Master Thesis
Computer Science
Thesis no: MCS-2011-11
March 2011

Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions

Muhammad Arshad Ali
&
Yasir Sarwar

School of Computing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden

This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to twenty weeks of full time studies.

Contact Information:
Author(s):

Muhammad Arshad Ali
Email: arshad_ali2b@yahoo.co.uk
Ph: +46-760608641

Yasir Sarwar
Email: yasabth@gmail.com
Ph: +46-738968436

University advisor(s):

Mr. Bengt Carlsson
Email: bengt.carlsson@bth.se
Department of Computer Science
Blekinge Institute of Technology
Karlskrona, Sweden

School of Computing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

THIS PAGE IS LEFT BLANK INTENTIONALLY

ABSTRACT

Now a day, it is no longer optional to have security solutions even inevitable for every kind of organizations and individuals. There are number of generic tools which are common for organizations as well as for individual users to provide security which includes; Anti-Spam, Anti-Virus etc., and network security have become essential issue in MANET. Security is one of the main issues in the MANET especially with respect to size and complexity of the network. The aim of the thesis is to discuss different aspects of security in MANET (e.g. multi-layer intrusion detection technique in multi hop network of MANET, security problems relates between multihop network and mobile nodes in MANET etc) and also implement some of the solutions (e.g. comparative study of different routing protocol (AODV, DSR and TORA) security threats within MANET network like intruder behavior, tapping and integrity, MANET link layer and network layer operations with respect to information security etc) with respect to MANET network.

This report also discusses different number of scenarios of MANET network which we implement in our simulation. In our simulation we use to implement different routing protocols and also did comparative study that which one is better with respect to different aspects. We also use to implements mechanisms of intruder behavior, tapping and integrity, and MANET link layer and network layer operations with respect to information security.

Keywords: MANET, Security, tapping, intruder

ACKNOWLEDGEMENTS

First, of all we are grateful to almighty Allah the greatest of all. Then we would like to thank our supervisor at University, Mr. Bengt Carlsson for his guidance, encouragement, patience and support throughout this thesis work.

Second, we would like to thank Sweden giving us an opportunity of studies which gives us an International exposure and also thanks to Blekinge Institute of Technology for giving us confidence of study and give us tremendous experience.

Muhammad Arshad Ali & Yasir Sarwar
Karlskrona, 2011

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AODV	Ad hoc On-Demand Distance Vector
CA	Certificate Authority
CIA	Confidentiality Integrity and Authenticity
DIPLOMA	DIstributed PoLicy enfOrceMent Architecture
DoS	Denial-of-Service
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
GPSR	Greedy Perimeter Stateless Routing
IDS	Intrusion Detection System
MAC	Media Access Control
MANET	Mobile Ad hoc Network
MPLS	Multi-Protocol Label Switching
ODMRP	On-Demand Multicast Routing Protocol
OPNET	Optimized Network Evaluation Tool
OSPF	Open Shortest Path First
PIM-SM	Protocol Independent Multicast-Sparse Mode
PDAs	Personal Digital Assistant
R&D	research and development
RFC	Request for Comment
RIP	Routing Information Protocol
RQ	Request
RREP	Route Reply
RREQ	Route Request
RTS	Request To Send
TC	Topology Control
TCP	Transmission Control Protocol
TORA	Temporally-Ordered Routing Algorithm
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

Chapter 1
Introduction

1 INTRODUCTION

1.1 General Overview of the Area

Mobile ad hoc network got outstanding success as well as tremendous attention due to its self maintenance and self configuration properties or behavior. At early stage mostly people focused on its friendly and cooperative environment and due to this way many different problems came in being; security is one of the primary concerns in order to provide secure communication between different nodes in a mobile ad hoc network environment. Due to different characteristics of Mobile ad hoc network security is an active research topic in wireless path, which is also a nontrivial challenging to security design. There are different types of challenges in mobile ad hoc network which are given below:

- Open network architecture
- Shared wireless medium
- Stringent resource constraints
- Highly dynamic network topology

It is also true that the solutions to the wired networks do not workable to mobile ad hoc networks domain

It is also true that security has long been an active research topic in wireline networks; but due to unique characteristics of MANET there are many challenges because of its self organizing behavior. These challenges are shared wireless medium, highly dynamic network topology, stringent resource constraints and open network architecture. It's true that existing security solutions for wired networks do not directly apply to the Mobile ad hoc networks domain.

Mobile ad hoc network has different challenges with respect to wireless security due to some of the following reasons:

1. The wireless network especially liable to attacks because of active eavesdropping to passive interfering.

2. Due to lack of Trusted Third Party adds, it is very difficult to deploy or implement security mechanisms.

3. Mostly Mobile devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.

4. Due to MANET's properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words we need to cover up from both insider and outsider attacks in MANET, in which insider attacks are more difficult to deal with.

5. It is difficult to distinguish between stale routing and faked routing information because of node mobility mechanism. In node mobility mechanism it enforces frequent networking reconfiguration which creates more chances for attacks.

1.2 Aims and Objectives

MANET is a type of multi-hop network, infrastructure less and the most important self-organizing. Due to its wireless and distributed nature there is a great challenge for system security designers. In the last few years security problems in MANETs have attached much attention; most of the research efforts focusing on specific security areas, like securing routing protocols or establishing trust infrastructure or intrusion detection and response.

One of the main characteristic of MANET's with respect to security design point of view is the lack of clear line defense. In case of wired networks we have dedicated routers; which perform routing functionalities for devices but in case of Mobile ad hoc network are concerned each mobile node acts as a router and forward packets for other nodes. It is also true that the wireless channel is accessible to both network users as well as to attackers. There is no well defined rule or place where traffic from different nodes should be monitored or access control mechanisms can be enforced. Due to this way there is no any defense line that separates inside network from the outside network. Due to this way the existing ad hoc routing protocols, like Dynamic Source Routing (DSR) [1] and Ad Hoc On Demand Distance Vector (AODV) [2], and wireless MAC protocols, such as 802.11 [3], typically assumed to be trusted. As a result, an attacker can become a router and disrupt network operations.

There are mainly three main security services for MANETs: Authentication, confidentiality, integrity.

- Authentication means correct identity is known to communicating authority.
- Confidentiality means message information is kept secure from unauthorized access.
- Integrity means message is unaltered during the communication between two parties.

Among all these security services, authentication is probably the most important and complex issue in MANETs because it is the bootstrap of the whole security system. Once authentication is achieved in MANET then confidentiality is just a matter of encrypting algorithm on the session by using keys. These security services can be provided singly or in combination, it only depends on our requirements.

In this thesis we will focus on the fundamental security problems of the Mobile ad hoc network connectivity between mobile nodes from one network to another network, and how it works in client (mobile nodes) server (mobile server) architecture with respect to security. We will identify security issues, discuss challenges to security and protect link layer and network layer operations over mobile ad hoc network with respect to information security. We will also try to implement one of the security components (means CIA), most probably in this fashion; security threats within MANET network like intruder behavior, tapping and integrity. We also implement comparative study of different routing protocols (AODV, DSR and TORA) with respect to security parameters (delay, load, throughput etc), which will not directly effect security but definitely, it will effect indirectly, even these parameters can be used further with respect to security concerns.

In this thesis we will also discuss different aspects of security in MANET (e.g. multi-layer intrusion detection technique in multi hop network of MANET, security problems relates between multihop network and mobile nodes in MANET etc as).

1.3 Research Goals

In this report we mainly focus on the security threats and challenges in MANET. There are two main parts of our thesis, in the first part we will discuss different security aspects and how these issues to be resolved? In the second part of the thesis there is an implementation of MANET network in OPNET simulator; first we will develop MANET network with different routing protocols and compare results with respect to throughput, bandwidth, delay etc in order to develop a better understanding of routing protocols with respect to different network situations. Second we will develop a MANET network with an intruder and discuss an integrity aspect in the network. Finally we will develop a scenario about information security. The solutions of the problem are also discussed in the document; our thesis also provides good understanding of the security challenges and solutions of the Mobile Ad hoc Network. In general there are following research questions which we will discuss in our thesis:

RQ1: How multi-layer intrusion detection technique works in multi hop network of MANET?

RQ2: What are the security problems that are related between multi-hop network and mobile nodes in MANET?

RQ3: What are the challenges for MANET link layer and network layer operations with respect to information security?

RQ4: How can we deal with security threats within MANET network like intruder behavior, tapping and integrity?

1.4 Research Methodology

The main goal to adopt research methodology is to produce new knowledge, and here is the form of research methods [3]:

- Constructive research

  It develops solutions to a problem. Here we will divide our work into two models theoretical model and simulation model. In the theoretical model we will study different security issues and their solutions. In the simulation model we will run simulation with MANET configuration and try to learn mechanisms which will help us to enforce security in Mobile Ad Hoc Networks.

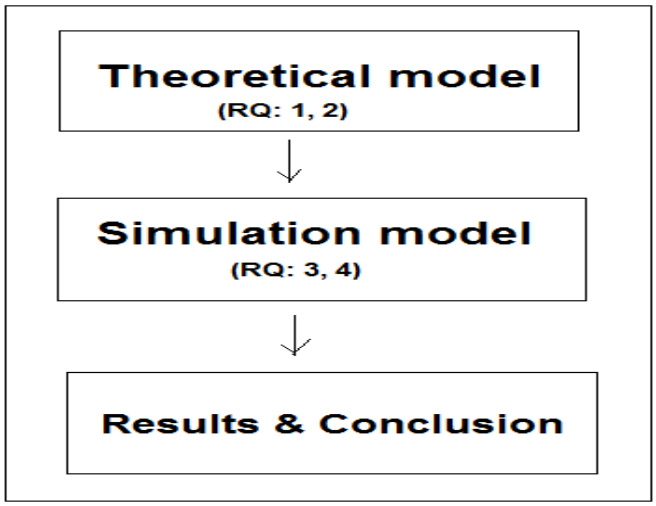

Figure 1.1 Research Methods

1.5 Risks

SWOT Analysis	
Strengths	**Opportunities**
• High motivation, dedication, commitment and Hardworking • Responsible • Optimistic and pessimistic attitude towards problem solving • Strong communication skills • Intellectual vibrant learning • Deepen and advance the knowledge	• Work under the supervision of experienced supervisor • Learn more about team work • Increasing our knowledge as well as strong our technical skills by developing simulation • Sharing and increasing knowledge and skills from each other(among group members)
Weaknesses	**Contingency Plan**
• Weak documentation/technical writing skills • Don't have excellent knowledge for developing simulation in OPNET.	• To learn technical writing skills we will read research papers & articles and try to learn • Try to read materials regarding OPNET, and also revise previous understanding of the tool.
Threats	**Contingency Plan**
• Critical schedule • Issues among the group members • Absent of any member for certain time due to some reason • Thesis implementation time may be more or less time demanding	• Try to complete internal deadlines and having some spare time. • Try to solve the issues with discussion • Other member try to manage work • Discussion with our supervisor may be we will add more scenarios and try to extend our project in order to utilize full time.

1.6 Chapter Organization

Chapter 1, Introduction: a general introduction of the area to what the thesis is all about; problem statement describes actual aim of the thesis, discusses problem solving approach and at last describes chapter organization throughout the report.

Chapter 2, Background: a brief section that gives necessary background information about our research area especially what have been done before?

Chapter 3, Types of Attacks: gives a brief description of attacks in MANET network, we will discuss different attacks in mobile ad hoc network and how we will avoid these attacks? This section also provides the detailed description of multi-layer intrusion detection technique and multihop network in mobile ad hoc network.

Chapter 4, Performance Evaluations and Design: This section provides the detailed description of our simulation design, and how we implementing our ideas.

Chapter 5, Opnet Simulation: describes actual aim of the thesis, it shows implementation mobile ad hoc network scenarios and also discusses different network devices which we use in our Opnet simulation.

Chapter 6, Results and Analysis: a brief description of our results. In this section we will discuss results behavior as a comparative study with respect to other network scenarios in MANET.

Chapter 7, Discussions of simulation analysis: gives the answers with respect to our research goals. This section also provides the detailed description of the previous section (means result and analysis).

Chapter 8, Conclusion and Future work: provides what we have learned, did we meet our goals, what are the suggestions about the research area, what we have untouched in the research area? Which will be the future work?

Chapter2
Background

2 BACKGROUND

In this chapter we will discuss background of the problem and discuss what have others already done? We will not discuss future work but off course in later chapter.

2.1 Description

There are some ultimate goals regarding security solutions with respect to Mobile ad hoc networks or we can say there are some security services which should be fulfill in order to enforce security like authentication, confidentiality, integrity to mobile users, we also use another term for them CIA which should be fulfill. In order to achieve goal in security, whatever the security solution it is? But it should provide complete protection to entire protocol stack. Table 2.1 shows the security issues with respect to each layer. In this thesis we will consider a fundamental security problem in MANET:

S. No	Layer	Security Issues
1	Application Layer	In this layer we should prevent viruses, application abuses, worms, as well as malicious nodes.
2	Transport Layer	It provide authentication and provide secure end-to-end communications through data encryption between two nodes.
3	Network Layer	This layer deals with the protection of routing as well as forwarding protocols.
4	Link Layer	In this layer we mainly concern with the protection of wireless MAC protocol and also provide link-layer security.
5	Physical Layer	In this layer we should prevent signal jamming as well as denial-of-service attacks.

Table 2.1: The security solutions for MANET's with respect to entire protocol stack.

We can say that first protect the network connectivity between mobile nodes and then provide potentially multihop wireless channels, which is one of the basic steps to support network security services.

Multihop connection established between two nodes in mobile ad hoc network through two steps:

1. It ensuring one-hop connection through link-layer protocols like wireless medium access control (MAC).
2. Through network layer it will extend connection between multiple hops and provide routing and data forwarding protocols.

As argued in [4], security is a chain, and it is only as secure as the weakest link. Missing a single point significantly degrade the strength of the overall security system. It is also true that security never comes for free. Due to more security features into the network, as a result it will also increase computation, as well as communication, and management overhead too.

