"QOS based Performance Evaluation of Secure on-Demand Routing Protocols for MANET's"

Developed By

Muhammad Naeem

&

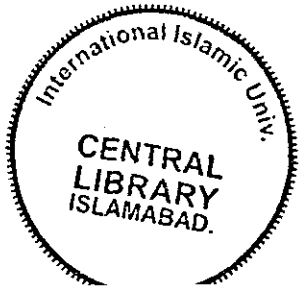
Zahir Ahmad

For the degree of
MS in Electronic Engineering
(Majors in Telecommunication Engineering)

Supervised By

Engr. Suheel Abdullah Malik

Department of Electronic Engineering
Faculty of Engineering & Technology
International Islamic University, Islamabad
June, 2009



Project in Brief

Project Title:	"QOS based Performance Evaluation of Secure on-Demand Routing Protocols for MANET's"
Organization:	Department of Electronic Engineering Faculty of Engineering & Technology International Islamic University, Islamabad Pakistan
Undertaken By:	Muhammad Naeem 22-FET/MSEE/F05 & Zahir Ahmad 26-FET/MSEE/F05
Supervised By:	Engr. Suheel Abdullah Malik Assistant Professor, Department of Electronic Engineering Faculty of Engineering & Technology International Islamic University, Islamabad
Languages:	C and Tcl
Simulation Tool Used:	Network Simulator (NS-2)
Operating System:	RedHat Linux
System Used:	Pentium IV, 1 GB RAM
Project starting Date:	April, 2008
Project Completion Date:	June, 2009

International Islamic University, Islamabad

Date: _____

Final Approval

It is certified that we have read the thesis titled "**QOS based Performance Evaluation of Secure on-Demand Routing Protocols for MANET's**" submitted by **Muhammad Naeem, Registration # 22-FET/MSEE/F05** and **Zahir Ahmad, Registration # 26-FET/MSEE/F05** which, in our judgment, is of sufficient standard to warrant its acceptance by the International Islamic University, Islamabad for the award of MS in Electronic Engineering degree having majors in Telecommunication Engineering.

External Examiner
Dr. Muhammad Zubair
Assistant Professor,
Department of Computing,
Riphah International University, Islamabad.

Internal Examiner
Dr.Tanveer Ahmad Cheema
Assistant Professor,
Department of Electronic Engineering.
Faculty of Engineering & Technology,
International Islamic University, Islamabad.

Supervisor

Engr. Suheel Abdullah Malik
Assistant Professor,
Department of Electronic Engineering,
Faculty of Engineering & Technology,
International Islamic University, Islamabad.

Declaration

We, hereby declare that this research work has not been copied from any source. It is further declared that we have developed this research work entirely based on our personal efforts under the supervision of Engr. Suheel Abdullah Malik. If this thesis is proved to be copied or reported at any stage, we accept the responsibility to face the subsequent consequences. No part of this work inscribed in this thesis has either been submitted to any other university for the award of degree / qualification.

Muhammad Naeem
22–FET/MSEE/F05

Zahir Ahmad
26–FET/MSEE/F05

Acknowledgement

"We simply bow our heads before Almighty Allah for giving us faith in our abilities and enabling us to accomplish this project and granting us with His Special Merci, Blessings and unlimited help throughout the phases of the project.

We dedicate this research project to our beloved Parents, Family members, respected Teachers and Sincere Friends".

We are especially grateful to ***Engr. Suheel Abdullah Malik*** *for his extended Cooperation by supervising and giving us advice whenever we needed and also providing hardware and software resources to develop this project in the department labs. We owe a great deal to all respected teachers especially* ***Prof. Dr. Ijaz Mansoor Qureshi*** *who extended towards us whatever help was required during our MS degree.*

In the nutshell, it is the blessings of Almighty Allah, parent's orisons, the guidance of our supervisor to complete this project work and report successfully.

Muhammad Naeem
22-FET/MSEE/F05

Zahir Ahmad
26–FET/MSEE/F05

"A Dissertation Submitted to the

Department of Electronic Engineering,

Faculty of Engineering & Technology,

International Islamic University, Islamabad,

As a Partial Fulfillment of the Requirements for the Award of

the Degree of MS in Electronic Engineering

(Majors in Telecommunication Engineering)"

ABSTRACT

With the course of era and boost in the want for mobility wireless or mobile networks emerged to swap the wired networks. This new age band of networks is different from the former one in many aspects like network infrastructure, resources and routing protocols, routing devices etc. These networks are bandwidth and resource constrained with no network infrastructure and dedicated routing devices. Moreover, every node in such networks has to take care of its routing module itself. Some work has been done to compare different protocols on basis of security but keeping in view the resource limitations in such networks, evaluation based on networking context is also important.

The objective of this thesis is to evaluate the two secure routing protocols that are SAODV and Ariadne for the mobile Ad-Hoc networks (MANETs) under the Random Way and Manhattan Mobility Model on the basis of performance metrics regardless of the security metrics. We implement the Secure Ad-Hoc on-Demand Distance Vector routing protocol (SAODV) extensions with AODV and Ariadne extensions with DSR in the Network Simulator 2 (NS-2). We try to compare out the Quality of Service parameters like End to End Delay, Jitter, Routing Overhead, Route Acquisition time, Throughput, Hop count, Packet Delivery Ratio using Manhattan Grid and Random Way Point mobility models to figure out the amount of extra work a mobile node has to do in order to provide good quality of service.

Table of Contents

Contents **Page#**

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Wireless

Normally the name of wireless wont to advert whatever case of electronic or electrical process established free from 'hardwired" link. Wireless communication is the process which transforms information across distance free from electrical "wires". This distance perhaps small or huge (television controlled by remote or thousands or several hundred thousands kilometers for radio communication). At the time framework is absolved the term frequently abbreviated to "wireless". Wireless communication generally is counted to be a furcated of telecommunication [1].

It covers various types of stationary, moveable, and mobile two way radios, personal digital assistants (PDAs), cellular telephones, and wireless networking. Following are the wireless technology examples:

Cordless telephones, GPS units, Satellite technology, garage door system to control the door of garage, wireless computer system and its attached devices keyboard and mice.

1.1.1 History of Wireless

The word "Wireless" acquired communal use to pertain a radio receiver and might be transceiver (send and receive data at same time), instituting its practice in wireless telegraphy field early on; now-a-days this term is put upon to depict modern wireless connections like in wireless broadband Internet and mobile networks[1].

In general sense this is referred to a kind of functioning which is applied without using cable, like "wireless remote control which is used for different purpose", "wireless energy transfer", etc. irrespective of the particular technology (e.g., ultrasonic, infrared, radio, etc.) which is applied to complete the task and operation[1].

1.1.2 Applications of wireless technology

Security Systems

Wireless applied science may complement or supplant hard wired effectuation for office buildings and homes security systems.

'evision Remote Control

Radio waves are also used in Modern television sets which are controlled by wireless (normally infrared technology) remote control units.

llular Telephones

Cellular phones are long familiar model of wireless technology. Radio waves are used to make possible operator/also used for making calls anywhere in the World.

ıplementation of this system needs of cellular site which house the equipment which sends t and receive the signal to transmit data and voice both to and from theses equipments.

ıis is explained in more detail by this example. The Tow Truck Dispatch service company es the cellular phone for sending Detailed and Quick Accident Reports through text ɜssage to Tow Truck Drivers and drivers are allowed to live in a radio free environment; ɛy continually receive Important Accident Information without waiting on peak of the dio.

2 Wireless LAN.

WLAN (*wireless local area network*) is technology to communicate, without using wires e can connect two or more than two devices. WLAN use OFDM modulation technique hich is based on radio waves to make possible bounded area communication among ɛvices, also acknowledge as the basic service set. This allows user to actuate and still be ɔnnected to the network within a wide coverage area.

/LAN got popularity for home users due to its rapid installation and alleviation, and ıcation exemption as the popularity of laptops is growing. Public business like malls, ɜminar rooms, hotels, coffee shops etc, has started to provide wireless access facility to their ıients; even some are providing free services.

1.2.1 History of WLAN

In the period of 1970 in University of Hawaii, the world's first computer communication network using inexpensive ham-like radios, named ALOHA net was produced and developed under the supervision of Norman Abramson [2]. This system use bi-directional star topology which consists of 7 computers positioned over 4 islands to communicate without phone lines with central computer which was located on the Oahu Island.

"In 1979, paper published in IEEE by F.R. Gfeller and U. Bapst [2] in which they Proceed and report about an experiment using mellow infrared communications on wireless local area network. Shortly thenceforth, in 1980, P. Ferrert in the IEEE National Telecommunications Conference reported a single code spread spectrum radio for wireless visual display unit communications. For wireless networks in 1984 comparison between CDMA and Infrared spread spectrum communications is made by Kaveh Pahlavan [3], later in the IEEE Communication Society Magazine his paper was published in IEEE Computer Networking Symposium [3]. In May 1985, Marcus also efforts to announce experimental ISM band for commercial and business application of spread spectrum technology. Afterwards, a report was made on an experimental wireless PBX system using CDMA by M. Kavehrad [3]. In the expansion of a new creation of wireless WLAN these efforts encouraged considerable industrial activities and by this in the mobile radio and moveable industry's old discussions are updates.

In early 1980, recreational radio operators developed the first generation of wireless data modems. The voice band data communication modem is added by these operators, this modem data rates was under 9600 bit/s, to subsisting radio system with little distance, typically have the recreational band in the two meter. When FCC is announced in the experimental band which is for non-military use of spread spectrum, at that time wireless modems second generation was developed. The speed of these modems was 100 kbit/s. The 3rd generation of wireless modem was aspired to make modems compatible with the existing LANs regarding data rates in the rate of Mbit/s. Modems having 1Mbit/s data rate is developed by various companies in the third generation of wireless modems and on the

occasion of first IEEE workshop on Wireless LAN, couple of modems already had been heralded.

In 1991 on Wireless LAN first IEEE Workshop [4] was held and in the market WLAN products and application had just appeared for sell and the efforts and activities in the development of Wireless LANs standards had just started by IEEE 802.11 committee. Assessment of the alternative technologies was the main focus of that 1st IEEE workshop. In 1996 this technology was comparatively ripe, many applications had been developed. For the brisk market growth of Wireless LAN implementation and applications, a chip sets was aspired and the key enabling technology. Wireless LANs usage were in multinational offices, for roaming access in campus and other buildings, hospitals, stock exchanges, Ad-Hoc networking, LAN bridges, point-to-point connection and more bigger applications through interworking. Rapid progress had been made by European HIPERLAN and wireless LAN interoperability forum in the IEEE 802.11 standard, some presents new opportunities, such as the proposed SUPER Net, then renamed as U-NII, unlicensed (Personal Communications Services) PCS [4].

At Macworld Expo which was held in New York City on July 21, 1999 firs time WLAN was available for consumer on low price rate. In the Wireless LAN history it happened the first time when WLAN is publicly available at customer pricing and useable for residence, before this WLAN was very expansive for customer and only used in big corporate sector.

In start, Wireless LAN hardware was much expensive because it was the alternative of cable LAN especially the cases where it is very complicated or near to impossible to make the wired connection. Its own protocols and industry-oriented solutions were included in the first developments but these were removed by standards at the end of 1990s, first and foremost IEEE 802.11 (Wi-Fi) versions like HIPERLAN, ATM 5 GHZ standardized technology had no success in market at that time.

