and 2 receive this, they check their route caches to see if they already have a route. If they don't have a route, they forward it to their neighbors, otherwise the destination sequence number in the RREQ packet is compared with the value in its corresponding entry in route cache. If the destination sequence number in RREQ packet is greater, then it replies to the source node with a RREP packet containing the route to the destination.

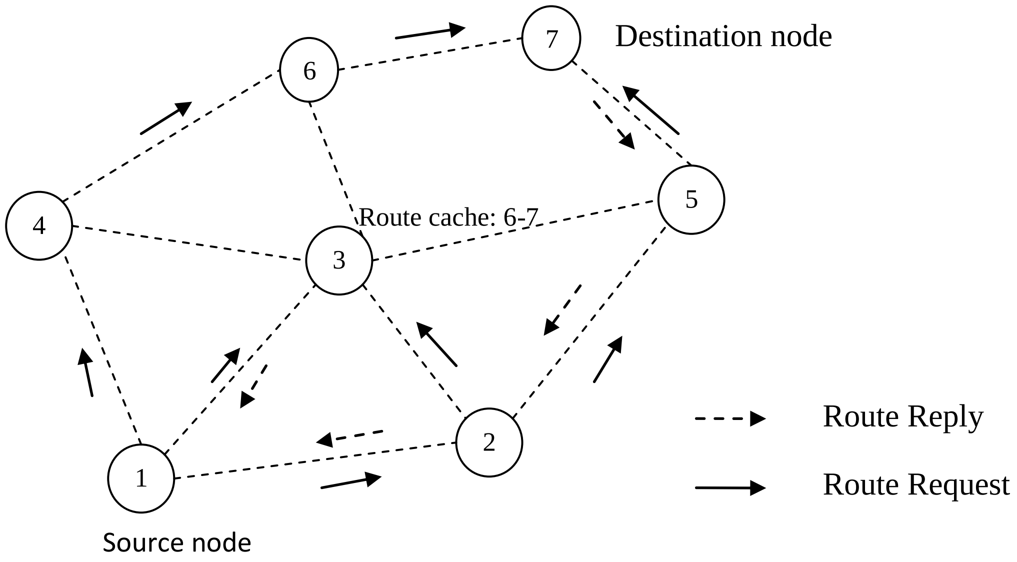

Figure 2.1: Route discovery in AODV

Node 3 has a route to 7 in its cache and its destination sequence number is higher compared to that in RREQ packet as shown in figure 2.3. So, it sends a RREP back to the source node 1. Thus the path 1-3-6-7 is stored in node 1. The destination node also sends a RREP back to the source. For example, one possible route is 1-2-5-7. The intermediate nodes on the path from source to destination update their routing tables with the latest destination sequence number in the RREP packet.

2.4.1.2 Hello Message and Route Table Information

A node may offer connectivity information by broadcasting local hello messages. A node uses hello messages only if it is part of an active route. In every hello message interval, the node checks whether it has sent a broadcast within 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. A timer, called the route request expiration timer is associated with reverse path routing entries. 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 Destination IP Address, Destination Sequence Number, Valid Destination Sequence Number flag, Other state and routing flags, Hop Count and Lifetime (expiration or deletion time of the route)[21].

2.4.1.3 Route Error Message and Route Expiration

An error message, RERR packet is used to notify other nodes that the loss of that link has occurred, when an active link breaks. 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 be used 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 a node in a precursor list.

Route error and link failure processing requires invalidating existing routes, listing affected destinations, determination of which neighbors may be affected and delivering an appropriate RERR to such neighbors.

The route maintenance mechanism is shown in figure 2.2. 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.

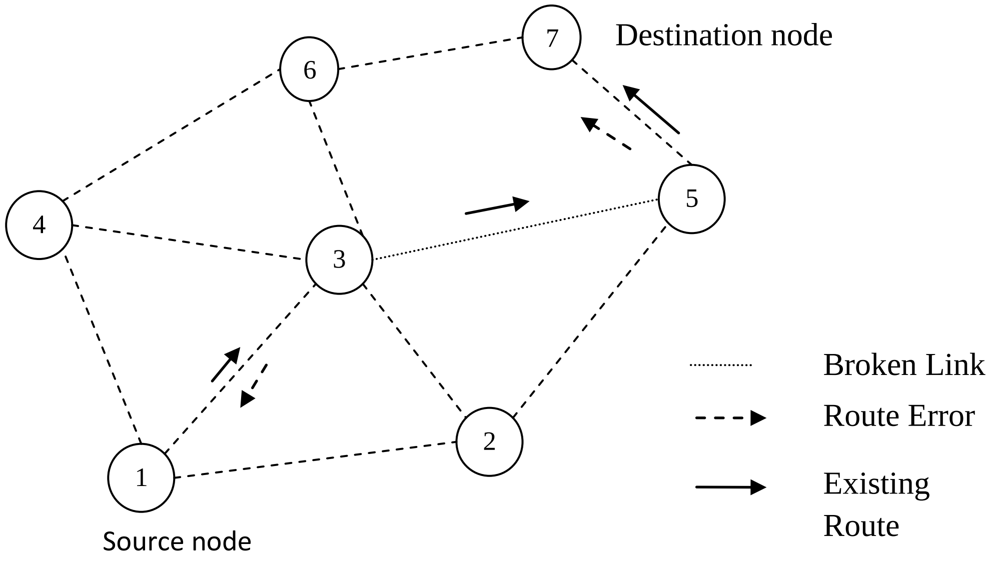

Figure 2.2: Route Maintenance in AODV

2.5 Security Issues of AODV

Any network is usually prone to a wide range of attacks depending on it architecture, functions, design and routing techniques. At the network layer, these attacks can be broadly classified into attacks on routing messages and attacks on packet forwarding. Since we are discussing the routing protocols, we will limit ourselves here to attacks on routing messages.

AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules [5]. Some of the common attacking techniques include cache poisoning, fabricating or forging the route messages, creating a wormhole, spoofing, packet dropping (black hole), malicious flooding(Denial of Service), rushing attacks, where the malicious or compromised nodes quickly disperse wrong routing messages to block legitimate messages from getting accepted [14]. These attacks may result in routing loops, network partitions, sleep deprivation (exhausting the battery) etc. While the on-demand property of AODV results in low protocol overhead and adaptability to host movement, it makes the protocol vulnerable to real time attacks on different nodes at different points in time. Since the routing functions and messages are distributed, it is difficult to trace back the sources of false information.

AODV does not have any security features in-built. Based on the above discussion the following points are necessary making AODV more secure [5, 6].

i. Node Authentication: Sender authentication is important to confirm the validity of the routing information.

ii. Message Integrity: The receiving node should be able to check that the message has not changed in transit.

These requirements must be achieved to perform authorization which might be helpful for access control into the network. AODV also allows intermediate nodes to reply to a RREQ, this could be a potential security threat. If we assume that the ultimate authority on routing information about a destination is the destination node itself and disable RREP from intermediate nodes, we might make the protocol more secure but slow down route discovery. There is always a tradeoff between security and route discovery time and the design should depend on the requirements of the network.

2.6 SAODV

To secure information many different approaches have been proposed over the years. The most common approaches use the DES and the RSA Cryptosystem [11]. A secure version of AODV called SAODV [5] provides features such as integrity, authentication and non-repudiation of routing data. The SAODV addresses the problem of securing a MANET network.

SAODV is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation [6]. SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. Key management scheme is used to achieve this job. Security in SAODV is based on public key cryptography that 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 [9] is used to authenticate and preserve integrity of non-mutable field data in RREQ and RREP messages. For non-mutable field the authentication is done in an end-to-end manner. Hash chain [8] is used to secure mutable field like hop count information.

2.6.1 Hash Chain

The hash chain mechanism helps any intermediate node to verify that the hop count has not been altered 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 [8].

i. A random number called seed is generated.

ii. The MAX_HOP_COUNT field is set to time to live value from IP header

   $$\text{Max\_Hop\_Count} = \text{TTL} \qquad (2.1)$$

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

   $$\text{Hash} = \text{seed} \qquad (2.2)$$

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

v. TOP_HASH field is calculated by hashing seed MAX_HOP_COUNT times.

   $$\text{TOP\_HASH} = h^{\text{MAX\_HOP\_COUNT}}(seed) \qquad (2.3)$$

Where, *h* is a hash function and $h^i(x)$ is the result of applying the function *h(x)* to the power *i* times.

For verifying the hop count, following operations are performed by nodes receiving the SAODV message:

a. Top_Hash verification-

   $$\text{Top\_Hash} == h^n(\text{Hash}) \qquad (2.4)$$

Where n = (Max_Hop_Count – Hop_Count)

h = hash function

b. Before rebroadcasting, the node hashes the value in the Hash field to account for the increment in the hop count.

The hash function (h), 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.

2.6.2 SAODV Digital Signature

Digital Signatures are used to protect the integrity of the non-mutable data in routing message. Two mechanisms can be used in SAODV [11] for verifying authentication of message using digital signature. In the first one, 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 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 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.

A node might want to have the feature of replying as an intermediate node for a route. In this case, 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 nodes who receives it.

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 [8]. However, SAODV also has some issues like it cannot detect tunnel attack and cannot do much about denial of service attack. This thesis work is 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.

2.7 TAODV

Trust is measure of uncertainty with its value represented by entropy. Information Theory states that entropy is a measure for uncertainty. Entropy based trust value [23] is defined as:

$$T\{Subject : agent, action\} = \begin{cases} 1 - H(p), \ for\ 0.5 < p < 1 \\ H(p) - 1, \ for\ 0 < p < 0.5 \end{cases} \qquad (2.5)$$

Subject T{subject : agent, action} denotes the trust value of the relationship {subject : agent, action} and P{subject : agent, action} denotes probability that the agent will perform the action in the subject's point of view. Function *H(p)* denotes the entropy of a variable p. Probability is opinion of subject only. Trust value is a continuous real number lies in interval [-1, 1]. Trust value is negative for 0<*p*<0.5 and positive for 0.5 < *p* <= 1.

2.7.1 Subjective Logic

Subjective logic is a kind of trust model which was proposed by A. Josang [16]. It is a logic which operates on subjective beliefs about the world, and uses the term opinion to denote the representation of a subjective belief [16]. The trust between two entities is represented by opinion. An opinion can be interpreted as a probability measure containing secondary uncertainty.

