PERFORMANCE ANALYSIS OF AODV FOR WORMHOLE ATTACK USING DIFFERENT MOBILITY MODELS

Dissertation Submitted to the Central University of Punjab

For the award of

Master of Technology

In

Computer Science & Technology

By

Gurmeet Kaur

Supervisor

Er. Amanpreet Kaur

Centre for Computer Science & Technology
School of Engineering & Technology
Central University of Punjab, Bathinda

September, 2014

DECLARATION

I declare that the dissertation entitled “PERFORMANCE ANALYSIS OF AODV FOR WORMHOLE ATTACK USING DIFFERENT MOBILITY MODELS” has been prepared by me under the guidance of Er. Amanpreet Kaur, Assistant Professor, Centre for Computer Science and Technology, School of Engineering and Technology, Central University of Punjab.

No part of this dissertation has formed the basis for the award of any degree or fellowship previously.

Name: Gurmeet Kaur
Centre for Computer Science and Technology,
School of Engineering and Technology,
Central University of Punjab,
Bathinda – 151001.

Date:

CERTIFICATE

I certify that GURMEET KAUR has prepared her dissertation entitled "PERFORMANCE ANALYSIS OF AODV FOR WORMHOLE ATTACK USING DIFFERENT MOBILITY MODELS", for the award of M.Tech degree of the Central University of Punjab, under my guidance. She has carried out this work at the Centre for Computer Science and Technology, School of Engineering and Technology, Central University of Punjab.

Er. Amanpreet Kaur
Assistant Professor
Centre for Computer Science and Technology,
School of Engineering and Technology,
Central University of Punjab,
Bathinda – 151001.

Date:

ABSTRACT

Performance Analysis of AODV for Wormhole Attack using Different Mobility Models

Name of Student: Gurmeet Kaur

Registration Number: CUPB/M.Tech/SET/CST/2012-13/12

Degree for which submitted: M.Tech

Name of Supervisor: Er. Amanpreet Kaur

Name of Centre: Centre for Computer Science and Technology

Name of School: School of Engineering and Technology

Key words: AODV, Average Throughput, Delay, Mobility, PDR, RPGM, RWP, Tunnel, Wormhole

Mobile Ad-Hoc Network (MANET) is a type of temporary wireless network, in which the nodes are mobile and have dynamic network topology. According to structural arrangement, wireless networks are classified into two main types: fixed infrastructure wireless networks and non-infrastructure wireless networks. Mobile Ad-Hoc Networks (MANETs) fall under the type of infrastructure less wireless networks. Mobile nodes can communicate to each other through wireless links in this type of an autonomous system. At any time, whenever required nodes can join or leave the network as nodes are free to move. Although various routing protocols are used in the communication process but those protocols have numerous security complexities. An intruder can perform many attacks (both active and passive attacks) through different security flaws. Wormhole attack is an active attack in the context of mobile ad-hoc networks that disrupts the normal routing functioning of any routing protocol. In this work, an attempt has been made to analyze and compare the performance of demand oriented or reactive routing protocol: Ad-hoc On Demand Distance Vector (AODV) with two approaches: AODV without wormhole attack and AODV under attack using two mobility models viz. Random Way Point Model and Reference Point Group Mobility Model. Evaluation of two examined approaches has been done in terms of performance metrics such as Average Throughput, PDR (Packet Delivery Ratio), Jitter, Average End to End Delay and Packet Drop Rate. An approach has also been used to analyze participated malicious nodes in the wormhole peer list. Along with this, the attack has been detected with the help of metrics such as Average Throughput, Average End to End Delay, Jitter and Packet Delivery Ratio.

Gurmeet Kaur Supervisor: Er. Amanpreet Kaur

DEDICATED TO GOD,
MY LOVING FAMILY MEMBERS AND MY FRIENDS

ACKNOWLEDGEMENTS

Firstly, I would express my heartfelt thanks to Almighty God whose wishes and blessings have always been showered on me.

Through this acknowledgement, I would like to express my sincere gratitude to all those people who have been associated with this research work and have helped me in the field of Mobile Ad-Hoc Networks and made it a worthwhile experience. I would like to express a deep sense of gratitude and thanks profusely to my supervisor Er. Amanpreet Kaur. Without her wise counsel and able guidance, it would have been impossible to conduct this work in this manner.

I would like to express my thanks to Prof. A.K. Jain (CoC of Centre for Computer Science & Technology) who has given me this opportunity, valuable suggestions and academic environment required for this research work.

I am also thankful to my parents and friends whose unconditional support and encouragement was always there throughout my research work. Last but not the least I am greatly honoured and thankful to Central University of Punjab, which has given me the opportunity to learn and spread the light of education.

Gurmeet Kaur

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

Sr. No.	Full Form	Abbreviation
1.	Abstract Window ToolKit	AWK
2.	Access Point	AP
3.	Ad-hoc On-demand Distance Vector	AODV
4.	Cluster Based Routing Protocol	CBRP
5.	Constant Bit Rate	CBR
6.	Count to Reach Next Hop	CRNH
7.	Defense Advanced Research Projects Agency	DARPA
8.	Delay Per Hop Indication	DeLPHI
9.	Destination	DEST
10.	Destination Sequenced Distance Vector	DSDV
11.	Distributed Dynamic Routing	DDR
12.	Dynamic MANET On-demand protocol	DYMO
13.	Dynamic Source Routing	DSR
14.	File Transfer Protocol	FTP
15.	Fisheye State Routing	FSR
16.	Global Mobile Simulator	GloMoSim
17.	Group Center	GC
18.	Group Movement	GM
19.	High-Speed Downlink Packet Access	HSDPA
20.	Hyper Text Transfer Protocol	HTTP
21.	Internet Engineering Task Force	IETF
22.	Kilobits per second	Kbps
23.	Lightweight Countermeasure for the Wormhole Attack in Multi Hop Wireless Networks	LITEWORP
24.	Long Term Support	LTS
25.	Media Access Control	MAC
26.	Mobile Ad-Hoc Networks	MANETs
27.	Moving Picture Experts Group	MPEG
28.	Multicast extension of AODV	MAODV
29.	Network Animator	NAM

Sr. No.	Full Form	Abbreviation
30.	Network Simulator version 2	NS2
31.	Normalized Routing Load	NRL
32.	Object-oriented Tcl	OTcl
33.	On-Demand Multicast Routing Protocol	ODMRP
34.	Optimized Link State Routing	OLSR
35.	Optimized Network Engineering Tools	OPNET
36.	Packet Delivery Ratio	PDR
37.	Processing Bit	PB
38.	Quality of Service	QoS
39.	Random Motion	RM
40.	Random Point	RP
41.	Random Way Point	RWP
42.	Reference Point Group Model	RPGM
43.	Route Error	REER
44.	Route Reply	RREP
45.	Route Request	RREQ
46.	Source	SRC
47.	Temporally Ordered Routing Algorithm	TORA
48.	TESLA with Instant Key disclosure	TIK
49.	Time Stamp	TS
50.	Toolkit Command Language	TCL
51.	Transmission Control Protocol	TCP
52.	User Datagram Protocol	UDP
53.	Variable Bit Rate	VBR
54.	Virtual Internet Testbed	VINT
55.	Wireless Broadband	WiBro
56.	Wireless Fidelity	WiFi
57.	Worldwide Interoperability for Microwave Access	WiMAX
58.	Wormhole Attack Detection Protocol using Hound Packet	WHOP

Sr. No.	Full Form	Abbreviation
59.	Wormhole Avoidance Routing Protocol	WARP
60.	Zone Routing Protocol	ZRP

CHAPTER 1

INTRODUCTION

Wireless Networking is very popular and interesting technology in today's time as everyone wants wireless connectivity regardless their geographic position. It includes various technologies such as WiFi, HSDPA, WiMAX and WiBro etc because of widespread deployment of wireless networks. Due to their natural mobility, scalability, improved technology and reduced costs, wireless networks have become more preferable over wired networks in the past few decades (Shakshuki, Kang & Sheltami, 2013).

1.1. Categories of Wireless Network

Based on structural arrangement, wireless networks are classified into two main categories (Khemariya & Khuntetha, 2013):

1.1.1. Fixed Infrastructure Wireless Networks

Wireless Networks, which have a fixed infrastructure that provides communication among mobile nodes through a central authority known as an Access Point (AP). In these networks, nodes cannot communicate directly. For example, traditional cellular or base station infrastructure systems. The features of fixed infrastructure wireless networks are summarized as follows (Perkins, 2013):

- Have fixed and wired backbone.
- Mobiles can communicate directly with access points.
- Suitable for locations where APs can be situated easily.

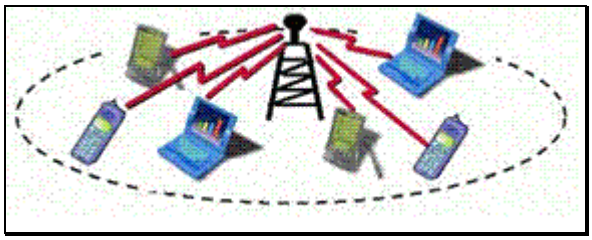

Figure 1.1: Fixed Infrastructure Wireless Network (ACoRN, 2010)

1.1.2. Non Infrastructure Wireless Networks

As the name indicates, it does not have fixed underlying infrastructure for the communication. Communication among nodes can be possible directly with

each other because there is no central administrator to control it. Here, wireless nodes themselves work as routers. An ad-hoc network is an example of this type of network. Some of the features of infrastructure less wireless networks are as follows (Perkins, 2013):

- No wired backbone.
- All nodes are capable of movement.
- All nodes act as routers known as multi-hop routers.
- Reduced administrative cost.
- Ease of deployment.

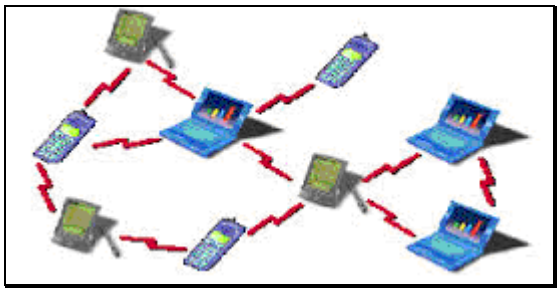

Figure 1.2: Non Infrastructure Wireless Network (Mobile Ad-Hoc Network) (ACoRN, 2010)

1.2. Mobile Ad-Hoc Networks (MANETs)

Mobile Ad-Hoc Networks (MANETs) fall under the type of infrastructure less wireless networks. In the early 1970s, the original idea of MANET was started out. During that period of time, MANET was known as “packet radio” network, which was sponsored by DARPA. The whole life cycle of ad hoc networks could be categorized into three generations and present ad hoc networking systems are considered the third generation, which was started out in 1990s (Kaur & Kaur, 2014) (Patil, 2012).

A MANET is that type of network, which can move from one location to another and configure itself automatically. Due to mobile nature of MANET, they can use wireless connections to connect different networks to each other. This can be a WiFi connection or cellular or satellite transmission medium (Shruthi, Shashikiran & Nagendra, 2014).

(Kaur & Kaur, 2014) (Shakshuki, Kang & Sheltami, 2013) have well defined the mobile ad-hoc networks. According to them, it is a group of mobile or

temporarily stationary devices, which may participate in the network either directly or indirectly via bidirectional wireless links as nodes are equipped with both a wireless transmitter and a receiver that communicate with each other.

The important characteristics, security issues and numerous applications of MANET are summarized in table 1 (Kaur & Kaur, 2014) (Kaur & Mittal, 2014) (Hoebeke, Moerman, Dhoedt & Demeester, 2004) (Cordeiro & Agarwal, 2002):

TABLE 1: Characteristics, Security Complexities & Application Scenarios of MANET

<table>
<tr><th>Characteristics</th><th>Security Complexities</th><th>Application Scenarios</th></tr>
<tr><td>Distributed, independent, and non-infrastructure wireless network.</td><td>MANET is much more attack prone system due to usage of open air medium.</td><td>MANETs can be employed in various military or police exercises.</td></tr>
<tr><td>Allow multi-hop routing.</td><td>Lack of centralized authority.</td><td>Include emergency services such as disaster relief operations.</td></tr>
<tr><td>Having dynamic network topology.</td><td>Dynamically changing network topology allows any malicious node to join the network without being detected.</td><td>Mine site operations.</td></tr>
<tr><td>Include heterogeneity among various devices such as mobile phone, personal digital assistance, laptop, personal computer and MP3 player etc.</td><td>Lack of clear line of defence.</td><td>Urgent business meetings.</td></tr>
<tr><td>Scalability.</td><td rowspan="3">Various bandwidth and energy constraints.</td><td>Robot data acquisition.</td></tr>
<tr><td>Provide mutual trust intrinsically.</td><td rowspan="2">In the era of education, entertainment and sensor networks etc.</td></tr>
<tr><td>Allow frequent updates in routing.</td></tr>
</table>

1.3. Mobile Ad-Hoc Network Routing Protocols

By definition, information transformation from a source to a destination in a network is known as routing. At least one intermediate node within the network

must be encountered during the process of routing. The routing concept basically includes two activities: firstly, computing optimum routing paths and secondly, transferring the information groups (called packets) through a network (Kumar, Singh & Chawla, 2011) (Marina & Das, 2005).

All the routing protocols perform well when the nodes are stable but in an environment having mobile nodes, the performance may degrade significantly. There are various routing protocols in MANET as no single protocol works well in all environments (Agrawal, Tripathi & Tiwari, 2012). The reason is that the traditional routing protocols (which have already written for the wired network) do not perform well in MANETs. Hence there was a need to design new protocols for mobile ad hoc networks (Upadhyay & Shukla, 2013).

(Kaur & Kaur, 2014) (Jathe & Dakhane, 2012) described that, in a network of two or more computers, a set of instructions or a common set of rules is required that each computer should follows to communicate with each other. Such a set of instructions or rules is called PROTOCOL. Depending upon the many ways by which computers can communicate, the routing protocols in mobile ad-hoc network can be divided into three categories (Gandhi, Chaubey, Tada & Trivedi, 2012):

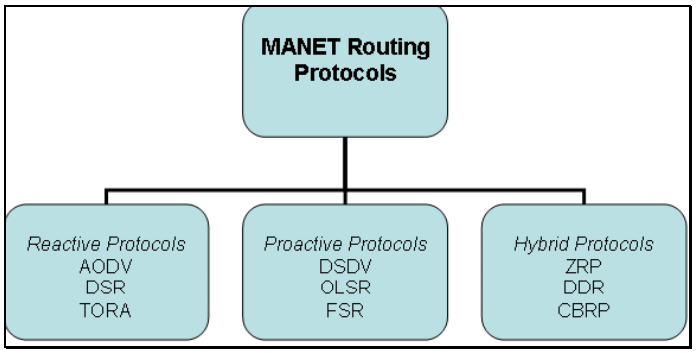

Figure 1.3: Classification of MANET Routing Protocols

1.3.1. Demand Based or Reactive Routing Protocols

Due to on-demand nature, demand based or reactive routing protocols compute the route to a specific destination only. So, there is no need to maintain the routing table containing all the nodes as entries at each node. For examples, AODV (Ad-hoc On-demand Distance Vector), TORA (Temporally-Ordered Routing Algorithm) and DSR (Dynamic Source Routing) etc (Gandhi et al., 2012).