1.2.2 Benefits of Wireless LAN

The wireless LANs benefits are following:

Convenience: Within the main networking environment, users are allowed to use nearly convenient location's network resources. This networking environment may be home or office. Within the increasing diffusion of laptop-style computers and nomadic devices, this is mostly relevant.

Mobility: As the public wireless network growing, user can use the internet away from their normal working environment, In most of the coffee shops, hotels the customers are offered wireless access to internet without paying or at very low cost.

Productivity: If the wireless users changes his place to another they can sustain a nearly regular link with their wanted networks. Employees can be more productive as they can finish their work from any suitable location.

Deployment: For wireless networking preliminary setup slightly more than a single access point is required but for the wired networks are costly and physical cabling is very complicated to do on the various locations.(If the building is very big it is even impossible to get connected with wires)

Expandability: The numbers of users in wireless networks can be increased abruptly. But in a wired network, additional wiring required when user increase.

Cost: Hardware for wireless network is more expansive as we compare to the wired networks.

1.2.3 Types of WLAN

The WLAN is categorized into two types according to their structure.

1.2.3.1 Infrastructured

Fixed base stations (BS) are used for Infrastructure WLAN. The communication between the mobile hosts (nodes) is done by these fixed base stations.

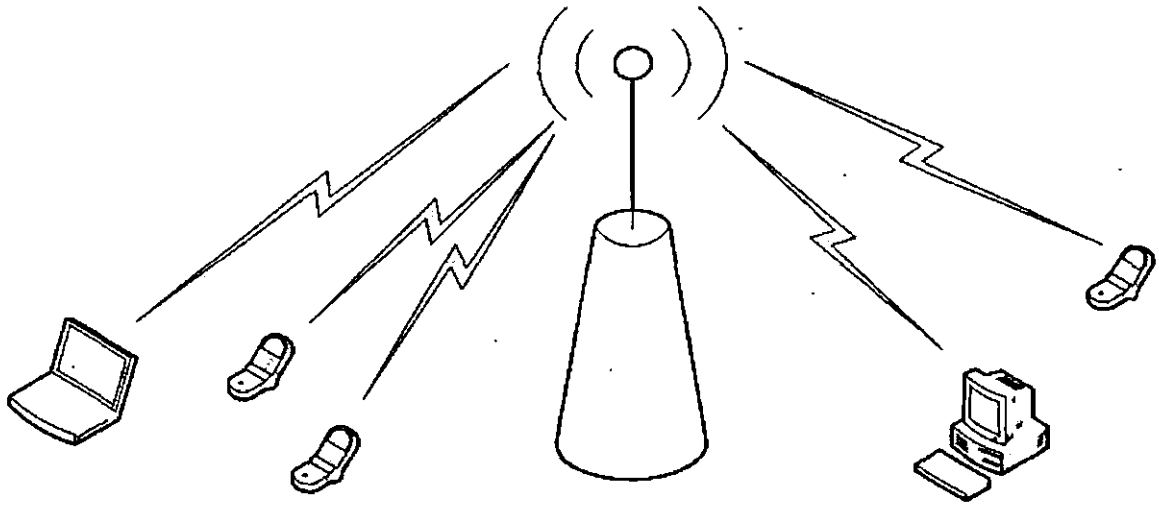


Figure1.1 Structured Wireless Networks

Infrastructured based network consist of a mechanism with fixed and wired media gateways. A mobile host or mobile user communicates with a bridge in the network which is called BS within its communication radius. The mobile user can move geographically while it can continue communication. When it goes out of desired range of one base station, it establishes connection with new base station and communicates through it. This mechanism is called a handoff mechanism. In this approach the base stations are fixed at some planed place.

1.2.3.2 Infrastructure less.

Ad-Hoc networks are also another important type of WLAN which are Infrastructure less. Ad-Hoc networks are the theme of this esteem, so our discussion in this section will focus on Ad-Hoc networks.

Ad-Hoc Network mobile nodes communicate with each other wirelessly as shown in Figure [1.2], and there is no base station or any fixed infrastructure in such networks.

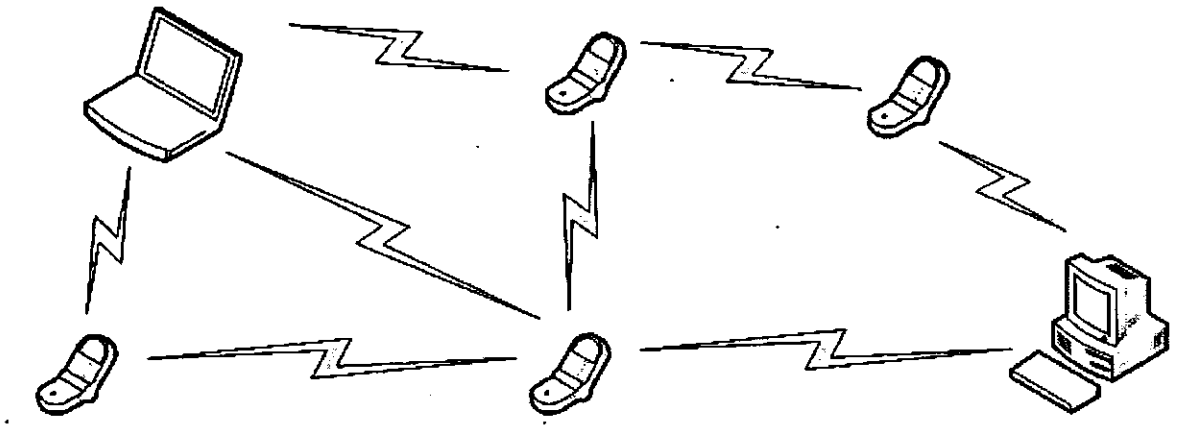


Fig 1.2 Structures less Wireless Networks

In an Ad-Hoc network mobile units only communicate peer to peer (P2P) mode. All this is achieved by using Independent Basic Services Set (IBSS); every mobile node can communicate freely without any permission from any central system.

Without the involvement of central access points an Ad-Hoc network wireless devices can communicate and discover each other directly. Using wireless as a medium of communication network is shaped by two or more computers to connect each other.

1.3 Mobile Ad-Hoc Networks

The dictionary meanings of the word "Ad-Hoc" is "specific", "for one specific case", for particular application's special network. A mobile Ad-Hoc network (MANET) is the network of mobile routers connected by wireless links; it is a self configuring network. Routers are allowed to organize themselves arbitrarily and to move randomly; hence the rapid and unpredictable changes occur in network's wireless topology.

1.3.1 History of MANETs

Ad-Hoc networks whole life cycle can be categorized in the 1st, 2nd and 3rd generation of Ad-Hoc network systems. Presently used Ad-Hoc networks systems are considered the 3rd generation.

This 1st generation period was 1972. At that time this kind of networks were called PRNET (Packet Radio Networks). With the colligation of ALOHA (Areal location of dangerous Atmospheres) and CSMA (Carrier Sense Medium Access), the PRNET were used to give different networking capabilities in a combat environment for distance-vector routing and for medium access control. All this work was on a trial basis at that time.

In 1980 the 2nd generation of Ad-Hoc networks came out, in this period Ad-Hoc networks were enhanced, its application as a part of SURAN (Survivable Adaptive Radio Networks) program was done. The packet-switched networks were provided to mobile battlefield without infrastructure.

The commercial concept of Ad-Hoc networks came in 1990 with the arrival of notebook computers and other viable communication equipment. At the same time several research conferences proposed the idea for the collection of mobile nodes.

The subcommittee of IEEE 802.11[5] adopts the phrase "Ad-Hoc networks" and in the other areas of application Ad-Hoc networks deployment possibility work had started by this subcommittee.

At the same time advancement in previously built Ad-Hoc networks was going on. GloMo and the NTDR was the result of all previous efforts. In handheld devices GloMo provide an office environment with Ethernet-type multimedia connectivity anywhere and anytime.

After some time a medium access protocol that was based on tolerated hidden terminals and collision avoidance was standardized by the IEEE 802.11 subcommittee. This standard was made usable for building mobile Ad-Hoc networks prototypes out of notebooks and 802.11 PCMCIA cards. Ad-Hoc networking was also benefited and addressed by the Bluetooth and HYPERLAN standards.

The current research focus is to standardize the various existing schemes for various network controls in single framework, for all the future applications using Ad-Hoc networks as a networking technology it could be taken as standard.

Wireless devices are getting cheaper, smaller, and more sophisticated. With the passage of time these devices become more omnipresent, the companies are looking to keep these devices connected for inexpensive ways.

1.3.2 Properties of MANET

There are many properties of MANETs but the most distinguishing are listed below:

- No Infrastructure
- Nodes have freedom of Mobility
- All Communicate is through wireless links
- Dynamic Topology
- Nodes can works as transceiver and router
- Communicate through Routing Protocols

1.3.3 Usage Areas of MANETs

- Search and Rescue Operations
- Policing and fire Fighting
- Personal Area Networks
- Meeting Rooms
- Sports Stadiums
- On Battle Fields

1.3.4 Merits and De-Merits of MANETs

Merits

- Cost Effective
- Quick and Easy Deployment
- Freedom of Mobility
- Self Learning

De-Merits

- Low Battery Power
- Less Processing because of Battery power
- Low range of transmission and reception
- Error rate is high

1.4 Problem Statement

At present there is lack of such performance evaluation in the network context which will consider the network performance.

Quality of Service is the demands of different MANET secure protocols, so security with QoS is desirable. Heart component of any communication network is an efficient QoS which satisfies the QoS requirement. There are following points which describe current problem that need to be addressed.

1) Most authors concentrate on security aspects of MANET's and they ignore the importance of the role the network plays in performance of MANET's.
2) Performance of secure routing protocols for MANET' to provide a QoS is needed to be explored.
3) Performance analysis of secure routing protocols using network performance metrics.
4) Performance evaluation of secure routing protocol under Manhattan Grid and Random Way Point Mobility models need to be explored further in the framework of network performance metrics.

1.5 Contribution of this Dissertation

The main contributions of our thesis are,

1) We made a detailed analysis of existing secure protocols of MANET's and setup a simulation architecture for SAODV and Ariadne to evaluate the performance, efficiency, and reliability.

2) This implementation characterizes and classifies the protocols according to Performance metrics such like Delay, Jitter, Throughput, Route Acquisition Time, Routing overhead, Hop Count etc.
3) We also made analysis, the performance of routing protocols under the Manhattan Grid and Random Way Point Mobility model.
4) Performance and analysis results are shown by simulation through Network Simulator 2 (NS-2), which have given significant reliable results as compare to other simulation tools.

1.6 Dissertation Organization

In Chapter next from this, we will give a description on the MANET's protocols in detail and especially their types, advantages and disadvantages concerned with those protocols. Chapter 3 will focus on concerned protocols and the work in this area which has already been done. Chapter 4 will present description of NS simulator, its operating system, benefits and limitations. In chapter 5, we will present the architecture, topology, implementation scenarios and implementation of our protocols and also performance parameters. In chapter 6, we will analyze our results under the performance parameters. Ultimately in Chapter 7, conclusion and future work is going to be discussed.

Chapter 2

Routing Protocols

In the previous chapter we gave a brief introduction of Wireless networks and later on we discussed an important type of Wireless Networks i.e. MANETs its history and applications. In this chapter we will discuss Routing Protocols of MANETs. Before going into the MANETs routing protocols let us see what are protocols and their types?