Nodes in MANET move with high mobility and may experience long distance in space among each other. A node may be uncertain about another node's trustworthiness because it does not collect enough evidences. This uncertainty is a common phenomenon; therefore we need a model to represent such uncertainty accordingly. In subjective logic, an opinion consists of belief, disbelief and also uncertainty, which gracefully meets our demands. Subjective logic also provides a mapping method to transform trust representation between the evidence space and the opinion space. Trust model used in TAODV is derived and modified from the subjective logic and is more applicable for the instance of MANET. The evidences used in trust model are collected through the successful or failed state when nodes perform routing actions or communications with other nodes.

2.7.2 Trust Representation

Trust model used in TAODV is an extension of the original trust model in subjective logic. Here opinion is modified to a 3-dimensional metric.

Let $\omega_B^A = (b_B^A, d_B^A, u_B^A)$ denote any node A's opinion about any node B's trustworthiness in a MANET, where the first, second and third component correspond to belief, disbelief and uncertainty, respectively. These three elements satisfy:

$$b_B^A + d_B^A + u_B^A = 1 \qquad (2.6)$$

In this definition, belief means the probability of a node B can be trusted by a node A, and disbelief means the probability of B cannot be trusted by A. Then uncertainty u_B^A fills the void in the absence of both belief and disbelief, and sum of these three elements is 1.

2.7.3 Mapping between the Evidence and Opinion Spaces

A node in MANET will collect and record all the positive and negative evidences about other nodes' trustworthiness. With these evidences we can obtain the opinion value by applying the following mapping definition [16].

Let $\omega_B^A = (b_B^A, d_B^A, u_B^A)$ be node A's opinion about node B's trustworthiness in a MANET, and let p and n respectively be the positive and negative evidences collected by node A about node B's trustworthiness, then ω_B^A can be expressed as a function of p and n according to:

$$\begin{cases} b_B^A = \frac{p}{p+n+2} \\ d_B^A = \frac{n}{p+n+2} \\ u_B^A = \frac{2}{p+n+2} \end{cases} \text{,where } u_B^A \neq 0 \text{ ,} \qquad (2.7)$$

2.7.4 Trust Combination

Each node will collect all its neighbors' opinions about another node and combine them together using combination operations. In this way, a node can make a relatively objective judgment about another node's trustworthiness even in case several nodes are lying. Nodes may adopt Discounting combination or Consensus combination.

2.7.4.1 Discounting Combination

Let's consider such a situation where a node A wants to know C's trustworthiness, then node B gives its opinion about C. Assuming A already has an opinion about B. Then A will combine the two opinions: A to B, B to C to obtain a recommendation opinion A to C. Discounting combination is for this purpose.

Let A, B and C be three nodes where $\omega_B^A = (b_B^A, d_B^A, u_B^A)$ is A's opinion about B's trustworthiness, and $\omega_C^B = (b_C^B, d_C^B, u_C^B)$ is B's opinion about C's trustworthiness. Let $\omega_C^{AB} = (b_C^{AB}, d_C^{AB}, u_C^{AB})$ be the opinion such that

$$\begin{cases} b_C^{AB} = b_B^A b_C^B \\ d_C^{AB} = d_B^A d_C^B \\ u_C^{AB} = d_B^A \end{cases} \qquad (2.8)$$

ω_C^{AB} is called the discounting of $\omega_C^B$by ω_B^A which expresses A's opinion about C as a result of B's advice to A.

The discounting combination can be used along a recommendation path.

2.7.4.2 Consensus Combination

Different nodes may have different, even contrary opinions about one node. To combine these opinions together to get a relative objective evaluation about that node's trustworthiness, we may use Consensus combination.

Let $\omega_C^A = (b_C^A, d_C^A, u_C^A)$ and $\omega_C^B = (b_C^B, d_C^B, u_C^B)$ be opinions respectively held by nodes A and B about node C's trustworthiness. Let $\omega_C^{A,B} = (b_C^{A,B}, d_C^{A,B}, u_C^{A,B})$ be the opinion such that

$$\begin{cases} b_C^{A,B} = (b_C^A u_C^B + b_C^B u_C^A)/k \\ d_C^{A,B} = (d_C^A u_C^B + d_C^B u_C^A)/k \\ u_C^{A,B} = (u_C^A u_C^B)/k \end{cases} \tag{2.9}$$

Where $k = u_C^A + u_C^A - 2u_C^A u_C^B$ such that $k \neq 0$, Then $\omega_C^{A,B}$ is called the consensus between ω_C^A and ω_C^B, representing an imaginary node [A,B]'s opinion about C's trustworthiness, as if it represented both A and B. The consensus combination can reduce the uncertainty of one's opinion.

2.7.5 Routing Operations in TAODV

In TAODV route selection is based on quantitative Route Trust and Node Trust values. Route Trust from a source node to a destination node is defined as the difference between the number of packets sent from the source node and the number of related packets received by the destination node. Route Trust is thus 0 for a perfect route and trustworthiness decreases for growing Route Trust values. For calculation of Node Trust each node monitors the behavior of all neighbor nodes by counting both successes and failures of events such as Control Packets Received, Control Packets Forwarded, Data Packets Received, Data Packets Forwarded, Route Established etc. Node Trust value for a certain monitored event type is

$$\text{Node Trust} = \frac{R_s - R_f}{R_s + R_f} \tag{2.10}$$

where R_s and R_f are the number of successful and failed events respectively.

The node trust value will lie between +1 (complete trust) and -1 (complete mistrust). Node Trust for a neighbor node is weighted sum of the trust values for all monitored event types.

2.8 TSAODV

Trust management scheme along with cryptography makes routing protocol more robust [4]. A trust table is introduced in network where each node is assigned with a trust values. Trust management scheme is introduced in SAODV that already provides encryption methods to authenticate individual nodes to provide network from external attacks.

- Route discovery is done as same as the SAODV does.
- Trustworthiness metric is used to find next hop of a route.
- Two new packets TRREQ, TRREP are used.
- On the basis of interactions made by nodes communication is continued.

The TSAODV protocol gives a robust solution on maliciously packet dropping because it excludes malicious nodes from its route. In terms of security it is most reliable protocol that can prevent from both external and internal attacks but if energy is not constrained. Use of promiscuous mode, to receive all the data packets in its wireless range consumes more energy. That is the biggest limitation.

2.8.1 Framework of TSAODV

There are mainly three modules in TSAODV system: SAODV routing protocol, a trust model, and trusted AODV routing protocol. TAODV routing protocol contains procedures such as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating. The structure and relationship among these components are shown in figure 2.3.

Trust recommendation is concerned the exchange of trust information. There are two types of messages used in trust recommendation procedures: Trust Request Message (TREQ), and Trust Reply Message (TREP). When a node A wants to know another node B's latest trustworthiness, it will broadcast an TREQ message to its neighbors. If one of A's neighbors C receives the TREQ message C will reply with a TREP message. The Type field of this TREP is set to 1 and the opinion field is filled with the opinion values from C to B.

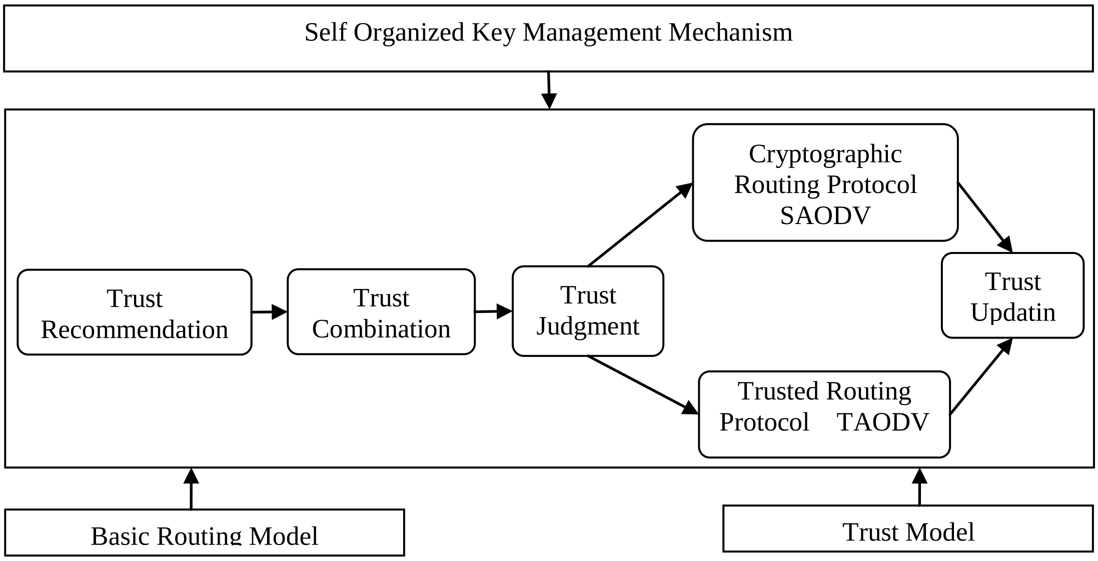
Self Organized Key Management Mechanism
Cryptographic Routing Protocol SAODV
Trust Recommendation
Trust Combination
Trust Judgment
Trust Updatin
Trusted Routing Protocol TAODV
Basic Routing Model
Trust Model

Figure 2.3: Framework of TSAODV

Each node after collecting all its neighbors' opinions about other node, trust combination operations are used to combine them together. A node then makes trust judgments based on the rules in table 2.1.

Table 2.1 Criteria for Judging Trustworthiness

belief	disbelief	uncertainty	Actions
		> 0.5	Request and verify digital signature
	> 0.5		Distrust a node for an expire time
> 0.5			Trust a node and continue routing
≤ 0.5	≤ 0.5	≤ 0.5	Request and verify digital signature

These rules tell a node how to perform the corresponding operation according to the values in its opinion about another node.

CHAPTER THREE: RESEARCH METHODOLOGY

The simulation based research was carried as depicted in figure 3.1 in order to accomplish the objectives. AODV routing protocol was studied and explored in detail to gain the understanding of their purpose, strengths and limitations. Then design of AODV routing protocol in NS-2 was studied and Tcl scripts were developed for implementation. A Random way point model was developed in NS-2 to simulate the mobility of the nodes. Different network scenarios with different number of nodes, node velocity and pause time were generated for simulation. The AODV routing protocol developed in NS-2 was modified and compiled to implement different attack models in different network scenarios.