1.3.2. Table Based or Proactive Routing Protocols

Table based or proactive routing protocols maintain complete routing information (in the form of routing table) from each node to every other node, which participates in a particular network. Whenever there is a change in network topology, changes are regularly reflected to this table to make information consistently up-to-date. For examples, DSDV (Destination Sequenced Distance Vector) and OLSR (Optimized Link State Routing) etc (Gandhi et al., 2012).

1.3.3. Hybrid Routing Protocols

Hybrid protocols have been developed to avoid data loss, congestion, routing overhead and long delay times. Hybrid routing protocols are the mixture of both demand based and table based routing protocols. Examples include CBRP (Cluster Based Routing Protocol), ZRP (Zone Routing Protocol) and DDR (Distributed Dynamic Routing) etc (Kaur & Kaur, 2014) (Khatkar & Singh, 2012).

1.4. Protocol Used for Analysis: Ad-hoc On-demand Distance Vector (AODV) Routing Protocol

In November 2001, Working Group for routing of the IETF community has been published the first version of AODV. AODV belongs to the category of routing protocols which are demand oriented. To reduce the traffic overhead, routes are only established whenever required due to purely on-demand nature. AODV supports unicast, broadcast and multicast. It uses sequence numbers to solve the count-to-infinity and loop creation problem (Baumann, 2002) (Kaur & Kaur, 2014).

AODV comes under non-infrastructure wireless networks, in which nodes are directly interacting to each other. So it is commonly used routing protocol in mobile ad hoc networks due to its simplicity, efficiency and effectiveness. AODV is an improvement of DSDV (Destination - Sequenced Distance - Vector Routing Protocol) because it reduces the number of required broadcasts by creating on demand routes as compared to DSDV, which maintains a complete list of routes (Kaur & Kaur, 2014) (Sarkar & Lol, 2010).

It uses traditional routing tables, one entry per destination. This is in contrast to DSR (Dynamic Source Routing), which can maintain multiple route cache entries for each destination (Sarkar & Lol, 2010).

1.4.1. Messages in AODV

According to (Gandhewar & Patel, 2012), four types of control messages are used by AODV as defined below:

- **RREQ:** It is a route request message. It is used when a source node wants to talk to a destination node and source is not in range of destination, then source broadcasts a RREQ to all its neighbors. And if the source node's neighbor does not know a route to the destination, then it rebroadcasts the RREQ.
- **RREP:** It is a route reply message. It is used when a neighbor of source node does know a route to the destination, then it unicasts a route reply (RREP) back to the source node.
- **RERR:** It is route error message that is mainly used by a node which detects that a link is broken.
- **HELLO:** The simple messages that are send by nodes to all its neighbors at certain time intervals to let them know about its existence.

1.4.2. Working of Ad-hoc On-demand Distance Vector (AODV) Routing Protocol

When a node wants to deliver a packet to destination, firstly it checks its routing table to determine if it has a current route to that destination. If route exists, it forwards the packet to next hop node. If no any route is there, it initiates a route discovery process as given below:

- **Route Discovery Phase:** It includes RREQ (Route Request) and RREP (Route Reply) messages. The route discovery begins with broadcasting of RREQ to its neighbors specified for certain destination. Once an intermediate node receives a RREQ, it checks its routing table for route to destination. If route is found, it sends RREP back to source**.** If route is not found, it rebroadcasts RREQ to its neighbor nodes by setting up a reverse route path to source node in its route table. It ignores RREQ if it is already processed by a node. Finally on reaching RREQ to destination node, it unicasts RREP to source node by using reverse route to source node (Gandhewar & Patel, 2012). The above procedure is illustrated in figure 1.4.

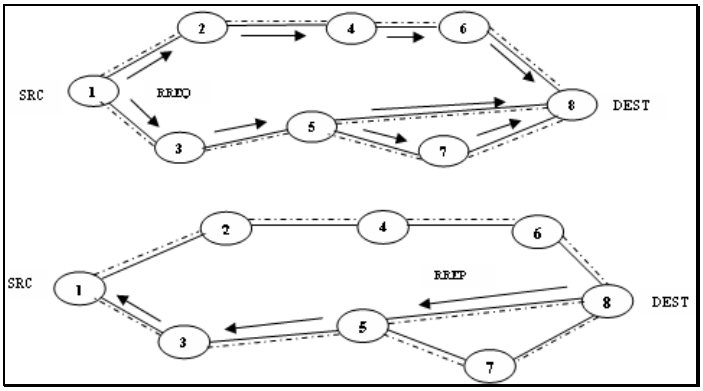

Figure 1.4: Process of Route Discovery with RREQ and RREP Messages (Gandhewar & Patel, 2012)

- **Route Maintenance Phase:** For the maintenance of route, HELLO and REER (Route Error) messages are used. A hello message is broadcasted by active nodes at certain time intervals. If no hello message received from a neighbor, then upstream node will notify the source with an RERR packet and entire routes based on the node is invalidated. Then source will initialize a new route discovery process and flood the RREQ packet again to its neighbors (Gandhewar & Patel, 2012). Above procedure is shown in the figure 1.5.

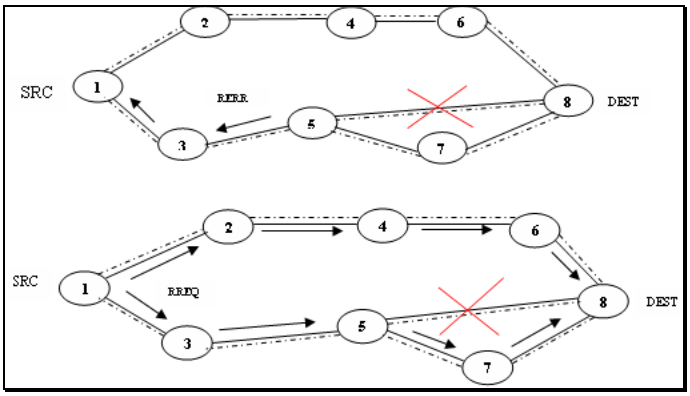

Figure 1.5: Route Maintenance Process (Gandhewar & Patel, 2012)

The table 2 (Boukhalkhal, Yagoubi, Djoudi, Ouinten & Benmohammed, 2008) (Kaur & Kaur, 2014) shows the comprehensive study of some salient features of AODV with other ad hoc routing protocols. Along with general characteristics, it illustrates some complexities such as communication complexity, storage complexity and time complexity. The parameters, on which complexities depend, are also mentioned.

TABLE 2: Comparison of AODV with other Routing Protocols

Characteristics	AODV (Demand Oriented)	DSDV (Table Oriented)	CBRP (Hybrid)
Distributed	Distributed in nature	Distributed in nature	Distributed in nature
Loop-free	Looping is not there in AODV	Looping is not there in DSDV	Looping is not there in CBRP
Multicast	Supports unicast, broadcast and multicast	No multicasting	No multicasting
Sequence number	Uses sequence number	Uses sequence number	Sequence number is not used
Complexity in communication	O(2N)	O(N)	O(N)
Complexity in storage	O(D)	O(N)	O(N/M)
Complexity in time	O(2K)	O(K)	O(2K)

where, N: Total number of nodes involved in network

M: Average number of nodes in cluster

D: Number of maximum desired destination

K: Diameter of Network

1.4.3. Loophole of AODV

A route is not discovered by AODV until a flow is initiated. So, this type of latency in route discovery process may be high in large scale networks. AODV lacks reliable and efficient route maintenance technique. Hence, the messages can be misused by many ways such as route disruption, node isolation and resource consumption etc (Gandhi et al., 2012). Due to this reason, AODV protocol has been chosen for this study under wormhole attack environment, which is discussed ahead.

1.5. Mobility Models

Nowadays, for the simulation of realistic movements that are produced by users of a mobile or wireless network, different mobility models are used. The mobility affects the stability of network. It is a fact that as higher is the mobility more will be link failures. It results in lower throughput and packet delivery fraction.

The mobility models give an idea about location, velocity and acceleration change over time for every mobile node. Hence these models help to lower the randomness of the mobile nodes (Kumar, Singh & Chawla, 2011).

There are two main categories of mobility models namely purely synthetic models and trace-based mobility models (Issariyakul & Hossain, 2011). But amongst them, purely synthetic models are commonly used in research. In this research work random waypoint and reference point group mobility models are used.

1.5.1. Classification of Mobility Models

(Jayakumar & Ganapathi, 2008) (Aschenbruck, Gerhards-Padilla & Martini, 2008) have given five classes of mobility models by considering the different kinds of dependencies and restrictions as listed below:

- **Random-Based:** Here, nodes can move randomly in any direction. It does not include any dependency or any other restriction. So nodes are independent to each other with respect to destination, speed and direction. Examples include RWP (Random Way Point), Random Direction and Random Walk Mobility Models.
- **Temporal Dependencies:** It depends upon time that is the actual or current velocity of a node which may be influenced by the movement in the previous state. Hence, the velocities of a single node at different time slots are correlated. Examples include Gauss-Markov and Smooth Random Mobility Models.
- **Spatial Dependencies:** It depends upon space as the name indicates. As mentioned above, in random-based models, the location, speed and direction of mobile nodes are not affected by other nodes in the neighborhood. But here the movement of a node is affected by nodes around it. Example includes RPGM (Random Point Group Model).
- **Geographic Restrictions:** Here, the restrictions are put on the area of a particular node in which that node is allowed to move. Examples include Pathway and Obstacle Mobility Models.

- **Hybrid Characteristics:** It is a combination of several dependencies and restrictions such as temporal dependencies, spatial dependencies and geographic restrictions.

1.5.2. Random Way Point Model (RWP)

It was first proposed by Johnson and Maltz. Later, it became a 'benchmark' model to evaluate various routing protocols of MANET due to its simplicity and wide availability. It is elementary synthetic model (Bai, Sadagopan & Helmy, 2004) (Bai & Helmy).

In Random Way Point Model, at every instant, a node randomly chooses a destination anywhere in the specified network field and moves towards it with a velocity chosen randomly from a uniform distribution between 0 and maximum allowable velocity for each mobile node i.e., 0 and V_max. When a node reaches at a destination, it stops for a time period called 'pause time'. To overcome sudden stop and start, pause time is used. After this time, a node again randomly chooses a destination and repeats the whole above procedure until the simulation ends. Figure 1.6 illustrates an example of a topography showing the movement of nodes for Random Way Point Mobility Model (Mohan, Rajan & Shanthi, 2012).

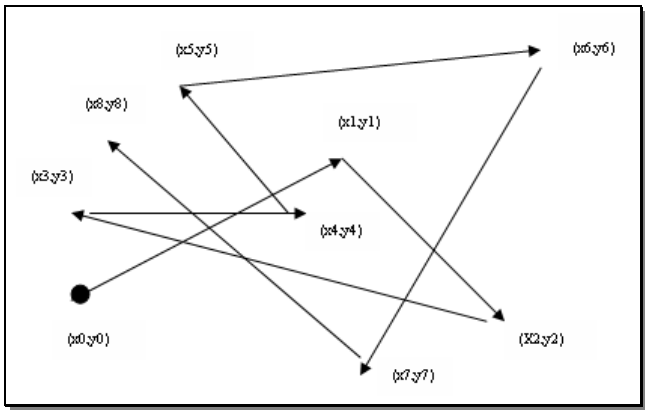

Figure 1.6: Node Movement in Random Way Point Mobility Model (Bai & Helmy)

1.5.3. Reference Point Group Mobility Model (RPGM)

In contrast to RWP, there are some spatial dependencies in RPGM. To simulate the group movement behavior in the real world such as communication in military battlefield and disaster areas, reference point group mobility model was proposed (Kumar, Srivastava & Gupta, 2013).

In RPGM, nodes are divided into groups. Each group has a logical center called group leader that defines the whole group's motion behavior and leader's mobility follows random waypoint (Kumar, Sharma & Suman, 2011).

(Kumar, Srivastava & Gupta, 2013) (Kumar, Sharma & Suman, 2011) have described that the RPGM mobility model makes two vectors as given below:

- A shared vector called Group Mobility Vector, which is shared by all members of the same group.
- To represent the relative mobility of a node inside the group, Internal Mobility Vector is used by nodes.

Hence, the vector sum of two mobility vectors decides the overall mobility of the node. Figure 1.7 shows an example topography illustrating the movement of nodes for Reference Point Group Mobility Model. Each node deviates from its velocity (both speed and direction) randomly as compared to that of the leader. It is expected that RPGM model behaves differently from the Random Way Point Model due to its inherent characteristics of spatial dependency between nodes (Mohan, Rajan & Shanthi, 2012).

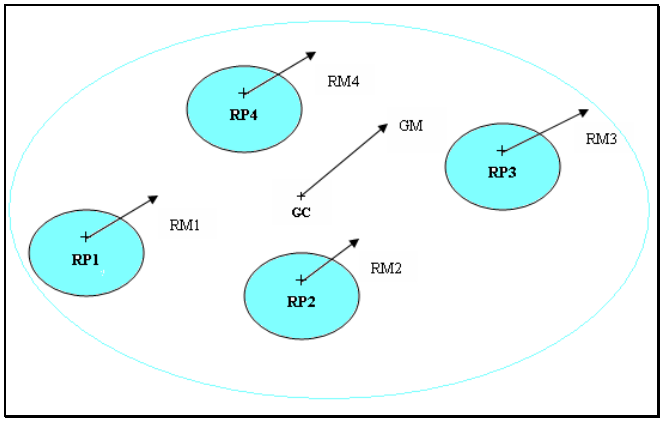

Figure 1.7: Reference Point Group Mobility Model (Romsaiyud, Premchaiswadi & Premchaiswadi, 2012)

where RP: Random Point

RM: Random Motion

GC: Group Center

GM: Group Movement

1.6. Wormhole Attack

To perform the basic functions of network, security plays a vital role in MANET. In order to combat active and passive attacks, an effective security architecture must ensure some basic requirements such as Availability, Confidentiality, Authorization, Non-repudiation and Integrity (Agrawal, Tripathi & Tiwari, 2012) (Kannhavong, Nakayama, Nemoto, Kato & Jamalipour, 2007) (Argyroudis & O'Mahony, 2005).

1.6.1. Wormhole Attack in AODV

According to (Singh, Kaur & Sangal, 2011) (Gupta, Kar & Dharmaraja, 2011) wormhole attack is an active attack. During this attack, two colluding nodes, that are far apart, are connected by an underlying tunnel. This transparent tunnel gives an illusion that those colluding nodes are neighbors to each other. In this attack, an attacker tunnels packet received at one point in the network to another colluding node which may replay them.

Wormhole intruder affects the original functionality of MANET routing protocols such as AODV, OLSR and DSR etc, but this research work emphasizes on wormhole attack in AODV routing protocol. A simplified view of wormhole attack is shown in figure 1.8.

Suppose a source wants to communicate with destination. And this communication is possible through shortest path provided by AODV protocol (called normal route). But if two malicious nodes are kept at two different locations in the network and a malicious node accepts the traffic at one location, tunnels them through wormhole link to another malicious node, then replays packets into the network at that location, then this is called wormhole route (Kaur & Kaur, 2014). Hence the functioning of AODV protocol is completely disrupted by this attack. It affects various QoS parameters such as delay, throughput, jitter, packet delivery ratio and power consumption etc (Singh, Kaur & Sangal, 2011) (Vandana & Devaraj, 2013).