2.1 Protocols

In MANETs as the communication is being done so there should be a language which all the participants can understand. What is that language is called a protocol. In specific we can define as "*A communication protocol is the set of regulations, or a contract, that determines the format and transmission of data*".

Many Protocols are there which are used for communication purpose most of the time the user cannot understand the working of a protocol. A simple user cannot understand the protocol that is why classification of protocols is very important to differentiate between the protocols according to their working rules. As we are working on MANETs which use routing protocols to update their routing tables so we will mainly discuss the classification of routing protocols which are used in the context of MANETs. Most important classification of routing protocols for MANETs is as under:

- Proactive Protocol
- Reactive Protocol
- Distance Vector Routing
- Link State Routing
- Source Routing Protocol

2.1.1 Proactive Protocols

In Proactive protocols, up to date routing table is always maintained through periodic updates which run after some specific time period and all the entries of routing table are updated accordingly. Best suited when the mobility of nodes is low, network size is small and there is reasonable load on the networks. Well known MANETs protocols are

- DSDV (Destination Sequence Distance Vector) routing protocol [6],

- OLSR (Optimized Link State Routing Protocol) [7]

The major drawbacks of Proactive protocols are as under:

- High processing required at nodes
- Difficult to run updates periodically in heavy loads
- Routing overhead is high

2.1.2 Reactive Routing Protocol

In case of Reactive routing protocols the routes are determined only when the source demands for that is why these protocols are often known as on-demand routing protocols. These are perfect when the topology of networks is rapidly changing and the mobility of nodes is high. Some well known reactive routing protocols are as under:

- SAODV (Secure Ad-Hoc On-demand Distance Vector)
- Ariadne

The major drawbacks of Reactive protocols that Delay increased if topology has changed rapidly

2.1.3 Distance Vector Routing

In distance-vector routing, the every node only knows its neighbours so routing table of each node has only the information about all his neighbours beyond that all the information about other nodes is hidden from particular node. Whenever route is required the request is broadcasted to the neighbours if rout is found at neighbours then the neighbour will reply the rout request if route is not found the intermediate node will broadcast the request to its neighbours and the process will continue till the destination node is found. All this process is very easy and less time consuming, requires less storage space on nodes, less processing and efficient route computation.

But the major problems with distance-vector routing are the creation of routing loop due to broadcast feature of distance-vector routing. Routing loops can be avoided by using Maximum hop-count, Split by horizon, Poisoning of route, Hold down timer schemes.

2.1.4 Link State Routing

In link state routing a node maintains routing table in such a way that there is always complete route information from source node to destination node. This is not in the case of distance-vector routing. Although the process to get route is quick but the major drawback with link state is the large storage capacity which is required to maintain large routing tables and due to the large size of the routing table at each node the extensive processing is required, to fulfil processing requirement it demand more battery power at each node. Routing loops are another problematic area of link state routing which is tackled by the use of Dijkstra algorithm which have strong feature to avoid loops in the network.

2.1.5 Source Routing

In source routing the source node put all information in each packet header which is required to deliver the packet. The major advantage of source routing is that no routing tables required to be maintained at each node. It means that less processing and less battery is consumed but the overall packet delay increases significantly due to large overhead associated with each packet. One more plus point of source routing is that it is loop free.

2.2 Routing protocols of Mobile Ad-Hoc Networks

In literature from start till date a large number of protocols for MANET's have been developed. With the hope that more and more protocol will be there as dedicated work is done to develop new protocols. There are many routing protocols of MANETs. But we picked some of them to be in list with little description because detailed description is not in the scope of this project so we will only explain some well known protocols.

2.2.1 Temporally-Ordered Routing Algorithm (TORA)

The Temporally Ordered Routing Algorithm (TORA) can work in environment where mobility is highly dynamic. TORA's algorithm concept is link reversal which is a highly adaptive loop-free distributed routing. It is categorized in source-initiated and provides multiple routes for any desired source/destination pair. Localization of control message is the key design of TORA which adopts topological changes very quickly.

2.2.2 Authenticated Routing for Ad-Hoc Networks (ARAN)

ARAN main feature is to find and protect from the misbehaving nodes from third party and peers environment. To do so ARAN introduces a minimal security policy to integrate, authenticate and non-repudiation of messages in an Ad-Hoc environment. While using ARAN one has to pay less performance cost to achieve high security.

2.2.3 Secure Routing Protocol (SRP)

SRP is categorized as an on-demand protocol, which enables SRP to be very dynamic, self-starting, multi hop routing to be established when a source and destination want to communicate. In SRP all routing packets are of fixed size. The key feature of SRP is less consumption of energy at nodes because of less overhead.

2.2.4 Secure Efficient Ad-Hoc Distance Vector (SEAD)

SEAD is an extended version of DSDV. In order to maintain less CPU processing and to be suitable for Denial of Service from attackers some efficient one-way has been implemented in SEAD rather than asymmetric cryptographic operation in DSDV. SEAD is robust against attackers in all scenarios where it has been tested so for.

2.2.5 Zone Routing Protocol (ZRP)

ZRP is not a separate protocol it only combines the advantages of both pro-active and reactive into a hybrid scheme, taking advantage of pro-active discovery within a node's local neighborhood, and using a reactive protocol for communication between these neighborhoods. In a MANET, it can safely be assumed that the most communication takes place between nodes close to each other. Changes in the topology are most important in the vicinity of a node, the addition or the removal of a node on the other side of the network has only limited impact on the local neighborhoods.

Chapter 3

Protocols and Literature Review

Our research is focused on SAODV and Ariadne, therefore, in this segment we will chat concerning these protocols in detail.

3.1 Proposed Protocols for Project

We are going to evaluate following two important secure protocols for MANET's

1 SAODV (Secure Ad-Hoc On-Demand Distance Vector): routing protocol.

2 Ariadne: A secure routing protocol for mobile Ad-Hoc networks.

3.1.1 SAODV (Secure Ad-Hoc On-demand Distance Vector Routing)

The name shows that SAODV is a secure routing protocol which uses hash chains and digital signatures to secure AODV packets. SAODV is the security extension of AODV [8]. In SAODV cryptographic signatures are used for the fields that cannot be muted to authenticate them. At each route discovery one way hash chain is formed for the security purpose. That's why a strong key management method is also required which can obtain and prove the key. There are many message format fields in the SAODV but basically following fields are added in the AODV fields which make the SAODV more secure, as shown in [Fig 3.1]

- Hash function: used for identification of one way hash function
- Max Hop Count: allowed number of hopes a packet can traverse.
- Top hash: top hash is calculated with the help of above two fields when a hash function is applied to max hop count times with a random values the output is called top hash
- Hash: a random number

Type	Length	Hash Function	Max Hop Count
Top Hash			
Signature			
Hash			

Figure: 3.1. SAODV Protocol Header

When in AODV a node transmit a route reply the following procedure is followed

1. From IP header the TTL field is put equivalent to Max hop count from SAODV packet
2. A random number is generated from hash and sets it equal to hash field.
3. Then hash function is applied by the randomly generated number, how many times to apply random number are determined from the Max hop count.
4. At the end all fields except hop count and hash field from AODV and SAODV respectively are digitally signed by each node.
5. Each intermediate node on request or reply is required to prove veracity of message using digital signatures.
6. Digital signatures are verified through the reverse engineering procure.
7. Before the packet is preceded from intermediate nodes to others the new one way hash is applied again. Which again follow all steps 1 through step 7

The major advantage while using the SAODV is that it also digitally signs the route error messages (RERR). For example if the route between the nodes shown as C and D nodes in the figure [3.2] does not exist the node C will generate RERR and will also digitally sign it. RERR is very strong feature of SAODV because on RERR basics the decision could be made that whether or not to put some route in routing table.

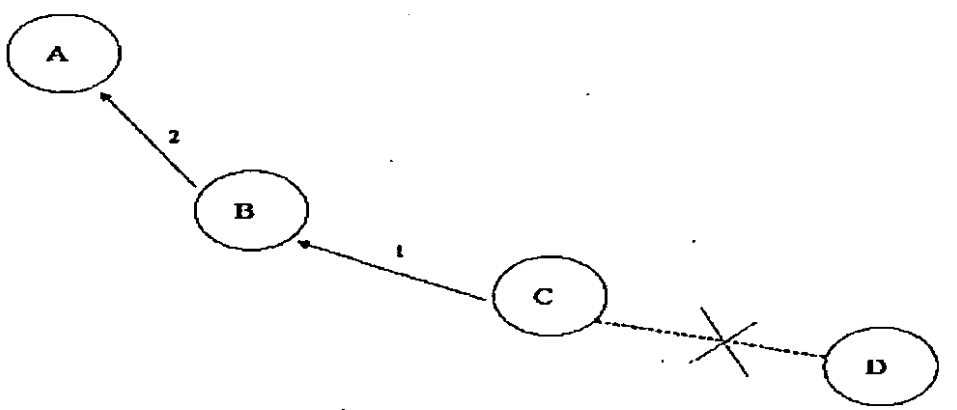


Figure 3.2 Route maintenance in the SAODV protocol.

3.1.2 Ariadne

Ariadne is another secure on demand routing protocol used for Ad-Hoc networks. Ariadne is based on DSR. SEAD and Ariadne are developed by the same author the key difference between SEAD and Ariadne is that SEAD is implemented through hop by hop security mechanism while Ariadne is implemented through end to end security mechanism. In Ariadne two communicating nodes establish a collective secret key and with them use MAC to authenticate messages between the end points [9].

Synchronization between the communicating nodes is compulsory if you are going to use the Ariadne because Ariadne uses TESLA protocol to authenticate the messages. Before going into more detail we would akin to give a brief description of TESLA.

The source node generates a one way key chain. After that it required to establish a procedure that how to disclose the key of that chain whenever the destination will require the key [10]. In the route request following parameters are included.

- Source Address
- Destination Address
- Time Interval (TESLA). Suitable time interval who key is not disclosed yet
- An ID to present route discovery
- A hash Chain
- Empty Node List
- Empty MAC List

If somehow any packet is there with invalid time interval then that packet will be discarded. If the time is valid then that specific node then that node input his address to node list the node the generates the new hash chain and replace it with the already existed one and add one with its address and puts the MAC of all the message to MAC list. The note able thing is that TESLA key with the combination of time interval helps to calculate the MAC. After all the above procedure the node broadcast the requests to neighboring nodes. The destination

will generate the reply only if it finds that request is valid. A valid request is that who's key is not disclosed from the given time interval.

Empty key list and Target MAC are tagged additional in reply with the request fields. The key field is filled with key which destination has to share with source. MAC is filled with former calculated MAC in the route reply. Then the route reply is sent back to source through reverse of the route. Each intermediate node discloses the key after some pre specified time interval if it finds ok the send back to its previous node. When the originator receives reply it checks for both that is MAC list and Key list it then validate it and if it's ok then the communication may be proceeded.

Route maintenance is also securely implemented in Ariadne. If a link brakes in the network the some neighbor generates the route error message. TESLA is involved when a node generates an error message to authenticate the message. Every involved node in the transmission is capable to authenticate the error message [12]. One thing to note down is that authentication can happen only when the originator discloses the key.

