

<p>CENTRAL LIBRARY TEZPUR UNIVERSITY</p> <p>Accession No. <u>T 313</u></p> <p>Date _____</p>
--

Addressing Some Issues in Packet Dropping Attack Detection in MANETs

*A thesis submitted in partial fulfillment of the requirements for the
degree of*

Doctor of Philosophy

by

Bobby Sharma Kakoty

Registration No. 001 of 2014



**Department of Computer Science and Engineering
School of Engineering, Tezpur University
Tezpur, Assam, India - 784028
October, 2014**

Abstract

Mobile ad hoc network (MANET) has emerged as an evolution of wireless network technology and is likely to be an integral part of future communication environments. Security remains a major challenge for these networks due to its intrinsic properties such as openness of media, lack of centralized control and dynamically changing topologies etc. Among the different attacks to which such networks are vulnerable to, packet dropping attack (PDA) remains a major concern.

This thesis addresses packet dropping attack detection methodologies under cooperation of nodes. In order to understand the problem of attack detection, a Centralized Packet Dropping Attack Detection Methodology has been worked out. It is a static off line system and can detect PDA from some audited data. In this system data from the individual nodes in the network are shipped to a central location. Data collected from different nodes are analyzed individually in order to detect PDA. From simulation results, it has been observed that centralized PDA detection methodology do not perform well in highly dynamic networks such as MANETs. The proposed PDA detection methodology gets initialized for every change in the network topology, which leads to an extra overhead in case of highly dynamic networks.

Thereafter a Distributed Packet Dropping Attack Detection Methodology based on ad hoc rules of cooperation has been proposed. In this methodology, PDA in the network is not only confirmed by the node that has been suffering, but it is also confirmed by the neighbor nodes dynamically. For this, proposed methodology evaluates initial TRUST of each node. Based on cooperative participation of nodes in communication as well as performance of the nodes in detection methodology, TRUST value of the node is dynamically updated. Distributed PDA detection methodology detects and isolates the malicious nodes from the network. This methodology is compared with two other existing methodologies namely SAODV and TAODV for various network performance parameters.

To formalize the cooperation, distributed packet dropping attack detection methodology has been modeled as a cooperative game. In game theoretic approach to

distributed PDA detection methodology, malicious nodes that are involved in packet dropping attacks are considered to be in one side of the game while genuine nodes that participate in network communication genuinely are in the other side of the game. Genuine nodes try to form a coalition for communication to maximize their payoffs; while those nodes that are not responding rationally or selfish or malicious nodes are considered to be outside the coalition of genuine nodes.

For Centralized as well as distributed PDA detection methodologies, simulations are done for various network environments to measure the effectiveness of the methodologies. In both the approaches, two network mobility models namely Random *Way Point* model and *Levy Walk* model are considered. Initially, Random way point mobility model has been tried as it is a commonly used mobility model for MANETs. This model explains the movement pattern of independent nodes in a simplified way. Random way point model is simple enough to be theoretically tractable and at the same time, to be simulated in network simulators in a scalable manner. However, no empirical evidence exists to prove the accuracy of such models. At the same time, it is observed that human walks are not random walks, but the patterns of human walks and mobility in Levy walks model are similar to each other in some statistical way. Hence to evaluate accuracy of both the proposed systems in a more realistic network mobility environment, simulations are done in Levy Walk model also. Furthermore, simulation has been carried out to validate the game theoretic formulation of the distributed PDA detection.

Keywords: MANETs, Packet Dropping Attack Detection, Distributed Packet Dropping Attack Detection, Cooperation, Random walk, Levy Walk, Game Theory, Performance Parameters.



TEZPUR UNIVERSITY

Certificate

This is to certify that the thesis titled "**Addressing Some Issues in Packet Dropping Attack Detection in MANETs**" submitted to Tezpur University in the Department of Computer Science and Engineering under the School of Engineering in partial fulfillment of the award of the degree of Doctor of Philosophy in Computer Science and Engineering is a record of research work carried out by Mrs. Bobby Sharma Kakoty under our supervision and guidance.