The various metrics such as strength, packet delivery ratio, path length, attraction and robustness etc can also be used to detect wormhole attack in the network (Mahajan, Natu & Sethi, 2008).

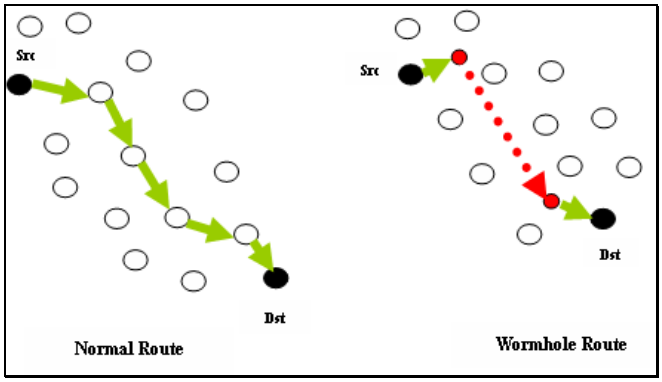

Figure 1.8: Scenario of Wormhole Attack (Vandana & Devaraj, 2013)

1.6.2. Types and Side Effects of Wormhole Attack

(Jenefer & Vydeki, 2013) (Kaur & Kaur, 2014) have described various types of wormhole attack as follows:

- **All Pass:** Irrespective of the size of packets malicious nodes can pass all the packets.
- **All Drop:** All the received packets are dropped by malicious nodes in the network.
- **Threshold:** Sometimes, threshold value can be used as a constraint in network and here all the packets (having size greater than or equal to the assumed threshold value) can be dropped by malicious nodes.
- **Replay:** After tunnelling, a malicious node can replay the packets in the network.
- **Tunnelling:** Wormhole attack is also known as tunnelling attack. So, through an underlying wormhole link, a malicious node tunnels the packets from one point to another point in the network.
- **Propagation Delay:** As more time is taken by malicious nodes to deliver packets from source to destination in the network. So, propagation delay is more in that case.

Depending upon above types, wormhole attack affects MANET in the form of four security threats namely modification, interception, fabrication and interruption. The description of these threats is discussed ahead (Upadhyay & Shukla, 2013) (Kaur & Kaur, 2014).

- **Modification:** Before forwarding the packet to the next node, a malicious node can modify the packet in the network. Due to it, message or data will lose its integrity.
- **Interception:** During interception, an unauthorized user (which acts as a malicious node as a part of network) can intercept the packet and can modify it to forward it to the next node. As a result, data integrity and confidentiality will be lost.
- **Fabrication:** Along with data modification and interception, generation of unwanted and unused packets also come under the category of an “attack”, called fabrication attack. In this type of attack, a malicious node can create a large number of useless packets and send it into the network continuously beyond its capacity. As a result, network will fail to accept more packets.
- **Interruption:** A malicious node can interrupt the received message by the destination node.

Due to above side effects of wormhole attack, the main goals of security such as authorization, integrity, confidentiality and availability get violated.

1.7. Problem Statement

The previous research work has been regarding the performance comparison of different routing protocols using different mobility models. This research work is carried out on AODV protocol with two scenarios: AODV without attack and AODV under wormhole attack and the analysis of the same using different mobility models.

1.8. Objectives of Research

The objectives of this research are listed below:

- To simulate, analyze and evaluate AODV and AODV under wormhole attack using Random Way Point and Reference Point Group Models.
- Graphical analysis and performance comparison of AODV and AODV under wormhole attack using RWP and RPGM.
- To analyze and detect wormhole attack in the network using different metrics.

CHAPTER 2

REVIEW OF LITERATURE

Literature survey is the most important step in any research. It gives a theoretical base for the research and helps to determine the nature of the research. This chapter presents different ways to analyze and evaluate the various MANET routing protocols through different mobility models and simulators. It also includes the discussion about the recent methods offered by researchers and describes about the wormhole attack, its modes and counter measurements.

Hu, Perrig & Johnson (2003) defined Packet Leashes method to defend against the wormhole attack. According to them any information, to restrict the packet's maximum allowed transmission distance, which is added to a packet is called a leash. Such leash information is of two types namely Geographical Leash and Temporal Leash: Geographical leash insures that the recipient of the packet is within a certain distance from the sender. On the other hand, temporal leash ensures that the packet has an upper bound of its lifetime (restricts the maximum travel distance) and each packet must be delivered to next node within computed deadline of a packet. The malicious nodes do not identify by packet leashes. Due to some potential problems, TIK (TESLA with Instant Key disclosure) protocol was used as a solution, which is an efficient authentication protocol designed for use with temporal leashes.

Khalil, Bagchi & Shroff (2005) introduced LITEWORP (lightweight countermeasure for the wormhole attack in multi hop wireless networks such as ad hoc and sensor networks), in which they used the special node called guard node. To detect the wormhole, guard node is used when one of its neighbors acts as the malicious node. Also this special node (guard node) can be a common neighbor of two nodes for the detection of legitimate link between them. The coverage analysis of LITEWORP brings out the variation of probability of missed detection and false detection with increasing network density. The cost analysis shows that LITEWORP has low storage, processing and bandwidth requirements.

Chiu & Lui (2006) introduced a delay analysis approach called DeLPHI (Delay Per Hop Indication). They identified two types of wormhole attacks. In the

first type, legitimate nodes do not know their existence as they do not participate in finding routes. But in the second type, legitimate nodes are aware of only the existence of malicious nodes due to creation of route advertisements by malicious nodes. It calculates mean delay per hop of every possible route. DELPHI applied a multi-path approach and recorded the delay and hop counts in transmitting RREQ and RREP through the paths. After collecting all responses, the sender computes mean delay per hop of each route. The path with wormhole attacks, the delay would be obviously longer than a normal path with the same hop count. Hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided but DELPHI protocol does not identify the malicious nodes which were making wormhole attack in the network.

Azer, El-Kassas & El-Soudani (2009) presented a full image of the wormhole attack and thought that wormhole attack can be launched by one or more than one malicious nodes. They used OPNET to simulate wormhole attack. They have considered this attack as two phase process. During first phase, the wormhole nodes make an illusion to force legitimate nodes to deliver data to the other nodes through them. And in the second phase, wormhole nodes can exploit the data in a variety of ways. They have also introduced the complex wormhole attacks in wireless ad hoc networks.

Sarkar & Lol (2010) simulated the MANET under the combined effect of node density, packet length and mobility. They analyzed the four MANET routing protocols: AODV, DSR, OLSR and TORA using OPNET Modeler 15.0. They considered the three network scenarios: a small network, a medium sized network and a denser network. They used two QoS parameters namely end-to-end delay and throughput, routing load and packet retransmissions to analyze different scenarios. Simulation results show that node density and mobility affects the routing protocols significantly.

Su (2010) proposed a modified AODV routing protocol called WARP (Wormhole Avoidance Routing Protocol) to defend against wormhole nodes by adopting link disjoint multi-path routing between source and destination. In WARP each node records all of its neighbor’s anomaly values (number of times it forms path from different source to destination). Due to wormhole node’s greater ability

to grab routing paths, if the occurrence of one links exceeds the threshold value, the two ends of this link may be wormhole nodes. If anomaly values of a node exceed a threshold value then its neighbor will discard all requests for forming route containing that node in the path. The most important merit is that it achieves degradation in packet loss rates without any additional support.

Amnai, Fakhri & Abouchabaka (2011) proposed a novel performance evaluation by using traffic VBR and studied the impact of various random mobility models (such as random way point, random-direction and mob gen steady state), node density with two different values of pause time for a fixed speed on the performance of AODV. They used Network Simulator 2.34 with multimedia traffic VBR (MPEG-4). Results show that the random direction mobility model performed well compared to other mobility models. At last they concluded that AODV protocol can only be used on applications having a small amount of packet loss.

Gupta, Kar & Dharmaraja (2011) proposed a different approach known as WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on the AODV protocol and designed to detect wormhole attack with the help of hound packets. In this approach a hound packet is sent after the route discovery process, means after the route has been discovered. This hound packet is processed by all the nodes, except the nodes which are involve in the path setup process. Basically the path discovery is done by the help of the two types of packet, called RREQ and RREP. When the sender gets the message, it creates a hound packet and computes its message digest and signs this message digest with its own private key and attach all this information with the hound packet. But due to it, processing delay of the packet becomes high.

Maulik & Chaki (2011) analyzed the performance of AODV and DSR under wormhole attack by considering multiple QoS parameters such as throughput, delay, packet delivery ratio, node energy and node density. They have used reference point group mobility model along with random waypoint to study the effect of node density and the initial energy on the throughput. Results show that the throughput increases with number of sources involved. In both mobility models (random waypoint and reference point group), the effect of initial energy is low for

smaller number of sources. The throughput under wormhole attack falls drastically under the RPGM model compared to the random waypoint model.

Singh, Kaur & Sangal (2011) presented an effective analysis of AODV and DSR routing protocols based on wormhole attack using only random waypoint mobility model with varying node mobility. They concluded that under wormhole attack with CBR traffic sources, AODV performs better than DSR for packet delivery ratio, average jitter and end to end delay parameters on both low (2 or 3 nodes) and high (4 nodes) number of malicious nodes scenarios.

Gandhi et al. (2012) presented a comprehensive simulation study of well-known protocols such as AODV, DSDV and ZRP in different mobility scenarios generated by random waypoint mobility model. The performance of three routing protocols is analyzed with respect to average end-to-end delay, average jitter, average throughput, normalized routing load (NRL) and packet delivery ratio (PDR). Overall AODV performs well in all parameters.

Mohan, Rajan & Shanthi (2012) evaluated the performance of two routing protocols such as AODV and DSDV based upon different mobility models to obtain a stable mobility model for MANET routing protocol. Four mobility models are considered: random waypoint, reference point group mobility, freeway and manhattan model. Performance comparison has been conducted across the varying node speed with fixed network size. The results show that the reactive protocol AODV experiences the most stable performance with all mobility models and both AODV and DSDV experience a good performance with the reference point group mobility model only.

Gupta et al. (2012) have studied that different mobility models affect greatly on the performance of routing protocols. They have used random waypoint, file and group mobility for study using QualNet simulator. The results show the significant impact of mobility models on the performance of routing protocol. Delay, throughput, jitter and PDR are the parameters that are used for analysis. On demand routing protocols perform well for all parameters and RWP mobility model has highest value of each parameter followed by file and group mobility.

Agrawal, Tripathi & Tiwari (2012) have compared the performance of two reactive routing protocols AODV and DYMO routing protocols under wormhole

attack environment in MANET. They considered various performance metrics for evaluation like throughput, packet loss, average end-to-end delay and numerous wormhole parameters such as frames intercepted all, frames dropped by wormhole, frames tunneled, frames replayed and frames dropped by queue. Results show that AODV is more affected than DYMO protocol by mobility, simulation time and density of the network.

Ehsan & Khan (2012) have implemented and analyzed AODV under different routing attacks such as selfish node, black hole, hello flood, RREQ flood, selective forwarding and sink hole attacks. To implement these attacks, NS-2.34 is used. Different performance metrics are considered namely packet efficiency, routing overhead and throughput. Results show that different routing attacks affect the network differently. They have performed about 5000 simulations so that the data can be used to detect the intrusions and identify the malicious nodes.

Jain & Shrivastava (2013) introduced an approach to prevent wormhole attack called hybridized WHOP along with time synchronization mechanism to lower the processing delay time using DSR protocol. The proposed mechanism gives efficient results to secure transmission of data packet and reduces the processing delay time without use of any expensive hardware.

Jenefer & Vydeki (2013) analyzed performance of MANET in the presence of wormhole attack using AODV. They compared the performance of MANET in the presence and absence of two kinds of wormhole attacks: replay and tunneling using metrics such as average end-to-end delay, throughput and jitter by varying the number of nodes (static and mobile) and number of attackers. They designed the MANET using QualNet simulator and designed the wormhole by changing the properties of the node in the MAC layer. The simulation results show that throughput decreases and end-to-end delay and jitter increases with the increase in the number of attackers in the network.

Khainwar, Jain & Tyagi (2013) implemented a new method which is used to detect malicious nodes and can work without protocol modification. It also includes a hop-count and time delay analysis without any special environment assumptions. They used OPNET simulator. AODV routing protocol is used for route establishment and when malicious nodes are found then these nodes are

not involved by the source node in future routes. This method gives good performance for the system having high node density as compared to average and low density system.

Kumar, Srivastava & Gupta (2013) analyzed and compared three routing protocols viz. AODV, OLSR and ZRP under reference point group mobility model using QualNet 5.0. They have considered two cases for simulation: During first case, whole network is taken as a single group and a common policy is applied to that group. And in second case, the whole network is divided into groups having average number of 4 nodes in each group. Graphs are plotted between PDR and Pause time; Normalized PDR and Pause time. Results show that the value of PDR for AODV increases up to the certain pause time as compared to OLSR and ZRP.

Nayak, Sahay & Pandey (2013) proposed a general mechanism called detection packet, which is the modification of hound packet. The main advantage of detection packet is that it can be used without any hardware, location information and clock synchronization for detecting malicious node in network, which is based on DSR routing protocol. Detection packet uses three fields namely Processing Bit (PB), Count to Reach Next Hop (CRNH) and Time Stamp (TS). For strongly detection with conformance, timestamp is used. As a result, detection packet improves throughput, packet delivery ratio (PDR) and reduces end to end delay.

Sanaei, Isnin & Bakhtiari (2013) evaluated the performance of two routing protocols: AODV and DSR in presence and absence of wormhole attack with constant bit rate traffic under dissimilar scalable network mobility. They also evaluated the effect and compared it with standard protocol in terms of different performance metrics. Results show that AODV gives better performance than DSR for average end to end delay and when node density is low and also shows that the DSR routing is more vulnerable to wormhole attack than AODV.

From above given literature review, we summarized the literature review in the tabular form which gives the description of names of authors, various protocols, approaches and parameters used by them and their limitations or future scope.