3.2 Literature Review

While discussing the security of Ad-Hoc routing protocols in literature most of the times the authors have stated that all the hops in the network are friendly, which is not true at all when ever a network is put into commercial use. Till there are many network aspects in the Ad-Hoc protocols need to be explored. The lack of effort in networking contexts for ah-hoc network despite of security has motivated many people to excel the work in this domain. Few of the efforts are as under.

3.2.1 LSR (Link State routing) protocol developed by Perlman [13] is very strong protocol if the consideration is made in the light of security. The security of LSR is very tight it also showed robustness but the only problem we see in the protocol is that it demands for high overhead for the implementation of public key encryption. This is not acceptable in real world.

3.2.2 The two authors Hass and Zhou [12] has done a good effort to make efficient secure routing while using key management and they concluded that " Nodes should care for routing information as they care for traffic data". This is the result their first section for security in their paper. In the second section that is dedicated for the improvement of QOS parameters for Ad-Hoc networks by using network misbehavior detection scheme. . All the work reaches to two main problems: First, there is no surety of consistency and accuracy of the routing messages. Second, it's hard to differentiate between nodes that is if they are misbehaving, transmission failed, or other type of failures

3.2.3 ARAN (Authenticated Routing for Ad-Hoc Networks) routing protocol has been developed by Dahill also reveals around the security matters. ARAN uses a server called server for verification that uses trusted certificate. A node in ARAN that needs to send a route discovery or to receive or send a route reply message the node requires signing it first. The procedure adopted by the author required very power full processing which cause the high power consumption which is very considerable parameter of Ad-Hoc network because energy is still the problem for Ad-Hoc nodes. One more lack in this paper is that signing on each node increases the size of the message to some extent which is not acceptable in the sense of overhead. Finally it's difficult to reply the attacks because time synchronization is required.

3.2.4 SRP (secure remote password) protocol proposed by Papadimitratos and Haas [13] can have many implementations in the pasture of Ad-Hoc networks. For example, in DSR and Interzone Routing Protocol. Source and destination must have some strong relationship in the context of security which is required if you are going to use SPR. We have analyzed that any nasty node can build error message with other nose as a source.

3.2.5 SAODV secure version of AODV developed by Zapata and Asokan [12] saying it to be a suitable secure clarification for Ad-Hoc networks. They implement by hash chains and signature for integrity and authentication respectively for routing message. They talk about a Key Management scheme for authentication purposes. The Public Key Cryptography is the

drawback of SAODV as Public Key Cryptography is a complicated process and it demands for some good processor to process the mechanism but if the processor is not of some good specification then it will slow down the whole mechanism.

3.2.6 In SEAD [14] the two authors Hu Johnson and Perring has used hash chain with combination of DSDV-SQ to make a check on the validity of hop count and sequence number. On a particular time each node contains his own hash chain. As in SAODV hash chain can be separated into two portions fundamentals in segments are used to secure hop count. Once hash chain is generated its size can be determined. To compute a new hash chain all fundamentals are required to be considered. We can use SEAD wherever the suitable authentication and key distribution is available. To find such scheme is a difficult task. Ariadne which is based on DSR [6] uses TESLA for key validation purpose is also proposed by the same author.

Beside of all above efforts the authors David B. Johnson, David A. Maltz [15] has done wide work on the Quality Of Service (QOS) based performance evaluation for MANET's but most of their work is for non secure routing protocols for MANET's. The other two authors L.S.E. Dennis, Ex Xianhe has worked for some secure routing protocols for MANET's. But all their work is related to security parameters not on network parameters. From their conclusion is that that Ariadne is more secure than SAODV. The above work has motivated us to make analysis of some secure routing protocols (SAODV and Ariadne) in the network contexts rather than security aspects.

Chapter 4

Network Simulator 2: An Implementation Tool

We have followed up our simulation, to examine MANET secure routing protocols in two mobility models applying the different performance matrices. We use NS-2 (version 2.27) [18] simulator for this work.

4.1 NS-2 Simulator

NS-2 is a simulator tool used to simulate different network protocols. Using object oriented technique. NS is implemented, written in C++, at the front end OTcl parser is used. The simulator contains a chain of class hierarchy in C++ and a similar chain of class hierarchy is followed in the OTcl parser. From the user prospective two hierarchies have a close relation with each other, in interpret and compile hierarchy one to one correspondence is there. The root of hierarchy is Tcl object. As for as end user is concerned the end user have to create new objects in the predictor; the new objects are surrounded within the predictor, which are in compiled hierarchy are mirror by relevant object.

To work for two different tasks, NS has two languages first to deal with simulation of protocols it required a system language to work with bytes, packet headers and after powerful processing these are put into algorithm to run over bulky data. Run time for these tasks is more significant than turnaround time. Second in the network simulation scenarios require quick configuration of some parameters in these situations iteration time is more considerable than run time. So NS provides the structure in which we can run simulations for real time networks for analysis of different scenarios and different parameters.

Some people are still confused that why NS uses two language. The answer is very clear simply said "OTcl is used only one time to set different parameters like delay, queuing etc but if you want some special to do rather than existing parameters that are supported by OTcl then you will require the use of C++ which will permit you to create new objects". That's why two languages are used by NS. There is a large amount of classes defined in ns–2. Out of which six classes are more frequently used in ns:

1. Tcl
2. TclObject

3. TclClass
4. TclCommand
5. EmbeddedTcl
6. InstVar

Figure 4.1 describes the simplified view from user perspective.

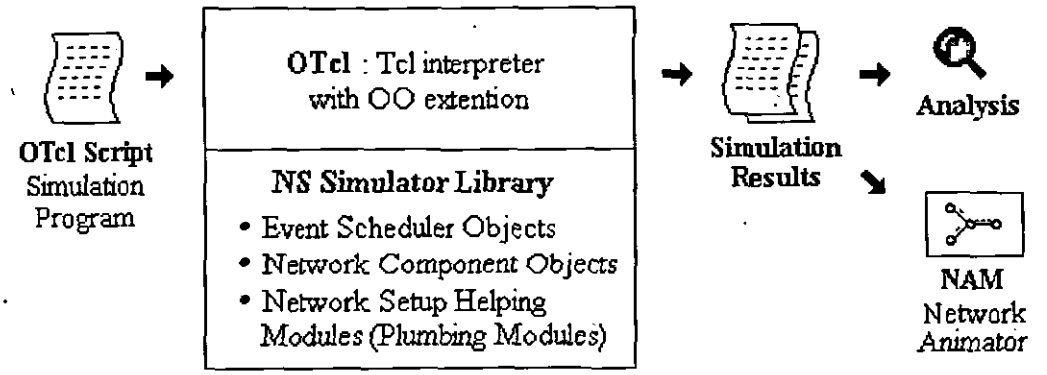


Figure 4.1: Simplified view of NS-2 for End User

4.1.1 TCL interpreter:

Ns-2 uses two languages which are entirely different from each other to make the two languages understandable for each other some sort of parser is required which could make possible the communication of the two languages. TCL interpreter is used for this purpose TclCL is used between the communication of OTcl and C++. Toolkit Command scripts are designed to solve the different topologies. The objects in C++ that do not need to be controlled in a simulation or internally used by another object do not need to be linked to OTcl. Likewise, an object (not in the data path) can be entirely implemented in OTcl. Figure [4.2] shows an object hierarchy example in C++ and OTcl. One thing to note in the figure is that for C++ objects that have an OTcl linkage forming a hierarchy, there is a matching OTcl object hierarchy very similar to that of C++.

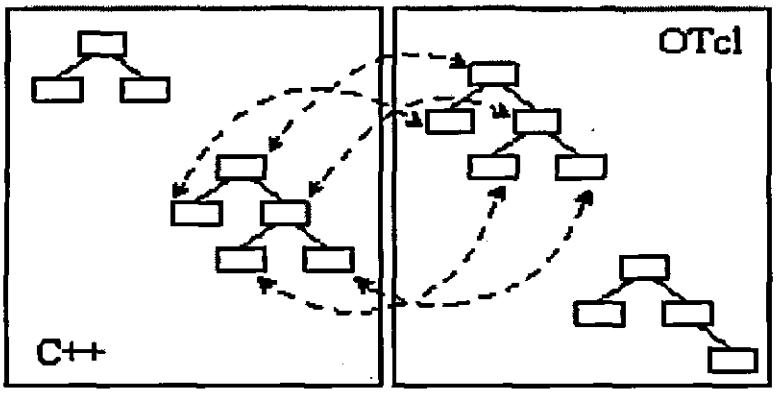


Figure 4.2: C++ and OTcl: The Duality

4.1.2 Network Animator (NAM): Visualization Tool

It is used as graphical visualization of different network scenarios which are created by user. It provides visual image of packet flows with different colors, node movements, packet queues, link between nodes, wireless nodes transmission range, drop packets and etc. NAM is a tool to visualize the imitations and traces for real world packets which is based on Tcl/TK. The theme to build NAM was to take the imitation and traces so that these results could be used in different visualization situations. The NAM when runs generate a file which could be used later if required. The advantage of NAM is that the generated file is of some significant size for some large simulations.

Trace file is required before one can NAM to visualize the simulations. More often trace file is produced by NS however many application can generate NAM trace file. When one run the NAM file one can see the topology design flow of packets in different direction depending upon the topology packets which are dropped due to some reasons can also be visualized from NAM visualization. All this can be seen in a separate window.

4.1.3 Trace Data Analyzers

There are many ways to analyze trace file from simulation. These are following four ways that are mostly used to analyze the trace file.

1) XGraph

It is an application including:

- *Interactive plotting and graphing*
- *Animation and derivatives*

TCL scripts are written to extract data from XGraphs in NS-2. After extraction of data one can see the information in the form of graphs from the trace file produced by NS.

2) *TraceGraph*

It's a windows base tracing. The supported formats in TraceGraph are as under:

- *Wired*
- *Satellite*
- *Wireless (old and new trace)*

3) *Awk scripts with Microsoft word*

It is shell scripting set of rules to extract data from trace file according to the requirement of user to arrange that extracted data. Then Microsoft Excel can be used to plot graph according to data. It can support any trace format.

4) *User built–in code*

It is a procedure where a user builds its own code according to the requirements to extract and compute data and show in graphical format. This code can be developed in any languages like c++ and java. It can support any trace format.

4.2 Characteristics of NS-2

NS-2 implements have following shining features

1) It supports Router queue Management Techniques such like RED, Droptail, CBQ,

2) It can provide a Multicasting and Routing based simulation.

3) Simulation of different wireless networks such like Terrestrial (cellular, Ad-Hoc, GPRS, WLAN and BLUETOOTH), satellite and IEEE 802.11.

4) It can also incorporate Transport Agents UDP/TCP and traffic sources Behavior www, CBR, VBR, telnet, FTP and Ping.

5) It provides functionality of Packets tracing on all specified links.

4.3 Operating Systems for NS-2

Following operating systems can be used for NS-2 simulations:

- UNIX
- Linux
- Microsoft Windows (Cygwing emulator is required)

4.4 Potential Benefits

1) It is open source and freely available on web.
2) It supports lot of protocols at different layers that facilitate the developer to simulate different network scenario without installing any other patches.
3) It can be configured very easily.
4) It takes short simulation time as compare to other simulators.
5) Its results are very accurate and acknowledge by researcher all over the world.
6) It is more scalable than any other simulators.