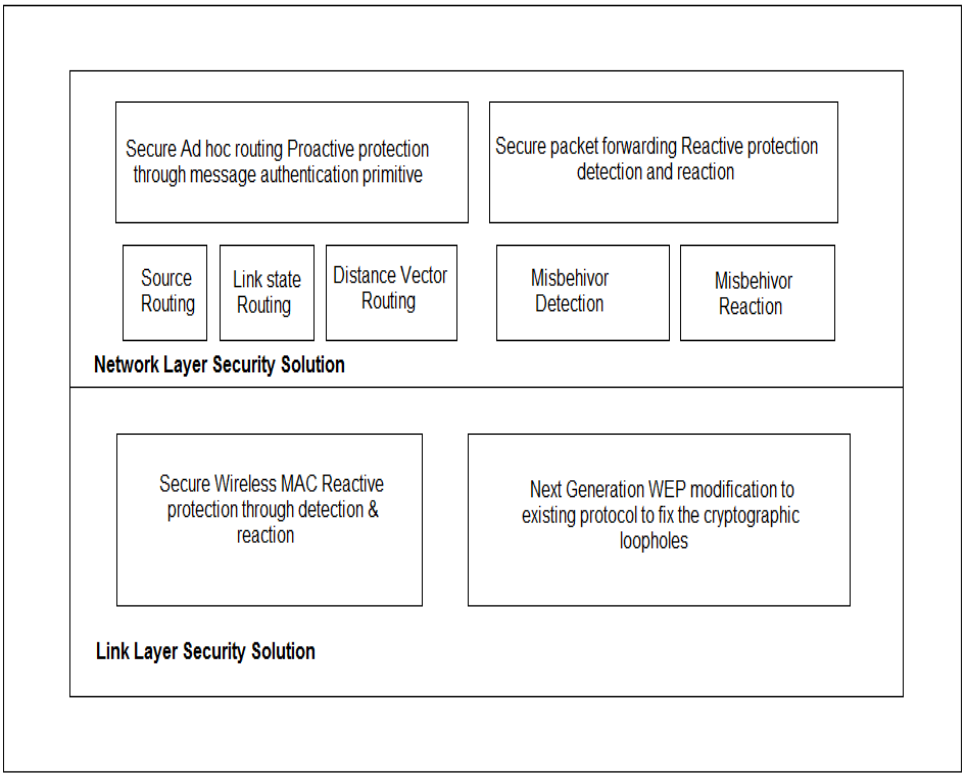

Figure 2.1 Components in Security Solution

2.2 Challenges

One of the fundamental vulnerability of MANETs comes from open peer-to-peer architecture. In case of wired networks there are dedicated routers but in case of mobile ad hoc network each mobile node acts as a router in order to forward packets for one node to other node. In mobile ad hoc networks there are no boundaries of wireless channel; it is accessible to both network users as well as to malicious attackers. Due to this reason there is no clear line of defense in MANET networks with respect to security design perspective. The boundary becomes blurred that is used to separates inside network from the outside network. Due to all this there is no well defined infrastructure in order to deploy single security solution over MANET.

According to security information with respect to MANET network are vulnerable compromises or physical capture, especially at the end of low-end devices due to weak protection. Intruders enter into the network and poses weakest link and incur a domino effect of security in the network. According to wireless channel is concerned bandwidth is one of constrained and use to share among multiple different network nodes. There is also one more restriction that is computation capability; like low-end devices for e.g. PDAs, can hardly perform low computation due to this way they usually use asymmetric cryptographic computation which is bit low complex, because mobile devices have very limited energy resources due to this way mostly mobile devices powered by batteries.

The wireless medium as compared to wireline network node mobility more dynamics in mobile ah hoc networks. The network topology is highly dynamic due to free movement in the network like nodes can frequently join or leave, as well as in the network by their own will. There are also interferences in the wireless channel due to this way error, exhibiting volatile characteristics in terms of bandwidth and delay occurs. Due to such dynamic behaviors mobile users request for security services at any anytime or anywhere whenever they move from one place to another in the network.

There are some characteristics of security solutions of MANETs which will clearly provide multi fence security solutions with respect to network protection and also provide desirable network performance.

1. The security solution should also implement across many individual components in order to provide collective protection to secure entire network. In terms of computation capabilities are concerned like energy supply, memory as well as communication capacity each device has to work within its own.

2. The security solution should also provide security with respect to different layers of the protocol stack and each layer provide line of defense. It is also not possible that only one single-layer solution can handle all potential attacks.

3. The security solutions should avoid threats from both outsiders as well as inside. According to outside attacks are concerned it should avoid attacks on the wireless channel as well as network topology where as in case of inside attacks are concerned an intruder who enter into the network through compromised devices and gain access to different network knowledge.

4. The security solutions should enforce all three components of security like prevention, detection, and reaction.

5. The security solutions should be affordable as well as practical in resource constrained and highly dynamic networking scenario.

2.3 Routing protocol description

There are basically there kind of routing protocols which are:

- **Table driven routing protocols**

  In these routing protocols each node in the network maintains the complete routing information of the network by occasionally updating the routing table, so when a node needs to send some data or information, so there is no any kind of delay for discovering the route in the whole network. This type of routing protocols approximately works the same way as the wired network routing protocol works. The table driven protocols are DSDV and WRP.

- **On-Demand routing protocols**

  While in this kind of routing protocols, a node simply maintains routes information to get destination that it needs to send required data packets. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used. These routing protocols are AODV, DSR and TORA.

- **Hybrid routing protocols (ZRP)**

  In this type of routing protocol is the combination of the above two categories. In which nodes belonging to a particular geographical area or within a certain detachment from an anxious node are said to be in routing area and uses table driven routing protocol. Communication between nodes in different areas will rely on the source initiated or on-demand routing protocols. This routing protocol Include ZRP.

We select the most popular routing protocols, which is On-Demand routing protocols according the these routing protocols they are used when they are need and also in this routing protocols a node simply maintains routes information to get destination that it needs to send required data packets. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used, which give less load on the network and that's why it's very hard to attack on such routing protocols.

2.3.1 AODV

AODV using a classical distance vector routing algorithm. It is also shares DSR's on-demand discovers routes. During repairing link breakages AODV use to provide loop free routes. It does not add any overhead to the packets, whenever a route is available from source to destination. Due to this way it reduces the effects of stale routes and also need for route maintenance for unused routes. One of the best features of AODV is to provide broadcast, unicast, and multicast communication. During route discovery algorithm AODV uses a broadcast and for reply it uses unicast.

2.3.2 DSR

The DSR is an on-demand routing protocol that is based on source routing. It uses no periodic routing messages like AODV, and due to this way it reduces network bandwidth overhead, and also avoids large routing updates as well as it also reduces conserves battery power. In order to identify link layer failure DSR needs support from the MAC layer. It is consist of the two network processes, Route Discovery and Route Maintenance. Both of neither AODV nor DSR guarantees shortest path.

2.3.3 TORA

The TORA is an adaptive, scalable and efficient distributed routing algorithm. It is mainly designed for multi-hop wireless networks as well as highly dynamic mobile environment. It is also called source-initiated on-demand routing protocol. It is also use to find multiple routes from source to destination node. One of the main features is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. It has three basic functions: Route maintenance, Route erasure and Route creation.

Table 2.2 lists some comparisons between the three routing protocols discussed above.

Comparative Parameters	**AODV**	**DSR**	**TORA**
Source Routing	No	Yes	No
Topology	Full	Full	Reduced
Update Information	Route error	Route error	Node's Height
Method	Unicast, Broadcast	Unicast, Broadcast	Broadcast
Update destination	Source, Neighbor's.	Source	Neighbor's

Table 2.2 Comparison between AODV, DSR and TORA [5]

Chapter 3
MANET Attacks & Security

3 MANET ATTACKS & SECURITY

3.1 Security

The aims of Ad hoc networks and particularly MANET have in recent years not only seen widespread use in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's range from simple wireless home and office networking to sensor networks and similarly constrained tactical network environments. Security aspects play an important role in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborate data injection attacks.

3.2 Protecting Mobile ad-hoc network

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network. In ad hoc networks, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them. Note that in a wider sense, ad-hoc protocol can also be used literally, that is, to mean an improvised and often impromptu protocol established for a specific purpose.

3.2.1 Reactive Approach

Seeks to detect security threats and react accordingly. This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

There are two main things in re-active routing protocols first is that it never take initiative in order to take routes for network, second is that whenever it creates routes it will developed on demand by flooding mechanism. In such kind of routing protocols there are some advantages and disadvantages which are given below:

- Whenever they need to find out the routes they use bandwidth otherwise it will not use bandwidth.
- There is lot of overhead because of the flooding process.
- At start there is delay in the network.

There are three steps which will explain the complete procedure of the re-active routing protocols.

1. If there are two nodes at position A and position B which want to communicate.
2. In order to communicate with the B, A needs to flood the routes towards the B.
3. In order to create communication between A and B unicast feedback will come back.

3.2.2 Proactive Approach

Attempts to prevent an attacker from launching attacks through various cryptographic techniques: This type of protocols maintains fresh lists of destinations

and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

In pro-active routing protocols the mechanism is different than the re-active routing protocols. In this category of protocols basically routes are depends upon the traffic control which is continuous. All routing information maintained at any time of the network because we know that network is dynamic which changes its size by making its size increasing or decreasing. There are also some advantages and disadvantages in this type of protocols which we will discuss here. Basically there are two main things which are keep in mind first one is that due to the continuous control traffic mechanism there is lot of overhead on the network which is one of the drawback of the pro-active routing protocols. One good thing among the pro-active routing protocols is that all the time routes are available, due to this way there is an ease of communication among the nodes or devices. There are three steps in pro-active routing algorithm which are given below:

1. Link/ Neighbor Sensing.
2. Multipoint Relaying.
3. Link-State messaging and route calculation.

3.2.2.1 Link / Neighbor Sensing

In Link and Neighbors sensing mechanism we know by its name that neighbors and links are developed relationship among each other by sending hello packets to each other so that there will be connectivity between the different devices. In mobile ad hoc network all nodes or devices send hello packets among each other due to this way relationship between the neighbors and links has been created. In figure 3.1 basic scenarios between the neighbors has been given.

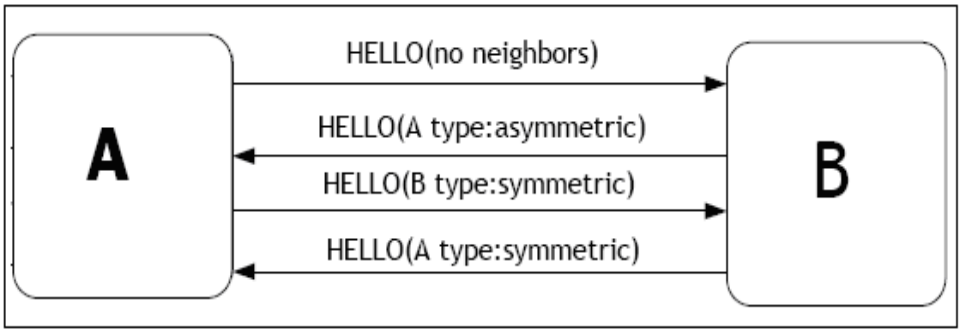

Figure.3.1 Link and neighbors sensing mechanism

3.2.2.2 Multipoint Relaying

In multipoint Relaying process whenever the devices send hello packets to each other or we can say that every node send broadcast hello packet to every other node except itself due to this way a lot of duplicate packets will generate in order to overcome these duplicate retransmission multipoint relaying mechanism is used which will reduce the duplicate packets in broadcast packets. It will also restricts other nodes or devices that at some regular time of interval you have to send the broadcast packets in order to know about the connectivity among the neighbors and links.

3.2.2.3 Link-State messaging and route calculation

3.2.2.3.1 Multipoint Relay selection

In multipoint relay selection mechanism every node in the network has to developed or maintain its own Multipoint Relaying procedure in order to run the protocol. One of the basic rule is that if there is a two nodes and they are neighbors to each other.

3.2.2.3.2 Forwarding of traffic

In forwarding of traffic step all nodes from the network has to established or maintain each and every node their own Multipoint Relaying Selectors. There is one basic rule for forwarding traffic that is when ever we are going to follow the pro-active routing protocols then all the packets from the routing protocols has been received by the Multipoint Relaying selector then packet is forward whenever its TTL value is greater then 0 due to this way packets will reach its all required destination in the network.

3.2.2.3.3 Link State functionality

The main functionality of Link State is that all devices in the network will flood out or broadcast link State information among the devices or nodes in order to make nodes updated. There are basically two main link state optimizations which are given below:

- Multipoint Relaying selectors are used for forwarding routes so that's why its better to be used for forwarding link state information that's why Multipoint Relaying selectors are selected to send link state messages due to this way size will decreases which is very useful in link state messages.

- We know that before forwarding routes there is a selection for Multipoint Relaying procedure so those nodes or devices which are choose as a Multipoint Relaying then only those devices and nodes are responsible for ending link state messages.

3.2.2.3.4 Link State Example

In link state procedure, the selected nodes has to send the link state message in the network but link state messages are called Topology Control messages(TC). TC has very important role in order to develop a network which because it will send messages towards the network devices and then relation among the nodes has been developed. There is an example of link state messages and Multipoint Relaying is given below:

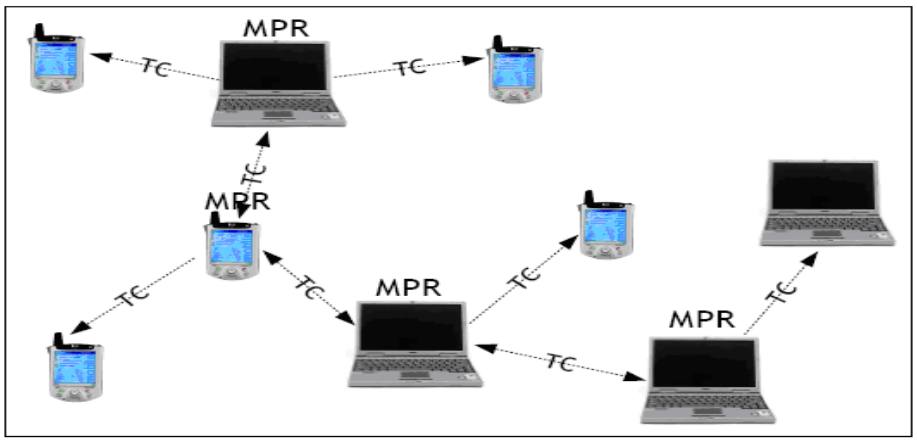

Figure.3.2 Link State Mechanism

Only the MPR nodes generate or forward link-state messages, thus small number of nodes is generating routing messages in the network as shown in the figure 3.2. The nodes associated to MPR are declared in link-state messages. The messages declaring link-state are called *Topology Control Messages* (TC), and have small message length.

3.3 Attacks

There are two mainly protocols are used in MANET networks, Link layer protocol are used to provide connectivity between different mobile nodes in order to ensure one-hop connectivity by using multihop wireless channels. On the other hand if we like to extend connectivity to different multiple hops then MANET network uses network layer protocols. In the coordination process distributed protocols typically assume that all mobile nodes are cooperating with respect to communication but actually this assumption is not possible in hostile mobile networks environment because cooperation is not enforced in MANET. The question arises why? The reason is because of malicious attackers violating protocol specification in order to disrupt network operations.

3.3.1 Network Layer operation

There are two main network-layer operations in MANET.

1. Ad hoc routing
2. Data packet forwarding

They interact with each other and delivering packets from source to destination. The main function of the ad hoc routing protocols is to provide routing among nodes; they exchange routing messages between different mobile nodes in order to maintain routing information at each node. According to the routing states, the second network layer operation data packets are used to forward data by intermediate next node which is an established route to the destination node. These both operations are vulnerable to malicious attacks, and which will lead to various types of malfunction in network layer.