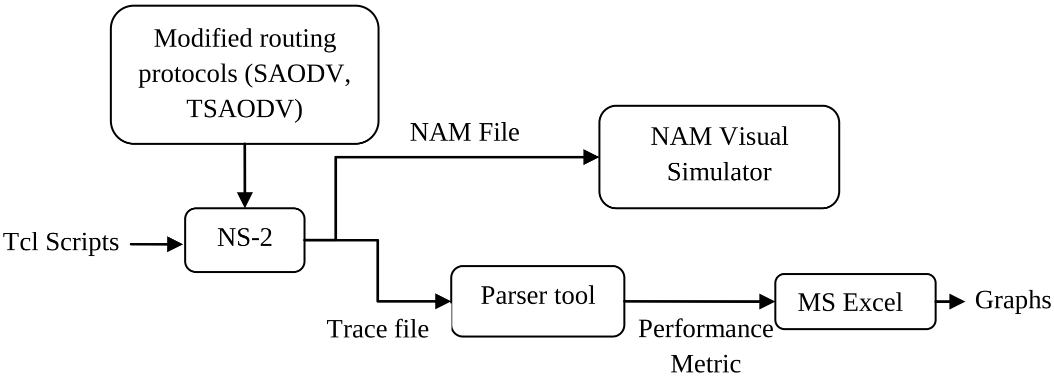

Figure 3.1. Procedure to implement routing protocols

SAODV algorithm was implemented in NS-2 by modifying AODV for security implementation. The protocol was compiled tested under different network scenarios. SAODV protocol designed was again modified to implement different attack model.

Trust model was incorporated with AODV to implement TAODV. TSAODV was designed by implementing trust algorithm in SAODV. The simulations were carried out in different network scenarios to analyze their performance in detail.

Trace files obtained from each simulation was analyzed using Java parser code implemented in Bluej to evaluate the performance metrics. Finally, the performance metrics were compared to evaluate the performance of the protocols in different scenarios.

3.1 SAODV Model

Route requests are managed by AODV route discovery algorithms which initiates with RREQ packets. Route discovery mechanism of SAODV [10] is described by following steps

```
i.    Sender Generates RREQ packet;
ii.   Sender signs all non-mutable fields (except hop count and hash chain fields)
      with its private key;
iii.  Apply Hash to a seed to generate hash chain field;
iv.   Append signature extension to RREQ packet;
v.    Broadcast RREQ to all neighbor nodes;
vi.   Intermediate node receives RREQ packet;
vii.  Node Verifies signature with public key of source (from RREQ packet);
       if (valid packet)
             update routing information of source (establishment of    reverse
      path);
viii.  If (destination id = = node id){
      Generate RREP;
      Sign all the 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
      ;}
ix.   Forward RREQ to all its neighboring node;
```

The procedure of route request is shown in figure 3.2. The route request procedure is initiated by sender node similar to that of AODV. Addition of digital signature and hash function are the key features. The security verification is done node by node as the route request packet propagates. Only the destination node is allowed to reply the route request.

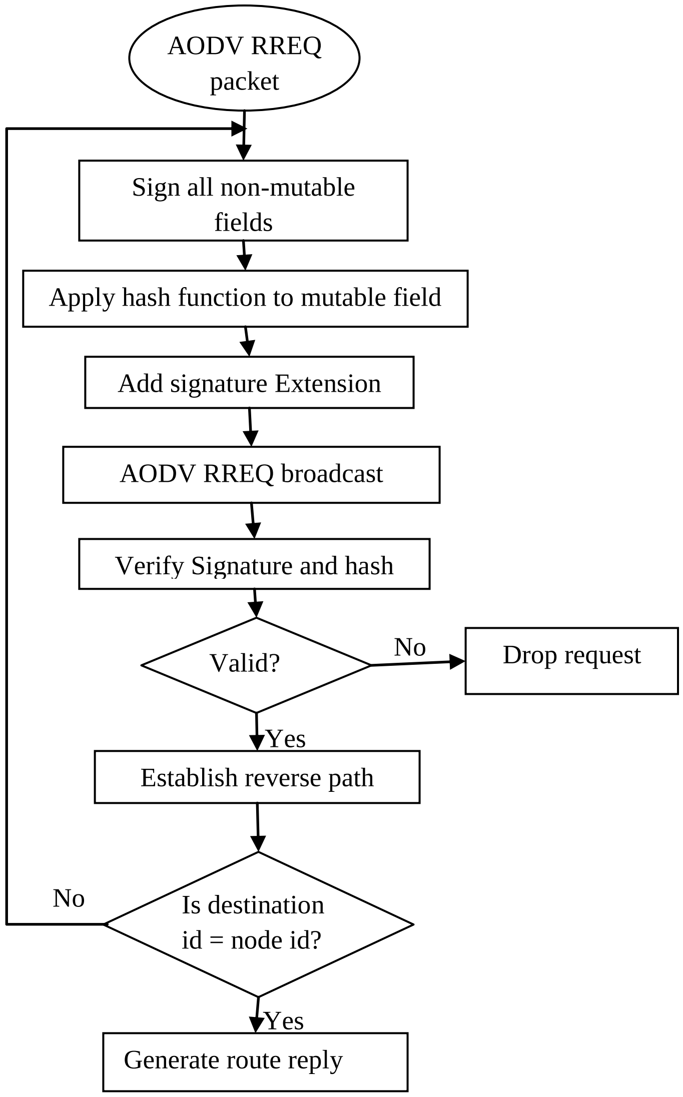

Figure 3.2 Flowchart for SAODV route request

As in route request procedure route reply procedure also considers for security verification as shown in figure 3.3. When route reply packet is issued by the destination node it travels back to source node using the reverse link created during flow of route request. All the non-mutable fields including destination id, source id and TTL fields are secured using digital signature and mutable field by hash function. As the route reply packet travels back to the source node the security verifications are done hop by hop basis as in case of route request. Finally, when the route reply packet reaches to the source node, a route is selected for communication.

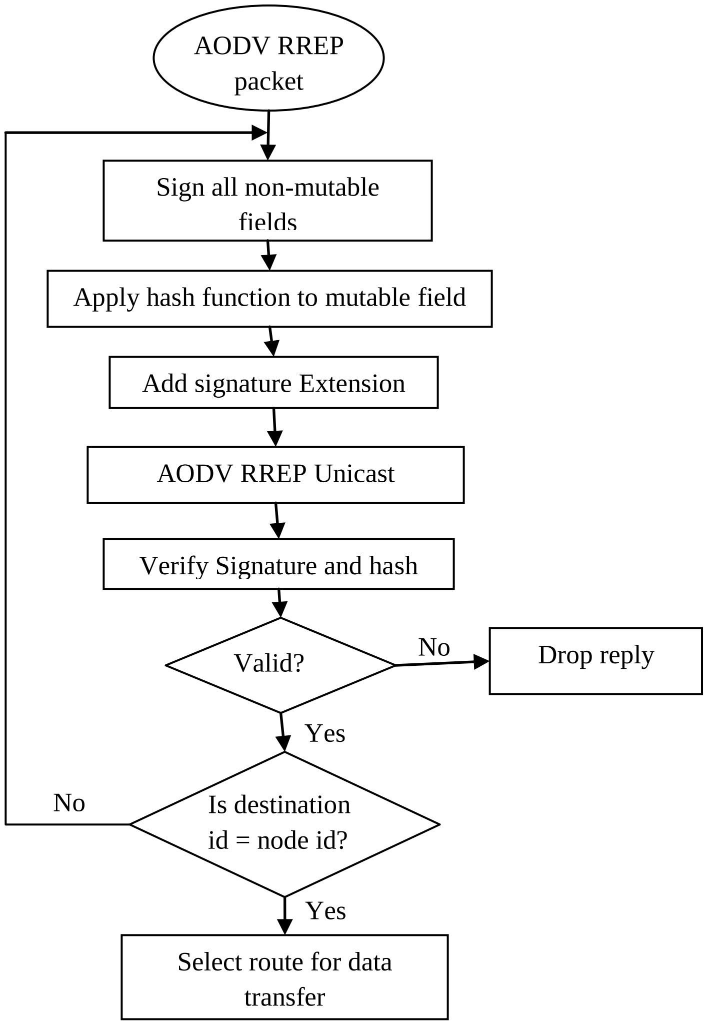
AODV RREP packet
Sign all non-mutable fields
Apply hash function to mutable field
Add signature Extension
AODV RREP Unicast
Verify Signature and hash
Valid?
No
Drop reply
Yes
No
Is destination id = node id?
Yes
Select route for data transfer

Figure 3.3 Flowchart for SAODV route reply

3.2 TSAODV Model

Route requests are managed by SAODV by route discovery algorithm which initiates with RREQ packets with fresh sequence numbers while discarding older ones. This updates routing table adding the new next hop of route. Each node chooses next hop of route on the basis of two metrics: Trust worthiness and Recommendation model [22]. Trust methodology and evaluation framework was used to implement the trust management capability to SAODV protocol. Based on recommendation model two new packet typologies TRREQ and TRREP are used [23, 24]. These packets have trust field addition to other fields in respective packets of SAODV which help in making intelligent decision to make choice of between nodes for communication.

TRREQ comprises of request originator and a list of requests about agents to check whether they are reliable. TRREP comprises of the originator, the recommender, who generates reply and a list of couples <agent, trust values>. Signature extension is added to make it cryptographically secure packets.

Let node A obtains k numbers of recommendation about B, the recommended trust value of B for A is T_A(B) and for every received recommendations, $T_A(i) > 0$ is given by

$$T_A(B) = (\sum_{i=1}^{k} T_A(i).T_i(B))/k \tag{3.1}$$

As nodes start to communicate, they interact with each other. Based on the history of interactions, direct trust value is computed after each interaction. For N number of interactions trust value of node B is computed by node A using direct trust computation as

$$T_A(B) = (1 + \sum_{i=1}^{N} w^{t_c - t_i} K_i)/(1 + \sum_{i=1}^{N} w^{t_c - t_i} P_i) \tag{3.2}$$

In equation (3.2) $K_i=0$ for failure interaction and 1 for successful interactions while $P_i=1$ for each interactions. The parameter w is weight used to account trust values with respective to time and t_c and t_i represent current time and initial time respectively.