4.5 Disadvantages

1) Due to lack of standard documents it's very difficult for new user to learn it.
2) Ns-2 requires lot of memory space, so there is lots of problem arises when simulating large network and as the number of nodes are increasing processing time also increasing.
3) We have significant self-belief in ns, but ns are not a polished and finished product,
4) There are many bugs in the NS–2 software which are still being discovered and corrected.
5) Users which use NS-2 are responsible for verifying for themselves that their simulations are not invalidating by bugs.
6) Lot of Patience is required to debug NS-2 source code when needed.
7) For More complex simulations NS-2 source code may require modifications.
8) Debugging process of NS-2 is complicated so user required a quick knowledge of C++ and Otcl.

Chapter 5

Implementation

In this chapter, we describe the methodology that we adopted to achieve the objective of this project. This chapter describes the implementation design, simulation topology, mobility models, traffic model, performance metrics and other simulation parameters. It also describes the criteria developed for the evaluation of selected routing protocols.

5.1 Simulation Architecture (Block Diagram)

The simulation procedure in NS-2 can be shown as Figure 5.1. The performances of the secure routing protocol are studied with this simulation tools. Upon receiving the input file of traffic pattern and mobility pattern a simulation is initiated.

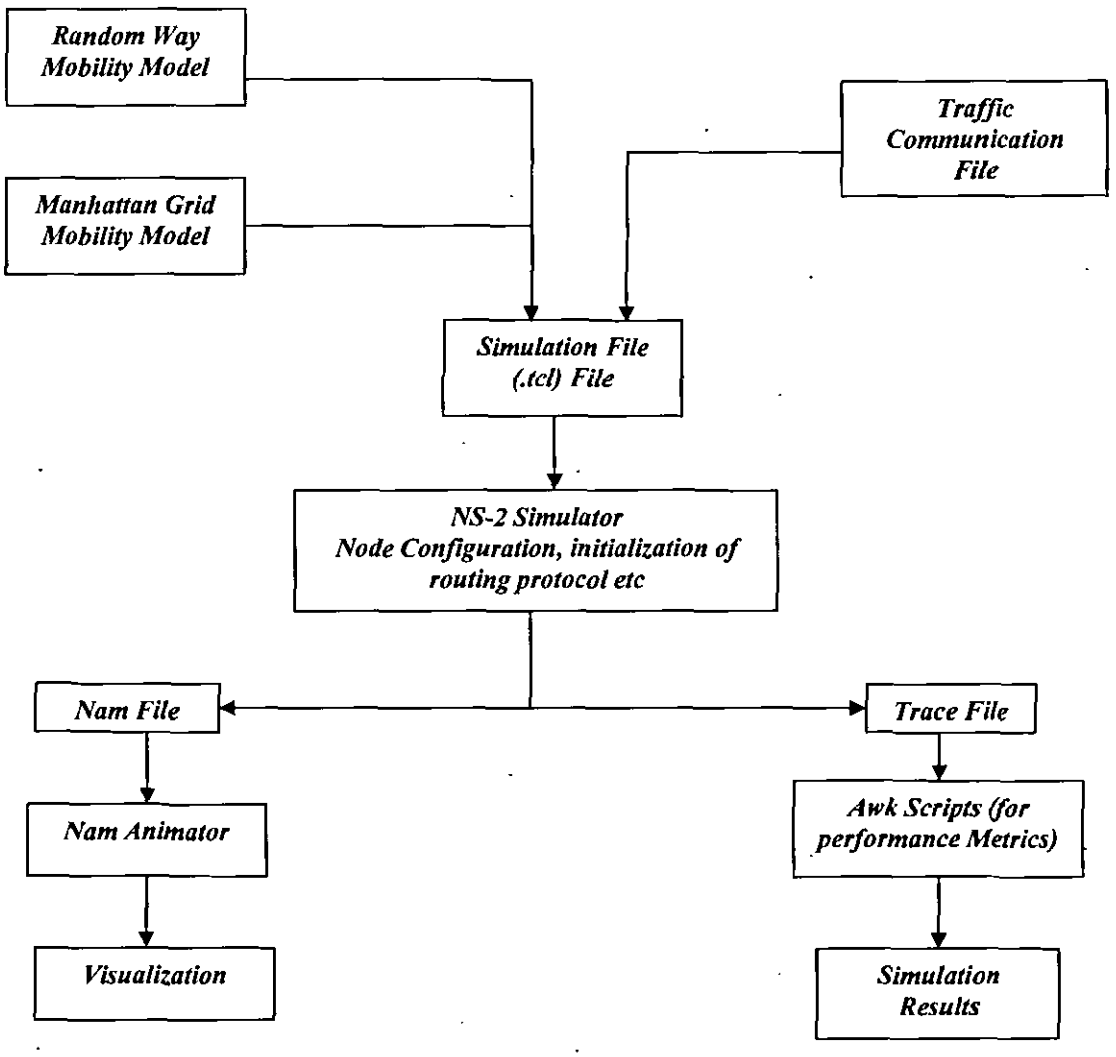


Figure 5.1 Block diagram of Scenario Implementation

After successful completion of simulation, there are two files produced one is NAM file which is used for the visualization process and second is trace file. Trace files containing the status of the nodes and types of packets (control and data packets) and on the basis of these trace files, delay, routing overhead and other performance matrices are calculated.

5.2 Scenario and Topology

In this section we are going to explain simulation setup. 10 to 50 nodes are deployed at an area of 1500 x 1500 pixels. Six communication channels are established among the nodes. Since we are talking about MANETs, intermediate nodes will play the role of routers. Range of each of the node is 100 meter over a wireless link.

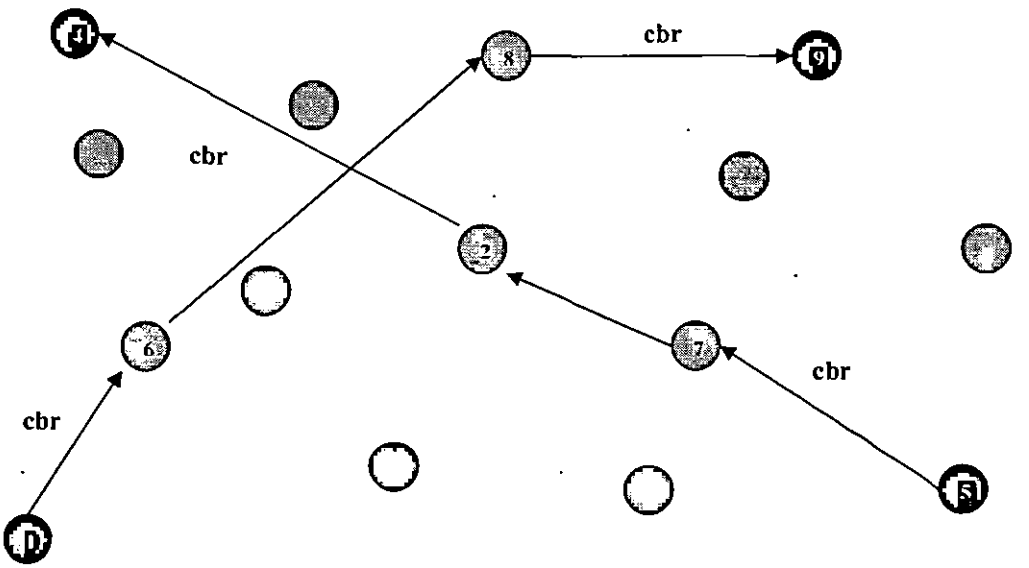


Figure 5.2: Simulation Scenario

20 mobile nodes are shown in figure 5.3 with the transmission range of 100 meter. Nodes are moving with the constant speed of 10 m/s and the experiment is carried out for 100 seconds.

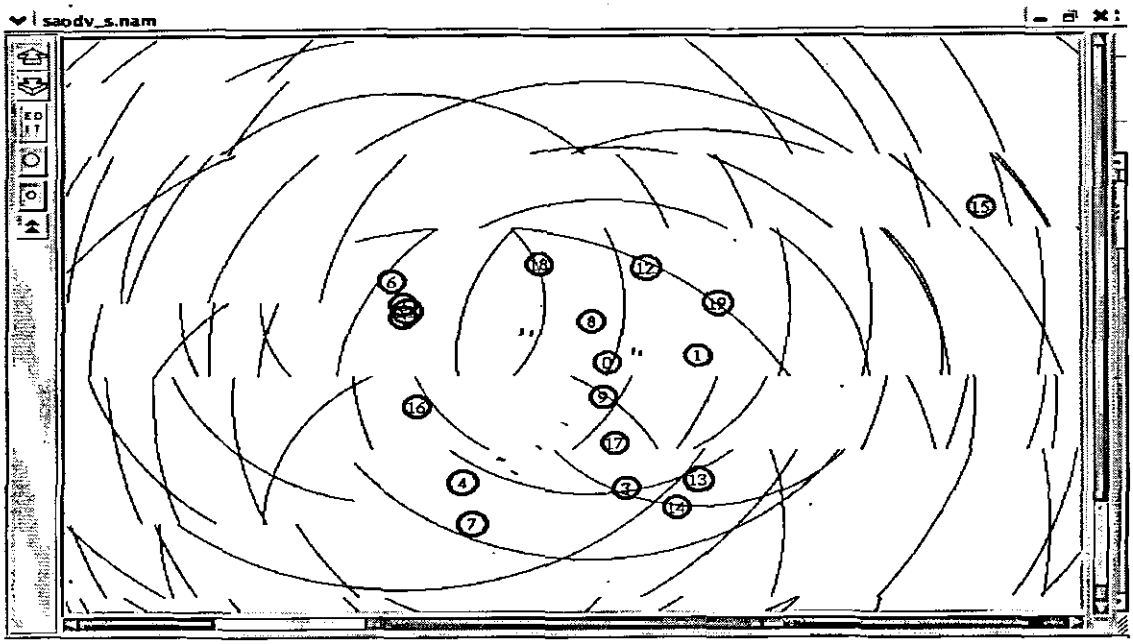


Figure 5.3: NS-2 Simulation Environment

5.3 Layered and Simulation Parameters

To broad measure of these secure routing protocols various context are observed and considered. In the following section different layered and simulation parameter are discussed.

5.3.1 TCP/IP Layered Parameters

Every layer of TCP/IP model plays its role in communication and involved different types of protocols. To clear our simulation setup now we are going to define different types of protocols that we deploy on different layers of TCP/IP model.

```
set val(chan)    Channel/WirelessChannel      ;#Channel Type
set val(prop)    Propagation/TwoRayGround     ;# radio-propagation model
set val(netif)   Phy/WirelessPhy              ;# network interface type
set val(mac)     Mac/802_11                   ;# MAC type
set val(ifq)     Queue/DropTail/PriQueue      ;# interface queue type
set val(ll)      LL                           ;# link layer type
set val(ant)     Antenna/OmniAntenna          ;# antenna model
set val(rp)      AODVUU                       ;# routing protocol
```

Physical layer: Wireless physical layer, TwoRayGround propagation model and omni-directional antenna specifications are used at Physical layer.

Data Link layer: it configured with specification of IEEE 802.11 wireless.

Network Layer: Internet protocol (IP), SAODV and Ariadne are used as routed and routing protocol at network layer.

Transport Layer: UDP is used as a transport layer protocol.

Application layer (Host Layer): Constant Bit Rate (CBR) traffic is used at application layer.