TABLE 3: Summary of Literature Review

Authors	Protocols/Parameters	Limitations/Scope
Hu, Perrig & Johnson (2003)	Packet Leashes method (including temporal and geographic leash) and TIK protocol for temporal leash	Geographic leashes are less efficient due to the requirement of broadcast authentication
Khalil, Bagchi & Shroff (2005)	LITEWORP based on DSR protocol	Low storage, processing and bandwidth requirements
Chiu & Lui (2006)	DeLPHI based on AODV protocol	Not identify the malicious nodes
Azer, El-Kassas & El-Soudani (2009)	Considered three scenarios with different number of malicious nodes using AODV routing protocol and OPNET modeler	Not considered complex wormhole attacks
Sarkar & Lol (2010)	Considered the combined effect of node density, packet length and mobility using AODV, DSR, OLSR and TORA under OPNET	None of the protocols can offer an optimum routing solution under various network scenarios
Su (2010)	WARP (modified AODV routing protocol)	Limited to only one path to transmit data
Amnai, Fakhri & Abouchabaka (2011)	Considered AODV under RWP, random direction and mobgen-steady models using delay, throughput and PDR	Not considered jitter
Gupta, Kar & Dharmaraja (2011)	Implemented an approach called WHOP based on AODV protocol and designed to detect wormhole attack with the help of hound packets	Processing delay of the packet becomes high
Maulik & Chaki (2011)	Considered AODV and DSR under RWP and RPGM models using delay, throughput, PDR, node energy and node density	Not identify the nodes and links which are actively involved in the wormhole attack

Authors	Protocols/Parameters	Limitations/Scope
Singh, Kaur & Sangal (2011)	Analyzed AODV and DSR protocols based on wormhole attack	Used only RWP model for analysis
Gandhi et al. (2012)	Considered AODV, DSDV and ZRP under RWP using delay, throughput, jitter, NRL and PDR	Not focus on standardization of security mechanism using AODV
Mohan, Rajan & Shanthi (2012)	Considered AODV and DSDV under RWP, RPGM, freeway and manhattan models using delay, throughput, PDF and packet loss	Not considered multicast routing protocols such as MAODV and ODMRP
Gupta et al. (2012)	Considered RWP, file and group mobility models under QualNet using delay, throughput, jitter and PDR	Not clearly defined routing protocols
Agrawal, Tripathi & Tiwari (2012)	Considered AODV and DYMO protocols using throughput, packet loss, delay and numerous wormhole parameters	Not considered the investigation of routing message processing mechanism of AODV
Ehsan & Khan (2012)	Considered AODV under different routing attacks using packet efficiency, routing overhead and throughput	Not considered wormhole attack
Jain & Shrivastava (2013)	Considered a reactive routing approach called hybridized WHOP that is based on DSR protocol	Limited to PDR, throughput and end to end delay
Jenefer & Vydeki (2013)	Considered AODV protocol with two kinds of wormhole attacks: replay and tunneling using average end-to-end delay, throughput and jitter under QualNet	Not detect wormhole attacks by analyzing the communication parameter such as link breakage in the network

Authors	Protocols/Parameters	Limitations/Scope
Khainwar, Jain & Tyagi (2013)	Implemented a new method using hop-count and time delay analysis based on AODV protocol under OPNET simulator to detect malicious nodes	Not considered mobility
Kumar, Srivastava & Gupta (2013)	Compared AODV, OLSR and ZRP under RPGM using PDR and normalized PDR	Considered only four average number of nodes in each group
Nayak, Sahay & Pandey (2013)	Considered a general mechanism called detection packet, which is based on DSR protocol	Detection packet can only be used to defend against wormhole attack
Sanaei, Isnin & Bakhtiari (2013)	Considered AODV and DSR protocols in the presence and absence of wormhole attack	Not considered the effect of different mobility models

CHAPTER 3

SIMULATION SETUP & METHODOLOGY

Cost and complexity is very high for the construction of real distributed testing environment. So, simulation is mostly involved in network research. By definition, simulation is the interpretation and manipulation of the system model to observe the nature of a particular system in a setup similar to real-life (Kaur & Kaur, 2014) (Singh, Kumar, Sachdeva & Sidhu, 2012).

3.1. Simulation Tool Used (ns-allinone-2.35)

There are various types of simulators available such as NS2, OPNET, GloMoSim, QualNet etc. NS2 simulator is used in this research work and it is the most widely used simulator in academia. This simulation study was conducted on Computer System with Intel Core i7 CPU and Operating System Ubuntu Linux 12.04 LTS.

NS2 stands for Network Simulator version 2. It was developed as a part of the VINT project (Virtual Internet Testbed). The first version of NS (NS version 1) was developed in 1995 and later released in 1996 with version 2. There is a scripting language known as Object-Oriented Tcl (OTcl), which is included in version 2 (Meeneghan & Delaney, 2004).

(Bakhshi, 2013) (Meeneghan & Delaney, 2004) have listed some salient features of NS2.

- It is an event driven packet level simulator for networking research.
- It is available free of cost.
- It provides support to simulate numerous protocols like TCP, UDP, FTP HTTP, DSR and AODV etc.
- Along with wireless networks, it can simulate wired networks too.
- It is available for both Windows (under Cygwin) and Linux platforms.
- It uses Tcl as its scripting language.

NS2 is implemented with two languages: C++ (in the back end) and OTCL (OO + TCL, in the front end). The Network Animator (NAM) is used to visualize packets. The parsing of the NS-2 trace file (e.g. Out.tr) can be done using AWK scripts (Rocha, 2010). Figure 3.1 shows the simplified view of the working of NS2.

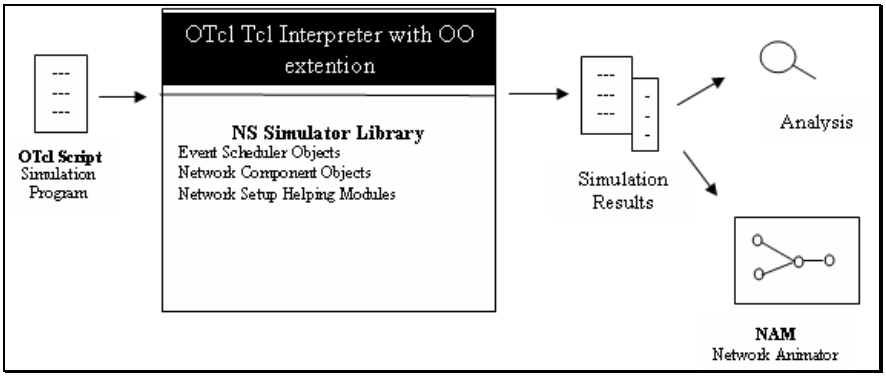

Figure 3.1: Simplified User's View of NS2 (Bakhshi, 2013)

Whenever any change is made in the .cc or .h file, the "make" command has to be executed in the following way:

$ make clean

$ make

$ ./configure

$ sudo make install

3.1.1. Installation of ns-allinone-2.35 Package on Linux Ubuntu 12.04 LTS

The various steps for successful installation of the ns-allinone-2.35 package are as follows (Dubey, 2013):

Step1: With good internet connectivity, download NS2.35 from http://sourceforge.net/projects/nsnam/files/latest/download.

Step 2: Copy and extract the downloaded files in HOME directory.

Step 3: Open terminal using Ctrl + Alt + t.

Step 4: Then run the following commands:

cd ns-allinone-2.35

sudo apt-get update

sudo apt-get install build-essential autoconf automake libxmu-dev

Step 5: Now execute the following command as

./install

Step 6: Run the following command for the installation of X-graph

$ sudo apt-get install xgraph

Step 7: To set environmental variables, execute the following command

gedit ~/.bashrc

After that gedit window will be opened. Then add the following lines to the end of the file. During this, replace “/your/path” by the folder where stored and extracted the NS-2 file has been kept.

 # LD_LIBRARY_PATH

OTCL_LIB=/your/path/ns-allinone-2.35/otcl-1.13

NS2_LIB=/your/path/ns-allinone-2.35/lib

X11_LIB=/usr/X11R6/lib

USR_LOCAL_LIB=/usr/local/lib

export
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$OTCL_LIB:$NS2_LIB:$X11_LIB:$U
SR_LOCAL_LIB

 # TCL_LIBRARY

TCL_LIB=/your/path/ns-allinone-2.35/tcl8.4.18/library

USR_LIB=/usr/lib

export

TCL_LIBRARY=$TCL_LIB:$USR_LIB

 # PATH

XGRAPH=/your/path/ns-allinone-2.35/bin:/your/path/ns-allinone
2.35/tcl8.4.18/unix:/your/path/ns-allinone- 2.35/tk8.4.18/unix
NS=/your/path/ns-allinone-2.35/ns-2.35/
NAM=/your/path/ns-allinone-2.35/nam-1.14/

PATH=$PATH:$XGRAPH:$NS:$NAM

Step 8: Now execute the following command:

source ~/.bashrc

After that, run ns by 'ns' command. The '%' symbol will appear on the screen. Then type 'exit' to quit.

3.1.2. TCL & OTCL

TCL stands for "Toolkit Command Language". And OTcl is the object oriented extended version of TCL. The creation of Tcl was started out as an embeddable command language by John Ousterhout in 1988. But today, the evaluation of Tcl is in the hands of the Tcl Core Team. The following are the features of Tcl (Sanfilippo, 2004):

- It allows fast development.
- It provides graphical interface.
- It supports rich platform.
- It is flexible and easy to use.
- It is free.

Event scheduling in Tcl script can be done as:

- Create scheduler: set ns [new Simulator]
- Schedule Event: $ns at <time> <event>
- Start scheduler: $ns run

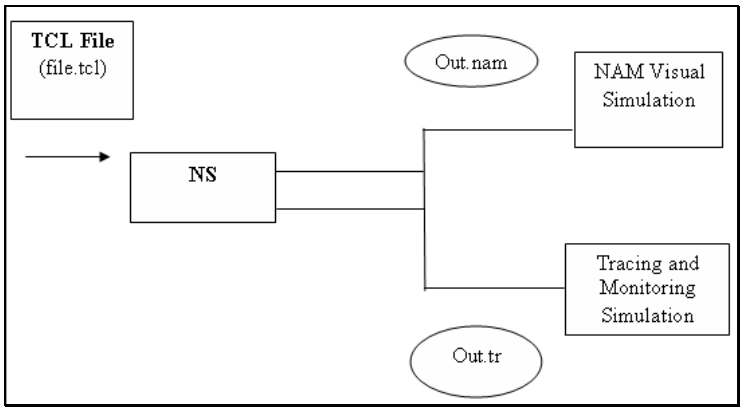

Figure 3.2: Flow of Events for a Tcl File run in NS (Bakhshi, 2013)

3.1.3. NAM (Network Animator)

NAM is the software tool used with NS-2. To visualize the interpretation of the network topology created, NAM is the most widely used software. Along with NS, it was also developed as part of VINT project. (Meeneghan & Delaney, 2004) have described features of NAM are as following:

- It can be directly executed from a scripting language (from Tcl script).
- It helps to control play, pause and a facility to monitor packets etc.
- It can present the information such as throughput and number of packets on each link.
- It provides drag and drop interface for creating topologies.

3.1.4. AWK (Abstract Window ToolKit)

The name ‘AWK’ came from the initials of its designers: Alfred V. **A**ho, Peter J. **W**einberger and Brian W. **K**ernighan. Its original version was written in 1977. The term ‘AWK’ refers to a particular program, and to the language to tell this program what to do (Close, Robbins, Rubin, Stallman & Oostrum, 1995).

AWK scripts can be used to calculate the performance metrics of the trace file with following command:

awk –f <awk_script_name> <trace_file_name>

e.g. awk –f throughput.awk out.tr

3.2. Bonnmotion Tool (bonnmotion-1.3a)

Bonnmotion is open source Java software, which is used to create and analyze mobility scenarios. In Germany, University of Bonn has been carried out the development of this tool, where it serves as an investigation tool for mobile multi-hop network scenario characteristics. The generated scenarios can be exported for various network simulators such as Ns-2, GloMoSim/QualNet, COOJA and MiXiM etc (Aschenbruck, Ernst, Gerhards-Padilla & Schwamborn, 2010) (Sadasivam).

3.2.1. Installation Steps

Step 1: Firstly make sure that Java is installed on system for the installation of this software, then double click on 'install' script inside the bonnmotion package.

Step 2: After that, terminal window will be opened and it will ask to enter your java path.

Step 3: Next it will ask for bonnmotion path, where its extracted files have been saved.

Step 4: After all above steps, three files: bm.bat, compile.bat and makedoc.bat will be created in the bin folder of bonnmotion package. These files are the proof of successful installation of bonnmotion.

3.2.2. Commands for generation of Movements for Nodes using Different Mobility Models

3.2.2.1. Command for Random Way Point Mobility Model

sh bm –f scenario_name RandomWaypoint –n <number of nodes> -d <simulation time duration in seconds> -i <initial phase cutoff in seconds>

e.g. sh bm –f sceng RandomWaypoint –n 10 –d 100 -i 3000

After execution of above command, two files (sceng.params and sceng.movements.gz) will be generated in bin folder, but these files are not compatible with NS-2. To make them NS-2 compatible, following command has to be run:

sh bm NSFile –f sceng

It will create a file: sceng.ns_movements.

Now this file can be incorporated to the Tcl script for the generation of node movements using Random Waypoint Mobility Model.

3.2.2.2. Command for Reference Point Group Mobility Model

The bonnmotion implementation of this model uses random waypoint for the creation of movements of the reference points (Aschenbruck, Ernst, Gerhards-Padilla & Schwamborn, 2010). Command is as follows:

sh bm –f scenario_name RPGM –d <duration of simulation> -i <initial phase cutoff

time> -n <number of nodes> -x <width of the simulation movement field> -y <length of the simulation movement field> -a <average number of nodes per group>

e.g. sh bm –f sceng1 RPGM –d 60 –i 3000 -n 50 -x 2000 -y 2000 -a 10

After execution of above command, two files (sceng1.params and sceng1.movements.gz) will be generated in bin folder, but these files are not compatible with NS-2. To make them NS-2 compatible, following command has to be run:

sh bm NSFile –f sceng1

It will create a file: sceng1.ns_movements.

Now this file can be incorporated to the Tcl script for the generation of node movements using Reference Point Group Mobility Model (Sadasivam).

3.3. Methodology Used

The dissertation work has been divided into following steps:

Step 1: Simulation of the demand-oriented routing protocol AODV under two synthetic mobility models: RWP (Random Waypoint) and RPGM (Reference Point Group Model).

To simulate AODV under random waypoint mobility model, a number of nodes (from 10-50) are uniformly distributed in an area size of 1186*584 sq. m. having CBR traffic type. The performance metrics such as Packet Delivery Ratio, Average Throughput, Jitter, Average End to End Delay and Packet Drop Rate have been measured for this scenario.

To simulate AODV under reference point group mobility model, five configurations with different number of nodes have been configured as follows:

Configuration I: When network size is small i.e. network is having 10 nodes only, then 1 group with 10 nodes is configured.

Configuration II: For 20 nodes, 2 groups are configured with 10 nodes each.

Configuration III: For 30 nodes, 3 groups are configured with 10 nodes each.

Configuration IV: For 40 nodes, 4 groups are configured with 10 nodes each.

Configuration V: For 50 nodes, 5 groups are configured with 10 nodes each.

The movement scenarios of nodes for both mobility models are generated through bonnmotion tool. An example is shown in Appendix C.

Step 2: Simulation of AODV under wormhole attack using two mobility models: RWP (Random Way Point) and RPGM (Reference Point Group Model).

To simulate wormhole attack, malicious nodes are kept at different locations in the already created topology for both mobility models and then required coding is done to create tunnel with the help of other nodes in the network, which further disrupts the normal route of AODV. In this scenario, minimum number of malicious nodes is 1, but tunnel length increases as network size increases. The way in which groups are configured in reference point group mobility model has been described above.

Wormhole attack can be launched through various modes, but this work emphasizes on that wormhole attack mode, in which a malicious node can tunnel packets between two distant nodes to make an illusion that they both are neighbors to each other. Sometimes, one malicious node is sufficient to perform this attack. As a result, it takes less time than the normal route. But if tunnel length is increasing, then it will be taken more time depending upon the number of hops between source and destination.

Step 3: Graphical analysis and performance comparison of AODV and AODV under attacked environment using RWP and RPGM.