3.3.2 Network Layer Attack

Due to this reason network-layer generally fall into two categories attacks:

1. Routing attacks
2. Packet forwarding attacks(based on the target operation of the attacks)

There are different categories of routing attacks that does not follow routing protocol specification. There are different routing protocols in MANET so therefore different attack behaviors related to different routing protocols. Some of them are discuss below:

1. According to the context of DSR [1] MANET routing protocol there are following different attacks which are given below [6]:
    - An attacker modifies source routing list with respect to RREQ or RREP packets.
    - Switching order of different nodes in the routing list.
    - Deleting entries from the list.
    - Appending new node entries into the list.

2. According to the context of AODV [2] MANET routing protocol there are also different attacks which are given below [7]:
    - An attacker advertise route with wrong distance metric with respect to actual distance to the destination.
    - Advertise wrong routing updates with a large sequence number with respect to actual sequence number.
    - An attacker invalidates all routing updates from other nodes.

3. According to the context of TORA routing protocol, there are also different attacking methods:

- Attackers construct routing paths by interfering with the protocols' mechanisms, e.g. routes can be forced to use attacking nodes to go through them.
- Attackers can also exhaust network resources by maliciously act of injecting, modifying and dropping data packets.

In order to divert traffic attackers attack on the routing protocols and divert traffic towards certain destinations under their control, and then they cause problematic situation in the network along a route which is not optimal or even nonexistent. The attackers can also create routing loops in the network, due to this way it creates network congestion in certain areas. There are also some other attacks like multiple colluding attacks which may cause to prevent source in order not to find route to the destination and also partition the network in the worst.

3.4 Active Attacks

There are also some different active attacks which are really difficult to locate or identify because these attacks are more sophisticated and they are considered as subtle routing attacks some of them are given below [8]:

- Attacker may further subvert existing nodes in the network.
- They can also fabricate their identity
- They can also impersonate other legitimate node
- Attackers in pair nodes may create a wormhole [9]
- They also creates shortcut in normal flows between each other
- The attackers target the route maintenance process and advertise operational link is broken [6]

According to context of routing attacks there are also some other kind of attacks like attacker launch attacks against packet forwarding operations as well due to this way it will not only disrupt the routing protocol it also poison the routing states at every node. For example, the attacker established route and drop packets, or also modify the content of the packets, or duplicate the packets. Another type of packet forwarding attack is denial-of-service (DoS) attack through network-layer packet blasting, in this type of attack attacker inserts large amount of junk packets in network. Due to this action significant portion of the network resources are wasted, and introduce severe wireless channel contention and network congestion in the network.

There are identified vulnerabilities of the link-layer protocols, especially in the IEEE standard 802.11 MAC protocols [3], for mobile ad hoc network. It's true that 802.11 WEP is vulnerable to different types of cryptography attacks by misusing the cryptographic primitives [10]. The IEEE 802.11 protocol is vulnerable to many DoS attacks due to this way it targeting reservation schemes and channel contention. The attacker exploits binary exponential back off scheme in order to deny access to the wireless channel from its local neighbors [11, 17].

3.5 Routing Attacks

Generally there are four different types of MANET routing protocol attacks which is divided in to two main types which are given below:

1. Routing disruption attacks [13][14]
2. Resource consumption attacks [13][14]

In case of routing disruption attacks, the main task of attacker is to disrupt routing process by routing packets in order to introduce wrong paths. In case of resource consumption attacks are concerned the main task of the attacker is to introduce some non-cooperative or selfish nodes that can be used to inject false packets due to this way

load on the network increases and it will become a cause of consuming network bandwidth.

Mainly both of these attacks in MANET routing protocols are the best examples of Denial of Service (DoS) attacks. In Figure 3.3 there is a broader classification attacks in MANET routing protocols which are given below.

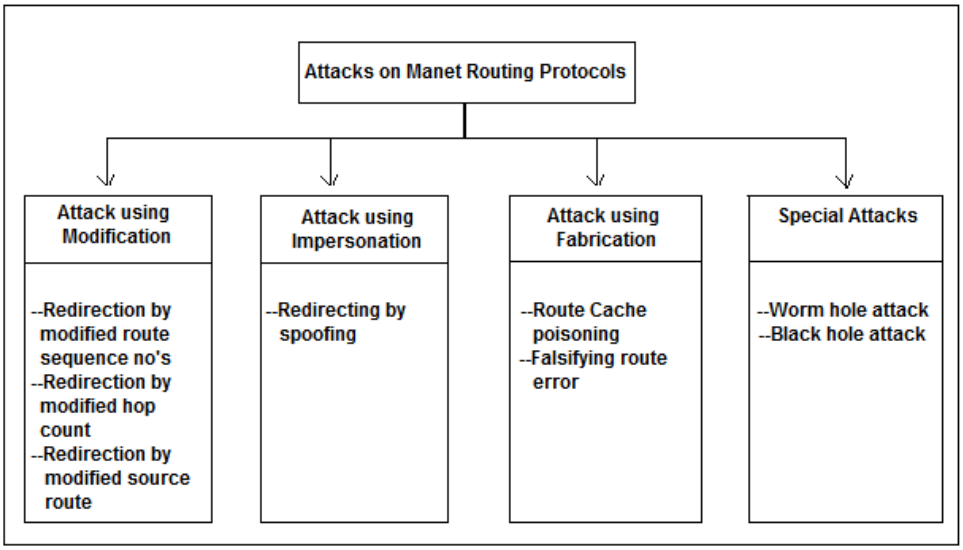

Figure 3.3 Classification of attacks on MANET routing protocols [13]

3.5.1 Attacks using Modification

In case of modification type of attacks some of the messages in the protocol fields are modified and then these messages passed among the nodes, due to this way it become the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks. There are some of these types of attacks are given below:

3.5.1.1 Route sequence numbers modification

In this type of attack which is mainly possible against the AODV protocol. In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

3.5.1.2 Hop count modification attack

In this type of attacks where it is also mainly possible against the routing protocol AODV, here attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

3.5.1.3 Source route modification attack

In this type of attack which is possible against DSR routing protocol where attacker (malicious node) modify source address and move traffic towards its own destination. In Figure 3.4 the mechanism is defined, where the shortest path between source S and destination X is defined (S-A-B-C-D-X). Which shows that node S and the node X cannot communicate each other directly, and in the scenario (3.4) where the node M which act as a malicious node which are going to attempt a denial-of-service attack. Let suppose that the node S which act as a source try to send a data packet towards the node X but if the node M intercept the packet and remove the node D from the list and the packet forward towards node C, where the node C will try to

send the picket towards the distention X which is not possible because the node C can't communicate with X directly, Due to this way the M node has successfully established a DoS attack on X.

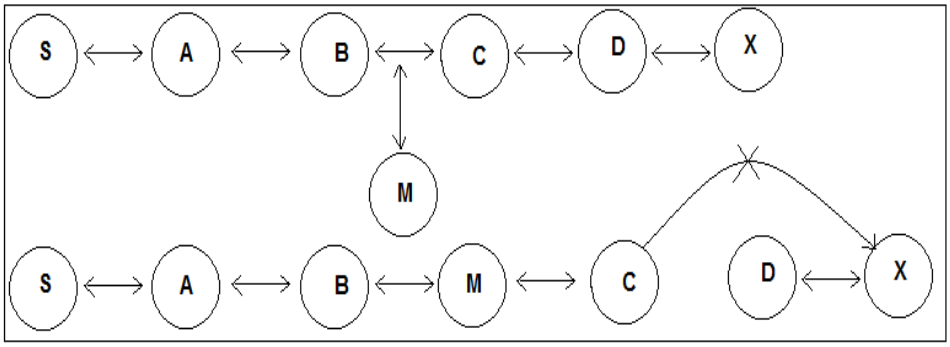

Figure 3.4 an example of route modification attack [13]

3.5.2 Attacks using Impersonation

In this type of attacks where attacker is used to violates authenticity and confidentiality of a network. In this attack an attacker (i.e. malicious node) uses to impersonate the address of other user node in order to change the network topology. This type of attack can be described in the Figure 3.5 given below:

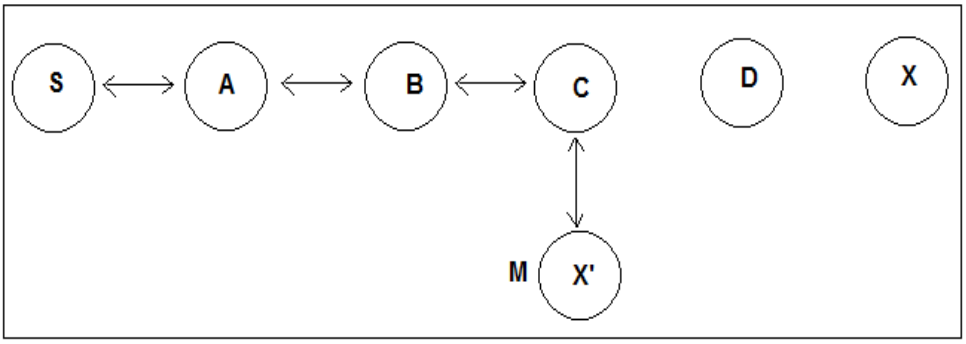

Figure 3.5 Type of impersonation attack [14]

In the above figure where the S node wants to send data towards the node X and before sending data to node X it starts a Route Discovery process. During route discovery process there is a malicious node M, when it receive route discovery packet regarding the node X then it modify its address and change to node X, like impersonates node X as X'. After that it send packet back to source node S that I am the destination node by RREP packet request. When the source node receives RREP packet information it doesn't authenticate node and accept the route and send data to the malicious node. This type of attacks also called routing loop attack which will become the cause of loops within the network.

3.5.3 Attacks using Fabrication

In this type of attacks, where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. The fabrication attacks are very much difficult to detect in the mobile ad hoc network. Attacks using fabrication process are discussed very well in [20] and [21]. In Figure 3.6 where fabrication attacks is explained by an example. In the example where the source node S wants to send data towards the destination node X, so therefore at start it sends broadcast message and request for route towards the destination node X. An attacker as a malicious node M try to pretends and modify route and returns route reply to the node (S). Furthermore, an attacker's nodes use to fabricate RERR requests and

advertise a link break nodes in a mobile ad hoc network by using AODV or DSR routing protocols.

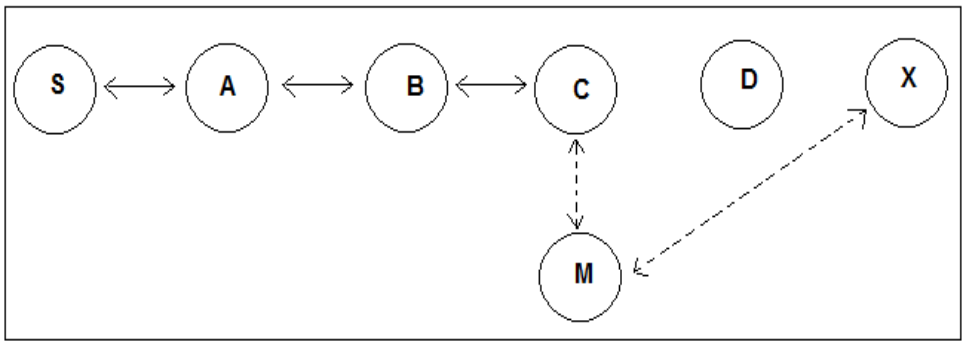

Figure 3.6 Fabrication attack example [14]

3.5.4 Special Attacks

There are also some other severe attacks in MANET network which are possible against routing protocols such as AODV and DSR.

3.5.4.1 Wormhole Attack

The wormhole attack [15] is one of the severe types of attack in which an attacker introduces two malicious nodes in the network where an attacker used to forward packets through a private "tunnel". This complete scenario described in Figure 3.7 which is given below:

3.5.4.2 Black hole attack

This kind of attack is described very well in detail in [21]. In this type of attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other.

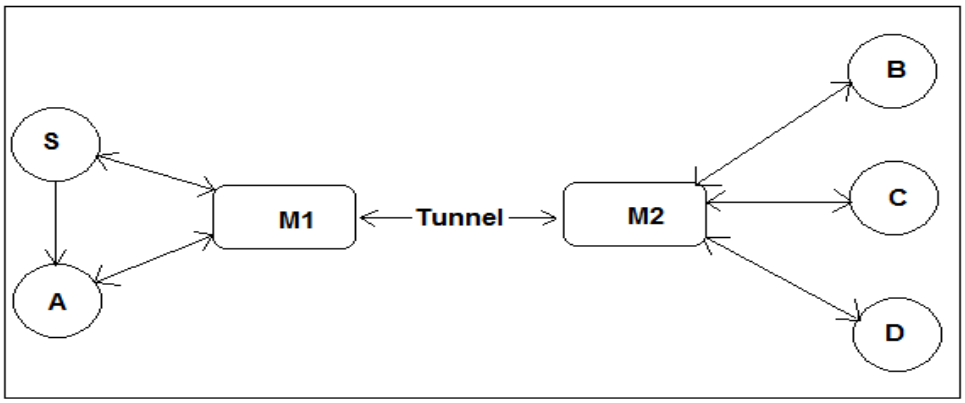

Figure 3.7 Wormhole attack example [15]

In the above example where there are two malicious nodes M1 and M2 which link through a private connection. In this type of attack every packet which an attacker receive from network 1 forward to other network where another malicious node exist, simple speaking these two nodes use to exchange network information and fabricate traffic among each other. The traffic between the two nodes passes through "wormhole" among each other. Due to this way it will become the cause of disrupts routing protocols and violating normal flow of routing packets. These types of attacks are very difficult to detect in a network, and become the cause of severe damages to the nodes. These types of attacks can be prevented by using mechanism packet leashes

[15], which are used to authenticate nodes among each other by timing information process.

3.6 Security steps to avoid Attacks in MANET

3.6.1 Secure Multicasting

Multicast is a mechanism where any user become the part of multicast group and even send traffic to the multicast users as well as receive traffic, but due to this procedure it can easily fall into denial of service attacks (DoS). There is an architecture usually used to secure multicast traffic that is DIPLOMA. DIPLOMA stands for DIstributed Policy enfOrceMent Architecture which is use to protect or secure end user services as well as network bandwidth. Audio and video traffic usually fall into the category of multicast traffic which is usually use by militaries as well as disaster backup plans (teams). There are some of the major responsibilities of DIPLOMA architecture which are given below [16].

- It gives solution for both sender and receiver whenever they access to the multicast group.
- It also used to limit the bandwidth.
- DIPLOMA integrates with common multicasting routing protocols like PIM-SM and ODMRP.
- It also uses to provide (allocate) network resources in a fair manner during attacks.