The following code shows the node configuration of all nodes in the simulation.

```
$ns_ node-config -adhocRouting $val(rp) \
                 -llType $val(ll) \
                 -macType $val(mac) \
                 -ifqType $val(ifq) \
                 -ifqLen $val(ifqlen) \
                 -antType $val(ant) \
                 -propType $val(prop) \
                 -phyType $val(netif) \
                 -topoInstance $topo \
                 -agentTrace OFF \
                 -routerTrace ON \
                 -macTrace ON \
                 -movementTrace OFF \
                 -channel $chan_1_
```

5.3.2 Simulation Parameters

Table 5.1 describes simulation parameter for carry simulation in ns-2.

Parameters Name	Value
Radio-propagation model	Two Ray Ground
Channel type	Wireless Channel
MAC type	802.11
Network interface type	Wireless Physical Layer
Interface queue type	Drop Tail/Priority Queue
Routing Protocols	SAODV and Ariadne
Antenna model	Omni-directional
Traffic Type	Constant Bit Rate
Packet size	100 Bytes

Max Packets	10000
X dimension of the Topography	1600
Y dimension of the Topography	1600
Queue Length	50
Simulation time	100 Sec
Transmission Range	100 m

Table 5.1 Simulation Parameters

5.4 Routing Protocols Implementation

This project is intended to carry out the performance evaluation of two known secure routing protocols i.e. Ariadne and SAODV.

5.4.1 Implementation of SAODV

There is an implementation of SAODV done by people at Upsala University (UU) [5]. The environment used to implement the SAODV is Network Simulator 2 (NS-2) and programming language used was C. It has been used extensively in the research projects of networks and its worth and performance improving with the passage of time. The underlying class hierarchy of the NS-2 has been built in C which provides the robustness in the execution of simulations and also provides a reliable base for the simulations made in a relatively unstable language like Tcl or OTcl. The UU implementation covers the all changes that made in the standard issued by the Internet Engineering Task Force (IETF) in latest draft [5]. All the amendments are targeted to achieve better performance results with the respect of security as the original version of SAODV. This implementation covers Cryptography, Message Formats, Hash and Signature Functions.

5.4.2 Implementation of Ariadne

To perform evaluation for our project, we have used the implementation of Ariadne by Monarch Project people [19]. The implementation makes use of TESLA as a broadcast authentication protocol for the efficient key distribution and key management. The implementation demands the use of earlier version of NS-2 i.e. ns-allinone2.1b4a along with the CMU's extensions to the network simulator i.e. cmu-extendedns. The protocol has been

implemented by modifying the original DSR implementation files and doesn't exist as an independent protocol. Using this implementation for simulations, requires having three different files i.e. a movement model file, a communication model file and a protocol specific file.

5.5 Mobility Model

NS-2 requires three different files i.e. a movement model file, a communication model file and a protocol specific file for the protocol to be used for implementation. We are considering only two movement models in our simulation to emulate the real life scenario.

5.5.1 Random Waypoint Mobility Model

Pause time, minimum speed and maximum speed are the main parameters of this model. Each mobile node in this model starts its movement from a position that is randomly selected and remains idle for the duration of the specified pause time. A mobile node randomly selected speed and destination whenever this pause time ends. The speed is selected by a node from ranges of specified minimum and maximum speed. After that mobile nodes will move towards its intended destination and after reaching there, the process of selection will start again by reset all previous values.

5.5.2 Manhattan Grid Mobility Model

It models a city section with streets and each street crossing each other perpendicularly. Each mobile node on these streets can move only horizontally or vertically. Each mobile node starts its movement from a randomly selected position on one of the point and move towards randomly selected destination. A mobile node can move according to defined speed range and after reaching its intended destination, it remains idle for some time equivalently to pause time and then start the process again.

5.6 Traffic Model

The communication which takes place between two nodes is mainly follow the constant data rate traffic. To emulate similar loads, constant bit rate (CBR) traffic used as the application

traffic running over a UDP connection. The CBR traffic generation TCL script available in NS-2 was modified to generate a packet. The following code shows a CBR communication between two nodes under different parameters of CBR traffic.

```
set udp_(0) [new Agent/UDP]
$ns_ attach-agent $node_(1) $udp_(0)
set null_(0) [new Agent/Null]
$ns_ attach-agent $node_(2) $null_(0)
set cbr_(0) [new Application/Traffic/CBR]
$cbr_(0) set packetSize_ 100
$cbr_(0) set interval_ 0.0050000000000000001
$cbr_(0) set random_ 1
$cbr_(0) set maxpkts_ 10000
$cbr_(0) attach-agent $udp_(0)
$ns_ connect $udp_(0) $null_(0)
$ns_ at 0.71023302185825687 "$cbr_(0) start"
```

Above code shows that a communication takes place between Node 1 and Node 2. Constant bit rate traffic is attached over the user datagram protocol on node 1. According to code a packet size 100 bytes is transferred after every 0.005 second. Along this communication another few nodes also communicate during simulation. A node can work as a source node of communication or routing node.

5.7 Performance Metrics

We have chosen Route Acquisition Time, Normalized Routing Overhead, Average Hop per count, Mean End-to-End Delay, Jitter, Throughput and Packet Delivery Ratio as a performance metrics.

5.7.1 What is Route Acquisition Time?

It is defined as the total time taken by Route Request and the time taken by the respective Route Response. It's describe total time taken by a particular route to establish. The following awk scripts code is used to calculate the route acquisition time of SAODV and Ariadne from a trace file.

// SAODV Code

```
{
        if($1=="s" && $3=="_"sendNode"_" && $4=="RTR" && $7=="AODVUU" &&
        $9=="[0" && $10=="0" && $11=="0" && $12=="0]" && $21=="["recvNode &&
        $23=="["sendNode && $25=="(REQUEST)")
        {
                sendTime=$2
        }
        if($1=="r" && $3=="_"sendNode"_" && $4=="RTR" && $7=="AODVUU" &&
        $20=="["recvNode && $22=="["sendNode"]" && $24=="(REPLY)")
        {
                recvTime=$2
                totalTime+=recvTime-sendTime
                count++
        }
}
END{
        print " SAODV Average Route Acquisition Time =",totalTime/count
}
```

// Aridane Code

```
{
        if ($1=="s" && $4=="MAC" && $7=="DSR" && $25!="[1"){
                sendTime[$6]=$2
        }
        if ($1=="r" && $4=="MAC" && $7=="DSR" && $25!="[1"){
                if (recvTime[$6]==0){
                        recvTime[$6]=$2
                        totalTime+=recvTime[$6]-sendTime[$6]
                        count++
                }
        }
}
END {
        print "Aridane Average Route Acquisition Time", totalTime/count
}
```

5.7.2 What is Normalized Routing Overhead?

The number of routing packets transmitted during per data packet transmission to the final destination. At intermediate node, every forwarded packet counted as one transmission. This performance metric is extremely correlated with the variable route changes occurred during entire simulation. To calculate normalized routing overhead following formula used:

Normalized Routing Overhead = Number of routing packets / Number of data packets

Average Hop per Count = number of MAC transmission / AGT Layer Transmission

The following awk script code is used to compute the average hop count of SAODV and Aridane from a trace file.

// SAODV and Aridane

```
{
    if($1=="s" && $4=="MAC" && $7=="cbr"){
        rcount++
    }
    if($1=="s" && $4=="MAC" && $7=="cbr"){
        cbrcount++
    }
    if($1=="f" && $4=="RTR" && $7=="cbr"){
        cbrcount++
    }
}
END{
        print "Average Hop Count=",cbrcount/rcount

}
```

5.7.4 What is Mean End to End Delay?

In network communication, delay is always considered as an important parameter. End to end delay includes queuing, propagation and processing delays. Delay is mostly considered and becomes important issue in real time application.

$$Mean\,Delay = \frac{\sum_{i=1}^{n} Delay\,Of\,Packet}{n}$$

Delay of Packet: time from the packet is transmitted to the time the packet is received.

Delay of Packet = Propagation delay + Queuing delay + Transmission delay

Propagation delay = distance / signal propagation speed

Queuing delay = depend on the network load

Transmission delay = Size / Bandwidth

The following awk script code is used to compute the end-to-end delay of SAODV and Aridane form a trace file.

// SAODV and Aridane Code

```
{
        if($1=="s" && $4=="MAC" && $7=="cbr" && $19=="0"){
                check=substr($15,":",1);
                nodeid[$6]=check
                sendU[$6]=$2
        }
        if($1=="r" && $4=="MAC" && $7=="cbr" ) {
                if($3=="_"nodeid[$6]"_"){
                        recvU[$6]=$2
                }
        }
}

END {
        for (i in recvU) {
          if (sendU[i] == 0) {
              printf("\nError %g\n",i)
          }
          delayU += recvU[i] - sendU[i]
          numU ++
      }
      if (numU != 0) {
          avg_delayU = delayU / numU
      } else {
          avg_delayU = 0
      }

printf("Total Delay=%5g Packet=%g Average Delay=%5g\n",delayU,numU,avg_delayU*1000)
}
```

5.7.5 What is Jitter?

Jitter is a variation (somewhat random) of the latency from packet to packet. Jitter is most often observed when packets traverse multiple hops from source to destination. Jitter is also considering the deviation in the packet latency at the target node. Some sensitive application like voice over IP (VoIP) might get affected by the high value of jitter.

Jitter can be measured by the following method.

$$\Delta arrival_n = | Arrival_n - Arrival_{n-1} |$$

Where, n is the current packet.

$$Jitter_n = |\Delta arrival_n - \Delta arrival_{n-1}|$$

Where, n is the current packet.

5.7.6 What is Throughput?

It can be expressed as the amount of data communicates from one node to another node during a specified amount of time. Typically, throughputs are measured in kbps, Mbps and Gbps. We usually think of throughput as ***measured performance***. Implementation inefficiencies may cause the achievable bit rate to be less than the bandwidth for which the networks was designed. Throughput is measured by following equation.

Throughput = Transfer Size / Transfer time

The following awk script code is used to calculate the throughput of SAODV and Aridane from a trace file.

// SAODV and Aridane

```
{
        if($1=="s" && $4=="MAC" && $7=="cbr" && $19=="0"){
                check=substr($15,":",1);
                nodeid[$6]=check
        }
        if($1=="r" && $4=="MAC" && $7=="cbr" ) {
                if($3=="_"nodeid[$6]"_"){
                        recvBU[$6]=$8
                        recvnumU++
                }
        }
}

END {
        totalBytesRecv=0
        for(i=0; i<recvnumU; i++) {
                totalBytesRecv+=recvBU[i]
        }
        printf("ThroughPut(Kbps)=%f\n",(totalBytesRecv/(50))*(8/1000))
}
```

5.7.7 What is Packet Delivery Ratio?

Packet delivery ratio is equal to the number of packets received on destination divided by number of packet send on source during a specified time. Packet delivery ratio can be measured by following equation.

*Packet Delivery Ratio = (no. of received packets / no. of send packets) * 100*

The following awk script code is used to calculate the packet delivery ratio of SAODV and Aridane from a trace file.