Using AWK scripts, various performance metrics have been analyzed graphically and comparison is done between AODV without attack and AODV under attack by varying number of nodes. The simulation performance metrics are as follows (Jain & Shrivastava, 2013) (Gandhi et al, 2012):

- **Packet Delivery Ratio:** Packet delivery ratio is a very important factor to measure the performance of routing protocol in any network. It is defined as

ratio of the amount of the data packets delivered to the destination to those generated by the traffic sources. It can be measured in percentage.

$$\text{Packet Delivery Ratio} = \Sigma\ (\text{recvLine}/\text{sendLine}) * 100$$

where

recvLine: Number of packets received

sendLine: Number of packets send

- **Average Throughput:** Throughput is the number of packets that are passed through the communication channel in a particular period of time. This performance metric shows the total number of successfully delivered packets from source to destination. It is proportional to a good channel capacity of network connections. It is measured in kbps.

  $$\text{Average Throughput} = (\text{recvdSize}/(\text{stopTime}-\text{startTime}))*(8/1000)$$

  where

  recvdSize: Received packet's size

  stopTime: Simulation stop time

  startTime: Simulation start time

- **Jitter:** The term jitter is often used as a variation in delay of the packets across a network, because the packets reach at the destination with different delays. It is measured in seconds. In general, it can be defined as:

  If A is the first packet and B is the second packet, then jitter can be expressed as:

  $$\text{Jitter} = |\text{RxA}-\text{TxA}| - |\text{RxB}-\text{TxB}|$$

  where

  Rx: Receive time of packet

  Tx: Transmit time of packet

- **Average End to End Delay:** The time taken by the packets to reach at the destination is called delay. It includes various types such as propagation

delay, source processing delay, network delay and destination processing delay. It is measured in seconds.

Average End to End Delay = Σ (end_time-start_time)/total no. of connections

where

end_time: Packet's arrival time

start_time: Packet's start time

- **Packet Drop Rate:** It is the rate at which the packets are dropped during transmission between source and destination. It is defined as the ratio of number of packets dropped to the total number of packets generated. It is expressed in percentage.

Packet Drop Rate = (Number of packets dropped/total number of packets generated) * 100

Step 4: Analysis of the malicious nodes which are participating to make wormhole peer list in the network.

To analyze malicious nodes, an implementation has been done at NS2 link layer. Required coding has been done in ll.cc and ll.h files at link level. Firstly, in ll.cc and ll.h files, parameters such as size of wormhole peer list (tunnel) and properties of nodes are defined and then in Tcl file, the definition of nodes is configured. During this analysis, the tunnel length varies from 1 to 5 nodes. The code is shown in Appendix D.

Step 5: Detection of wormhole attack using different metrics under RWP and RPGM models.

To detect wormhole attack, various metrics such as Average Throughput, Average End to End Delay, PDR and Jitter have been used under random waypoint and reference point group mobility models.

The simulation parameters for all above steps are shown in table 4, which describes various parameters such as type of simulator (NS-2.35), number of

nodes (10-50 nodes), simulation area (1186*584 sq. m.), traffic type (CBR), tunnel length (1-5 nodes) etc.

TABLE 4: Simulation Parameters

Parameters	Value
Simulator	NS-2 Version 2.35
Number of Nodes	10-50 nodes
Area of Simulation (m*m)	1186*584
Simulation Time	90 seconds
Traffic Type	CBR
Signal Propagation Model	Two Ray Ground Model
MAC Type	802.11 MAC Layer
Data Rate	2.0 Mb
Mobility Models	Random Way Point, Reference Point Group
Routing Protocol	AODV
Interface Queue	Drop Tail/Priority Queue
Channel Type	Wireless Channel
Link Layer Type	LL
Antenna Type	Omni direction
Minimum Number of Malicious Nodes	1
Tunnel Length	1-5 nodes
Probability of Group Change	0.01
Maximum Distance between Groups	1.0
Average Number of Nodes in a Group	10
Min Speed and Max Speed of Nodes	0.5 and 1.5 m/s
Performance Metrics	PDR, Average Throughput, Average End to End Delay, Jitter and Packet Drop Rate
Examined Approaches	without attack and under attack

CHAPTER 4

RESULTS & DISCUSSION

The two approaches namely normal AODV and AODV under wormhole attack are simulated using random way point model and reference point group mobility model. Also analysis of malicious nodes and detection of attack is done using different metrics. The number of simulations that are performed is listed in Appendix A.

4.1. Performance Analysis of AODV Protocol under RWP and RPGM

AODV protocol is simulated by varying number of nodes using CBR traffic and two mobility models. The results are discussed below:

4.1.1. Comparison of Average Throughput of AODV under Random Way Point and Reference Point Group Mobility Models.

The throughput tends to fluctuate with the increase in network size under random way point model. Overall, reference point group mobility model offers higher throughput than the random waypoint.

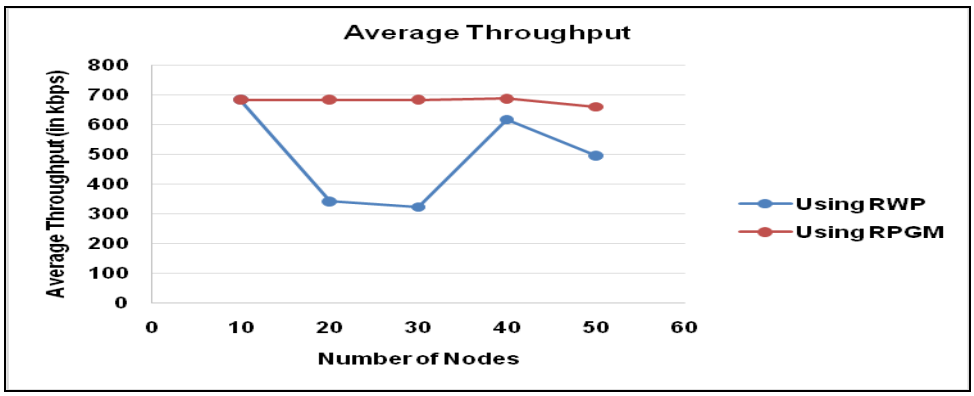

Figure 4.1: Average Throughput of AODV under Different Mobility Models

4.1.2. Comparison of Average End to End delay of AODV under Random Way Point and Reference Point Group Mobility Model.

Random waypoint model exhibits lesser delay than the reference point group mobility model. Due to configuration of various groups in reference point group model, delay is high in case of RPGM, but value of delay decreases as number of nodes or groups increases in RPGM. Because distance among groups

decreases as number of groups increase under RPGM. Delay remains constant for network size of 10 nodes in both scenarios.

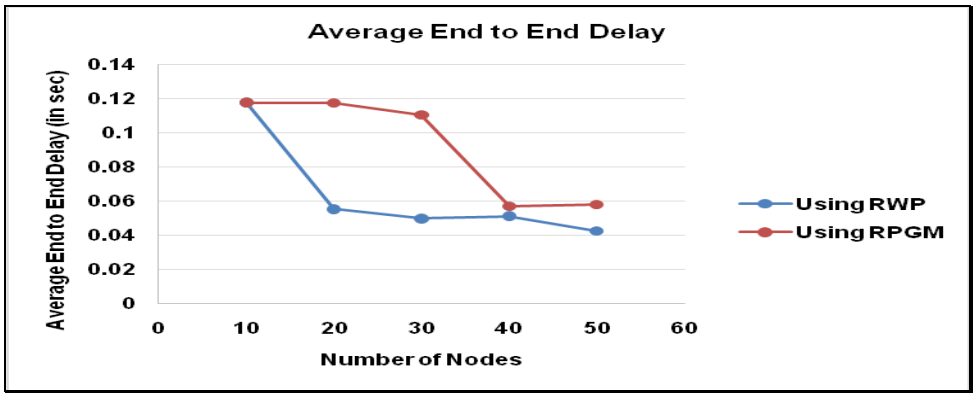

Figure 4.2: Average End to End Delay of AODV under Different Mobility Models

4.1.3. Comparison of Packet Delivery ratio of AODV under Random Way Point and Reference Point Group Mobility Model.

The packet delivery ratio decreases with increase in network size. And the value of PDR under RPGM is more as compared to RWP. Initially, packet delivery ratio remains constant for network size of 10 and 20 in RPGM, but then decreases suddenly. After that it again remains nearly same for 40 and 50 number of nodes in RPGM.

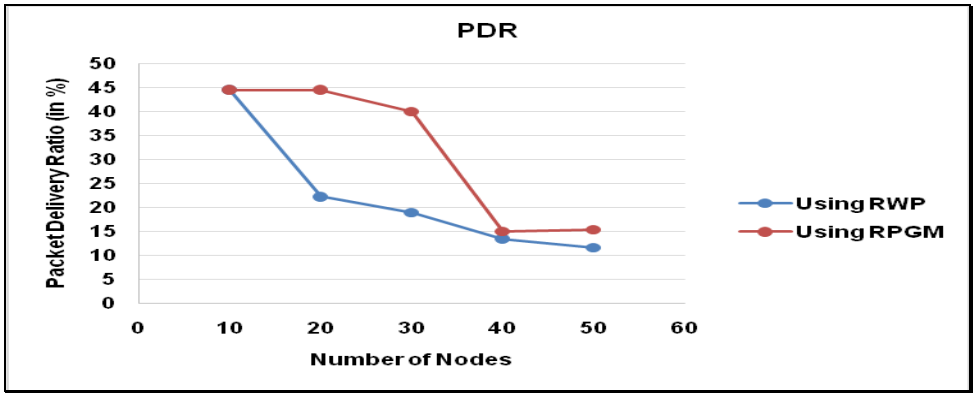

Figure 4.3: Packet Delivery Ratio of AODV under Different Mobility Models

4.1.4. Comparison of Jitter of AODV under Random Way Point and Reference Point Group Mobility Model.

There is a fluctuation in jitter graph for RWP. But for RPGM, the values are nearly same as number of nodes increases up to 40 nodes, but after that it decreases. Overall jitter is high in case of RPGM.

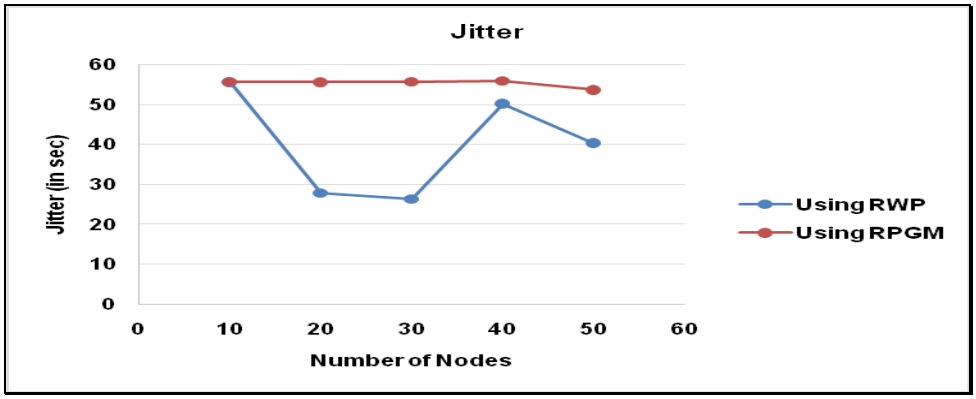

Figure 4.4: Jitter of AODV under Different Mobility Models

4.1.5. Comparison of Packet Drop Rate of AODV under Random Way Point and Reference Point Group Mobility Model.

The packet dropping rate increases as network size increases for both cases. More packets are dropped in random waypoint mobility model. It results in lesser throughput and packet delivery ratio under RWP.

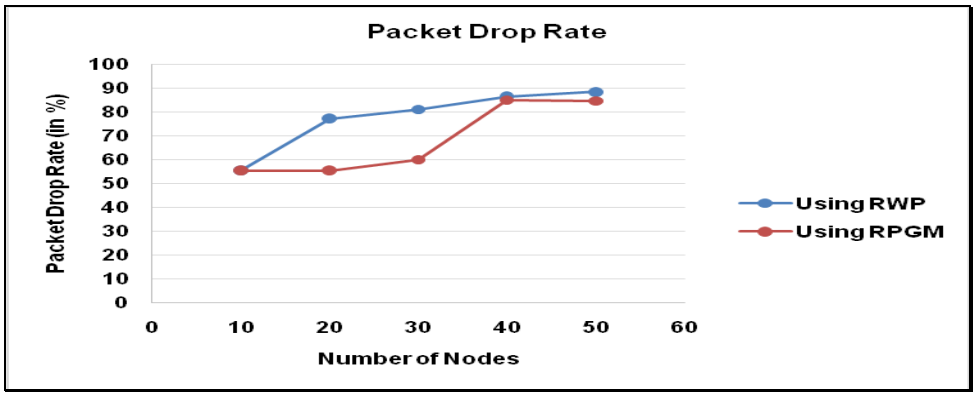

Figure 4.5: Packet Drop Rate of AODV under Different Mobility Models

4.2. Performance Analysis of AODV under Attack Environment using RWP and RPGM

AODV protocol is simulated under wormhole attack environment by varying number of nodes using CBR traffic and two mobility models. The results are discussed below:

4.2.1. Comparison of Average Throughput of AODV under attack using Random Way Point and Reference Point Group Mobility Models.

The value of throughput decreases as network size and tunnel length increases in case of RPGM. But in RWP, throughput varies. But, average

throughput of AODV under attack environment is low under random waypoint model as compared to reference point group model.

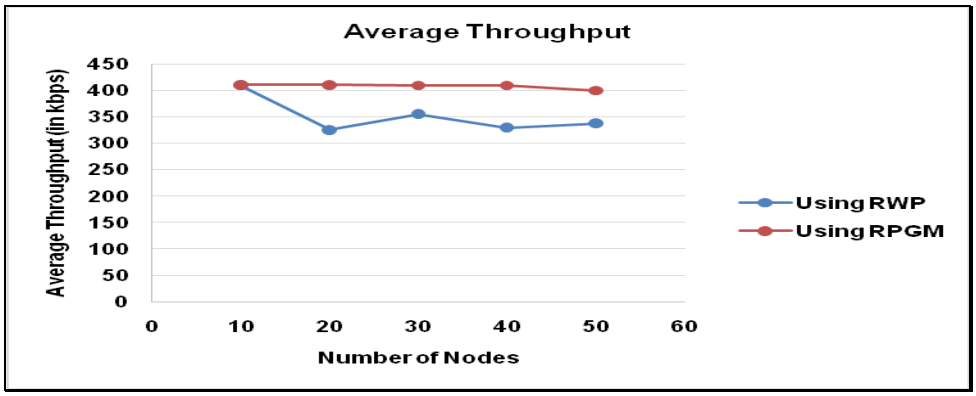

Figure 4.6: Average Throughput of AODV under Attack using Different Mobility Models

4.2.2. Comparison of Average End to End Delay of AODV under attack using Random Way Point and Reference Point Group Mobility Models.

There is a variation in delay in both scenarios. But delay increases as network size and tunnel length increases. Overall RPGM exhibits more delay due to increase in network size, tunnel length and number of groups.