All helps received by her from various sources have been duly acknowledged.

No part of this thesis has been submitted elsewhere for award of any other degree.

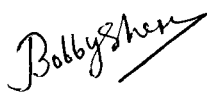
Signature of Supervisor
(Shyamanta Moni Hazarika)
Professor,
Computer Science and Engineering
Tezpur University, Tezpur, Assam

Signature of Co-Supervisor
(Nityananda Sarma)
Professor,
Computer Science and Engineering
Tezpur University, Tezpur, Assam

Candidate's Declaration

I hereby certify that the work which is being presented in thesis entitled **“Addressing Some Issues in Packet Dropping Attack Detection in MANETs”**, in partial fulfillment of the requirement of the award of the Degree of Doctor of Philosophy and submitted in the Department of Computer Science and Engineering under School of Engineering, Tezpur University, is an authentic work carried out by me under the supervision of Prof. Shyamanta Moni Hazarika and Prof. Nityananda Sarma of Department of Computer Science and Engineering, School of Engineering of Tezpur University.

The results embodied in this thesis have not been submitted in part or in full, to any other university for award of any degree or diploma.


(Bobby Sharma Kakoty)



TEZPUR UNIVERSITY

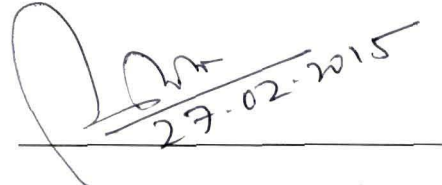
Certificate

This is to certify that the thesis titled "**Addressing Some Issues in Packet Dropping Attack Detection in MANETs**" submitted by Bobby Sharma Kakoty to Tezpur University in the Department of Computer Science and Engineering under the School of Engineering in partial fulfillment of the award of the degree of Doctor of Philosophy in Computer Science and Engineering has been examined by us on and found to be satisfactory.

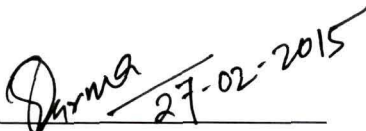
The committee recommends for award of the degree of Doctor of Philosophy.



Signature of Supervisor
(Shyamanta Moni Hazarika)
Professor,
Computer Science and Engineering
Tezpur University, Tezpur, Assam



Signature of External Examiner
**EXTERNAL
EXAMINER**



Signature of Co-Supervisor
(Nityananda Sarma)
Professor,
Computer Science and Engineering
Tezpur University, Tezpur, Assam

Acknowledgement

First of all, I take this opportunity to express my heartiest gratitude to my both supervisors- Prof. Shyamanta Moni Hazarika and Prof. Nityananda Sarma for their continual trust on my work and accepting me as research scholar under them. I am very much thankful to both of them for their various guidance, encouragement and support in carrying out this work smoothly. I also take this opportunity to express my gratitude towards all the teachers, office staff and research scholars of this department for their constant support.

My sincere thanks to the entire administrative staff of this University for providing necessary administrative assistance in the completion of the work.

I am extremely grateful to all the successful authors, whose precious works are consulted and referred in my work. I am also thankful to Mr. Sanjeev Kr. Deka, Asst. Prof. and Mr. Prakash Chauhan, Project Associate, Dept. of CSE, Tezpur University, for their esteem help.

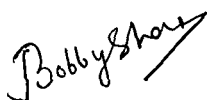
My special thanks goes to my child "Google" for his scarifies and patient in his early stage of childhood to continue my research work.

I am very much thankful to my husband "Vikram" for his constant inspiration.

My sincere thanks to my parents, mother-in-law and Late father-in-law, for their blessings, constant support and encouragement to carry my work sincerely.

I am thankful to any other persons who had inspired me to carry out my research smoothly.

Finally, I bow down my head in front of the almighty for assigning this job and blessing me to accomplish the task successfully.