The table is updated periodically, so the recommendations and the direct observations are stored in buffers until the update. If T_{i-1} is a trust record in table and T_{cal} be its calculated trust value based on recommended trust computation or direct trust computation, then the updated trust value T_i is given by

$$T_i = 1 - a(1 - T_{i-1}) - b(1 - T_{cal}) \tag{3.3}$$

where a and b are weighting factor.

The obtained value is normalized to the range [-1, 1] before update. Destination node is responsible for route selection form route discovery phase if multiple routes are available. Route selection is based route trust (RT) which depends on average trustworthiness of nodes and hop count. For a route with n number of nodes and x hop count

$$\mathrm{RT} = a(\text{max\_hop\_count} - x) + b(\textstyle\sum T/n) \qquad (3.4).$$

Where a and b are weight given to minimum hop count and maximum average trust of nodes.

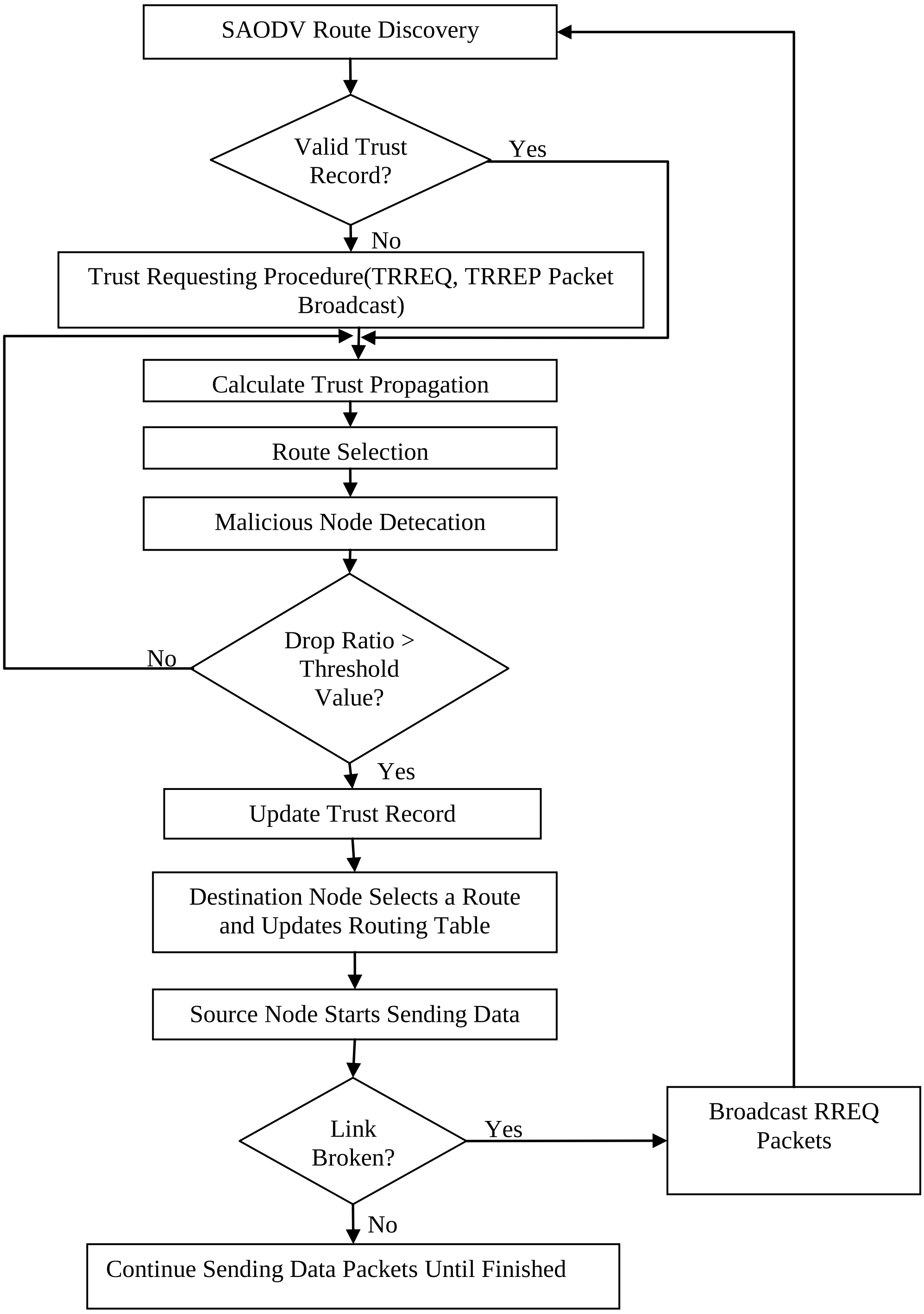
SAODV Route Discovery
Valid Trust Record?
Yes
No
Trust Requesting Procedure(TRREQ, TRREP Packet Broadcast)
Calculate Trust Propagation
Route Selection
Malicious Node Detecation
Drop Ratio > Threshold Value?
No
Yes
Update Trust Record
Destination Node Selects a Route and Updates Routing Table
Source Node Starts Sending Data
Link Broken?
Yes
Broadcast RREQ Packets
No
Continue Sending Data Packets Until Finished

Figure 3.4: Flowchart of TSAODV implementation

Detailed Steps of algorithm as shown in figure 3.4 are explained below:-

- Each node calculates the trust values of its neighboring nodes based on the observation and interactions.
- Source node performs on-demand routing to find possible routes to Destination nodes.
- As TRREQ packet flows from source node, each node also check the trustworthiness of forwarding nodes in addition to cryptographic verification.
- If a route selected for communication has a single blacklisted node as next hop, route is invalidated and new route discovery process is started.
- If a link is broken, route error packet will be sent to source node and source node will select alternate route from its route table otherwise does route discovery. Then whole algorithm is repeated.
- For each success and failure of communication through a node its trust value in recalculated and updated.

3.2 Mobility Model

Mobility models are broadly classified into three classes according to the degree of randomness [18]. If models are built based on traces, then everything is deterministic and these models are called trace based models. Using these model mobile hosts can be traced in the real world scenarios. If there is only partial randomness, the models are called constrained topology based models. Here hosts' movements are constrained by obstacles, pathways, etc., but speed and direction are still randomly chosen. If there is total randomness, we call these statistical models. Total randomness means that hosts can move anywhere in the area and the speed and direction are randomly chosen. Random Walk Model and Random Waypoint Mode Model are its example. Different mobility models introduce different mobility patterns which in turn introduce different network topology changes. The Random Waypoint Model was used in the simulation.

Random Waypoint Model is the most widely used and studied mobility model. In this model, a host randomly chooses a destination called waypoint and moves towards it in a straight line with a constant velocity which is selected randomly from some given range. After it reaches the waypoint, it pauses for some time and then repeats the same procedure.

The Random Waypoint Model can be described by a discrete time stochastic process [3]. In any time period, a host moves from present waypoint to next waypoint P(i), at a random speed V (i) . Its pause time at P(i) is denoted by T(i). Random Waypoint Model is represented by a three dimensional stochastic process{(P(i),V(i),T(i)), i = 1,2,...}.

Statistical properties of Random Waypoint Model [18] is describe using distributions of transition length, transition time and host position. Transition length is defined as the distance between two consecutive waypoints. Stochastically, transition length is the distance between two random points (uniformly distributed) chosen in a rectangular area.

Let us consider a random variable L denotes transition length and suppose the rectangle area be a×b. Then its probability density function is

$$f_L(l) = \frac{4l}{a^2b^2} f_0(l) \qquad (3.6).$$

Where

$$f_o(l) = \begin{cases} \frac{\pi}{2}ab - al - bl + \frac{1}{2}l^2 & \text{for } 0 \leq l \leq b \\ ab\sin^{-1}\frac{b}{l} + \sqrt{l^2 - b^2} - \frac{1}{2}b^2 - al & \text{for } b < l < a \\ 0 & \text{otherwise} \end{cases} \qquad (3.7).$$

3.3 Metrics for evaluation

The original AODV protocol is used as a benchmark to study the pure processing overheads of SAODV. Performance metrics are calculated using different attributes and parameters taken from the output of the executed simulation (.tr files) to measure and analyze the network behavior. To spot eventual weaknesses, evaluate the performance, effectiveness of different routing protocols and impact on the performance caused changes or modifications in routing protocols different metrices were identified.

In MANET there are several factors which characterize the network performance making all those metrics highly depending from each other. PDF, NRL and AED were used as metrics for evaluation.

PDF is the ratio of successfully delivered packets at the destination to the number of generated packets. It shows the capacity of each protocol for successful transmission of data packets to the destination, the reliability of the routing protocol.

$$\text{PDF} = \frac{\text{Number of Received Data Packet}}{\text{total Number of Sent DataPacket}} \tag{3.8}$$

The PDF metric shows the reliability and correctness of routing protocol.

NRL is the total number of routing packets transmitted per data packet delivered at the destination. This accounts for the overhead of the routing protocols. The number of total routing packets includes the number of RREQ, RREP, RERR, acknowledgement packets, hello protocol packets, etc.

$$\text{NRL} = \frac{\text{Number of Sent Routing Packet}}{\text{total Number of Sent DataPacket}} \tag{3.9}$$

The NRL metric allows analyzing other metrics pointing to the routing load.

AED measures the time that packets travel from the source to the application layer at the destination node. It includes various delays at different stages. Each data packet's sent time is subtracted from the receiving by the destination node, and then this number is divided by the total number of sent packets. It is expressed in milliseconds.

$$\text{AED} = \frac{\sum \text{t}_\text{r} - \sum \text{t}_\text{s}}{\text{total Pac kets sent}} \tag{3.10}$$

where t_r represents time at which packet was received and t_s being time at which packet is sent. The lower end-to-end delay, the shorter is the packet delivery time and better is the application performance of the routing protocol.

CHPTER FOUR: IMPLEMENTATION

Simulation environment was created using NS2.35 installed on Ubuntu14.04. AODV protocol designed in NS2.35 was used for simulation. To implement SAODV the AODV protocol was modified to implement cryptographic features. Digital signature was used to secure non-mutable field and hash chain to secure mutable fields. In implementation of TSAODV a trust model was added to SAODV. A trust value was initially defined for each node.