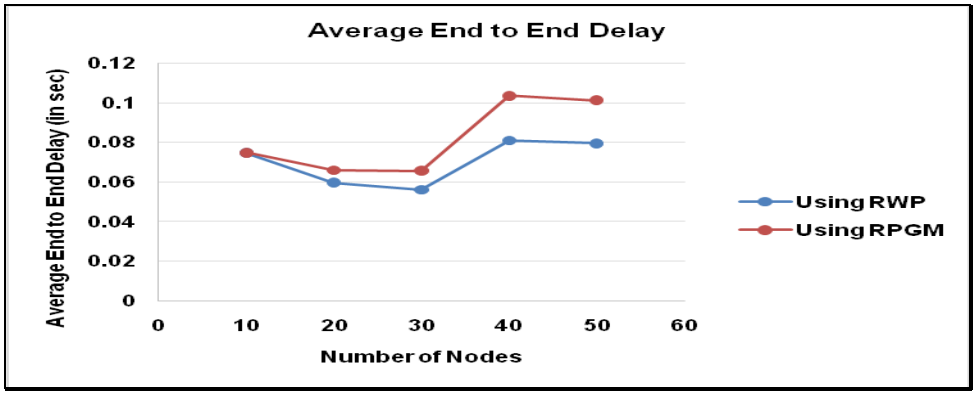

Figure 4.7: Average End to End Delay of AODV under Attack using Different Mobility Models

4.2.3. Comparison of Packet Delivery Ratio of AODV under attack using Random Way Point and Reference Point Group Mobility Models.

Initially, the value of PDR decreases up to 30 nodes and then suddenly increases for 40 nodes and then again decreases. The sudden increase is due to

the tunnelling and replaying nature of attack. More tunnel length and replay, more packets will be delivered.

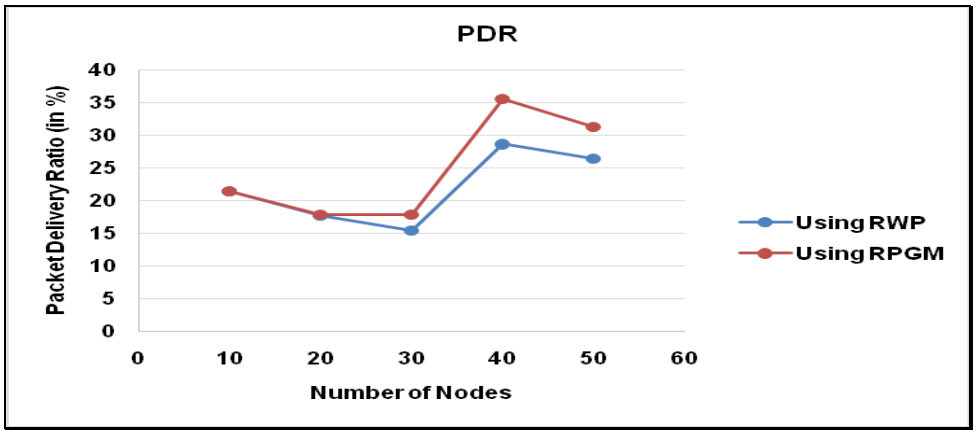

Figure 4.8: Packet Delivery Ratio of AODV under Attack using Different Mobility Models

4.2.4. Comparison of Jitter of AODV under attack using Random Way Point and Reference Point Group Mobility Models.

Jitter is more in case of reference point group mobility model and it remains almost same up to 40 nodes and then decreases. But in case of random waypoint model, initially jitter is high and then variation starts.

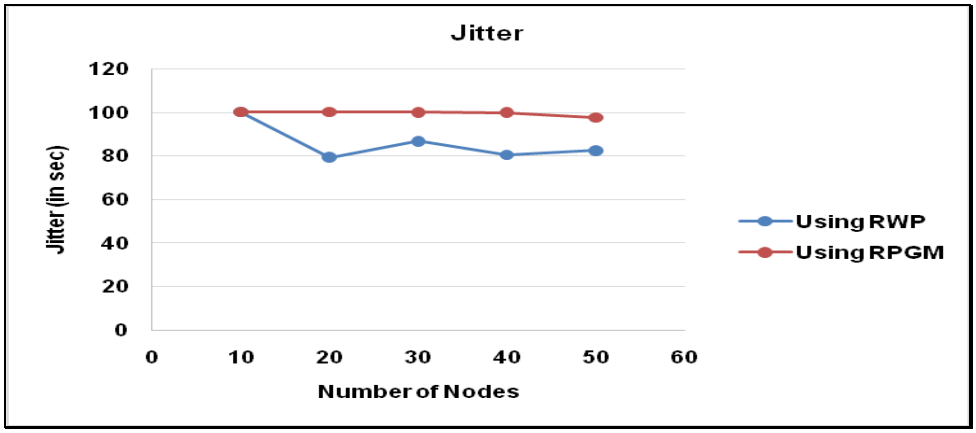

Figure 4.9: Jitter of AODV under Attack using Different Mobility Models

4.2.5. Comparison of Packet Drop Rate of AODV under attack using Random Way Point and Reference Point Group Mobility Models.

The drop rate of packets is high in case of random waypoint as compared to reference point group mobility model. More packet dropping, lesser will be throughput and packet delivery ratio in case of RWP.

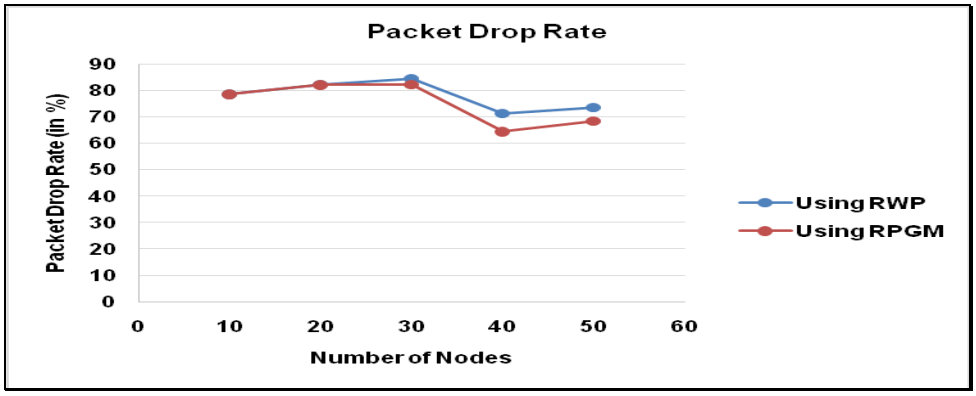

Figure 4.10: Packet Drop Rate of AODV under Attack using Different Mobility Models

4.3. Analysis of Malicious Nodes in Wormhole Peer List

To analyze malicious nodes which are participating to make a tunnel, an implementation is done at link layer (LL) of NS2, which is the part of data link layer.

The figure 4.11 shows that malicious nodes 20, 21 and 22 are participating to make tunnel (having tunnel length 3 nodes) and disrupt the normal path of AODV protocol. The NAM visualization of attack containing malicious nodes is shown in Appendix B.

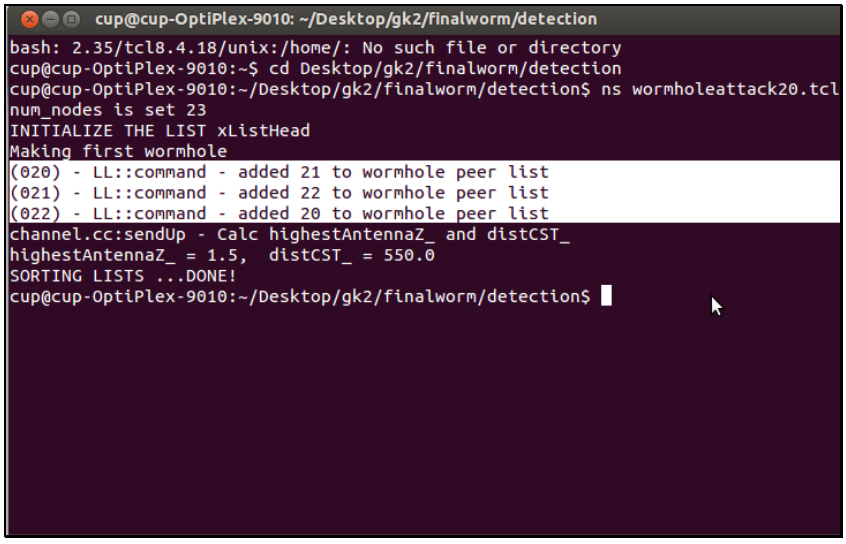

Figure 4.11: Analysis of Three Malicious Nodes

Similarly, the figure 4.12 shows that malicious nodes 30, 31, 32 and 33 are participating to make tunnel (having tunnel length 4 nodes) and disrupt the normal path of AODV protocol.

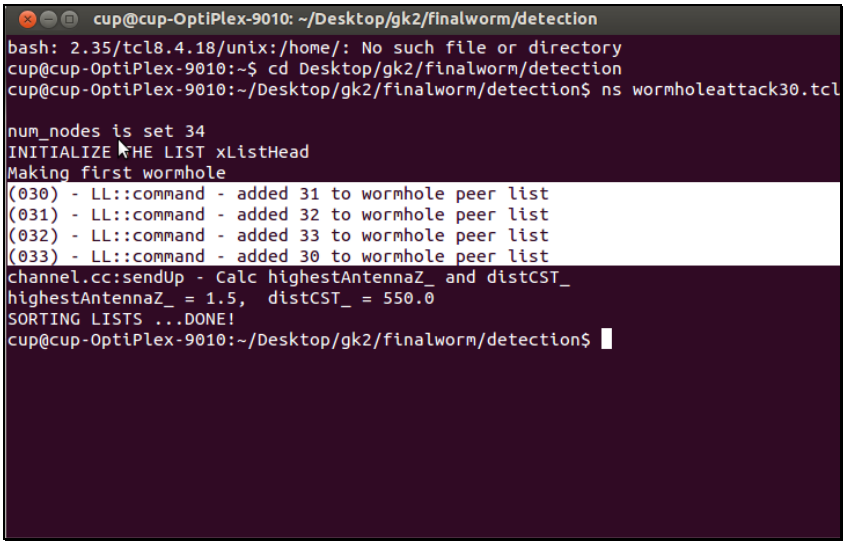

Figure 4.12: Analysis of Four Malicious Nodes

4.4. Metrics to Detect Wormhole Attack

There are different metrics to detect attack in the network. Average throughput, delay, jitter and PDR are the metrics that have been used for this research using random way point and reference point group models.

4.4.1. Detection of Attack under Random Way Point Model

- **Average Throughput:** The decrease in average throughput of AODV with attack can be used as a possible symptom of the wormhole attack. The maximum throughput difference can be observed is 287.3 kbps, when network size is 40 nodes and tunnel length is 3 nodes.

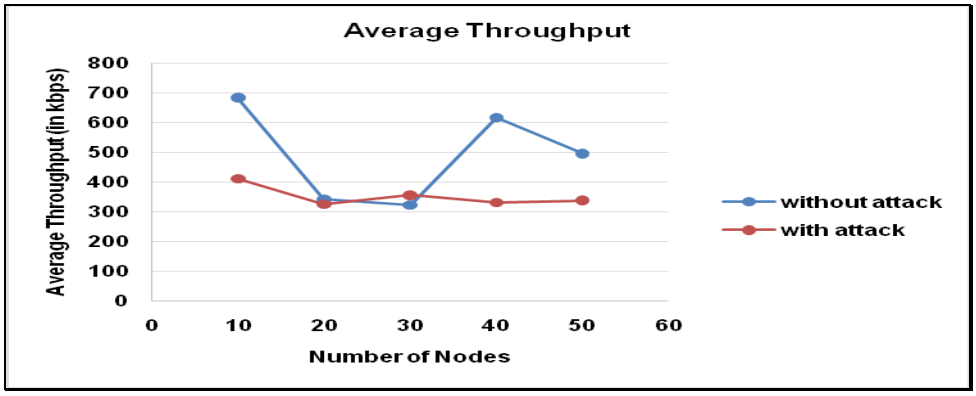

Figure 4.13: Average Throughput with and without Attack under RWP

- **Average End to End Delay:** An abrupt increase in end to end delay on the path can also be used to suspect the presence of wormhole. Initially, delay is low under attack when only one malicious node is present. But after that delay increases as network size and tunnel length increases.

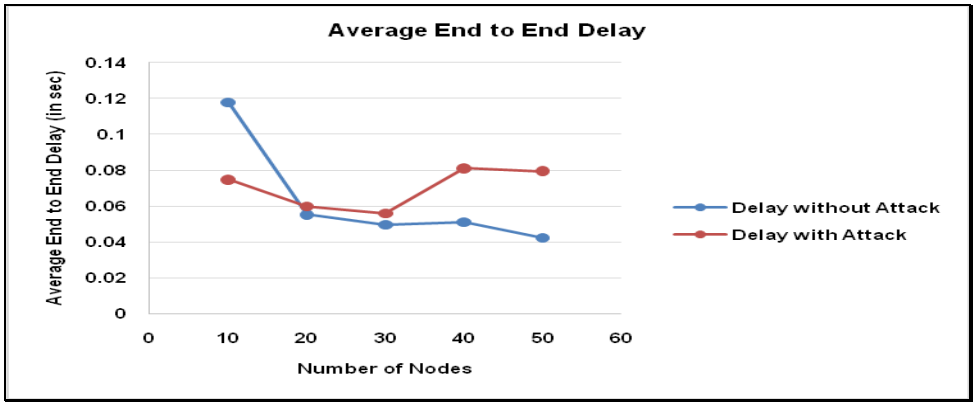

Figure 4.14: Average End to End Delay with and without Attack under RWP

- **Packet Delivery Ratio:** Packet delivery ratio is another metric for the detection. Initially, packet delivery fraction is less in case of AODV with attack. Then suddenly PDR increases in an attacked environment due to more tunnel length and node density.

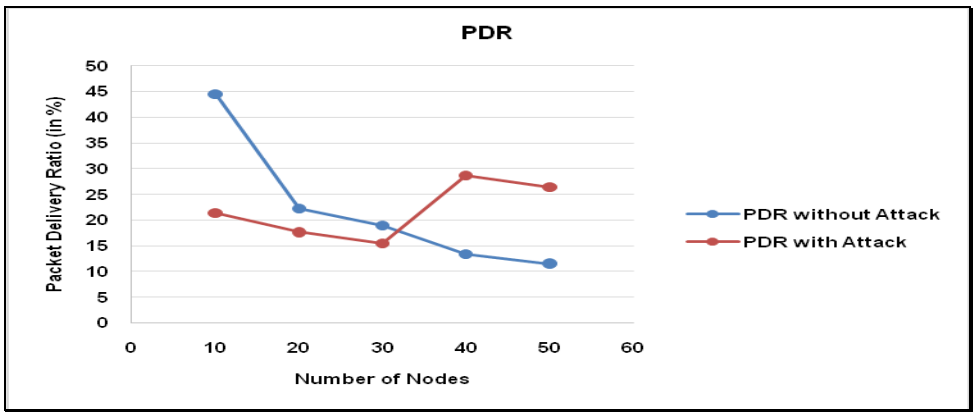

Figure 4.15: Packet Delivery Ratio with and without Attack under RWP

- **Jitter:** Jitter comes due to the variation in delay between packets which are arriving at the destination. Jitter is high in an attacked environment. The maximum jitter difference can be observed is 60.53 seconds when network size is 30 nodes and tunnel length is 3 nodes.