3.6.2 Secure routing

MANET is a self organized wireless network, due to the fact it has vulnerable attacks that can easily damage the whole network; that's why there should be some solutions which works even some of the mobile nodes compromised in the network. One of the primary challenges of secure routing is to provide authentication (trustworthiness) of users in the network. In case of distributed communication environment in MANET, authentication is open and any un-authentic node may be use to compromise routing traffic in order to disrupt the communication. There are some of the major responsibilities of secure routing which are given below.

- It provides assurance that modified and replayed route replies should be rejected in order to avoid fabrication of attacks.
- Routing protocol responsiveness itself provide safety among different routing attacks.

In section [17] there is detail description of secure routing mechanism and in our simulation we also worked on the authentication mechanism in MANET.

3.6.3 Privacy-aware and Position based Routing

MANET is a kind of wireless network in which mobile nodes move from one station to another. In this type of network environment routing process among different nodes is important that's why privacy-aware and position based routing is used to avoid route overhead. In case of position based routing mechanism, a mobile node within the MANET network broadcast its position co-ordinates as well as its one-hop neighbors. This information can easily be attacked, so therefore privacy-aware mechanism is together with position based routing in order to provide secure communication. PPBR stands for privacy aware and position based routing in which a mobile node mainly takes pseudo identifiers that are usually dynamic and it is also use to provide end-to-end inconspicuousness to other nodes.

3.6.4 Key management

Certified Authority (CA) is one of the mechanism which provide key management; if it is compromised then entire network can easily be damaged. One of the major functionality of key management and distribution for MANET, it provide solutions for mobility related issues. In section [19] writers discuss different aspect of key management and distribution for MANET. In the paper, the approach for key management use to solve high mobility issue as well as it provide an efficient method to reduce control overhead also gives an idea how to increase reliability in key management with respect to conventional key management process.

3.6.5 Intrusion detection System

Intrusion detection system is a complete security solution which provides information about malicious activities in the network, it also uses to detect and report about malicious activities. MANET is also design for route traffic mechanism when there is congestion in the network, faulty nodes as well as topology changes due to its dynamic behavior. IDS use to detect critical nodes and then analyze its data traffic, critical node also degrade network performance. There are different IDS systems which has some specific features, some of them are given blow

- Cluster based voting
- Neighbor-monitoring
- Trust building

For detail description of these IDS system see section [20].

3.6.6 Multi-layer Intrusion detection technique

Multi-layer intrusion detection technique is a technique in which an attacker attacks at multiple layers in order to stay below the detection threshold so that they will escape easily whenever a single layer impropriety detects. These type of attacks mainly attack at cross layer which are more alarming and frightening as compare to single layer attack and they can easily be escaped. Although these type of attacks can be detected by a multiple layer insubordination detector, where with respect to all network layer's input are use to combine and examine by the cross-layer detector in a detailed fashion. There is also another way to detect these kinds of attacks by working together with RTS/CTS and network layer detection with respect to dropped packets.

Chapter 4
Performance Evaluation & Design

4 PERFORMANCE EVALUATION & DESIGN

4.1 OPNET usability

One of the most common methods is to conduct research in the fields of networking as well as security is to simulate and evaluate the routing protocol(s) in different kinds of network based scenarios. We know that there are different kinds of network as well as computer simulation software's or applications are available in order to perform these kinds of research tasks for example NS-2 [24], OPNET [25], etc. Our thesis is mainly based on two tasks, one is concern with theoretical study and the other one is based on the implementation and experiments of the MANET in security which we perform in OPNET simulation environment. We are using the Optimized Network Engineering Tool (OPNET) software for our simulations. It is a network simulator which is used to provide multiple solutions for managing networks and applications e.g. research and development (R&D), network operation, network engineering, planning and performance management. It is designed for modeling of different communication devices, technologies, protocols and in order to simulate performance of these technologies.

Now a day OPNET is one of the most powerful and very useful software in research fields. The OPNET usability is divided into four main steps

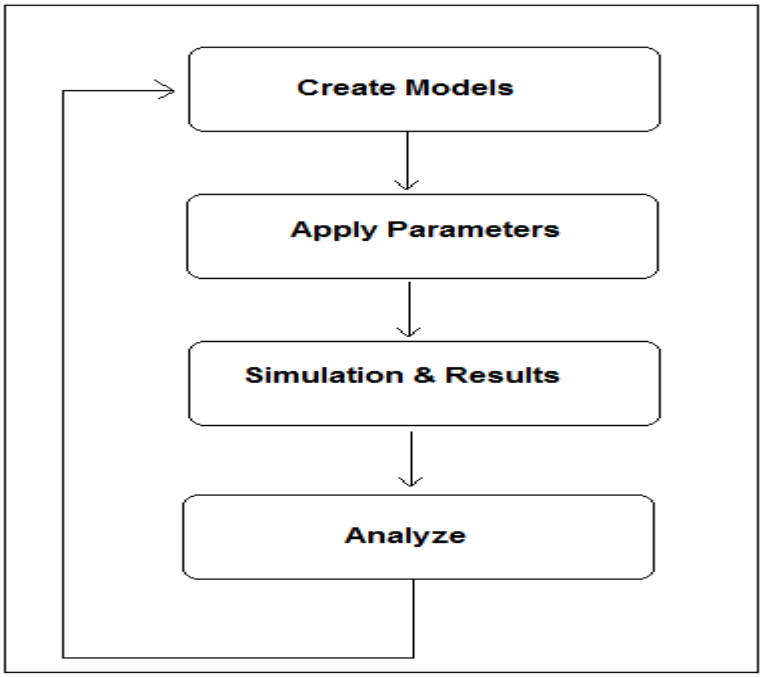

Figure 4.1 Flow chart of OPNET

OPNET provides solutions for the academic research and provide assessment and improvement of different wireless network technologies such as:

- WiMAX (Worldwide Interoperability for Microwave Access)
- Wi-Fi, UMTS (Universal Mobile Telecommunications System)
- Seamless communication
- Design and assessment of MANET protocols
- Analysis of optical network
- Enhancement in the core network technologies like IPv6, MPLS etc
- Power management schemes in wireless sensor network [5]

4.2 Security Metrics Review

Certain metrics are required in order to review a routing protocol. Those metrics can be qualitative and quantitative. Suitability and performance can be called as the key factors of these metrics. Here are some quantitative metrics which can be used to evaluate the performance of routing protocol [9].

1. End-to-end load, throughput and delay
2. Packet sent and received
3. Download response time
4. Efficiency

It is useful to track several ratios that illuminate the internal efficiency of a protocol in doing its job:

1. Average number of data bits transmitted/data bit delivered
2. Average number of control bits transmitted/data bit delivered
3. Average number of control and data packets transmitted/data packet delivered

Also, we must consider the networking context in which a protocol's performance is measured. Essential parameters that should be varied include [10]:

1. Network size: It is used to measure the number of nodes.
2. Network connectivity: It is use to measure the average number of neighbors of a node.
3. Topological rate of change: It is mainly concern with the speed with which network's topology changes.
4. Link capacity: It is used to measure an effective link speed in terms of bits/second.
5. Fraction of unidirectional links: It is used to measure that how effectively protocols perform its function in the presence of unidirectional links?
6. Traffic patterns: It concern that how effective a protocol is used in non-uniform or bursty traffic patterns?
7. Mobility: It deals with temporal and spatial topological correlation relevant to the performance of a routing protocol.
8. Fraction and frequency of sleeping nodes: It concerns with protocol that how it performs in the presence of sleeping and awakening nodes?

Chapter 5
OPNET Simulation

5 OPNET SIMULATION

5.1 Task

The main task of this chapter is to perform the empirical study which is based on OPNET simulation and we also implement some of the solutions e.g. comparative study of routing protocols with respect to security, security threats within MANET like intruder behavior, tapping, integrity , MANET link layer and network layer operations with respect to information security.

In this section of the report, we also discuss different number of scenarios of MANET network which we implement in our simulation. In our simulation we use to implement different routing protocols and also did comparative study of them, that which one is better with respect to different aspects; which is use to analyze the behavior of the MANET routing protocols as well as how it work in security environment with respect to different performance metrics parameters which are given below:

- Delay,
- Load (bits/s and packets/s), and
- Throughput (bits/s and packets/s)
- Page response time

We will implements mechanisms of intruder behavior (tapping and integrity). Its true integrity protection is important, without integrity an attacker can perform following attacks:

- It can destroy messages.
- It can even manipulate packet headers in order to control traffic.
- It can also generate wrong way traffic.

In the end we will implement MANET link layer and network layer operations with respect to information security. According to security aspect of Mobile ad hoc networks, it can be protected in the link layer or network layer. It is also true that link layer provide strong security services.

5.2 Network Design

In this section we discuss different network designs with respect to our simulation and there are different terminologies which we use in the OPNET module. We also have different scenarios as well as network topologies which we will discuss.

5.2.1 Network Scenarios

In case of network scenarios are concerned there are almost seven different network scenarios which we implement in OPNET module. First three network scenarios are concerned with MANET routing protocols, it will concern with the comparison of delay, load and throughput with respect to each other routing protocols. In the fourth network scenario we concerned with the mechanism of an intruder where we bypass an intruder from the network and there will no use of traffic which we use in our network like FTP traffic and the main task of fourth scenario is to provide an authenticity. The most important aspect in Mobile ad hoc networks is to provide an access control: there should be a method in the network which uses to restrict the access of un-authentic user's node to the network. Moreover, whenever there is a valid communication between the inside nodes among each other in the network, then it should be protected from intruder attacks on confidentiality. In the last three scenarios we implement information security mechanism by implementing firewall and VPN and compare our results with respect to the without firewall and also with each other.

If there is a threat regarding information security with respect to routing traffic then adversary (attacker) would be in a position to identify or in order to locate other mobile nodes in the network by monitoring the routing traffic, which usually mobile nodes send and forward to each other. For instance, we should ensure physical security in the network because in case of web-based intranets where firewalls, proxies, VPNs or any other centralized elements among secure and non-secure domains are single points of failure. There are seven different network scenarios which we implement in our OPNET simulation and they are given below:

1. MANET with DSR routing protocol.
2. MANET with TORA routing protocol.
3. MANET with AODV routing protocol.
4. MANET with routing protocol with respect to security parameters with an intruder.
5. MANET with routing protocol without firewall.
6. MANET with routing protocol with firewall.
7. MANET with routing protocol with firewall as well as with VPN.

5.2.2 Network Topology

According to network topology a physical communication among different network devices and follow scheme consisting of connected devices is known as network topology. All the below scenarios which we discuss below are following the same mesh type of network topology.

5.2.2.1 Network Scenarios Descriptions

In the below following figures there are some of the block diagrams of the network scenarios which we mention above.

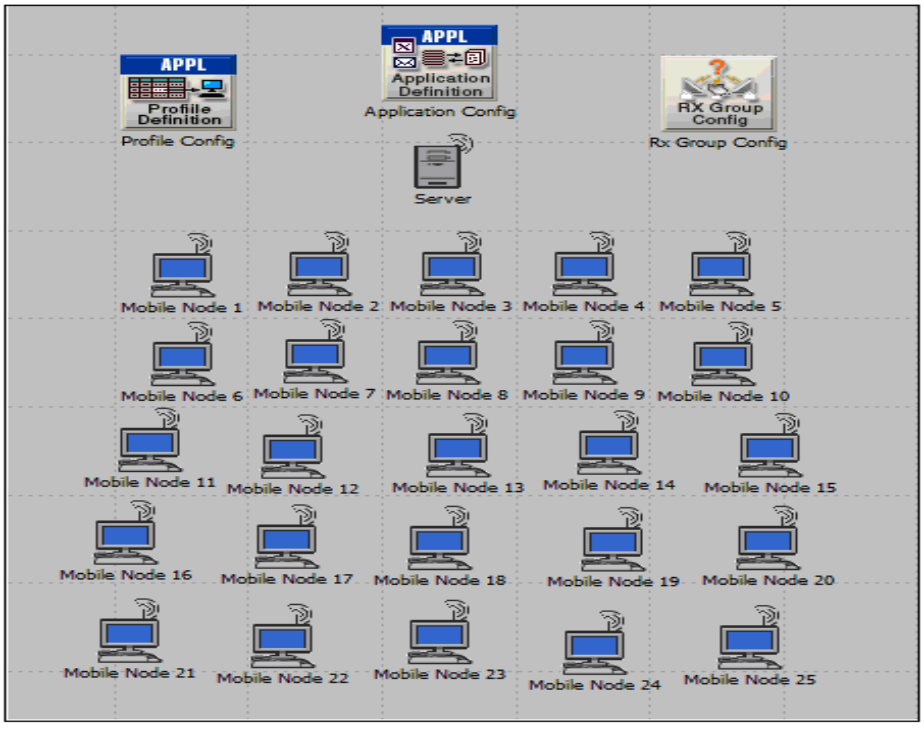

Figure 5.1 Network topology having 25 wireless mobile nodes and an FTP Server.

In figure 5.1 we implement first three scenarios with different routing protocols with profile config, application config and Rx Group config and server for communication and also use 25 mobile nodes for wireless communication. All these devices are explained well in the below network component section. All nodes in the network are configured to run AODV, DSR, and TORA routing protocol one by one in the first three scenarios respectively; and we also use to configure FTP traffic for our

result observations. The Rx group config node is added to speed up the simulation. It is configured to eliminate all receivers that are over 1500 meters away. In case of AODV scenario, AODV parameters are used as suggested by RFC and WLAN data rate is 1Mbps.