4.1Simulation Tool

NS-2 is an object-oriented simulator developed as part of the VINT project at the University of California in Berkeley. It provides substantial support for simulation of TCP, routing, multicast protocols over wired and wireless (local and satellite) networks, etc[19]. The simulator is event-driven and runs in a non-real time fashion. It consists of C++ core methods and uses Tcl and OTcl shell as interface allowing the input file (simulation script) to describe the model to simulate. Users can define arbitrary network topologies composed of nodes, routers, links and shared media. A rich set of protocol objects can then be attached to nodes, usually as agents. It has already become the de facto standard in networking research.

The key to get to know NS-2 is it is a discrete event network simulator. In NS-2 network physical activities are translated to events, events are queued and processed in the order of their scheduled occurrences. And the simulation time progresses with the events processed. Typically, it can configure transport layer protocols, routing protocols, interface queues, and also link layer mechanisms. We can easily see that this software tool in fact could provide us a whole view of the network construction, meanwhile, it also maintain the flexibility for us to decide. Thus, just this one software can help us simulate nearly all parts of the network [19]. This definitely will save us great amount of cost invested on net work constructing.

NS-2 was used as the simulation tool as it was a powerful open-source simulation tool that had the basic modules needed for simulations. NS-2 has the capability to simulate many features such as, traffic source behavior (CBR and VBR), routing, packet flow, network topology, multicasting and mobile nodes. NS-2 supports different ad-hoc routing protocols [19]. The AODV routing is one of the built in protocols of NS-2.

NS-2 is a discrete-event driven and an object oriented simulator with a frontend OTcl interpreter and backend C++ modules. The topology of the simulated network and its overall configuration is initially described in OTcl and then a simulator object is defined through the C++ code detailing the network protocols, packet headers, etc. OTcl is more suitable for the configuration part of the simulation compared to C++, as it is faster to change but slower to run.

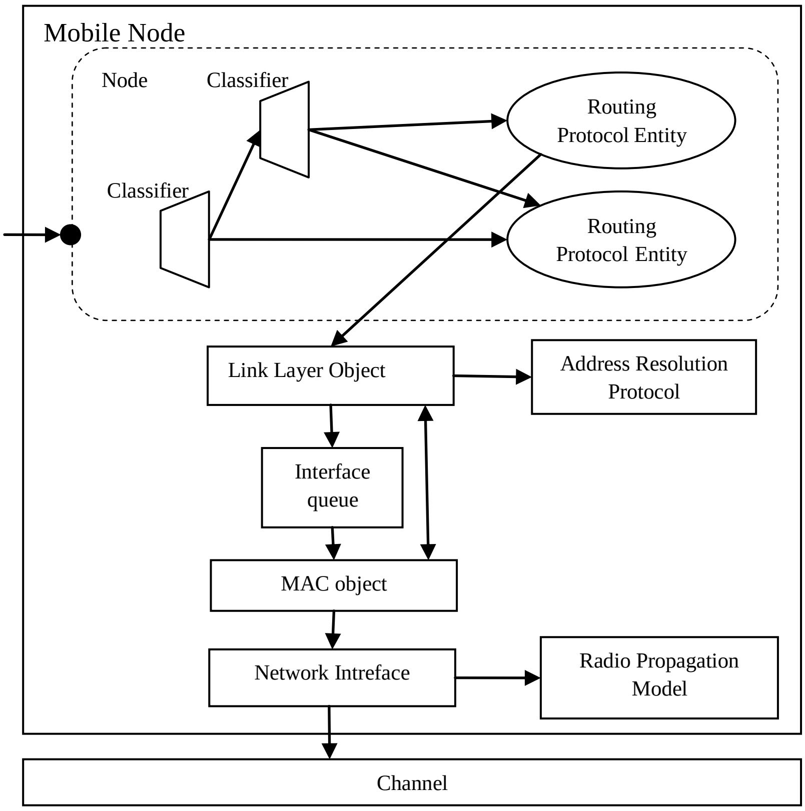

Figure 4.1: Structure of mobile node

The basic component used to develop our experiment is the ns2 mobile node module. A mobile node is a basic NS-2 node with the added abilities of mobility and transmitting or receiving from a wireless channel. Figure 4.1 shows the mobile node structure, which depicts a basic NS-2 node connected to an ad hoc routing agent and a network stack consisting of a link layer object, interface queue, a MAC object and a physical network interface connected to an antenna.

4.2 Experimental Setup

The main simulation and network configuration in NS-2 takes place in the Tcl script. The procedure of executing simulation is described in figure 4.2. After describing the routing protocol in NS-2, Tcl script was run and the output files are analyzed for results.

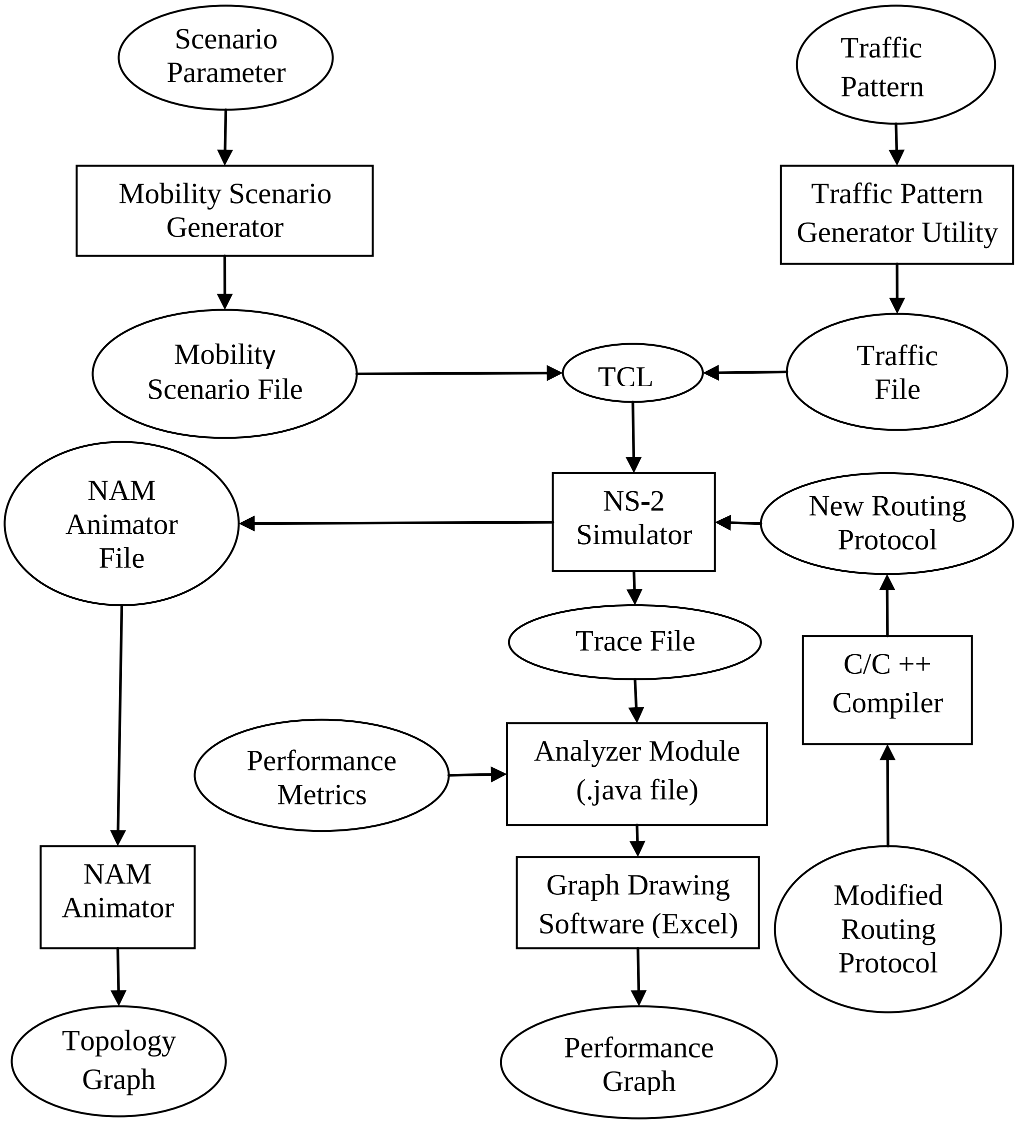

Figure 4.2: Implementation of Routing Protocols

The two main output files, a trace file with all the events such as send, receive, packet drop, etc. and a NAM file were obtained from simulation. NAM file can be used by the network animator to view the simulation in graphical mode using NAM tool, a separate component used with ns to provide a visual interpretation of the network topology. The trace files were analyzed using Java parser code to calculate the performance metrics and the main features were then illustrated as a graph using MS Excel.

4.3 Scenario setup

During simulation, scenarios with number of nodes varied from 10 to 200 were created and random waypoint model was used as mobility model. Simulations were carried in both malicious and non-malicious environment. In malicious environment up to twenty percent of nodes were declared malicious. The simulation scenario is summarized below:

Table 4.1 Simulation scenario

Parameter	Value
Mobility Model	Random waypoint Model
Simulation Time	500 seconds
Number of Nodes	10 to 100
Simulation Area	500m*500 m
Node Velocity	0 to 25 m/s
Pause Time	0 to 100 seconds
Traffic Type	CBR
Packet Size	512 Bytes

CHAPTER FIVE: RESULTS

5.1 Non-malicious Scenario

The performance of AODV, SAODV and TSAODV in terms of PDF was found to be comparable. Since a secured environment was assumed, there were fewer packet drops in all and hence the similar behavior. The main difference was observed in terms of AED. Higher delays were observed in SAODV and TSAODV due to implementation of node by node digital signature and hash chain verification. In terms of NRL also, AODV outperforms SAODV and TSAODV in secured environment.