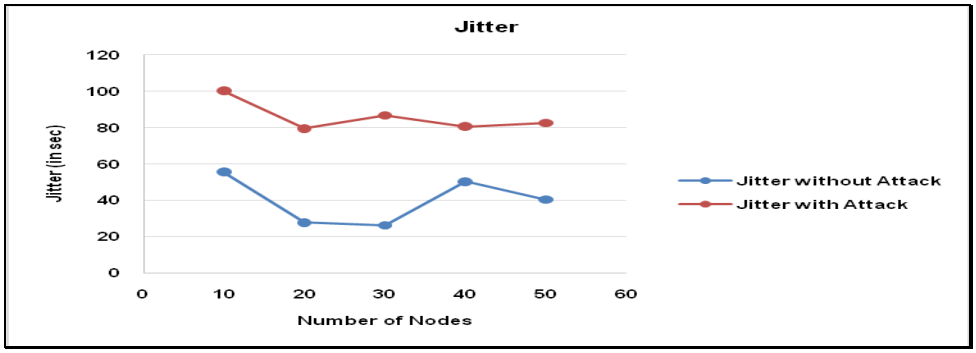

Figure 4.16: Jitter with and without Attack under RWP

4.4.2. Detection of Attack under Reference Point Group Model

- **Average Throughput:** It is clearly depicted from the graph that average throughput decreases in attack scenario due to number of groups and tunnel length increases in RPGM.

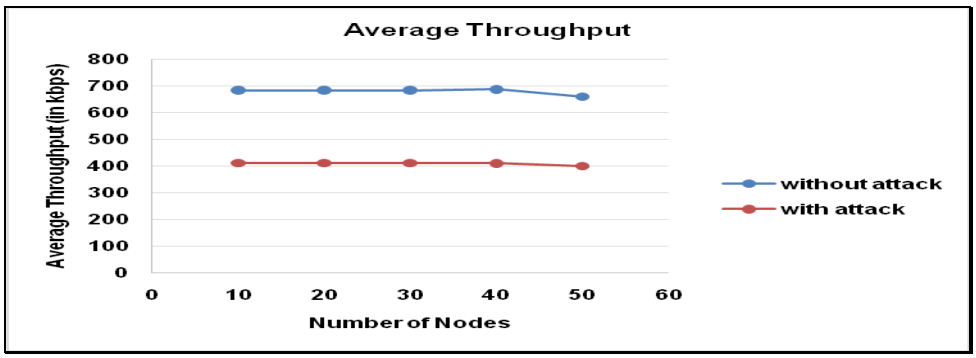

Figure 4.17: Average Throughput with and without Attack under RPGM

- **Average End to End Delay:** Initially, when node density is low, delay is less under attack environment. But as number of groups or node density and tunnel length increase, delay increases.

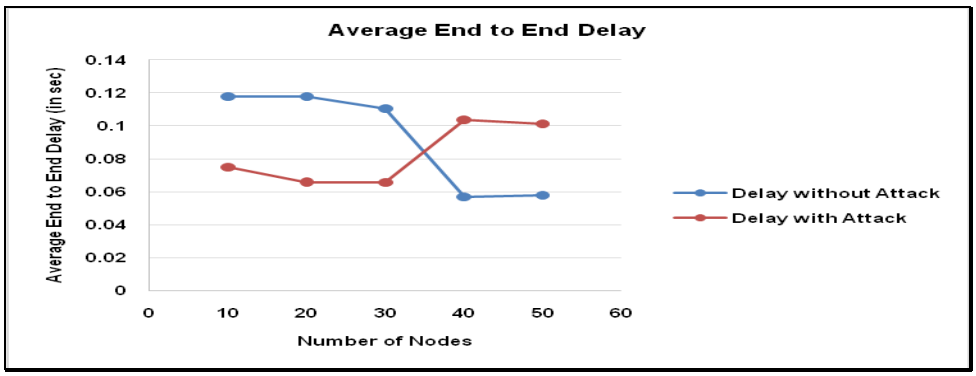

Figure 4.18: Average End to End Delay with and without Attack under RPGM

- **Packet Delivery Ratio:** Similar to delay graph, less packets are delivered under attacked environment initially. But after that PDR suddenly increases. Although PDR increases, but throughput decreases as tunnel length increases.

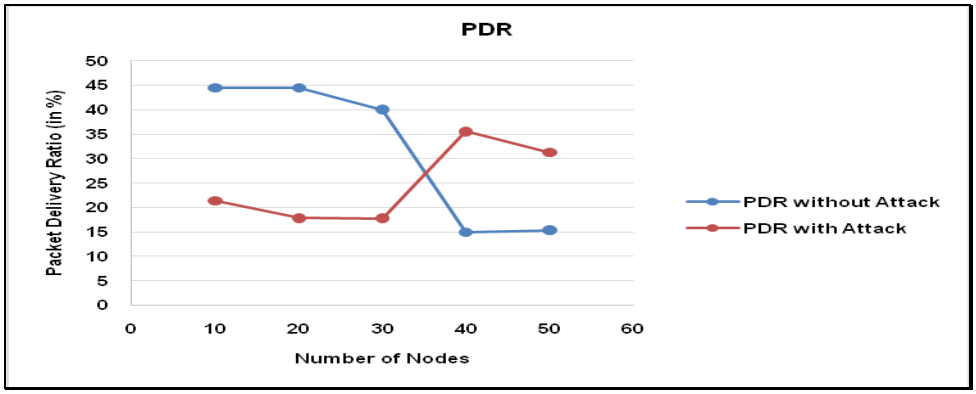

Figure 4.19: Packet Delivery Ratio with and without Attack under RPGM

- **Jitter:** It can be easily depicted from jitter graph that jitter is high with attack. It is due to the increase in tunnel length and tunnelling nature of attack.

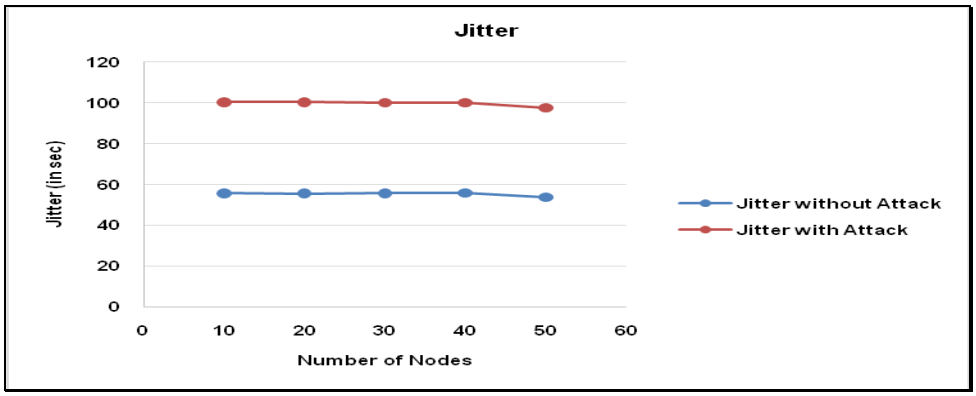

Figure 4.20: Jitter with and without Attack under RPGM

CHAPTER 5

CONCLUSIONS & FUTURE SCOPE

In the context of the important objectives of security such as authentication, privacy, integrity and availability, wormhole attack is very serious threat and it must be treated as the highest priority threat. The performance analysis of AODV without attack and under attack has been carried out in a comprehensive manner using random way point model and reference point group mobility model along with its detection.

Firstly, AODV without attack is analyzed under random waypoint and reference point group models. In reference point group model, the value of throughput, PDR, end-to-end delay and jitter is high but packet drop rate is low. It shows that AODV performs well for throughput, PDR and packet drop rate under RPGM and for delay and jitter under RWP.

Secondly, AODV under wormhole attack is analyzed using two mobility models namely random waypoint and reference point group models. Analysis shows that AODV under attack gives high value for throughput, PDR, delay and jitter in RPGM and low for packet drop rate in RWP. It shows that delay and jitter is increased in RPGM as number of groups and tunnel length increased and packets are more dropped in case of RWP.

Along with above, one more step has been taken to analyze the malicious nodes which are making tunnel to perform attack.

Then the detection of attack with the help of various metrics such as throughput, delay, packet delivery ratio and jitter for both models has been done. And it is concluded that throughput decreases and delay and jitter increases under attack environment. It can also be analyzed that the value of PDR is less for small network size. But as number of nodes increases, PDR increases.

As a future work, this work can be enhanced by analyzing AODV routing protocol under wormhole attack using other mobility models and by considering various metrics such as routing overhead and normalized routing load etc. An attempt can also be made to mitigate malicious nodes which help to make wormhole tunnel.

REFERENCES

ACoRN. (2010). Ad Hoc Networks. ARC Communications Research Network. <http://www.acorn.net.au/telecoms/adhocnetworks/adhocnetworks.html>. Accessed 2014 May, 21.

Agrawal, R., Tripathi, R., and Tiwari, S. (2012, April). Performance Comparison of AODV and DYMO MANET Protocols under Wormhole Attack Environment. International Journal of Computer Applications. ***44*(9):** 9-16.

Amnai, M., Fakhri, Y., and Abouchabaka, J. (2011). Evaluation of Impact of Traffic VBR and Mobility on the Performance of AODV Routing Protocols in Mobile Ad hoc Networks. IEEE Transactions. 1-5.

Argyroudis, P. G., and O'Mahony, D. (2005). Secure Routing for Mobile Ad Hoc Networks. IEEE Communications Surveys & Tutorials, Third Quarter. ***7*(3):** 2-21.

Aschenbruck, N., Ernst, R., Gerhards-Padilla, E., and Schwamborn, M. (2010, March). Bonnmotion- A Mobility Scenario Generation and Analysis Tool. ICST. 1-10. <203.144.248.23/ACM.FT/1810000/1808207/a51-aschenbruck.pdf>. Accessed 2013 Dec, 5.

Aschenbruck, N., Gerhards-Padilla, E., and Martini, P. (2008). A Survey on Mobility Models for Performance Analysis in Tactical Mobile Networks. Journal of Telecommunications and Information Technology. 54-61.

Azer, M., El-Kassas, S., and El-Soudani, M. (2009, May). A Full Image of the Wormhole Attacks towards Introducing Complex Wormhole Attacks in Wireless Ad Hoc Networks. International Journal of Computer Science and Information Security. **1:** 41-52.

Bai, F., and Helmy, A. Chapter 1: A Survey of Mobility Models. 1-30. <www.cise.ufl.edu/~helmy/papers/Survey-Mobility-Chapter-1.pdf>. Accessed 2014 Feb, 17.

Bai, F., Sadagopan, N., and Helmy, A. (2004, February). User Manual for IMPORTANT Mobility Tool Generators in NS-2 Simulator. 1-12.

Bakhshi, B. (2013). Introduction to NS-2. <http://www.ceit.aut.ac.ir/~bakhshi/ns-2/NS-2.pdf>. Accessed 2013 Oct, 14.

Baumann, R. (2002, April). AODV: Ad Hoc On Demand Distance Vector Routing Protocol. 1-19. <http://www.rainer-baumann.ch/public/qec.pdf>. Accessed 2013

Nov, 3.

Bonnmotion. <http://sys.cs.uos.de/bonnmotion/download.shtml>. Accessed 2014 Jan, 16. University of Osnabruck.

Boukhalkhal, A., Yagoubi, M. B., Djoudi, M., Ouinten, Y., and Benmohammed, M. (2008). Simulation of Mobile Ad hoc Routing Strategies. IEEE Transactions. 128-132.

Chiu, H.S., and Lui, K.S. (2006, January). DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks. In Proceedings of the 1st International Symposium on Wireless Pervasive Computing. pp. 6–11.

Close, D. B., Robbins, A. D., Rubin, P. H., Stallman, R., and Oostrum, P. V. (1995, December). The AWK Manual. 1-136. <www.staff.science.uu.nl/~oostr102/docs/nawk/nawk_toc.html>. Accessed 2013 Oct, 6.

Cordeiro, C. M., and Agarwal, D. P. (2002). Mobile Ad Hoc Networking. OBR Research Center for Distributed and Mobile Computing, ECECS, University of Cincinnati, USA. <www.dia.unisa.it/~vitsca/RC-0809I/survey_ad_hoc.pdf>. Accessed 2013 Aug, 21.

Dubey, A. (2013, March). How to Install NS2.35 in Ubuntu 12.04. <http://princeabhinav.blogspot.in/>. Accessed 2013 Sep, 12.

Ehsan, H., and Khan, F.A. (2012). Malicious AODV. In Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communication, IEEE Computer Society. pp. 1181-1187. Liverpool.

Gandhewar, N., and Patel, R. (2012). Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad Hoc Network. In Proceedings of the Fourth International Conference on Computational Intelligence and Communication Networks, IEEE Computer Society. pp. 714-718. Mathura.

Gandhi, S., Chaubey, N., Tada N., and Trivedi, S. (2012). Scenario-based Performance Comparison of Reactive, Proactive & Hybrid Protocols in MANET. In Proceedings of the IEEE International Conference on Computer Communication and Infomatics. pp. 1-5. Coimbatore.

Gupta, S., Kar, S., and Dharmaraja, S. (2011). WHOP: Wormhole Attack Detection Protocol using Hound Packet. In Proceedings of the IEEE International Conference on Innovation Technology. pp. 226-231. Abu Dhabi.

Gupta, S., Kumar, C., Rani, S., and Bhushan, B. (August 2012). Performance Comparison of Routing Protocols Using Different Mobility Models. International Journal of Modern Education and Computer Science. **8:** 54-61.

Hoebeke, J., Moerman, I., Dhoedt, B., and Demeester, P. (2004). An Overview of Mobile Ad Hoc Networks: Applications and Challenges. Journal-Communications Network. ***3*(3):** 60-66. <cwi.unik.no/images/Manet_Overview.pdf>. Accessed 2014 Jan, 26.

Hu, Y.C., Perrig, A., and Johnson, D.B. (2003). PACKET LEASHES: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. IEEE INFOCOM. 1976–1986.

Issariyakul, T., and Hossain, E. (2011). Introduction to Network Simulator. Computer Networks. <books.google.co.in/books?isbn=1461414067>. Accessed 2013 Sep, 9.

Jain, N., and Shrivastava, A.K. (2013, August). Reactive Routing Approach for Preventing Wormhole Attack using Hybridized WHOP. IOSR Journal of Computer Engineering. **13:** 87-95.

Jathe, S. R., and Dakhane, D. M. (2012, January). Indicators for Detecting Sinkhole Attack in MANET. International Journal of Emerging Technology and Advanced Engineering. **2:** 2250-2459.

Jayakumar, G., and Ganapathi, G. (2008, December). Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols. Hindawi Publishing Corporation, Journal of Computer Systems, Networks, and Communication. ***1*(11):** 1-5.

Jenefer, F. A., and Vydeki, D. (2013). Performance Analysis of Mobile Ad Hoc Network in the Presence of Wormhole Attack. International Journal of Advanced Computer Engineering and Communication Technology. ***1*(1):** 13-18.

Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., and Jamalipour, A. (2007, October). A Survey of Routing Attacks in Mobile Ad Hoc Networks. IEEE Wireless Communications. ***14*(5):** 85-91.

Kaur, A., and Mittal, M. (2014, March). A Comprehensive Review on Performance of AODV and DSDV Protocol using Manhattan Grid Mobility Model. International Journal of Research in Engineering and Technology. **3:** 496-505.

Kaur, G., and Kaur, A. (2014, May). A Comprehensive Review on Performance of AODV Protocol for Wormhole Attack. International Journal of Research in Engineering and Technology. ***3(5):*** 531-537.

Khainwar, R.J., Jain, A., and Tyagi, J.P. (2013). Elimination of Wormhole Attacker Node in MANET Using Performance Evaluation Multipath Algorithm. Network and Complex Systems. ***3*****(7):** 22-29.