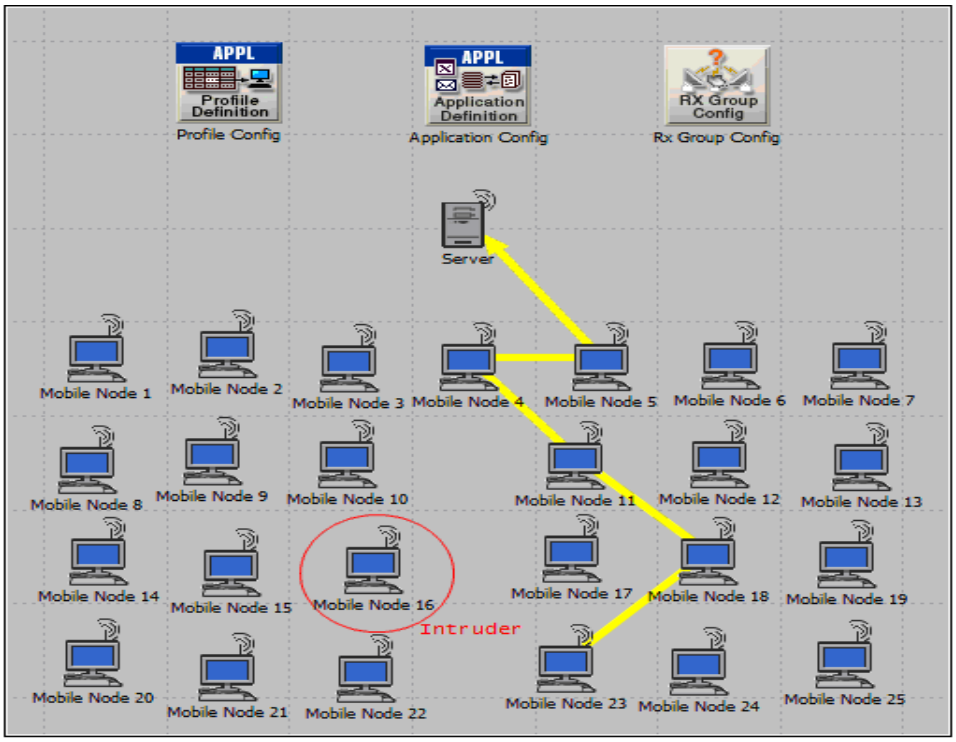

Figure 5.2 Network topology having 25 wireless mobile nodes with an intruder

In figure 5.2, second most important scenario with respect to security policy implementation, in this scenario we use an intruder which is an un-authentic user, how a network would be safe and secure in different network attacks by an intruder. We discussed all these issues in this scenario. In above figure there is a yellow line between server and different mobile nodes (mobile node 5, mobile node 4, mobile node 11, mobile node 18 and mobile node 23 respectively), which is mainly use to represent path of traffic with respect to different mobile nodes towards server. In this scenario we also implement security demands mechanism in order to permit (the demands are expected to reach destination) and deny (the demands are expected to be blocked) to full mesh between server and all mobile nodes. According to socket information is concerned source IP address and destination IP address is the same as the source and destination node and we also use best effort as a type of service. According to source port and destination port is concerned ftp-data considered to be permitted or denied and only IP protocol traffic keep in mind.

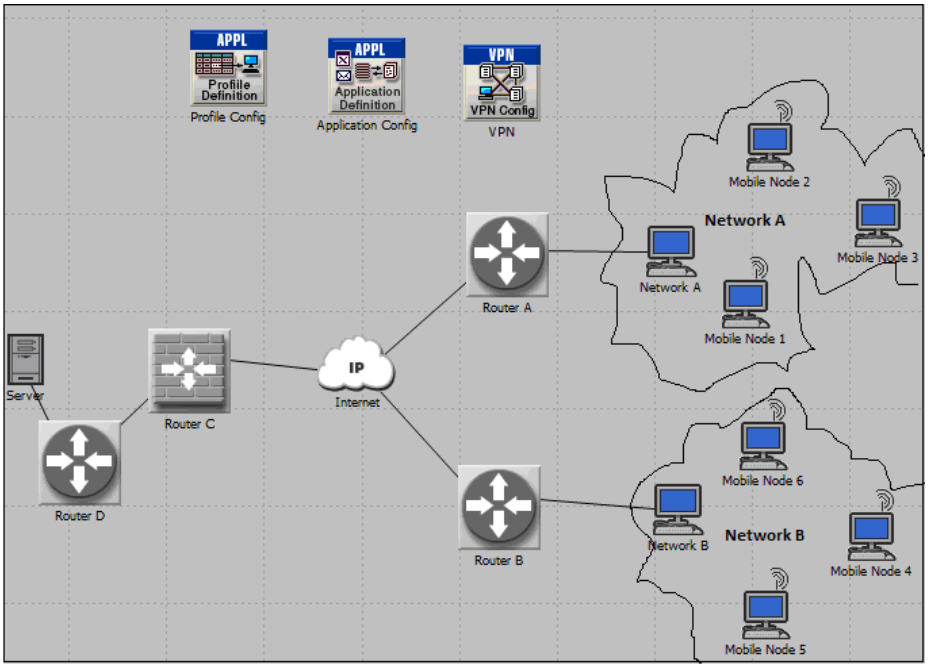

Figure 5.3 Network Topology of two networks connected with IP Cloud (VPN) having Firewall at router C.

In figure 5.3 we implement two mobile ad hoc networks which are sharing information through internet and how we make information secure that's the main task of last three scenarios. In the first scenario we implement network scenario without firewall and VPN and how will we make network free of information security we will discuss this in the next two scenarios.

In the next scenario in which we implement our network scenario with firewall setting and we also compare our result with the previous scenario where we implement our scenario without firewall network settings. In the firewall scenario, firewall (Router C) use to configure IP Forwarding Rate, IP Gateway Function, RIP Start Time, RIP Process Mode and Proxy Server Information mechanisms.

In the last scenario, we implement the secure information mechanism by comparing our results. In this scenario we implement firewall as well as VPN network configuration in order to secure our information and safe our communication. In VPN scenario, it configures Virtual Private Network (VPN) attribute configuration details for tunneling supported at the IP layer.

5.2.2.2 Network Components

In the above simulation model there are different types of network components are used and these are given below:

- There are 25 Wlan workstations with mobile node type are used in first four network scenarios. The Wlan workstation node model represents a workstation with client-server applications running over TCP/IP and UDP/IP. The workstation supports one underlying Wlan connection at 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps. This workstation requires a fixed amount of time to route each packet, as determined by the "IP forwarding rate" attribute of the node. Packets are routed on a first come first server basis and may encounter queuing at the lower protocol layers, depending on the transmission rates of the corresponding output interfaces.

- There is one Wlan server with mobile node type is used. The Wlan server model represents a server node with server applications running over TCP/IP and UDP/IP. This node supports one underlying IEEE 802.11 connection at 1 Mbps or 2 Mbps. The operational speed is determined by the connected link's data rate.

- There is one application configuration model is used in the network topology. The application config node can be used for the following specification.
    1. ACE Tiers information
    2. Application spécification
    3. Voice encoder schèmes

- There is also one profile configuration model is used in the network topology. The profile config node can be used to create user profiles. These user profiles can then be specified on different nodes in the network to generate application layers traffic.

- There is also one dynamic receiver group config node is used in the network model. The dynamic receiver group configuration node is used to compute the set of possible receivers that nodes can communication with. It is computed based on the following three criteria:
    1. Channel match
    2. Distance threshold
    3. Path loss threshold

    All possible receivers that have a channel match with the transmitter channels and fall within the distance and path loss threshold and receivers that a node can communicate with.

- The network (A & B are actually ppp_wkstn) node model represents a workstation with client-server applications running over TCP/IP and UDP/IP. The workstation supports one underlying SLIP connection at a selectable data rate. This workstation requires a fixed amount of time to route each packet, as determined by the "IP forwarding rate" attribute of the node. Packets are routed on a first-come-first-serve basis and may encounter queuing at the ports, depending on the transmission rates of the output interface.

- The router (A, B, C are actually ethernet4_slip8_gtwy devices) node model is use to represent a router and it is also use to represent an IP based gateway supporting almost four different Ethernet hub interfaces, and eight serial line interfaces. IP packets arriving on one of the interface and then forward to destination output interface based on their destination IP address. There are two protocol uses to route traffic that may be used to dynamically and automatically create the gateway routing tables and then select rules and apply rules according to adaptive manner. This gateway requires fixed number of time to route traffic to route each packet as determined by the IP routing speed attribute of the node. This gateway is also use to route packet in a fixed amount of time and all these packets are used on first come first serve basis and they can even encounter queuing at lower layers. It also supports 4 Ethernet hub connections and 8 serial line IP connections.

- In our last three scenarios we use IP cloud model which is used to represents an IP cloud supporting up to 32 serial line interfaces at a selectable data rate through which IP traffic can be modeled. In IP cloud traffic arrive at any interface and then forward to output interface and it is based on the destination IP address.

- We also use another kind of router which is actually ethernet2_slip8_firewall and that firewall node which is use to represent an IP based gateway with firewall features and server support. It supports more almost two Ethernet and eight serial line interfaces at selectable data rates. IP packets can arrive on any interface but it only forward to those destination interfaces where destination IP address matches. It also supports one Ethernet connection with respect to data rates and also support one serial line IP again with respect to data rate. There are different attributes of firewall like IP forwarding rate, IP gateway function, Proxy server information etc.

- We also use an IP VPN node which is used to define a virtual private network (VPN) attribute configuration details for tunneling supported at the IP layer.

Chapter 6
Result & Analysis

6 RESULT & ANALYSIS

At start of results and analysis we like to discuss little bit about our scenarios and how it is useful in case of security. We already know that we have seven scenarios in our simulation. In the first three scenarios in, which we discuss performance behaviors in the network. If there is load on the network and lots of delay in the network and minimum throughput then for such kind of network it's an easy for an intruder to introduce DoS attacks in the network. It's true that delay, load and throughput have indirectly impact on the network with respect to security. If we don't care about these simple but important features then definitely we have to face major problems with respect to security.

In the fourth scenario where we discuss the behavior of an intruder in the network and how we block its accessibility and avoid its communication among the network and provide security to our information?

In last three scenarios, where we implement two important mechanisms of security firewall and VPN. The main task of these features is to provide information security.

6.1 COMPARATIVE STUDY OF ROUTING PROTOCOLS

6.1.1 Throughput among AODV, DSR and TORA

The network throughput and load are main parameters that are use to reflect the network capability. If we define Load then we come to know that it is the amount of traffic entered to the "Network". In contrast, if we define throughput then we come to know that it is the amount of traffic that is leaving the "Network". We measure both these statistics in bits per second unit.

We measure the statistics in bits per second unit. If we look at the graph then we come to know that AODV has high throughput as compare to DSR and TORA. After that DSR is on the second and TORA respectively on third. As we know that throughput use to describe loss rate which usually seen on transport layer. The graph reflects completeness; it also shows accuracy of the routing protocol. It is also clear that throughput is inversely proportional to mobility i.e. throughput decrease and on other side mobility increase. If there is high load traffic then packet drop, in case of high mobility TORA performs better but in other cases it has low throughput. AODV shows best performance in case of throughput.

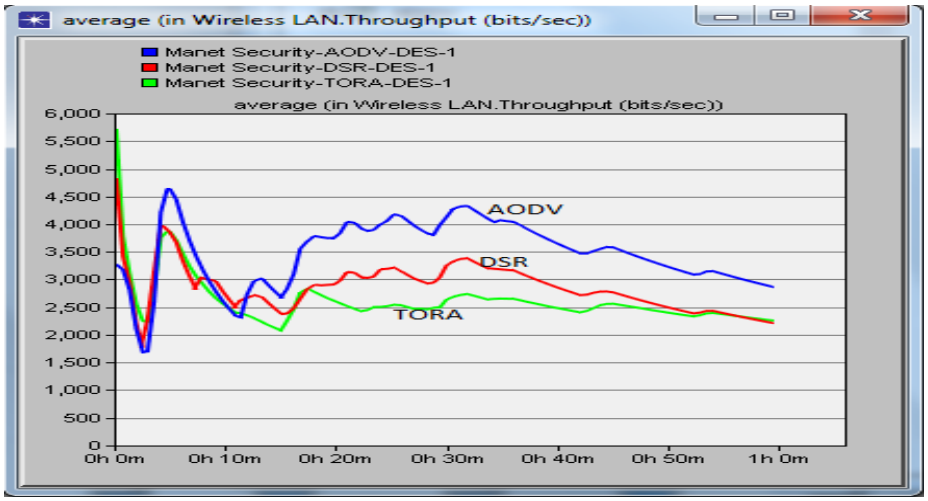

Figure 6.1 Throughputs among DSR, AODV and TORA

6.1.2 Delay among AODV, DSR and TORA

This statistic gives the End-to-End delay for traffic through an AODV, DSR and TORA. This delay is measured as time elapsed between traffic entering the "Network" through one of the routing protocols and traffic leaving the "Network" through the same routing protocol. We run our simulation up to maximum one hour. Generally if we look at the graph then we can conclude that AODV has low delay as compare to the DSR and TORA while DSR has high load as compare to the other routing protocols.

DSR and TORA show poor delay due to the reason of its routes because typically their routes are not the shortest. At start of route discovery phase; their routes are not shortest over a period of time due to its node mobility. AODV shows low delay and even it can be better with some fine-tuning.

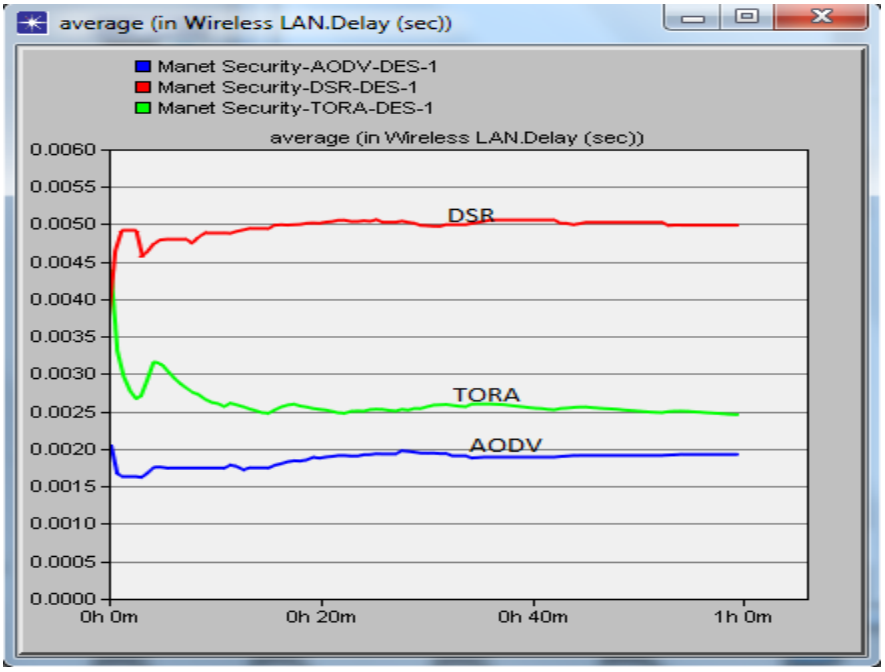

Figure 6.2 Delays among AODV, DSR and TORA

6.1.3 Load among AODV, DSR and TORA

If we look at the graph then we come to know that TORA has low traffic load as compare to the other routing protocols and on the other side AODV and DSR both overlapping each other during simulation time domain, sometimes AODV has high load and sometime DSR has high load. In the next chapter in table 7.1 we come to know exactly the difference.

In case of load TORA's performance is very impressive due to its substantial work to erase routes even when those routes are not in use; we know that TORA shows good performance for small networks with high mobility. AODV also perform well as compare to DSR because byte overhead and packet overhead of AODV are less than DSR's overhead. DSR has high load because of high number of its route discoveries and wide flooding network discovery.