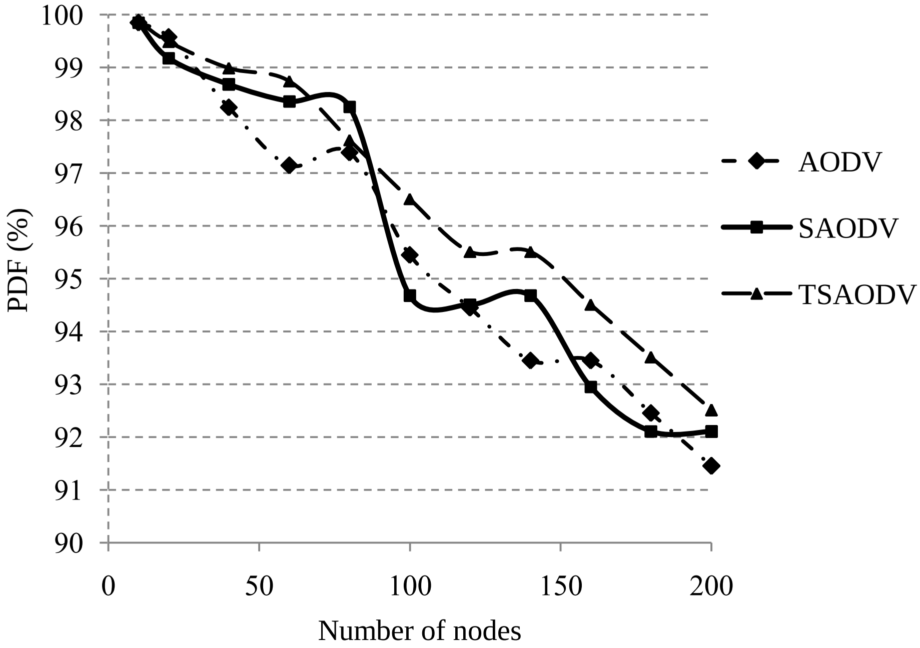

Figure 5.1: Variation of PDF with number of nodes

There is slight decrease in PDF with increase in mobile nodes as shown in figure 5.1.. The performance of all three protocals were found to be comparable regarding PDF metric. There is abrupt decrease in PDF metric with maximum velocity of mobile nodes as shown in figure 5.2. The increase in the velocity of mobile nodes increases the probability of link failure hence increases the packet loss. The variation of PDF with pause time is shown in figure 5.3. PDF metrics of all three protocols are still found to be comparable.

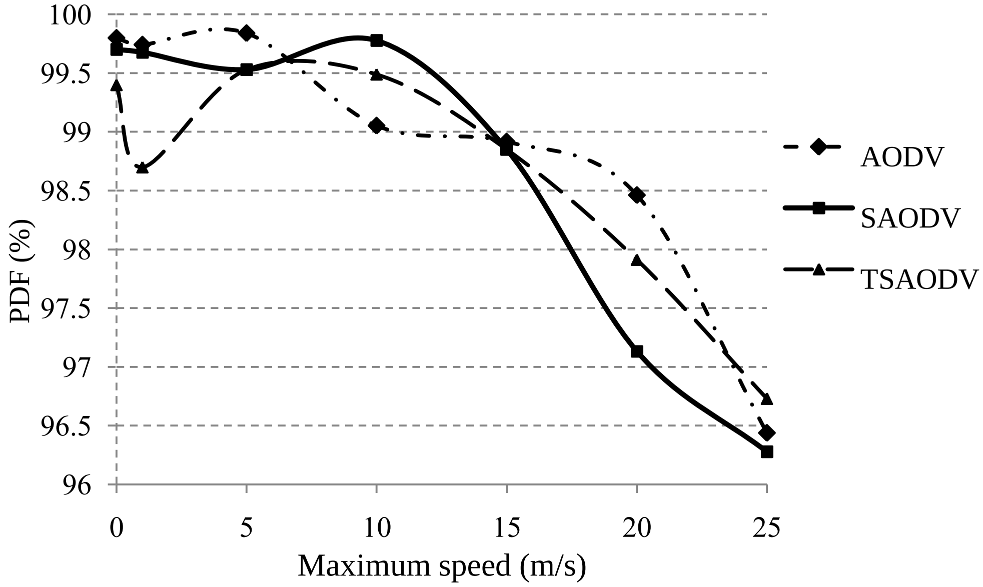

Figure 5.2: Variation in PDF with maximum speed

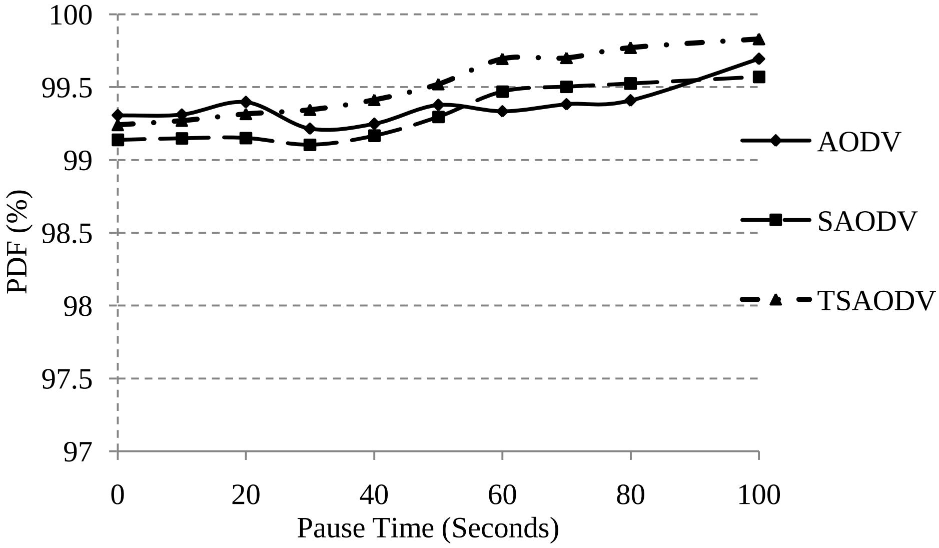

Figure 5.3: Variation in PDF with pause time

Average end to end delay was found to be higher in SAODV and TSAODV. These protocols involve node to node authentication which consumes significant processing time and hence increase in delay. There is increase in AED with the number of mobile nodes as shown in figure 5.4. Increase in pause time causes decrease in AED. As the pause time increases there are fewer route errors and hence fewer route repairs. This causes significant decrease in AED as shown in figure 5.5. In the similar manner figure 5.6 shows in increase of AED with maximum velocity of the nodes. In all the three cases AODV is found to perform better.

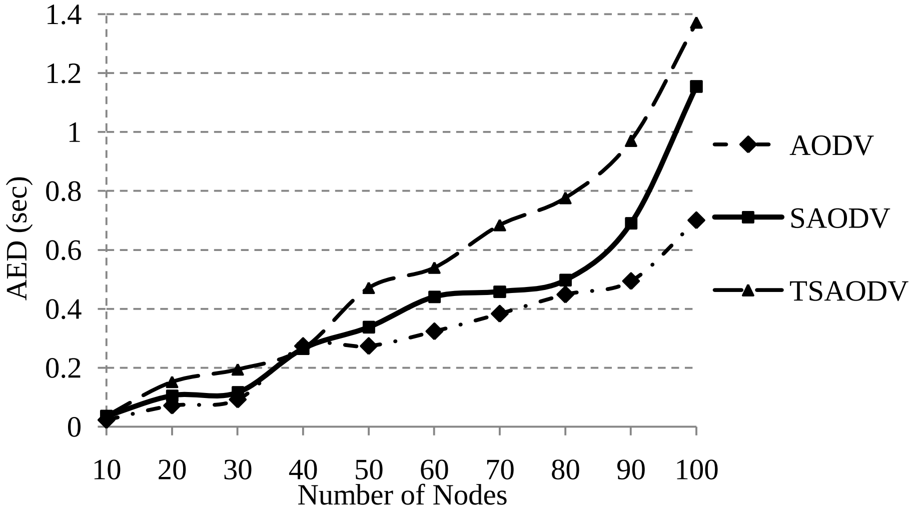

Figure 5.4: Variation in AED with number of nodes

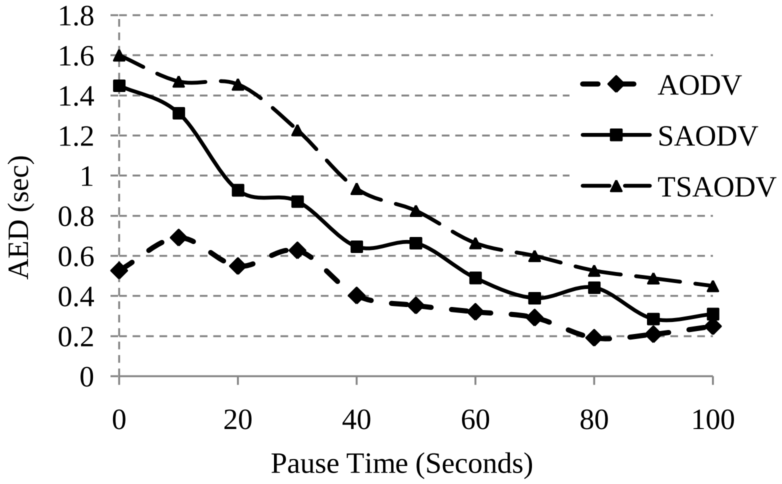

Figure 5.5: Varition in AED with pause time

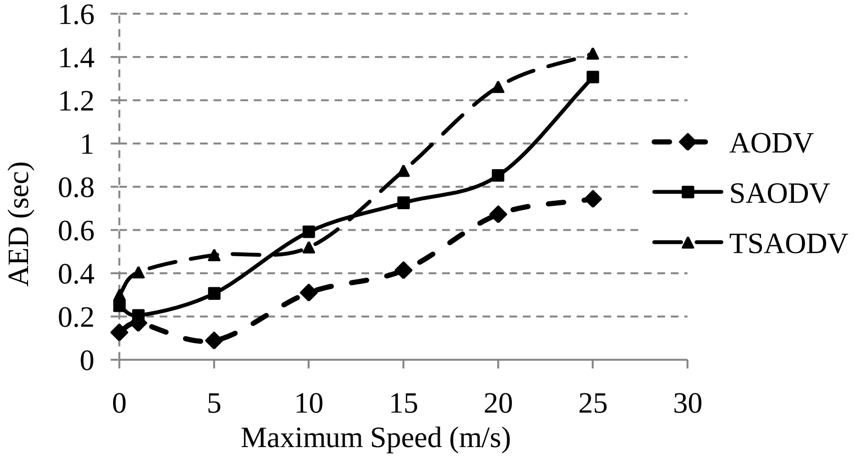

Figure 5.6: Variation in AED with maximum speed

Packets are sent for cryptographic purpose in SAODV in addition to normal AODV routing packets. This increases the routing load. In TSAODV packets from only trusted nodes are processed and forwarded which makes its performance better than SAODV. Figure 5.7 shows that with lower number of nodes AODV has lower value of NRL but for higher values TSAODV performs better. Decrease in NRL with pause time is shown in figure 5.8 and figure 5.9 shows significant increase in NRL with the maximum velocity. In all three cases performance of SAODV is found to be worst. The improvement in performance of TSAODV is due to communication between only selective nodes.