// SAODV and Aridane Code

```
{
        if($1=="s" && $4=="MAC" && $7=="cbr" && $19=="0"){
                check=substr($15,":",1);
                nodeid[$6]=check
                sendnumU++
        }
        if($1=="r" && $4=="MAC" && $7=="cbr") {
                if($3=="_"nodeid[$6]"_"){
                        recvnumU++
                }
        }
}

END {
        print "Packet Delivery Ratio=",(recvnumU/sendnumU)*100
}
```

Chapter 6

Simulation Results

In this chapter we describe our simulation results which show the effectiveness of the routing protocols. We have done number of simulations to show the performance of these routing protocols. We evaluate the following in our proposed scheme:

1) Effect of mean delay due to increase in communication flows.
2) Effect of route acquisition time during communication.
3) Effect of normalized routing overhead over the data communications.
4) Effect of intermediate nodes during communication by calculating average hop count.
5) Effect of delay variation due to increase in number nodes and communication flows.
6) Effect of average throughput and packet delivery ratio due to increase in number of nodes.

6.1 Results Explanation

We have performed number of simulations to show the effectiveness, usefulness and performance of routing protocols architecture. We have run number of simulations with variable nodes and communication flows in each simulation, a node may have send data to other node or act as an intermediate node. Each simulation runs for 100 second. Route Acquisition Time, Normalized Routing Overhead, Average Hop per Count, Mean End-to-End Delay, Throughput, Jitter and Packet Delivery Ratio is considered as a performance metrics to evaluate the protocols.

6.1.1 Route Acquisition Time

The figure 6.1 and 6.2 shows average route acquisition time of SAODV and Ariadne in manhattans grid and random way point mobility model respectively. We run the simulations for 100 seconds with constant traffic. The average route acquisition time is measured with respect to number of variable nodes. The given graphs show route acquisition time of Ariadne is lesser than SAODV with nodes increases in both mobility models. As shown in given graph SAODV consumes larger time whenever nodes is equal to10 and it is gradually decreasing as the number of nodes increasing from 20-50. The Ariadne performance is due to a reliable authentication protocol like TESLA with Ariadne. We have analyzed that an

overhead coupled with SAODV which are hashes or verify existed signature, processing new signatures and extra time is occurred in link establishment.

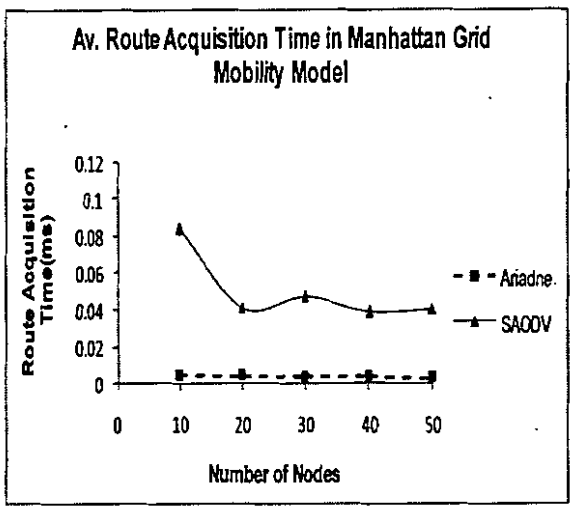


Figure 6.1 Route Acquisition Time in Manhattan Grid Mobility Model

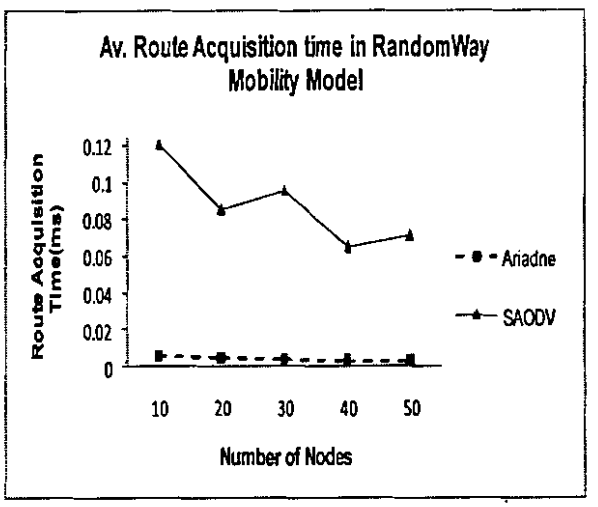


Figure 6.2 Route Acquisition Time in RandomWay Mobility Model

6.1.2 Normalized Routing Overhead

The figure 6.3 and 6.4 shows the normalized routing overhead of SAODV and Ariadne in manhattans grid and random way point mobility model respectively. We run the simulations for 100 seconds with constant traffic. The below graph show normalized routing overhead with respect to number of nodes. Both graphs illustrate that SAODV routing overhead increases as the number of nodes increases and Ariadne routing overhead slightly change as number of nodes increases throughout simulation time. SAODV routing overhead mainly due to the lot of routing message generated by frequently after route failure.

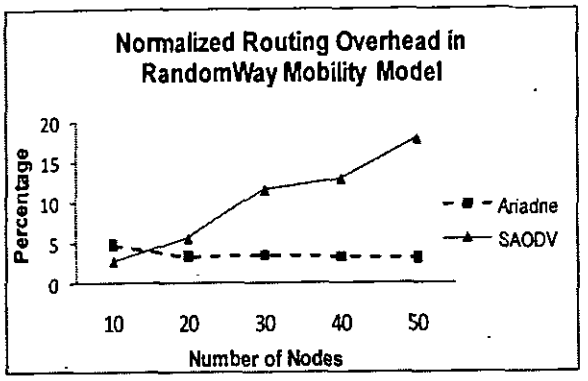


Figure 6.3 Normalized Routing Overhead in Manhattan Grid Mobility Model

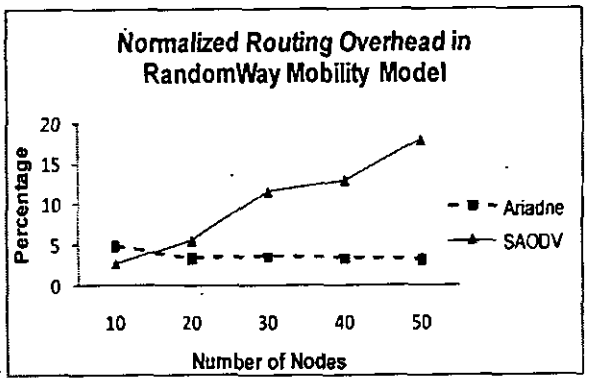


Figure 6.4 Normalized Routing Overhead in Random Way Mobility Model

6.1.3 Hop per Count

The figure 6.5 and 6.6 shows the hop per count of SAODV and Ariadne in manhattans grid and random way point mobility model respectively. The both graphs show average hop per count with respect to number of nodes. Both graphs illustrate that SAODV and Ariadne hop count vary from 1.2 to 1.6. The average hop count value of Ariadne is greater than SAODV because, SAODV establish route from scratch after the link breaks and Ariadne uses already updated path information for route establishment.

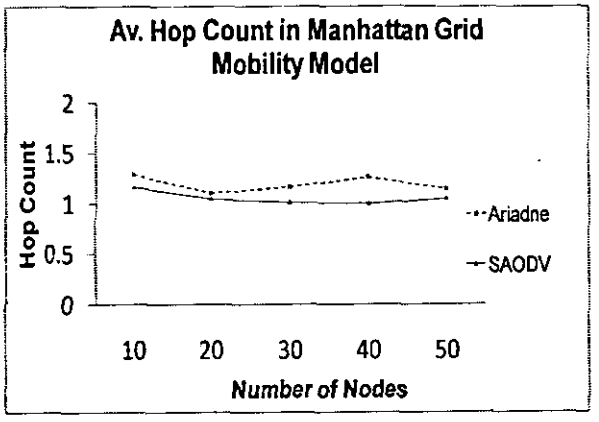


Figure 6.5 Av. Hop Count in Manhattan Grid Mobility Model

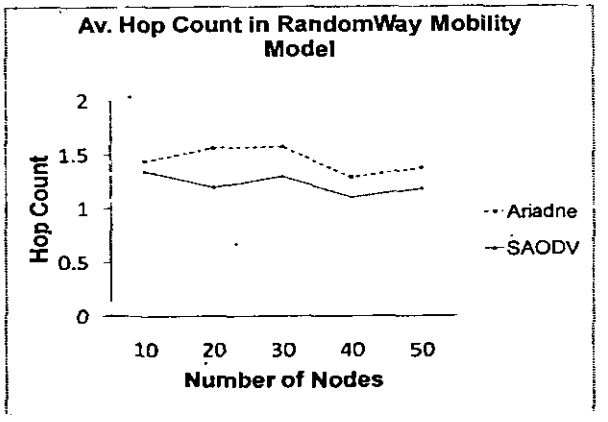


Figure 6.6 Av. Hop Count in Random Way Mobility Model

6.1.4 Mean End to End Delay Analysis

The figure 6.7 and 6.8 shows the end-to-end delay of SAODV and Ariadne in manhattans grid and random way point mobility model respectively. We carried out number of simulations to get the average end-to-end delay for both secure routing protocols with variable nodes. The average end to end delay is decreases with respect to number of nodes increases throughout simulation time. SAODV has much lower delay compared to Ariadne. This delay occurs due to the packets are remain in the buffer of intermediate nodes for a variable duration. In the case of SAODV intermediate nodes involvement is less during packets transmission. The value of hop count is evidence for this average delay trend.

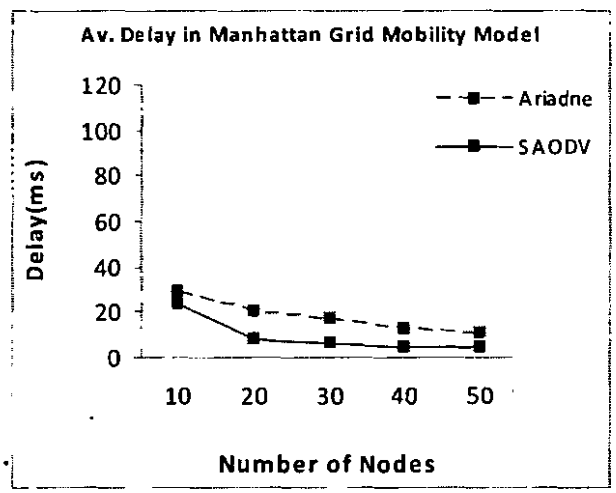


Figure 6.7 Av. Delay in Manhattan Grid Mobility Model

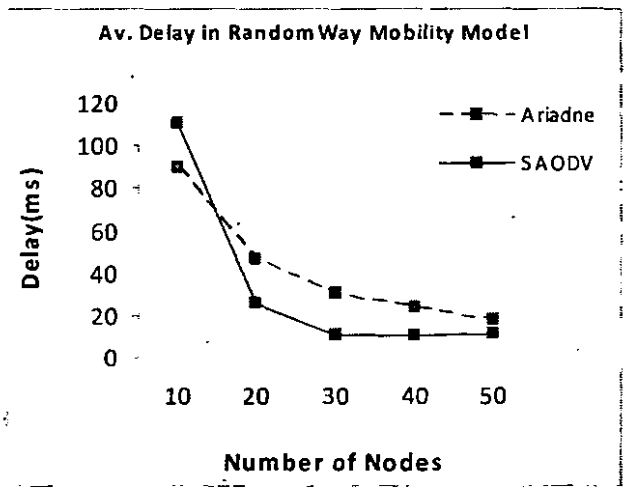


Figure 6.8 Av. Delay in Random Way Mobility Model

6.1.5 Throughput

The figure 6.9 and 6.10 shows the throughput of SAODV and Ariadne in manhattans grid and random way point mobility model respectively. We carried out number of simulations to find out the average throughput for both the secure routing protocols with varying values of node density. The average throughput value varying from 130 to 170 Kbps and there is slight variation as the number of nodes increases.