Bobby Sharma Kakoty

Contents

List of Figures

List of Tables

List of Algorithm

List of Abbreviations

Chapter 1. Introduction

1.1 MANETs and its vulnerabilities	1
1.2 Packet dropping attack: its remedies & mitigation	4
1.3 Motivation	7
1.4 Objective	9
1.5 Thesis outline	11

Chapter 2. Literature Review and General Discussion

2.1 Introduction to MANETs	14
2.1.1 Characteristics	14
2.1.2 Routing in MANETs	16
2.1.3 Routing Protocols	18
2.1.4 Mobility Model	20
2.1.4.1 Random Model	21
2.1.4.1.1 Random Waypoint Model	22
2.1.4.2 Levy Walk Model	23
2.1.4.3 Model with Temporal Dependency	24
2.1.4.3.1 Gauss Markov Mobility Model	25
2.1.4.4 Model with Spatial Dependency	25
2.1.4.4.1 Reference Point Group Model	25
2.1.4.5 Model with Geographic Restriction	26
2.1.4.5.1 Pathway Mobility Model	26

2.1.5	Security Issues	27
2.1.5.1	Introduction	27
2.1.5.2	Types of Attack in MANETs	28
2.1.5.3	Security Goals	32
2.1.5.4	Vulnerabilities in Existing Protocol	32
2.1.5.5	Security Mechanism	34
2.1.5.6	Secure Routing Protocol	35
2.1.5.6.1	SAODV	37
2.1.5.6.2	TAODV	38
2.1.5.6.3	OCEAN	41
2.2	Packet Dropping Attack in MANETs	43
2.2.1	Types of Packet Dropping Attack	44
2.2.1.1	Selective Packet Dropping Attack	44
2.2.1.2	Malicious Packet Dropping Attack	45
2.2.2	Mitigation of Impact of Packet Dropping Attack in MANETs	46
2.2.2.1	Selfish Node Mitigation	46
2.2.2.2	Malicious Node Mitigation	47
2.3	PDA Detection Methodology	48
2.3.1	Categories of PDA Detection Methodology	49
2.3.2	Existing Detection Methodologies	53
2.3.3	Desirable Properties of Detection Methodology	55
2.4	Game Theoretic Approach	56
2.4.1	Introduction	56
2.4.2	Game Theoretic Approach to PDA Detection in MANETs	58
2.4.3	Equilibrium Concept	59
2.4.4	Nash Equilibrium	59
2.5	Summary	60
Chapter 3. Centralized PDA Detection		
3.1	Introduction	61
3.2	The Architecture	62

3.2.1	Assumption	62
3.2.2	System Model	62
3.2.3	Proposed Methodology	64
3.2.4	Performance Parameters	67
3.3	Performance Evaluation	68
3.3.1	Centralized PDA Detection vs. AODV (RWP)	68
3.3.1.1	Detection Rate	69
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.1.2	False Positive Rate	71
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.1.3	Throughput Analysis	73
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.1.4	Packet Delivery Ratio Analysis	75
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.1.5	Normalized Routing Load Analysis	77
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.1.6	End-to-end Delay Analysis	79
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.1.7	Round Trip Time Analysis	81
	Effect of Percentage of Malicious Node	

	Effect of Node Mobility	
	Effect of Pause Time	
3.3.2	Centralized PDA Detection vs. AODV (LWM)	83
3.3.2.1	Detection Rate	84
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.2.2	False Positive Rate	86
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.2.3	Throughput Analysis	88
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.2.4	Packet Delivery Ratio Analysis	90
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.2.5	Normalized Routing Load Analysis	92
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.2.6	End-to-end Delay Analysis	94
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
3.3.2.7	Round Trip Time Analysis	96
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	