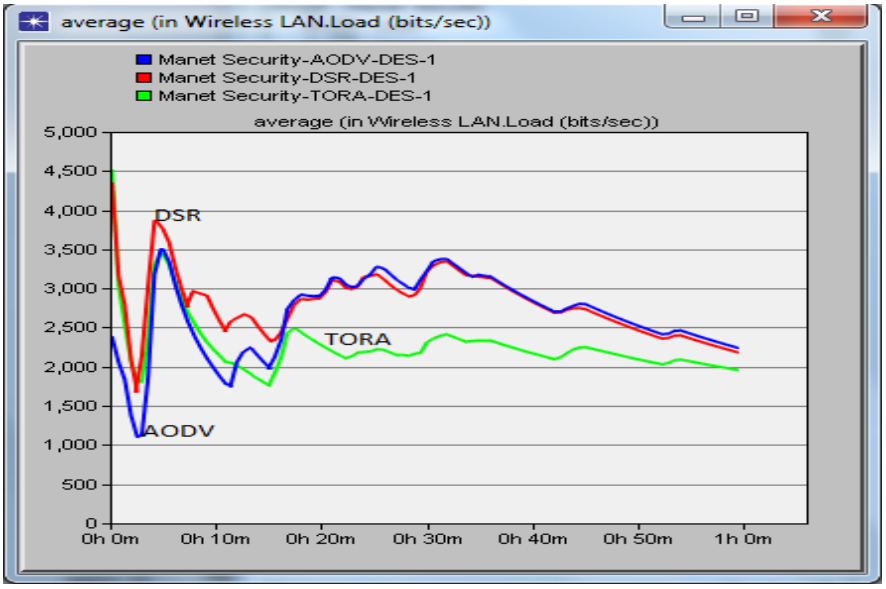

Figure 6.3 Loads among AODV, DRS and TORA

6.1.4 Traffic sent among AODV, DSR and TORA

In case of traffic received among the three different routing protocols AODV, DSR and TORA we see traffic intensity among them as compare to the traffic sent. Here traffic receives and traffic sent is mainly concerned with ftp traffic. If we look at the below figure then we come to know that again DSR has high traffic sent as compare to other two routing protocols, after that AODV and TORA respectively.

If we look at table 7.1 then we come to know that traffic sent is equal to traffic receive because it is an FTP traffic which is working on TCP protocol (aim to avoid completely data loss). There may be possibility of delay, load etc during data transfer which we already discuss above. DSR control messages gets loss and it also eliminating one of the advantage of fast establishing new route. Due to such reason it has a relatively high delay then AODV as well as TORA. In most cases, both the packet overhead and the byte overhead of AODV are less than of DSR and TORA overhead.

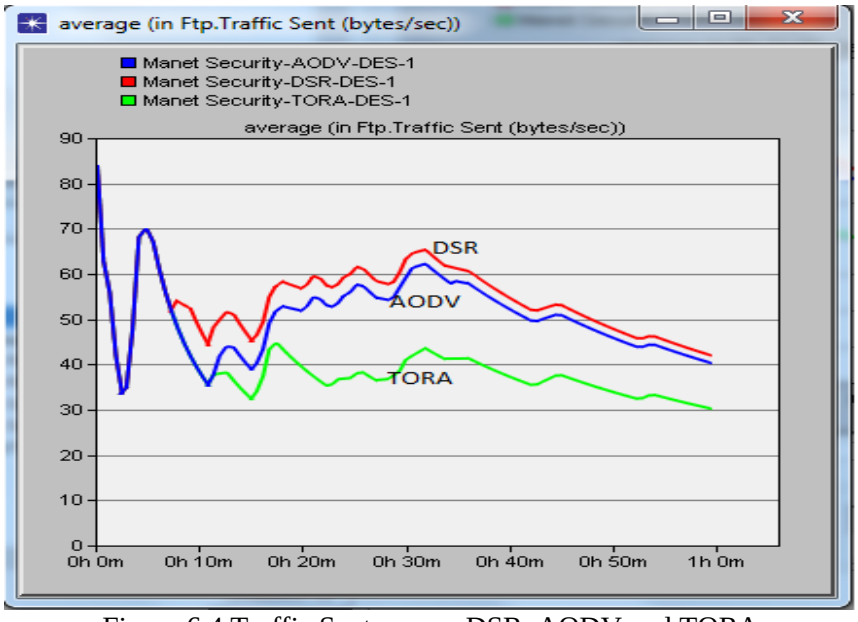

Figure 6.4 Traffic Sent among DSR, AODV and TORA

6.1.5 Traffic received among AODV, DSR and TORA

If we look at the below figure then we come to know that DSR has high traffic as compare to other two routing protocols, after that AODV and TORA respectively.

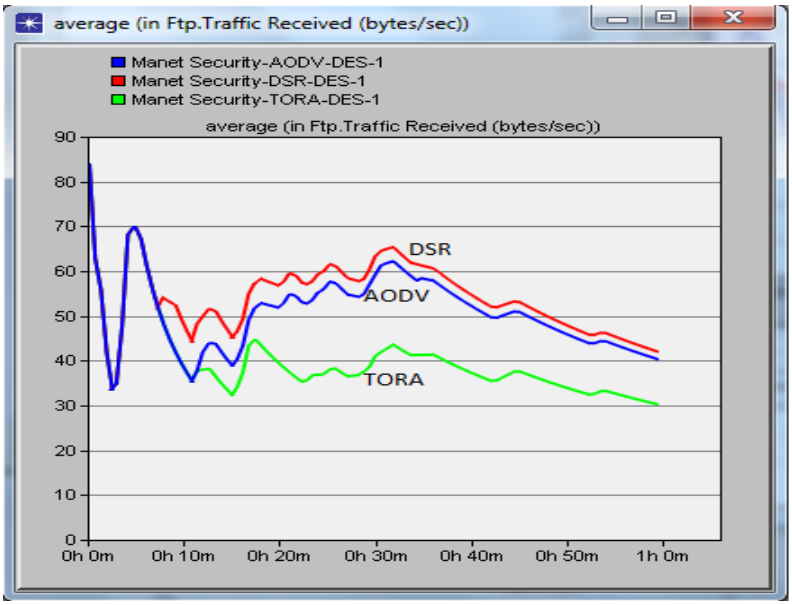

Figure 6.5 Traffic received among DSR, AODV and TORA

6.1.6 Download response time among AODV, DSR and TORA

In the last graph we see download response time during file transfer procedure. In the below figure it is stated that AODV has high download response time and then TORA and DSR respectively.

AODV is a hop-by-hop routing protocol, due to the fact it has better downlink response time. Source routing approach has one very tremendous advantage that is its route discovery process because it learns more routes. Whenever a network has high speed, high mobility and low throughput then in such cases TORA performs better as compared to AODV and DSR.

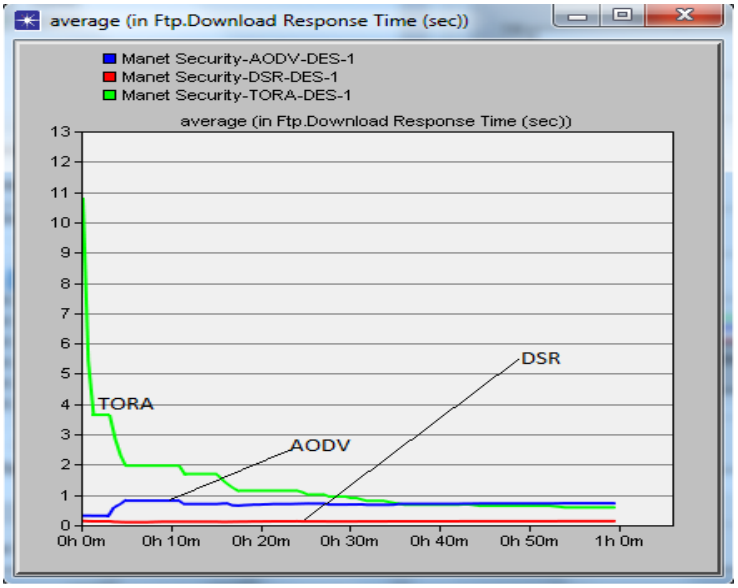

Figure 6.6 Download response time among DSR, AODV and TORA

6.2 INTRUDER BEHAVIOR (INTEGRITY ASPECT)

6.2.1 Network route discovery map (before Intruder)

In figure 6.7 (A) it is shown complete network route discovery map before intruder. There are different colors which used to represent route map towards server (node_0). Each node forwards its data to its nearest node and even node can communicate with each other. Once a complete network route discover then each node can communicate with respect to its route. If any node disappeared from the network then again route map re-allocation procedure allocate new routes in order to avoid distortion of communication.

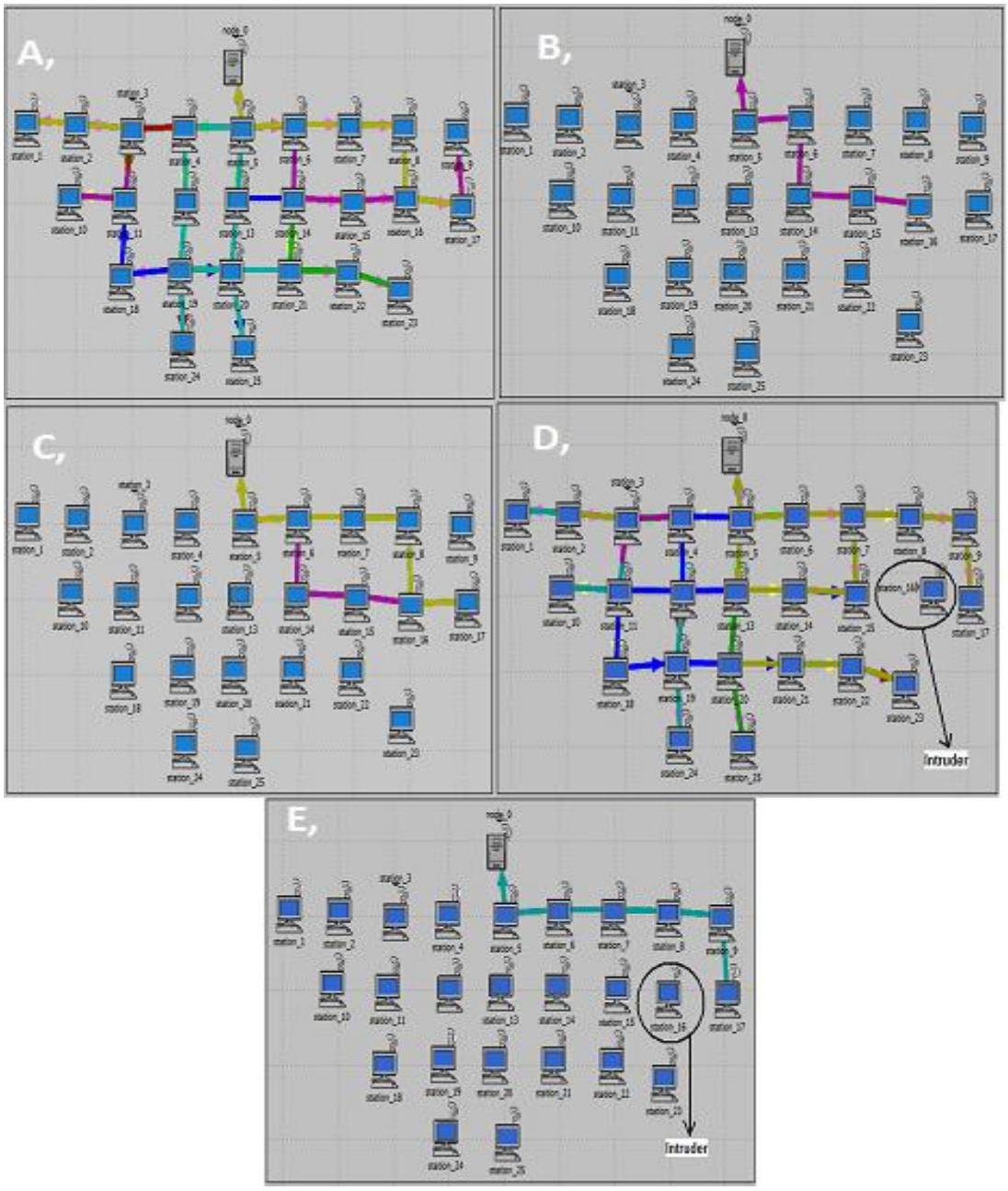

Figure 6.7 Network route discovery map

In figure 6.7 (B) shows network route discovery map from node 16 towards server. Here its only represent that how node 16 communicate with server and even other nodes like 15, 14, 6 as well as node 5 also using the same route for communication towards server.

In figure 6.7 (C) shows network route map from node 16 and node 17 towards server. Each routing protocol route discovery method is different from each other which we already discuss in the above discussions results. If one node is missing from the network and many routes depend on it then for communication re-route methods discover new routes; like in figure 6.7 (C) at node 17 is depends on node 16 because all of its data pass through it and even node 16 also depends on each node which helps its data towards server.

6.2.2 Network route discovery map (after Intruder)

In figure 6.7 (D) shows an intruder in the network and once an intruder allocate in the network then its block by the server for security by using Net Doctor and security demands in order to avoid intruder behavior from the network. Once server finds an intruder then it will develop complete network route discover map among nodes. It is also shown below complete route map without node 16.

In figure 6.7 (E) shows a route map from node 17 to server node. If we compare figure 6.7 (E) to figure 6.7 (C) then we come to know that before all traffic of node 17 pass through the node 16 but once server finds node 16 is an intruder then it will re-allocate its route and all of traffic of node 17 pass through node 9 as well as node 8, 7, 6, and 5.

6.2.3 Traffic sent and received at an Intruder

If we look at the Figure 6.8 then we come to know that there we have a network scenario where we deal with an intruder. Once we come to know that its an intruder and try to damage our network then through security demand mechanism we block complete application traffic at intruder mobile node because our security system tells us that its an intruder and it should be blocked in the network so that's why in the below diagram you will come to know that there is no traffic sent as well as receive at node 16 which we declare as an Intruder node. This is one of the way through which we avoid intruders in the network and try to make our network safe and secure. One more thing we like to add is that its application traffic for example FTP traffic. By using security demand procedure we blocked its application traffic so that there will be no miss use of the network recourses as well as network information among the users and here we are not talking about the overall traffic.

In Figure 6.9 we see that traffic sent and receive at node sixteen before intruder. In the following figure we have two graphs traffic sent and traffic receive; we come to know that there is activity with respect to traffic in and traffic out before discovery of an intruder. In Figure 6.9 we run our simulation up to two hours because after two hours traffic comes in a constant behavior.