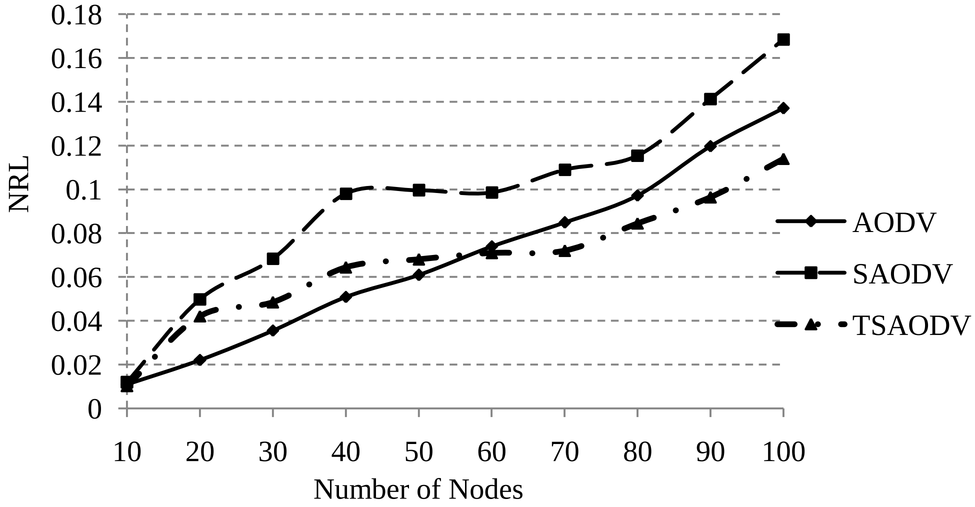

Figure 5.7: Variation in NRL with number of nodes

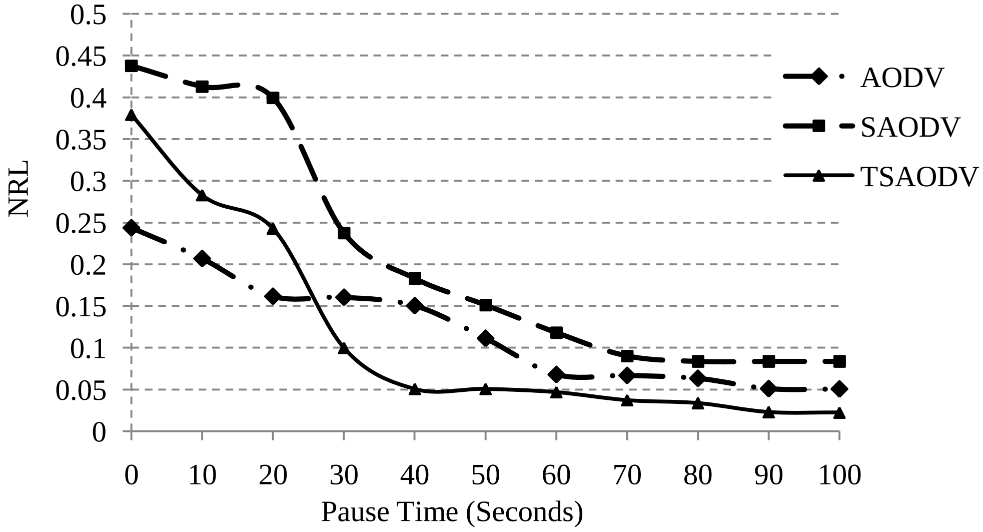

Figure 5.8: Varition in NRL with pause time

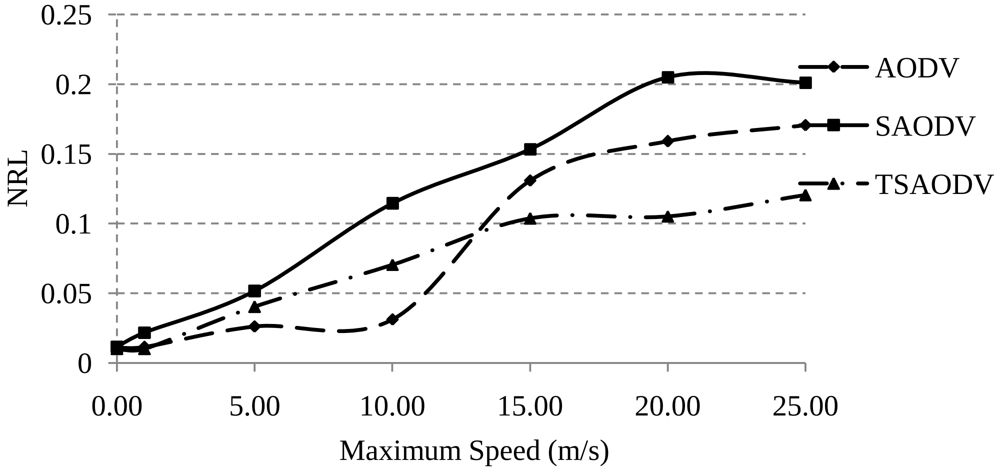

Figure 5.9: Variation in NRL with maximum speed

Route selection time for TSAODV has significantly increased as shown in figure 5.10. The use of cryptographic verification in each hop as route request and route reply packet travels through the network is the prime cause of increase in route selection time of SAODV. This time further increases in case TSAODV where routes are maintained using highly trusted nodes. The trust verification often results longer routes which means higher route selection time.

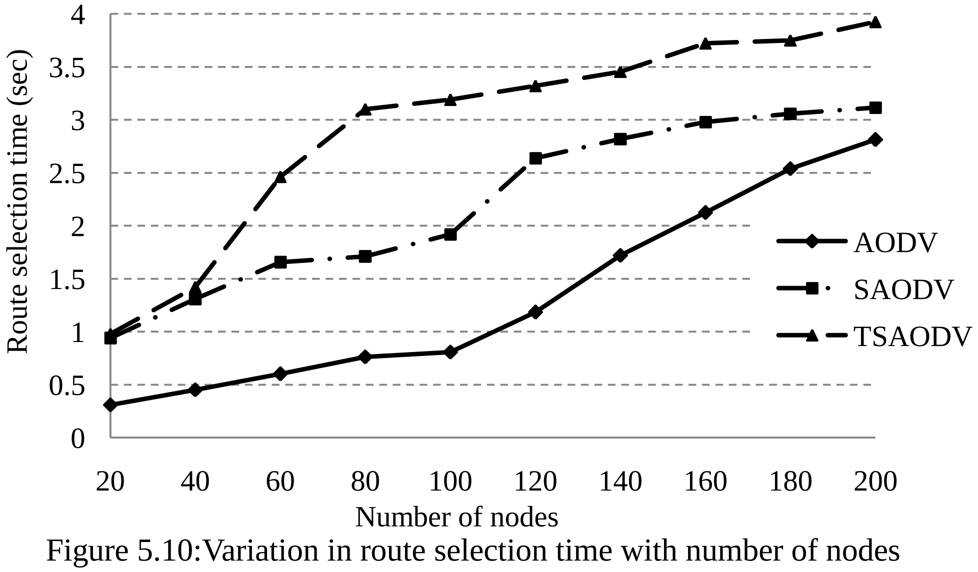

Figure 5.10:Variation in route selection time with number of nodes

5.2 Malicious Scenario

AODV was found to be vulnerable to all types of security threats and there was a significant decrease in PDF metric with the increase in the number of malicious nodes. SAODV was found to be vulnerable to impersonation attacks though it was found to be immune to attacks like route modification, hop count modification and route drop attacks. The inclusion of trust model in TSAODV made it immune to these attacks. TSAODV outperforms all other protocols in terms of PDF.

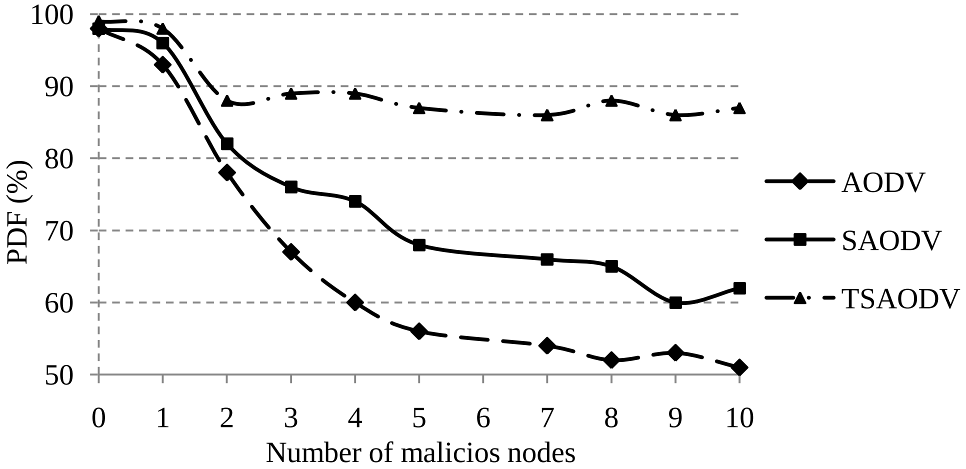

Figure 5.11: Variation in PDF with number of malicious nodes

With AODV, when the number of malicious nodes was increased, the number of data packets dropped by them also increased. This was the cause for the decline in the PDF metric of AODV and SAODV protocol. The PDF metric of TSAODV remained unchanged even when number malicious nodes are increased as shown in figure 5.11.