3.4 Discussion	98
Chapter 4. Distributed PDA Detection	
4.1 Introduction	101
4.2 The Architecture of NAODV	101
4.2.1 Assumption	101
4.2.2 System Model	103
4.2.3 Algorithm of the Proposed System (NAODV)	105
4.2.4 Performance Parameters	110
4.3 Multi Agent System for Proposed Methodology	110
4.3.1 Introduction	110
4.3.2 Multi Agent Architecture	111
4.3.3 Collaboration-Multi Agent System	112
4.4 Performance Evaluation of the Detection Mechanism	113
4.4.1 NAODV using Random Way Point Model	113
4.4.1.1 Detection Rate (NAODV, SAODV, TAODV)	114
Effect of Percentage of Malicious Node	
Effect of Node Mobility	
Effect of Pause Time	
4.4.1.2 False Positive Rate (NAODV, SAODV, TAODV)	115
Effect of Percentage of Malicious Node	
Effect of Node Mobility	
Effect of Pause Time	
4.4.1.3 Throughput Analysis	117
(NAODV, SAODV, TAODV)	
Effect of Percentage of Malicious Node	
Effect of Node Mobility	
Effect of Pause Time	
4.4.1.4 Packet Delivery Ratio Analysis	118
(NAODV, SAODV, TAODV)	
Effect of Percentage of Malicious Node	
Effect of Node Mobility	
Effect of Pause Time	

4.4.1.5	Normalized Routing Load Analysis (NAODV, SAODV, TAODV) Effect of Percentage of Malicious Node Effect of Node Mobility Effect of Pause Time	120
4.4.1.6	End-to-end Delay Analysis (NAODV, SAODV, TAODV) Effect of Percentage of Malicious Node Effect of Node Mobility Effect of Pause Time	122
4.4.1.7	Round Trip Time Analysis (NAODV, SAODV, TAODV) Effect of Percentage of Malicious Node Effect of Node Mobility Effect of Pause Time	124
4.4.2	NAODV using Levy Walk Model	126
4.4.2.1	Detection Rate (NAODV, SAODV, TAODV) Effect of Percentage of Malicious Node Effect of Node Mobility Effect of Pause Time	126
4.4.2.2	False Positive Rate (NAODV, SAODV, TAODV) Effect of Percentage of Malicious Node Effect of Node Mobility Effect of Pause Time	128
4.4.2.3	Throughput Analysis (NAODV, SAODV, TAODV) Effect of Percentage of Malicious Node Effect of Node Mobility Effect of Pause Time	130
4.4.2.4	Packet Delivery Ratio Analysis (NAODV, SAODV, TAODV) Effect of Percentage of Malicious Node	131

	Effect of Node Mobility	
	Effect of Pause Time	
4.4.2.5	Normalized Routing Load Analysis (NAODV, SAODV, TAODV)	133
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
4.4.2.6	End-to-end Delay Analysis (NAODV, SAODV, TAODV)	135
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
4.4.2.7	Round Trip Time Analysis (NAODV, SAODV, TAODV)	137
	Effect of Percentage of Malicious Node	
	Effect of Node Mobility	
	Effect of Pause Time	
4.5	Discussion	139
Chapter 5. Game Theoretic Approach		
5.1	Introduction	141
5.2	Game Model	143
5.3	The Proposed Framework	144
5.4	Design of Utility Function	145
5.5	Coalition Stability	146
5.6	Definition of Pareto Order	146
5.7	Coalition Rule	146
5.8	Stability Condition	147
5.9	Simulation and Results	148
5.10	Discussion	152
Chapter 6. Conclusion and Future Work		
6.1	Conclusion	153
6.1.1	Centralized PDA Detection	153

6.1.2	Distributed PDA Detection	154
6.1.3	Game Theoretic Approach	154
6.2	Future Research Direction	155
Appendix-A	Network Simulator 2	156
A.1	Introduction	156
A.2	NS 2 for Wireless Network	158
A.3	Running A New Routing Protocol	160
Appendix-B	Decision tree algorithm – ID5R	163
B.1	Introduction	163
B.1.1	Introduction to ID5R	163
B.1.2	Algorithm of ID5R	164
Appendix-C	Protocol structure for SAODV and TAODV	166
Bibliography		171
Publication		195