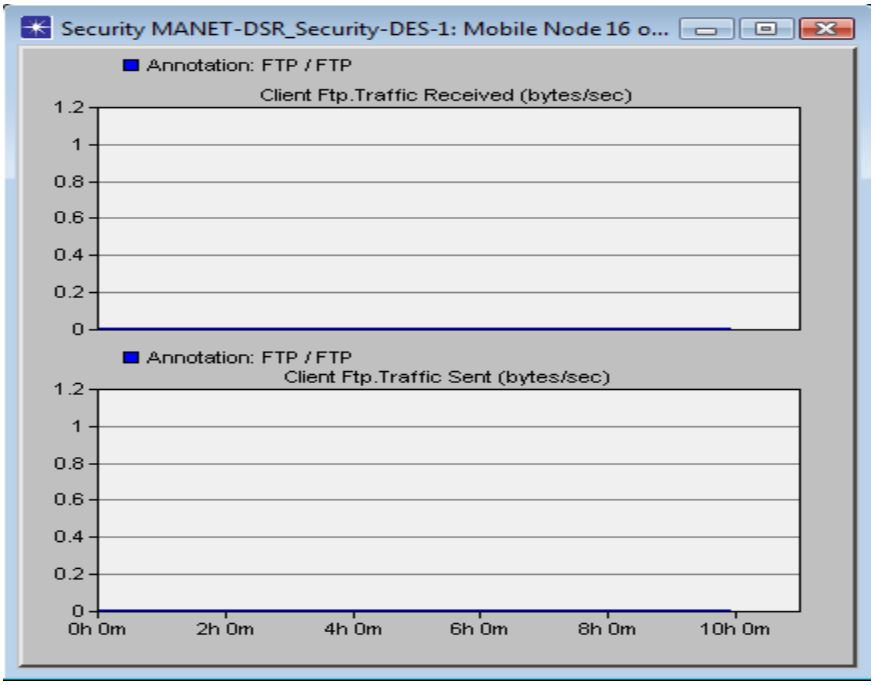

Figure 6.8 Traffic sent and received at an Intruder

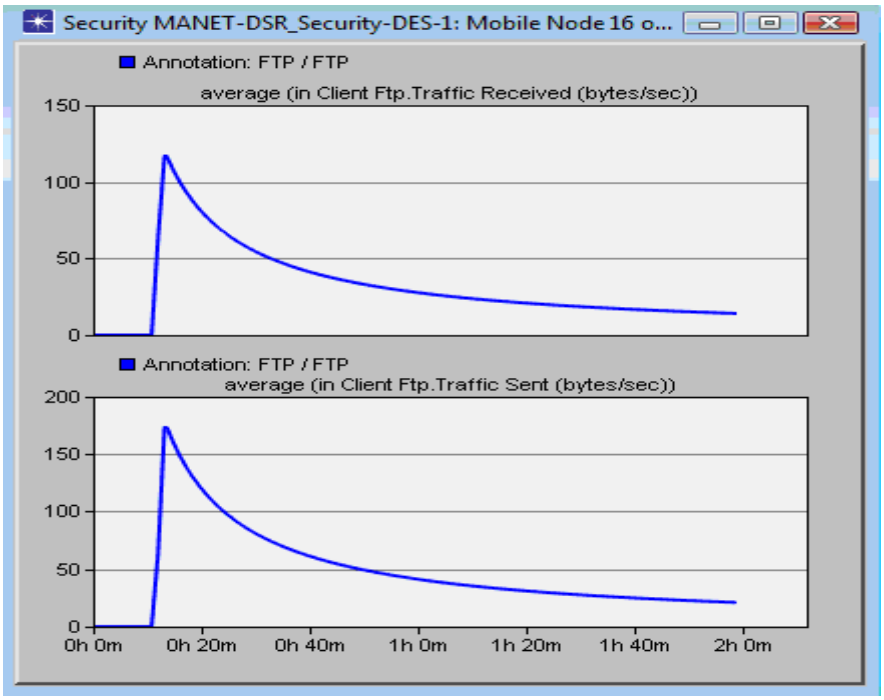

Figure 6.9 Traffic sent and receives before intruder

6.2.4 Load and throughput at an Intruder

According to the above discussion (in section 6.2.1 to 6.2.3) we come to know that there is no incoming as well as outgoing traffic at node 16 because of an intruder behavior activities that's why its traffic blocked and here it is also a proof that load as well as throughput at node 16 is also zero. If we like to discuss graphs in Figure 6.10 then we come to know that at start there is some traffic that's why it shows some Load and throughput but after detecting intruder in the network then all of its traffic blocked and then we also see from graphs no traffic no load and throughput.

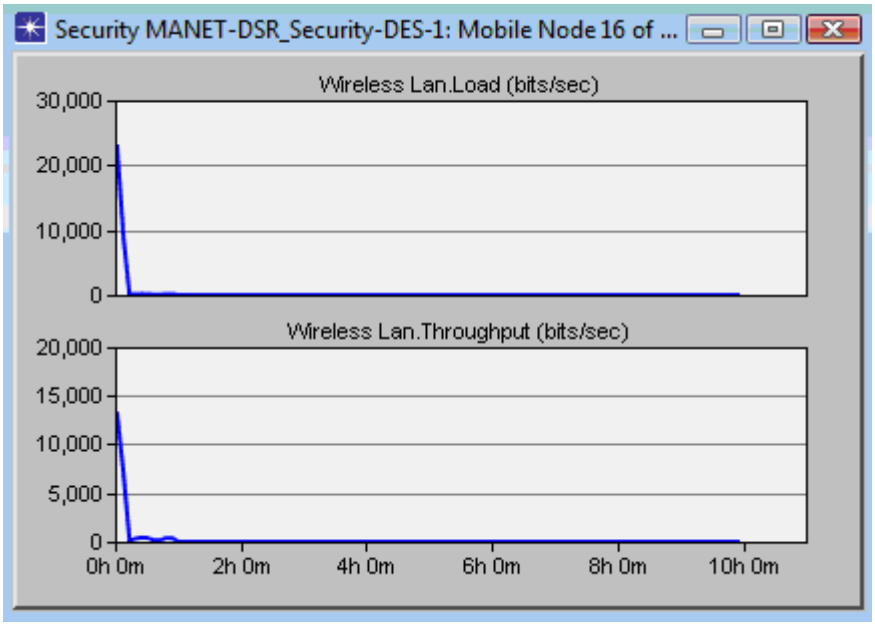

Figure 6.10 Load and throughput at an intruder

In Figure 6.11 we discuss load and throughput at node 16 before an Intruder activity. Before in the network when there is no activity of an intruder then node 16 performs normal functionalities like using network application for example ftp traffic and also do communication among nodes and sharing information each other to other nodes. In the first graph which is dealing with load on the node 16, we have 1,089.04 sample mean load in bits per second. In the last graph we have throughput at node 16, we have 992.800 sample mean in bits per second.

Finally we like to say that we have two different behaviors of node 16 but one is dealing with an intruder activity and the other one concern with no normal activity. We also learn that how we secure our network and secure our information at the network and also provide one way of security.

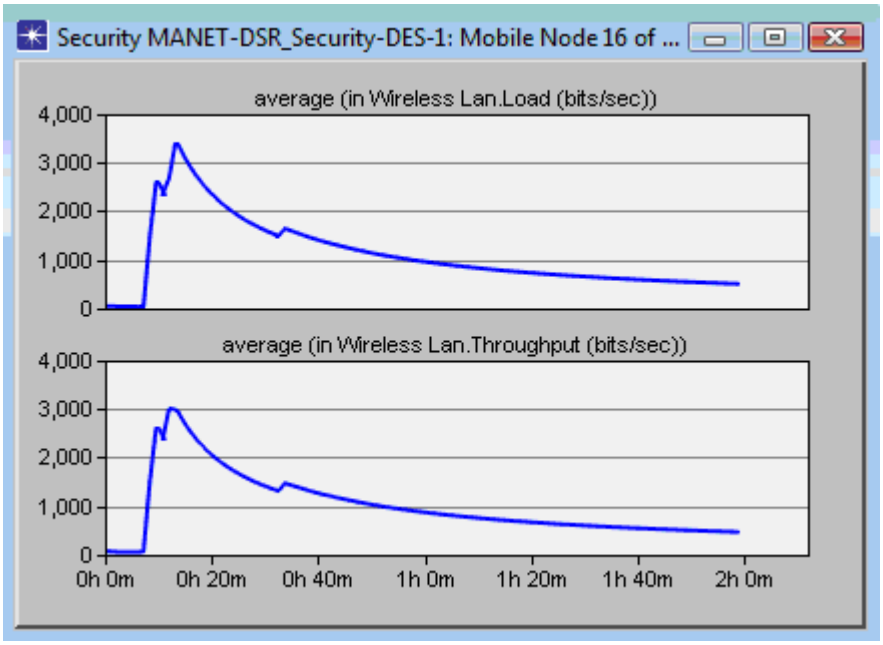

Figure 6.11 Load and throughput before Intruder

6.3 INFORMATION SECURITY OVER LINK LAYER AND NETWORK LAYER

According to network scenario in Figure 5.3 you will see that we implement Mobile ad hoc network in terms of two networks means Network A and Network B. Their traffic passing through the Internet among each other networks. Here we implement a secure network methodology with respect to without firewall and with firewall and at the end we discuss with firewall and VPN. In the first scenario which is bit simple as compare to the next two scenarios where we only check our page response time and in the last three scenarios we analyze http traffic that's why we discussed page response time with respect to each scenario. In the first case we have 0.00220 sample sum mean with respect to traffic.

We also implement network methodology with respect to firewall. In the first scenario we implemented network without firewall and here we implement with firewall in order to compare page response time; with firewall load on the network increase because it will check traffic packet one by one for the safety of network so that there will no attack by any intruder or any malicious data in the network. As we know that in the last three scenarios we analyze http traffic that's why we discussed page response time. In the second case we have 0.00610 sample sum mean with respect to traffic. If we compare this sample mean with respect to to previous case then we come to know that its high value of page response time as compare to without firewall case because when security increase so it takes more time to give response and thus the page response time increase.

Now as we can see that the response time is high value so we try to overcome that problem thus we implement the idea of VPN which give us more security and also the page response time value decrease. So we implement network methodology with respect to firewall as well as VPN. In the first two scenarios we implemented network without firewall and with firewall and in the last scenario here we implement network with firewall as well as with VPN in order to overcome the difference which we got in the first two scenarios. with firewall increases load on the network because it will check traffic packet one by one for the safety of network so that there will no attack by any intruder and there is no malicious data in the network. In the third case we have 0.00368 sample sum mean with respect to traffic. If we compare this sample mean with respect to to previous two cases then we come to know that now our network is also more secure due to encapsulation of data in VPN tunneling and also the page response time value decreases as compare to with firewall case. As shown in the figure 6.12.

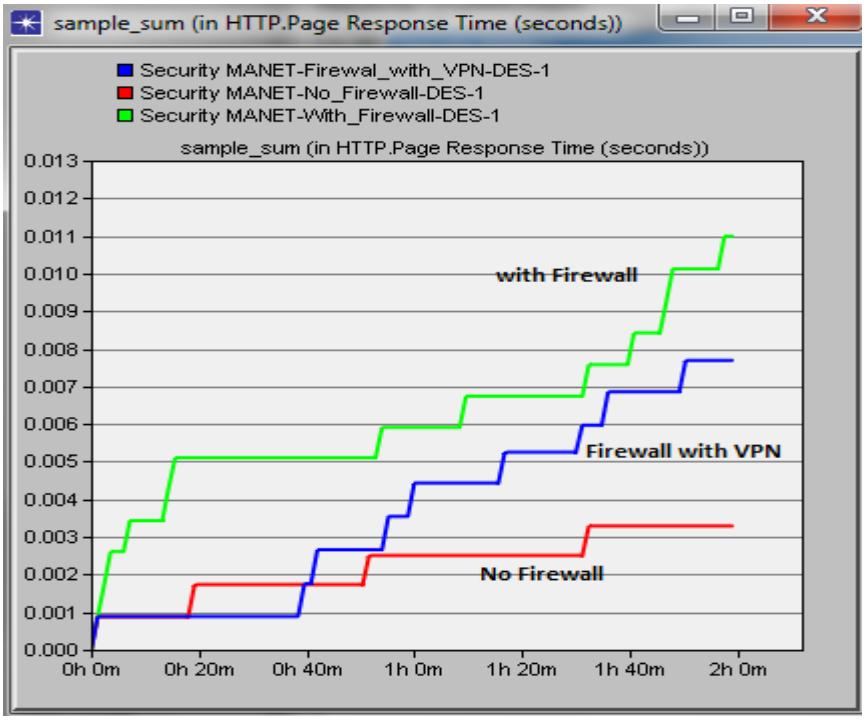

Figure 6.12 Comparison of No Firewall, Firewall and Firewall with VPN w.r.t Page response

Chapter 7
Discussions of simulation Analysis

7 DISCUSSIONS OF SIMULATION ANALYSIS

7.1 Overall comparison with respect to AODV, DSR and TORA

Here is the overall comparison of AODV, DSR and TORA with respect to delay, throughput, load, traffic sent, traffic received, Upload response time and download response time.

S.No	Parameters	DSR	AODV	TORA
1	Throughput (bits/sec)	2850	3460	2605
2	Delay (sec)	0.0050	0.0019	0.0026
3	Load (bits/sec)	2800	2663	2260
4	FTP Traffic sent (bytes/sec)	53	50	39
5	FTP Traffic received (bytes/sec)	53	50	39
6	Download response time (sec)	0.12	0.70	1.30

Table 7.1 Comparison among routing protocols

At transport layer throughput are used to describe the loss rate. It is used to reflect accuracy and completeness of the routing protocol. It is also clear that mobility is inversely proportional to throughput; it means if mobility increases then throughput decreases. If we look at the table 7.1 then it is clear that TORA has low throughput i.e. it performs better at high mobility.

In case of delay characteristics AODV and TORA shows us low delay even if their routes are not typically shortest. AODV gives lowest delay and it can be improved by reducing more in order to perform some fine-tuning process. DSR has worst delay characteristics due to the loss of distance information and even route construction may not occur quickly. Due to the fact it has delays and waits for new routes to be determined. In AODV Route Discovery is fast that's why it shows better performance than the other routing protocols and has lowest delay.

In case of load TORA's performance is impressive with respect to on-demand and distance vector protocols. It is due to the fact TORA to do substantial work to erase routes even when those routes are not in use. However, TORA shows a good performance for small networks with high mobility rate. AODV also outperforms in terms of overhead without any periodic hello messages. Bite overhead of AODV is less than DSR's overhead. If we look at the above table then we come to know that DSR has the largest routing load due to some of these facts; it has high number of its route discoveries and it has also wide flooding network discovery. If there are more connections, then more routing is needed; it also has high proportion of hello messages which become the cause of high overhead.

Due to high traffic especially in case of congestion; DSR control messages get loss and it also eliminating one of the advantages of fast establishing new route. Due to such reason it has a relatively high delay than AODV as well as TORA. In most cases, both the packet overhead and the byte overhead of AODV are less than of DSR and TORA overhead. If we look at our table 7.1 then we will come to know that traffic sent is equal to traffic received because it is a FTP traffic which is working on TCP protocol (aim to avoid completely data loss). There may be possibility of delay, load etc during data transfer which we already discuss above.