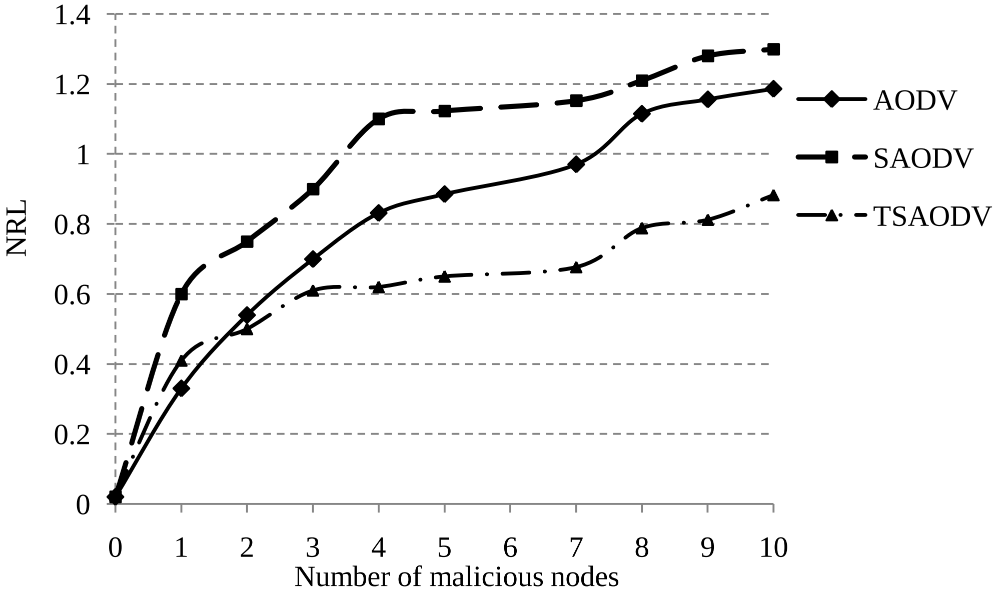

Figure 5.12: Variation in NRL with number of malicious nodes

The AODV protocol was also fooled by the packet modification attack and impersonates attack. There were no new routing packets generated, so the number of routing packets was nearly constant. The NRL metric is inversely proportional to the number of received data packets. Consequently, the NRL metric was slightly raised when the number of malicious nodes was increased. But, with SAODV, during route modification attack, due to its capability of detecting and discarding changed routing packets, many more new routing packets were sent to find a new route. This reason caused the increase in the NRL metric of SAODV. In case of TSAODV the routing packets from the only trusted nodes were routed which significantly decreased the number of routing packets causing significant improvement in NRL metrics as shown in figure 5.12.

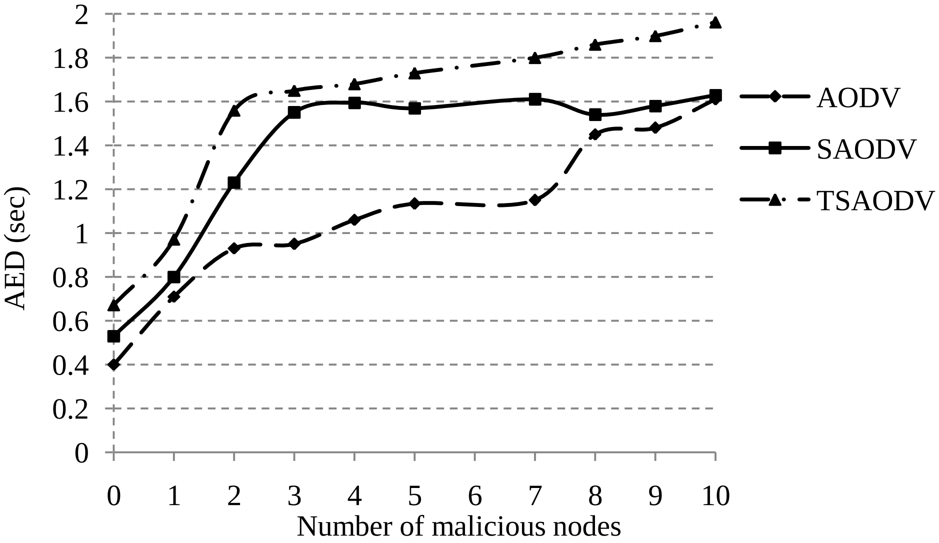

Figure 5.13 Variation in AED with number of malicious nodes

Performance of AODV was still found best in terms of AED even in malicious scenario as shown in figure 5.13. The reason of higher value of AED in TSAODV was due to the processing time involved in trust verification and cryptographic processes involved.

CHAPTER SIX: EPILOGUE

6.1 Discussions

Security has become the primary focus of research efforts in ad hoc communication environment. Dynamic nature of MANET results into unique and considerable difficulties of providing security. The results of this thesis are based on extensive simulation of different network environments in determining the performance and security issues of MANET using AODV routing protocol and its security extensions. Protocol efficiency was analyzed in different environment using various attributes. The detailed analysis of AODV and secured extensions of AODV (SAODV and TAODV) were performed to propose a security enhanced protocol, TSAODV that includes features of both SAODV and TAODV.

AODV uses no security measures so is always prone to security threats. SAODV can fight various types of vulnerabilities of AODV. SAODV uses hybrid cryptography and provides security features such as integrity, authentication and non repudiation of routing data. The use of cryptographic approach that provides hop by hop security in SAODV again presents issues in routing performance in terms of routing overload and end to end delay. However, trust management and cryptographic solutions merging together provides a robust solution to secure routing protocols.

6.2 Conclusion

Offering security only through cryptography is not always a suitable solution if the high dynamic context of MANET is considered. Security measures with cryptographic solutions overload the network. As a result, network performance is degraded. A trust mechanism that reduces the computationally intensive number of security operations becomes strategic. To improve performance of SAODV and offer more resilience to attack from malicious nodes authenticated by the network, a trust model must be added. Trust evaluation system can improve network throughput as well as effectively detect malicious behavior in ad hoc networks. It was observed that security and performance improves if nodes can make intelligent choices of non-malicious nodes and if contextual information is known in the form of routing tables.

REFERENCES

[1] A. May Cho, A. Moe Aung, “Energy efficient multipath routing for multipath routing for mobile ad hoc networks,” International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.3, August, 2014.

[2] Y.C. Hu, D. B. Johnson, A. Perrig, “Secure efficient distance vector routing in mobile wireless ad hoc networks,” Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp 3–13, June 2002.

[3] A. Todd, Y. Alec, “Surveying security analysis techniques in MANET routing protocols,” IEEE Communications Surveys & Tutorials, Vol. 9, No. 4, 2007.

[4] J. G. Viji , V.S. Anna, “A survey on security analysis of routing protocols,” Global Journals Inc. (USA) , Volume 11 Issue Version 1.0,April 2011.

[5] J. C Imrich, C. Marco, “Mobile ad hoc networking: imperatives and challenges,” Ad-hoc networks, 2003.

[6] P. Narayan, V. R. Syrotiuk, “Evaluation of the AODV and DSR routing Pprotocols using the MERIT tool,” ADHOC-NOW, 2004.

[7] L. Yuxia Lin, A. Hamed Mohsenian Rad, W. Vincent, S. Joo-Han. “Experimental comparisons between SAODV and AODV routing protocols,” ACM workshop on Wireless multimedia, 2005.

[8] L. Celia, W. Zhuang, Y. Cungang, “Secure routing for wireless mesh networks,” International Journal of Network Security, Vol.12, No.3, May 2011.

[9] A. A. Pirzada and C. McDonald, “Establishing trust in pure ad-hoc networks,” Twenty-Seventh Australasian Computer Science Conference (ACSC2004), volume 26 of CRPIT, pages 47– 54, Dunedin, New Zealand, 2004.

[10] S. Arif, “Security approaches in IEEE 802.11 MANET —performance evaluation of USM and RAS,” Int. J. Communications, Network and System Sciences, 2014.

[11] P. Kavita, S. Abhishek, “A comprehensive performance analysis of proactive, reactive and hybrid MANETs routing protocols,” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 3, November 2011.

[12] A. Jayanand, T. Jebarajan, “A secured routing protocol for MANETs,” IJCSET, Vol. 2, Issue 8, August 2012.

[13] L. Anil, G. Sohan, “A study on the behavior of MANET: along with research challenges, application and security attacks,” International Journal of Emerging Trends & Technology in Computer Science, Vol. 4, Issue 2, April 2015.

[14] S. Munish, K. Manish, B. Tarunpreet, “Simulation analysis of MANET routing protocols under different mobility models,” International Journal of Wireless Communications and Networking Technologies, Vol. 4, No.1, January 2015.

[15] H, Yih Chun, C. Adrian Perrig, J.David, “Packet leashes: a defense against wormhole attacks in wireless networks,” IEEE INFOCOM, 2003.

[16] M.Hetal, H. Nital, “A Survey: Use of ACO on AODV and DSR routing protocols in MANET,” IJIRT, Vol. 1 Issue 5, 2014.

[17] M. Sarah, Z. Saman, M. Sikander, K. Hayat, M. Sheraz Baig “Secure zone based routing for bluetooth,” Journal of Theoretical and Applied Information Technology, Vol. 54, No.3, August, 2013.

[18] Z. Qunwei, H. Xiaoyan, R. Sibabrata, “Recent advances in mobility modeling for mobile ad hoc network research,” ACMSE April, 2004, Huntsville, Alabama, USA.

[19] V. Kannan, “The ns manual,” The VINT Project, November, 2011.

[20] L. Janne, “Counting to Infinity,” Seminar on internetworking sjökulla, 2004.

[21] D. Aditya, D. Amruta, D. Rahul, “Modified AODV protocols: a survey,” National Conference on Information and Communication Technology, 2011.

[22] A. Lupia, F. De Rango “Evaluation of the energy consumption introduced by a trust management scheme on Mobile ad-hoc networks,” Journal of Networks, vol. 10, no. 4, April 2015.

[23] K. Jaspreet, H.Sandeep “An energy efficient, secure and trust aware routing protocol in MANET,” IJCSET, vol. 5, issue7, July 2015.

[24] S.Pankaj, J.Yogendra Kumar “Trust based secure AODV in MANET,” Journal of Global Research in Computer Science, vol. 3, No. 6, pp. 107-117, June 2012.