List of Figures

	Page Number
Figure 1.1 :Mobile Ad hoc Network (MANET)	2
Figure 1.2 :Vehicular Ad hoc Network (VANET)	2
Figure 2.1 :MANETs characteristics	14
Figure 2.2 :Routing in MANETs	16
Figure 2.3 :MANET routing protocols	18
Figure 2.4 :Working of AODV	19
Figure 2.5 :Mobility models in MANETs	20
Figure 2.6 : Mobility pattern for random way point model	22
Figure 2.7 :Group Mobility in RPGM: Multiple Groups	26
Figure 2.8 :Security issues in MANETs	28
Figure 2.9 :Types of attack on MANET	29
Figure 2.10 :Security mechanism in MANET	34
Figure 2.11 :Framework for TAODV	40
Figure 2.12 :Trusted routing step at a node	41
Figure 2.13 :A single example of packet dropping attack	45
Figure 3.1 :Schematic diagram of proposed centralized packet dropping attack detection methodology	64
Figure 3.2 :Effect of increase of malicious node on detection rate (RWP Model)	70
Figure 3.3 :Effect of node mobility in detection rate (RWP Model)	71
Figure 3.4 :Effect of pause time in detection rate (RWP Model)	71
Figure 3.5. :Effect of increase number of malicious node in false positive alarm (RWP Model)	72
Figure 3.6. :Effect of node mobility in false positive alarm (RWP Model)	72
Figure 3.7 :Effect of pause time in false positive alarm (RWP Model)	72
Figure 3.8 : Effect of increase number of malicious node in throughput (RWP Model)	73
Figure 3.9 :Effect of node mobility in throughput (RWP Model)	74
Figure 3.10 :Effect of pause time in throughput (RWP Model)	74

Figure 3.11	:Effect of increase number of malicious node in PDR (RWP Model)	76
Figure 3.12	:Effect of node mobility in PDR (RWP Model)	76
Figure 3.13	:Effect of pause time in PDR (RWP Model)	76
Figure 3.14	: Effect of increase number of malicious node in NRL (RWP Model)	78
Figure 3.15	:Effect of node mobility in NRL (RWP Model)	78
Figure 3.16	:Effect of pause time in NRL (RWP Model)	78
Figure 3.17	:Effect of increase number of malicious node in End-to-End delay (RWP Model)	79
Figure 3.18	:Effect of node mobility in End-to-End delay (RWP Model)	79
Figure 3.19	:Effect of pause time in End-to-End delay (RWP Model)	80
Figure 3.20	:Effect of increase number of malicious node in RTT (RWP Model)	81
Figure 3.21	:Effect of node mobility in RTT (RWP Model)	82
Figure 3.22	:Effect of pause time in RTT (RWP Model)	82
Figure 3.23	:Effect of increase of malicious node on detection rate (LWM)	85
Figure 3.24	:Effect of node mobility in detection rate (LWM)	86
Figure 3.25	:Effect of pause time in detection rate (LWM)	86
Figure 3.26	:Effect of increase number of malicious node in false positive alarm (LWM)	86
Figure 3.27	:Effect of node mobility in false positive alarm (LWM)	87
Figure 3.28	:Effect of pause time in false positive alarm (LWM)	88
Figure 3.29	: Effect of increase number of malicious node in throughput (LWM)	89
Figure 3.30	:Effect of node mobility in throughput (LWM)	89
Figure 3.31	:Effect of pause time in throughput (LWM)	88
Figure 3.32	:Effect of increase number of malicious node in PDR (LWM)	91
Figure 3.33	:Effect of node mobility in PDR (LWM)	91
Figure 3.34	:Effect of pause time in PDR (LWM)	92
Figure 3.35	: Effect of increase number of malicious node in NRL (LWM)	93