Khalil, I., Bagchi, S., and Shroff, N.B. (2005). LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. In Proceedings of the International Conference on Dependable Systems and Networks. pp. 612–621.

Khatkar, A., and Singh, Y. (2012). Performance Evaluation of Hybrid Routing Protocols in Mobile Adhoc Networks. In Proceedings of the IEEE Second International Conference on Advanced Computing & Communication Technologies. pp. 542-545. Rohtak, Haryana.

Khemariya, N., and Khuntetha, A. (2013, March). An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs. International Journal of Computer Applications. **66:** 18-24.

Kumar, D., Srivastava, A., and Gupta, S. C. (2013). Routing in Ad Hoc Networks under Reference Point Group Mobility. European Modelling Symposium, IEEE Computer Society. 595-598.

Kumar, S., Sharma, S. C., and Suman, B. (2011, July). Impact of Mobility Models with Different Scalability of Networks on MANET Routing Protocols. International Journal of Scientific & Engineering Research. ***2*****(7):** 1-5.

Kumar, S., Singh, D., and Chawla, M. (2011). Performance Comparison of Routing Protocols in MANET Varying Network Size. International Journal of Smart Sensors and Ad Hoc Networks. ***1*****(2):** 51-54.

Mahajan, V., Natu, M., and Sethi, A. (2008). Analysis of Wormhole Intrusion Attacks in MANETs. In Proceedings of the IEEE Military Communications Conference (MILCOM). pp. 1-7. San Diego, CA.

Marina, M. K., and Das, S. R. (2005). Routing in Mobile Ad Hoc Networks. 63-90. <http://link.springer.com/chapter/10.1007%2F0-387-22690-7_3>. Accessed 2014 Feb, 16.

Maulik, R., and Chaki, N. (2011). A Study on Wormhole Attacks in MANET. International Journal of Computer Information Systems and Industrial Management Applications. **3:** 271-279.

Meenaghan, P., and Delaney, D. (2004, April). An Introduction to NS, Nam and OTcl Scripting. National University of Ireland, Maynooth. 1-39.

Mohan, R., Rajan, C., and Shanthi, N. (2012, December). A Stable Mobility Model Evaluation Strategy for MANET Routing Protocols. International Journal of Advanced Research in Computer Science and Software Engineering. ***2*(12):** 58-65.

Nayak, P., Sahay, A., and Pandey, Y. (2013, June). Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet. International Journal of Scientific & Engineering Research. ***4*(6):** 1216-1222.

ns-allinone-2.35 Package. <http://sourceforge.net/projects/nsnam/files/latest/download>. Accessed 2013 Sep, 23.

Patil, V. C. (2012). Chapter-3: Overview of Mobile Ad Hoc Networks. 19-36. <http://www.shodhganga.inflibnet.ac.in/bitstream/10603/4106/.../11_chapter%203.pdf>. Accessed 2013 Dec, 21.

Perkins, C. E. (2013). Ad Hoc Networking with AODV. <http://www.psg.com/~charliep/txt/Daedeok2002/AODV-Daedeok.pdf>. Accessed 2013 Nov, 2.

Rocha, F. (2010, April). NS2 Visual Trace Analyzer. 1-17. <mailman.isi.edu/pipermail/ns-users/2012-July/072075.html>. Accessed 2013 Aug, 4.

Romsaiyud, W., Premchaiswadi, W., and Premchaiswadi, N. (2012). An Autonomous Group Mobility Prediction Model for Simulation of Mobile Ad-hoc through Wireless Network. Journal of Wireless Networking and Communication. ***2*(5):** 126-135.

Sadasivam, K. Tutorail for Simulation-based Performance Analysis of MANET Routing Protocols in NS-2. <sce.uhcl.edu/yang/teaching/csci5931netSecuritySpr05/ns-tutorial.doc>. Accessed 2014 Jan, 4.

Sanaei, M.G.P., Isnin, I.F., and Bakhtiari, M. (2013, June). Performance Evaluation of Routing Protocol on AODV and DSR under Wormhole Attack.

International Journal of Computer Networks and Communication Security. ***1*(1):** 1-6.

Sanfilippo, S. (2004). TCLWISE: An Introduction to Tcl Programming Language. <http://www.invece.org/tclwise/introduction.html>. Accessed 2013 Aug, 20.

Sarkar, N.I., and Lol, W.G. (2010). A Study of MANET Routing Protocols: Joint Node Density, Packet Length and Mobility. IEEE Personal Communications. 515-520.

Shakshuki, E. M., Kang, N., and Sheltami, T. R. (2013, March). EAACK – A Secure Intrusion – Detection System for MANETs. IEEE Transactions on Industrial Electronics. ***60*(3):** 1089-1098.

Shruthi, M., Shashikiran, B. S., and Nagendra, S. K. (2014, May). Mobile Ad-hoc Network: Working of Routing Protocols and Applications. International Journal of Innovative Research in Computer and Communication Engineering. ***2*(2):** 110-117.

Singh, G. K., Kaur, A., and Sangal, A. L. (2011). Performance Analysis of DSR, AODV Routing Protocols based on Wormhole Attack in Mobile Ad-hoc Network. In Proceedings of the 5th IEEE International Conference on Advanced Computing & Communication Technologies. pp. 31-36.

Singh, J., Kumar, K., Sachdeva, M., and Sidhu, N. (2012, June). DDoS Attack's Simulation using Legitimate and Attack Real Data Sets. International Journal of Scientific & Engineering Research. **3:** 1-5.

Su, M.Y. (2010, March). WARP: A Wormhole Avoidance Routing Protocol by Anomaly Detection in Mobile Ad Hoc Networks. Computers & Security. **29:** 208-224.

Upadhyay, V. K., and Shukla, R. (2013). An Assessment of Worm Hole Attack over Mobile Ad-Hoc Network as Serious Threats. International Journal of Advanced Networking and Applications. **5:** 1858-1866.

Vandana, C. P., and Devaraj, A. F. S. (2013). Evaluation of Impact of Wormhole Attack on AODV. International Journal of Advanced Networking and Applications. ***4*(4):** 1652-1656.

APPENDIX A

SIMULATIONS FOR AODV

Performance Analysis of AODV without Attack: There are two scenarios for simulation of AODV without attack. The protocol is simulated under random waypoint and reference point group models by varying the number of nodes. A number of simulations are performed as:

TABLE 5: Simulation Scenario for AODV without Attack

Mobility Model	**Number of Nodes**	**Performance Metrics**
Random Waypoint Model	10, 20, 30, 40, 50	Average Throughput, Average End to End Delay, Jitter, Packet Drop Rate and Packet Delivery Ratio
Reference Point Group Mobility Model	10 (1 group), 20 (2 groups), 30 (3 groups), 40 (4 groups), 50 (5 groups)	Average Throughput, Average End to End Delay, Jitter, Packet Drop Rate and Packet Delivery Ratio

Performance Analysis of AODV under Attack: There are two scenarios for simulation of AODV under attack. The attack is simulated under random waypoint and reference point group models by varying the number of nodes. A number of simulations are performed as:

TABLE 6: Simulation Scenario for AODV under Attack

Mobility Model	Number of Nodes	Tunnel Length	Performance Metrics
Random Waypoint Model	10, 20, 30, 40, 50	1, 3, 3, 5, 5 nodes resp.	Average Throughput, Average End to End Delay, Jitter, Packet Drop Rate and Packet Delivery Ratio
Reference Point Group Mobility Model	10 (1 group), 20 (2 groups), 30 (3 groups), 40 (4 groups), 50 (5 groups)	1, 3, 3, 5, 5 nodes resp.	Average Throughput, Average End to End Delay, Jitter, Packet Drop Rate and Packet Delivery Ratio

APPENDIX B

NAM VISUALIZATION OF MALICIOUS NODE ANALYSIS

Figure B.1 shows the normal route that is taken by AODV between source and destination.

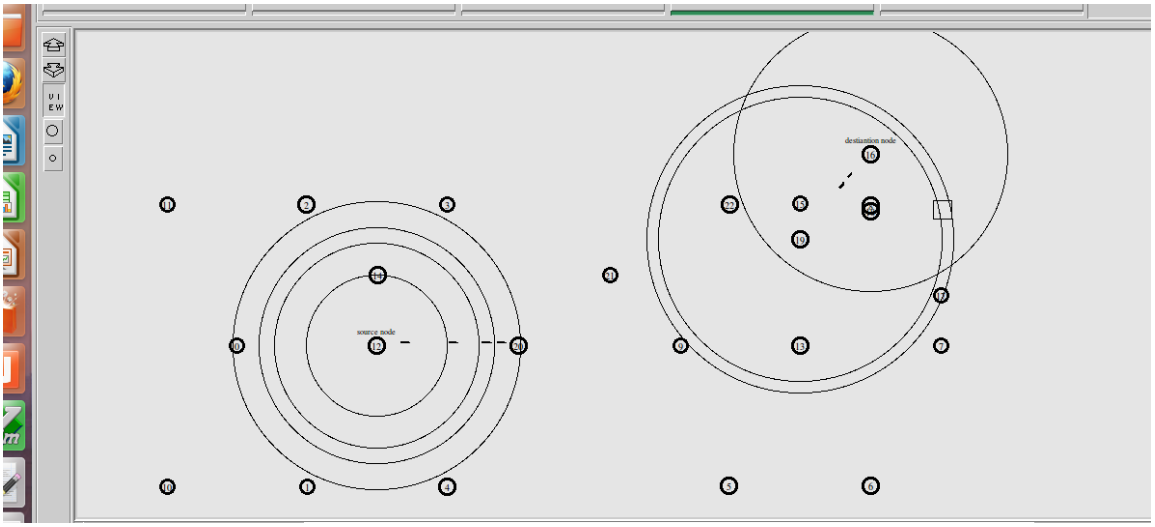

Figure B.1: NAM Visualization of Normal Route

Figure B.2 shows the wormhole route, in which malicious nodes 20, 21 and 22 are participating to make tunnel (having tunnel length 3 nodes) and disrupt the normal route of AODV.

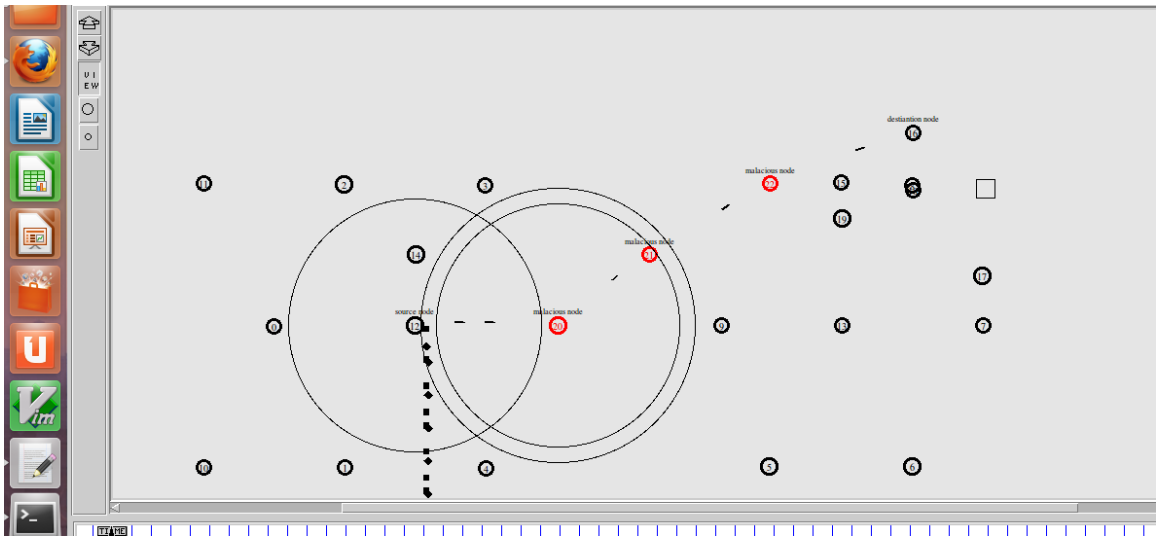

Figure B.2: NAM Visualization of Wormhole Route

APPENDIX C

MOVEMENT SCENARIOS USING DIFFERENT MOBILITY MODELS

The mobility models such as Random Way Point and Reference Point Group Mobility Models are used to generate movements for various nodes. All the nodes are kept mobile. Following codes are incorporated in the Tcl scripts for movement generation:

Movement generation for a node using Random Way Point Model:

$node_(0) set X_ 137.51203233411772

$node_(0) set Y_ 108.58918965821965

$ns_ at 0.0 "$node_(0) setdest 21.673269943956164 52.674727394871304 1.1030698767836309"

$ns_ at 116.60870281605776 "$node_(0) setdest 21.673269943956164 52.674727394871304 0.0"

$ns_ at 135.6951346926237 "$node_(0) setdest 29.434828889017147 57.319921712880074 0.63233117316327368"

Movement generation for a node using Reference Point Group Mobility Model

$node_(0) set X_ 138.76203273476995

$node_(0) set Y_ 96.30016355264706

$ns_ at 0.0 "$node_(0) setdest 121.13035349280683 24.838188980171658 0.7360495854688456"

APPENDIX D

INSERTED REQUIRED CODE TO VARIOUS FILES

Inserted code in ll.cc to initialize wormhole peer list head

```
// initialize wormhole peer list head
Wormhole_head.ll = NULL;
Wormhole_head.id = -1;
Wormhole_head.next = NULL;
```

Inserted code in ll.cc to allocate the size of wormhole peer list

```
else if (strcmp (argv[1],  "wormhole-peer") == 0) {
wormhole_peer* wp = (wormhole_peer*) malloc (sizeof (wormhole_peer));
    if (!wp) {
            fprintf(stderr, "(%03d) - LL:command - error allocating memory for
    new wormhole peer! ");
            exit(-1);
}
// init fields
wp->ll = (LL *) TclObject :: lookup(argv[2] );
wp->id = wp-> ll-> mac_->addr();
//insert at head of list
wp->next = wormhole_head.next;
wormhole_head.next = wp;
printf ("(%03d) - LL :: command – added %d to wormhole_peer list\n", mac-
    >addr(), wp->id):
return TCL_OK;
}
```

Inserted code in ll.h to define elements for the wormhole peer list

```
Class LL;
typedef struct wormhole_peer_struct {
        LL* ll;
        int id;
        struct wormhole_peer_struct* next;
} wormhole_peer;
```

Inserted code in attack.tcl to configure malicious nodes

```
Puts "Making first wormhole"
set wh1 [$ns node]
$wh1 color "red"
$ns at 0.0 "$wh1 color red"
$wh1 set X_ 300.0
$wh1 set Y_ 500.0
$wh1 set Z_ 0.0
$ns initial_node_pos $wh1 20
$ns at 0.01 "$wh1 label \"malicious node\" "

set wh2 [$ns node]
$wh2 color "red"
$ns at 0.0 "$wh2 color red"
$wh2 set X_ 800.0
$wh2 set Y_ 500.0
$wh2 set Z_ 0.0
$ns initial_node_pos $wh2 20
$ns at 0.01 "$wh2 label \"malicious node\" "

[$wh1 set ll_(0)] wormhole-peer [$wh2 set ll_(0)]
[$wh2 set ll_(0)] wormhole-peer [$wh1 set ll_(0)]
```