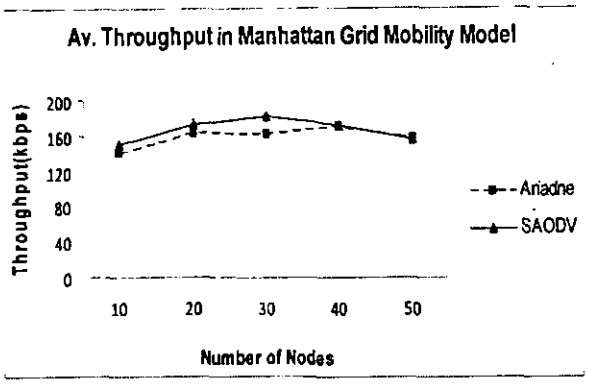


Figure 6.9 Av. Throughput in Manhattan Grid Mobility Model

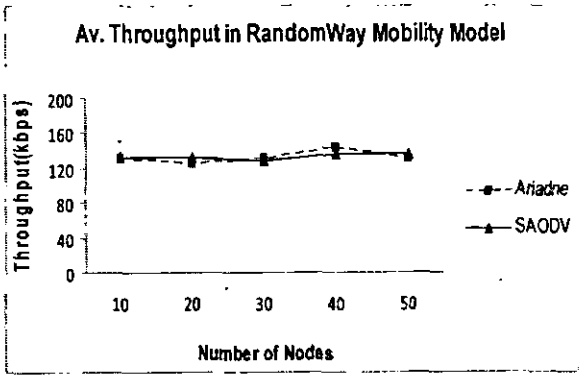


Figure 6.10 Av. Throughput in Random Way Mobility Model

6.1.6 Jitter

The figure 6.11 and 6.12 shows the jitter of SAODV and Ariadne in manhattans grid and random way point mobility model respectively. We carried out simulations to find out the jitter for both the secure protocols with variable nodes. The average jitter value of Ariadne is lesser than SAODV and this value slightly decreases with respect to number of nodes. This trend show that there is continuously packet transfer from one node to another node despite the intermediate nodes and in the case of SAODV there is larger variation because of route failure and route establishment.

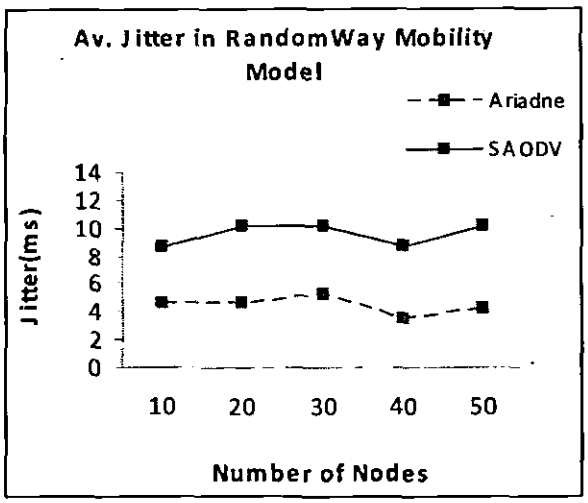


Figure 6.11 Av. Jitter in Manhattan Grid Mobility Model

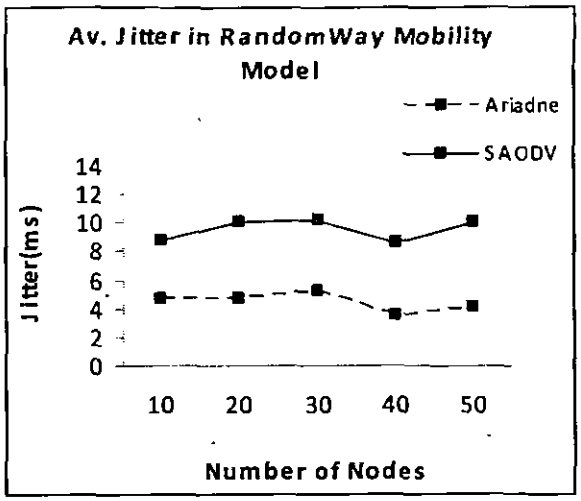


Figure 6.12 Av. Jitter in Random Way Mobility Model

6.1.7 Packet Delivery Ratio

The figure 6.13 and 6.14 shows the packet delivery ratio of SAODV and Ariadne in manhattans grid and random way point mobility model respectively. Both figures show there is slight variation in ratio throughout simulation time. At some point it approximately reaches the value of 100 which show the performance and effectiveness of these secure routing protocols.

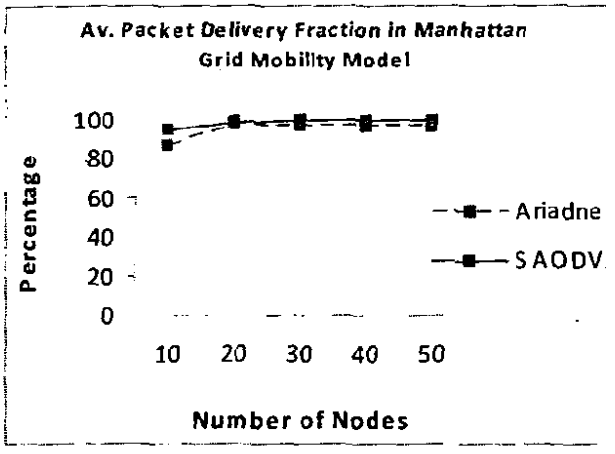


Figure 6.13 Packet Delivery Fractions in Manhattan Grid Mobility Model

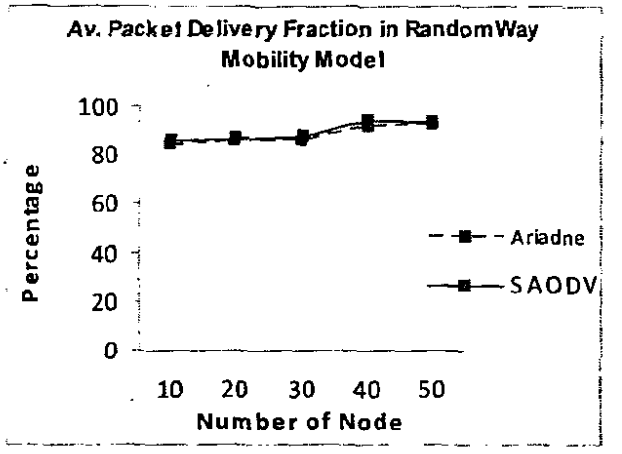


Figure 6.14 Packet Delivery Fractions in Random Way Mobility Model

Chapter 7

CONCLUSION AND FUTURE WORK

This chapter explains the conclusion of the research and the possible future work that can be done in this field.

7.1 Conclusion

In this thesis, we evaluated two secure routing protocols for the mobile Ad-Hoc networks (MANETs) under the Random Way and Manhattan Mobility Model on the basis of performance metrics despite the security metrics. Based on our simulations results following conclusions can be drawn:

Ariadne performs better in term of route acquisition time and routing overhead over the SAODV. The routing protocol SAODV takes advantage in term of end to end delay and packet delivery fraction over the Ariadne. As we have seen in the graphs the performance of the routing protocols are increasing as the number of nodes increased. The protocol overhead of SAODV is greater as compared to Ariadne. The routing protocol Ariadne has the edge of TESLA over the SAODV. Ariadne is more secure, reliable and efficient than SAODV as the number of nodes increasing.

In conclusion, secure Ad-Hoc routing protocols are an essential for the secure routing of data packets. In the implementation of such a routing protocols, the need is to eliminate the shortcoming of these protocols by evaluating performance of them on a simulation platform. Both protocols need further optimizations so that they can minimize the overhead associated with these protocols like delay, routing overhead and etc. And more specifically SAODV needs to tackle some processing requirements due to its use of security techniques like hash chain and digital signatures.

7.2 Future Work

Our work can be extended in following direction.

Security Aspects: In the current project we evaluated two secure routing protocols of mobile Ad-Hoc networks based on the performance metrics. This aspect of evaluation is very

important for each node but there is need to evaluate these routing protocols in security aspects.

Mobility Models: There is separate study required to evaluate these routing protocol under other mobility models.

Variant Traffic: Our approach to evaluate these routing protocols can be extended for FTP and TCP traffic.

Extensive Simulation: An extensive simulation study with complex scenario also required to check efficiency of this architecture.

Comparative Study: There is comparative study required to find out the best secure routing protocol under performance and security metrics.

References

[1] William Stallings, "Wireless Communication and Networks," Prentice Hall, 2nd Edition, December 2004.

[2] G. Bianchi, L. Fratta and M. Oliveri, "Performance Evaluation and Enhancement of the CSMA/CA MAC Protocol for 802.11 Wireless LANs", *In the Proceeding of PIMRC*, Taipei, Taiwan, pp. 392- 396, October 1979.

[3] L. Kleinrock and F.A. Tobagi, "Packet Switching in Radio Channel," *In proceeding of IEEE Trans on Comm.*, vol.23, no.5, pp. 1400-1416, 1990.

[4] S.S. Lam, "A Carrier Sense Multiple Access Protocol for Local Networks," *In proceedings of Computer Networks,* vol. 4, no. 16, pp.21-32, 1991

[5] M.M.A. Assaf, "Wireless Ad-Hoc Networks," *In Department of EECS, Syracuse University*, Syracuse, New York, November 2004.

[6] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad-Hoc Networks," *Wireless Networks (WINET),* vol. 11, no.1-2, pp. 21-38, January 2005.

[7] T.H. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," *IETF RFC3626 - Experimental Standard*, October 2003.

[8] M.G. Zapata and N. Asokan, "Secure Ad-Hoc On-Demand Distance Vector Routing," *In proceeding of ACM Mobile Computing and Communications Review,* vol. 3, no. 6, pp.106-107, July 2002.

[9] Y.C. Hu, A. Perrig and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad-Hoc Networks," *In Proceeding of 8th ACM International Conference Mobile Computing and Networking (Mobicom'02),* Atlanta, Georgia, pp. 12-23, September 2002.

[10] A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and Secure Source Authentication for Multicast," *In proceeding of Network and Distributed System Security Symposium (NDSS'01)*, San Diego, California, USA, February 2001.

[11] R.J. Perlman, "Fault-Tolerant Broadcast of Routing Information," *In proceeding of Computer Networks,* North-Holland, vol. 7, no. 9, pp. 395- 405, 1983.

[12] L. Zhou and Z. J. Haas, "Securing Ad-Hoc networks," *IEEE Network Magazine*, pp.24–30, November/December 1999.

[13] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad-Hoc Networks," *In Proceeding of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS '02),* Texas, USA, January 2002.

[14] Y. C. Hu, D. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad-Hoc Networks," *In proceeding of Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02),* pp. 3-13, June 2002.

[15] J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu and J.Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad-Hoc Network Routing Protocols," *In Proceedings of the Fourth Annual International Conference on Mobile Computing and Networking (MobiCom'98)*, ACM, Dallas, Texas, USA, October 1998.