Figure 3.36	:Effect of node mobility in NRL (LWM)	93
Figure 3.37	:Effect of pause time in NRL (LWM)	94
Figure 3.38	:Effect of increase number of malicious node in End-to-End delay (LWM)	95
Figure 3.39	:Effect of node mobility in End-to-End delay (LWM)	95
Figure 3.40	:Effect of pause time in End-to-End delay (LWM)	95
Figure 3.41	:Effect of increase number of malicious node in RTT (LWM)	97
Figure 3.42	:Effect of node mobility in RTT (LWM)	97
Figure 3.43	:Effect of pause time in RTT (LWM)	98
Figure 4.1	:Schematic diagram of distributed PDA detection Methodology	103
Figure 4.2	:Activity diagram of distributed PDA detection Methodology	107
Figure 4.3	:Schematic diagram of multi agent system of distributed PDA detection methodology	111
Figure 4.4	:Effect of increase of malicious node on detection Rate (RWP Model)	114
Figure 4.5	:Effect of increase of node mobility on detection Rate (RWP Model)	115
Figure 4.6	:Effect of increase of pause time on detection rate (RWP Model)	115
Figure 4.7	:Effect of increase of malicious node on false positive rate (RWP Model)	116
Figure 4.8	:Effect of increase of node mobility on false positive Rate (RWP Model)	116
Figure 4.9	:Effect of increase of pause time on false positive rate (RWP Model)	116
Figure 4.10	:Effect of increase of malicious node on throughput (RWP Model)	117
Figure 4.11	:Effect of increase of node mobility on throughput (RWP Model)	118
Figure 4.12	:Effect of increase of pause time on throughput (RWP Model)	118
Figure 4.13	:Effect of increase of malicious node on packet delivery ratio (RWP Model)	119
Figure 4.14	:Effect of increase of node mobility on packet delivery Ratio (RWP Model)	119

Figure 4.15	:Effect of increase of pause time on packet delivery Ratio (RWP Model)	119
Figure 4.16	:Effect of increase of malicious node on normalized routing load (RWP Model)	120
Figure 4.17	:Effect of increase of node mobility on normalized routing load (RWP Model)	121
Figure 4.18	:Effect of increase of pause time on normalized routing Load (RWP Model)	121
Figure 4.19	:Effect of increase of malicious node on end-to-end Delay (RWP Model)	123
Figure 4.20	:Effect of increase of node mobility on end-to-end delay (RWP Model)	123
Figure 4.21	:Effect of increase of pause time on end-to-end delay (RWP Model)	123
Figure 4.22	:Effect of increase of malicious node on round trip time (RWP Model)	124
Figure 4.23	:Effect of increase of node mobility on Round trip time (RWP Model)	125
Figure 4.24	:Effect of increase of pause time Round trip time (RWP Model)	125
Figure 4.25	:Effect of increase of malicious node on detection Rate (LWM)	127
Figure 4.26	:Effect of increase of node mobility on detection Rate (LWM)	127
Figure 4.27	:Effect of increase of pause time on detection rate (LWM)	128
Figure 4.28	:Effect of increase of malicious node on false positive rate (LWM)	128
Figure 4.29	:Effect of increase of node mobility on false positive Rate (LWM)	129
Figure 4.30	:Effect of increase of pause time on false positive rate (LWM)	129
Figure 4.31	:Effect of increase of malicious node on throughput (LWM)	130
Figure 4.32	:Effect of increase of node mobility on throughput (LWM)	131
Figure 4.33	:Effect of increase of pause time on throughput (LWM)	131

Figure 4.34	:Effect of increase of malicious node on packet delivery ratio (LWM)	132
Figure 4.35	:Effect of increase of node mobility on packet delivery Ratio (LWM)	132
Figure 4.36	:Effect of increase of pause time on packet delivery Ratio (LWM)	133
Figure 4.37	:Effect of increase of malicious node on normalized routing load (LWM)	134
Figure 4.38	:Effect of increase of node mobility on normalized routing load (LWM)	134
Figure 4.39	:Effect of increase of pause time on normalized routing Load (LWM)	135
Figure 4.40	:Effect of increase of malicious node on end-to-end Delay (LWM)	136
Figure 4.41	:Effect of increase of node mobility on end-to-end delay (LWM)	136
Figure 4.42	:Effect of increase of pause time on end-to-end delay(LWM)	136
Figure 4.43	:Effect of increase of malicious node on round trip time (LWM)	138
Figure 4.44	:Effect of increase of node mobility on Round trip time (LWM)	138
Figure 4.45	:Effect of increase of pause time Round trip time (LWM)	139
Figure 5.1	:Average Utility Per Node vs. Malicious Node (%)	149
Figure 5.2	:Average Utility per node vs. Number of Malicious node (M)	150
Figure 5.3	:Average Utility Per Node vs. Number of Genuine Nodes	151