The aim of first three scenarios of the simulation is to measure the performance evaluation among AODV, DSR and TORA MANET routing protocols. AODV shows overall best performance in our first three scenarios in most of cases and it is also found that AODV shows the best performance in terms of end-to-end delay, throughput, routing message overhead, downlink response time and delivery ratio. DSR use to perform poorly in more stressful network scenarios. AODV is more desirable in those situations because of the fact that it is a hop-by-hop routing protocol, that's why it has high downlink response time. Source routing approach has tremendous advantage that is its route discovery process because it learns more routes so in such case if we use another routing protocol like DSR or TORA then it is very easy for an intruder to attach on such network. Whenever a network has high speed, high mobility and low throughput then in such cases TORA performs better as compared to AODV and DSR so if we use AODV or DSR instead of TROA so it will be very easy for an intruder to attack on such network. For lightweight adaptive multicast algorithms it is use to serves as the underlying protocol. In case of DSR routing protocol is concern it suits for such kind of networks in which mobiles nodes move at moderate speed. It also has a significant overhead as compared to other routing protocols due to large packet size because it is use to carrying full routing information so now in such situation if we use another routing protocol like AODV or TORA so it is very easy for an intruder to attack on such network.

7.2 Intruder Identification and Isolation

In Mobile ad hoc networks it is difficult to identify an Intruder as compare to wired networks; due to constantly changing of network topology and also in case of malicious hosts because they don't have fixed points.

In MANET every host participates with each other in order to provide connectivity and to deliver data to their required destination. It is important for communication safety of a host that there should be proper choice of path selection towards the destination, and even it is also important for a host to have reliable route paths. According to Mobile Ad Hoc network routing protocols (like AODV, DSR, and TORA, etc.) and wired network routing protocols (like RIP, OSPF, and EIGRP etc.) they share number of common methods like destination sequence, distance vector, source routing and link state. There are different numbers of attacks which targeting on these methods which we mentioned above with respect to different routing protocols that will be use to examine and exceptional patterns of these attacks will be extracted.

In the second part of our simulation which is based on studying an analysis of Intruder, where first we discuss discovering route map among MANET network. At first we discuss route discovery mechanism without an intruder and then discuss with respect to an Intruder. According to previous chapter's discussion on intruder section, where a node (for e.g.) A chooses another node B to forward its data, there is a possibility of risk with respect to integrity of data. Due to the fact; in order to establish a trustworthy relationship between node A and node B, use high degree of trust among mobile nodes by implementing handshake methodology in order to avoid risk and even it helps to make rational decisions. Trustworthy hosts only trusted on those routes which will provide complete degree of trust and information security. It is definitely true that if we send data/packets through these trusted routes then there will be no malicious attacks and information leakage. As we see in the previous chapter of intruder section before intruder e.g. mobile node 16 in scenario A, B and C (figure 6.7) acts as a trusted node but once notified as an intruder then node 17 in scenario D and E change its route map.

We also discuss traffic sent and receive at an intruder node, we only discuss FTP traffic and according to results which we discuss in the previous chapter, we come to know that there is no traffic at all during FTP session because there is no route map for node 16 towards any node so therefore there will be no communication. We also discuss throughput and load factors before and after intruder. There may be possibility of unexpected delay that could be caused due to unreliable and unrealistic channel instead of malicious discard. In order to develop the most trustworthy route map towards other nodes then definitely it requires more delay as well as extra computation.

7.3 Page response time comparisons

A firewall is a router with some special program features with respect to security that is mostly used between a site and the rest of the network. The main task of the firewall is to filters the traffic packets that flow through the network. A firewall is use to implement a security policy in the network in one centralized place. There is different type of firewalls; filter-based firewall is the simplest and most widely used. They are configured with respect to table of addresses and mainly use to characterize the packets.

A VPN is used to provide a controlled connectivity over the public network for e.g. the Internet. VPN is a concept called an IP tunnel which is a virtual link and used to create within the router at the start of the tunnel. Whenever the traffic comes at the entrance of the tunnel then it will forward towards virtual link but before sending traffic it is use to encapsulates the packet. The destination address at each packet of the traffic in the IP header is the address of the router at the other end of the IP tunnel.

You will see that how firewalls and VPNs are use to provide security to the information in the servers as well to the mobile nodes and mean while it also maintaining access for the nodes with respect to appropriate privilege.

According to last three scenarios we came to know that in case of without firewall scenario where response time is bit high due to low load on the network it means it gives high no of response but it provide no security. In case of firewall where we have lower page response as compare to the without firewall scenario because firewall creates load on the network but it provide security of information. In the last scenario we will see that we have lowest page response as compare to the last two scenarios. One thing is clear if we talk about more security then its true that load on the network definitely increases. In the first scenario there is no extra security parameter so therefore load on the network in not so high that’s why page response time is high. In the second scenario we implement security by using one of the simple mechanism firewall and then we see that page response time increased. In the last scenario we see that after implementing VPN and Firewall mechanism over the network then load increased and page response time decreased.

One more thing we like to discuss that here if we see at the value of the page response time with respect to last three scenarios then we came to know that page response time shows us a minor difference but the thing is if we say that there are hundreds of users in network A and hundreds of users in network B then hundreds of hundreds of request for http traffic arrive then this little become worse for the network. In order to overcome load on the network, network administrator introduce proxy servers in order to avoid http traffic over the Internet if there is already entry for the requested page.

Chapter 8
Conclusion & Future Work

8 CONCLUSION & FUTURE WORK

8.1 Conclusion

In this thesis work we tried to deal with security issues in Mobile ad hoc networks. A Mobile ad hoc network has open media nature and free mobility that's why it needs much more prone with respect to security risks e.g. intrusions, information disclosure and denial of service etc. A Mobile ad hoc network needs high level of security as compare to the traditional wired networks. Our thesis report discusses different characteristics of the Mobile ad hoc networks and some of the typical and some dangerous vulnerabilities issues in Mobile ad hoc networks. The aim of the thesis was to discuss different aspects of security in MANET; firstly discuss multi-layer intrusion detection technique in multi hop network of Mobile ad hoc network; secondly discuss security problems related between multi hop network and mobile nodes in Mobile ad hoc network. The second most important aspect of the thesis was to implement some of the solutions; firstly we did comparative study of different routing protocol (AODV, DSR and TORA); secondly we also implemented security threats within MANET network like intruder behavior, tapping and integrity; thirdly we also implemented MANET link layer and network layer operations with respect to information security. This report also discusses different number of scenarios of MANET network which we implement in our simulation. In our simulation we use to implement different routing protocols and also did comparative study, that which one is better with respect to different aspects of security. We also use to implements mechanisms of intruder behavior, MANET link layer and network layer operations with respect to information security.

We start with the discussion in the early chapters and focus on the security criteria in mobile ad hoc network, which is mainly used to acts as guidance to the security-related research works in Mobile ad hoc network. Then we discuss some of the main attack types of mobile ad hoc network that is used to threaten the networks. We also came to know that Multi-layer intrusion detection technique is workable in multi hop network of MANET; not even this we also discuss different security problems which relates between multi hop network and mobile nodes in mobile ad hoc network. In the end, we implement routing protocols, intruder behavior and how to dealing with intruders and also implement some of the security mechanisms that can be used to help the mobile ad hoc networks from external and internal security threats. There are different challenges for MANET link layer and network layer operations over multi hop wireless network which we discuss in our first part of the thesis and even we also try to implement in our simulation by showing information security scenarios; where we work on firewall as well as on VPN which shows secure communication between one MANET network to other network. As we mentioned above that we discuss and also implement different security threats within MANET network. Especially we work on the information security by implementing firewall and VPN scenarios and also work some part of the authenticity while working on intruder section.

Finally we conclude that which routing protocol is better for which kind of environment, e.g. if we use the suitable protocol for a MANET, so it make difficult for an intruder to be attack on such network, like if we have large network than the better option is to use AODV as compare to DSR and TORA, which makes very hard to an intruder to attack on such network, while if we have a small network with high mobility so than TORA is performing better and it's make difficult for an intruder to attack on such network. By this work we also find out that we can secure a MANET

network using authentication and integrity constrains by implementing Net doctor and security demand mechanism on a FTP server to block an unauthenticated user with in a MANET, but there is still a problem that if an authenticated user start misbehaving than it is very hard to find out such nodes and block them, but we will work in future on that part. We also find out that if we have communication between two MANETs, than using firewall to secure data between two MANETs, but due low page response time we also implement VPN connection to enhance the page response time and encapsulate date, which provide more security.

There are mainly four research questions in our thesis, which we tried to answer. According to the first research question, how multi-layer intrusion detection technique works in multi hop network of MANET? Multi-layer intrusion detection technique is basically resource-constrained, it also works on multi hop network by introducing different methods into the network; Distributed Policy enforcement Architecture (DIPLOMA), Privacy-aware position based routing (PPBR), Greedy Perimeter Stateless Routing (GPRS) are different method which can be implemented into multi hop network in order to implement multi-layer intrusion detection technique. All these different techniques we discussed in section 3.6. In order to detect multi-layer intrusion detection attacks in multi-hop network RTS/CTS work together.

According to the second research question, what are the security problems that are related between multi hop network and mobile nodes in MANET? A Mobile ad hoc network can be a single-hop network (mobile nodes) or a multi hop network, in single-hop networks adjacent cells do not reuse channels for policy implementation but in case of multi-hop networks data as well as control channel can be shared in the entire service area. We believe that multi hop network's security problems do not related to mobile nodes at any high level even there are some benefits of multi-hop network over single-hop network for e.g. availability of higher bandwidth, frequency reuse and robustness. It is well explained in above section 3.2, 3.3 and 3.6, where we discussed different aspects of reactive and proactive approaches of MANET; we also discussed network layer attacks and how to avoid by taking effective security steps.

According to the third research question, what are the challenges for MANET link layer and network layer operations with respect to information security? Link layer security technique for e.g. encryption is use to reduce threats with respect to information security. At network layer, the most important threat is inter-router authentication which usually happens during exchange of network control information. Authentication and simple shared-key approaches can be use to secure information security. In our simulation scenarios we usually work with firewall and VPN in order to provide information security at both link layer and network layer. In order to overcome load on the network, network administrator introduce proxy servers in order to avoid http traffic over the Internet if there is already entry for the requested page. It is well explained in above sections of 5.2.2.1, 6.3 and 7.3.

According to the fourth research question, how can we deal with security threats within MANET network like intruder behavior, tapping and integrity? In MANET, it is easy to launch an intruder attack in order to impersonate other mobile node. In our simulation we implement Net Doctor and security demands in order to avoid intruder behavior from the network. We discuss route discovery mechanism without an intruder and with respect to an Intruder; there is a possibility of risk with respect to integrity of data. Due to the fact; in order to establish a trustworthy relationship between nodes, use high degree of trust among mobile nodes by implementing intruder behavior, tapping and integrity in order to avoid risk and even it helps to make rational decisions. It is well explained in above section 5.2.2.1, 6.4 and 7.2.

8.2 Future Work

During our thesis, we also find some of the points that can be further researched and explored in the future, such as there should be some standardized intrusion detection techniques can be used and the techniques which already have get further improved. However, in our thesis we recognized that the current evaluation for state-of-the-art wireless security solutions is quite ad hoc. There are some drawbacks which should be improved and some of them are given below:

- Lacks of effective analytical tools especially in case of large scale wireless network setting.
- Find out and block an authenticated user, which start miss behaving inside the network.
- The multidimensional trade-offs among security strength,
- Communication overhead,
- Computation complexity,
- Energy consumption, and
- Scalability still remains largely unexplored.

There should be developed an effective evaluation methodology and toolkits that will probably be used and need interdisciplinary efforts from different research communities which are working in mobile systems, cryptography, and wireless networking. In case of Transient Multicast security is still an open problem.

Chapter 9
References

9 REFERENCE

[1]. D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, T. Imielinski and H. Korth, Ed., Kluwer, 1996.

[2]. C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," *2nd IEEE Wksp. Mobile Comp. Sys. and Apps.*, 1999.

[3]. IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1997.

[4]. B. Schneier, *Secret and Lies, Digital Security in a Networked World*, Wiley, 2000.

[5]. Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks.

[6]. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks," *ACM MOBICOM*, 2002.

[7]. M. Zapata, and N. Asokan, "Securing Ad Hoc Routing Protocols," *ACM WiSe*, 2002.

[8]. B. Dahill *et al.*, "A Secure Protocol for Ad Hoc Networks," *IEEE ICNP*, 2002.

[9]. Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," *IEEE INFOCOM*, 2002.

[10]. N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *ACM MOBICOM*, 2001.

[11]. V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *IEEE MILCOM*, 2002. [11] P. Kyasanur, and N. Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks," *DCC*, 2003.

[13]. Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer. *"A Secure Routing Protocol for Ad Hoc Networks"*. Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002, pp. 78-90.

[14]. Yi-an Huang and Wenke Lee. *"Attack analysis and Detection for Ad-hoc Routing protocols"*. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France. September 2004.

[**15].** Y. Hu, A. Perrig, D. Johnson. "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks"*. Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), March 2003.

[16]. M. Alicherry and A.D. Keromytis, "Securing MANET Multicast Using DIPLOMA", in Proc. IWSEC, 2010, pp.232-250.

[17]. Panagiotis, Papadimitratos; Zygmunt, J. Haas;,"Secure Routing for Mobile Ad hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002

[18]. Zhang, Chenxi; Lin, Xiaodong; Ho, Pin-Han; Sun, Xiaoting; Zhan, Xin; , "PPBR: Privacy-Aware Position-Based Routing in Mobile Ad Hoc Networks," Military Communications Conference, 2007. MILCOM 2007. IEEE , vol., no., pp.1-7, 29-31 Oct. 2007 doi: 10.1109/MILCOM.2007.4454856

[19]. Biswas, J.; Nandy, S.K.; , "Efficient Key Management and Distribution for MANET," Communications, 2006. ICC '06. IEEE International Conference on , vol.5, no., pp.2256-2261, June 2006 doi: 10.1109/ICC.2006.255106

[20]. Karygiannis, A.; Antonakakis, E.; Apostolopoulos, A.; , "Detecting critical nodes for MANET intrusion detection systems," Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on , vol., no., pp.9 pp.-15, 29-29 June 2006 doi: 10.1109/SECPERU.2006.8

[21]. IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010 ISSN: 1793-8236 "Performance analysis of AODV, DSR & TORA Routing Protocols" Anuj K. Gupta, Member, IACSIT, Dr. Harsh Sadawarti, Dr. Anil K. Verma

[22]. Bharat Bhargava), Michael Zoltowski and Pascal Meunier "Trusted Routing and Intruder Identification in Mobile Ad Hoc Networks" Research Proposal for CERIAS 2002 Purdue University, West Lafayette, IN 47907, USA

[23]. Hao Hao Yang, Haiyun Luo al. et. "Security in Mobile Ad Hoc Networks: Chanllenges and Solutions." Computer Science Department.

[24]. Hongmei Deng, Wei Li, and Dharma P. Agrawal. "*Routing Security in Wireless Ad Hoc Network*,"**.** IEEE Communications Magazine, vol. 40, no. 10, October 2002.