List of Tables

Table 2.1	: Security extension of some of MANET routing protocol
Table 2.2	: Comparison of the best known secure routing protocols.
Table 3.1	: Simulation Environment (RWP Model)
Table 3.2	: Simulation Environment (LWM)
Table 4.1	: Simulation Environment (RWP Model)
Table 4.2	: Simulation Environment (LWM)

List of Algorithm

- Algorithm 3.1 :Algorithm for Centralized PDA detection methodology
- Algorithm 4.1 : Algorithm for distributed PDA detection methodology
- Algorithm 4.2 : Algorithm to update TRUST level of node
- Algorithm 4.3 : Algorithm to find initial TRUST evaluation of a node
- Algorithm 5.1 : Coalition Based Malicious Node Detection (CBMND)
algorithm

List of Abbreviation

ABR	: Associativity based routing
AODV	: Ad hoc on demand distance vector
ARA	: Ant-colony-based routing algorithm
ARAN	: Authenticated routing for ad hoc networks
CBRP	: Cluster-based routing protocol
CGSR	: Cluster-head gateway switch routing
CL	: Confidence level
CBMND	: Coalition Based Malicious Node Detection algorithm
DDoS	: Distributed Denial of Service
DDR	: Distributed dynamic routing
DRARPA	: Defense Advanced Research Project Agency
DoS	: Denial of Service
DREAM	:Distance routing effect algorithm for mobility
DSDV	: Destination-sequenced distance vector
DSR	: Dynamic source routing
DST	: Distributed spanning trees
FORP	: Flow oriented routing protocol
FSR	: Fisheye state routing
GD	: Global decision
GSR	: Global state routing
HFT	: hybrid tree-flooding
HSR	: Hierarchical state routing
ISLURP	: Scalable location update routing protocol
LAR	: Location-aided routing
LORA	: Least overhead routing approach.
LM	: Location manager
LMR	: Light-weight mobile routing
LWM	:Levy walk mobility
MAC	: Medium access control
MANET	: Mobile Ad hoc Network

MAODV : Multicast Ad hoc On Demand Distance Vector
MMWN : Multimedia support in mobile wireless networks
MN : Mobile Node
NAODV : New Ad hoc on Demand Distance Vector
NTDR : Near Term Digital Radio
OFT : One-way function tree
OLSR : Optimized link state routing
PDA : Packet dropping attack
PRB : Predictable Random Backoff
PRNET : Packet Radio Network
QoS : Quality of Service
RDMAR : Relative distance micro-discovery ad hoc routing
ROAM : Routing on-demand acyclic multi-path
RPGM : Reference point group mobility
RREP : Route Reply
RREQ : Route Request
RWP : Random way point
SAR : Security aware ad hoc routing
SEAD : Secure efficient ad hoc networks
SCM : side channel monitoring
SAODV : Secure ad hoc on demand distance vector
SLSP : Secure link state routing protocol
SRP : Secure routing protocol
SSA : Signal stability adaptive
STAR : Source-tree adaptive routing
SURAN : Survivable Adaptive Radio Network
TAODV : Trusted ad hoc on demand distance vector
TBRPF : Topology broadcast reverse path forwarding
TL : Trust level
TORA : Temporally ordered routing algorithm

TRREQ : Trust REQ
WRP :Wireless routing protocol
ZRP : Zone routing protocol
ZHLS : Zone-based hierarchical link state

Chapter 1

Introduction

In recent years, the use of mobile ad hoc networks (MANETs) has been widespread in many applications, including some mission critical applications such as military operations, emergency situations as well as civilian ad-hoc situations like conference and classroom. In ad hoc network potential users are within the same range of radio link and participate in communication. Nodes in such networks are mobile nodes and they communicate with one another through wireless link with multi hop routing. Mobile ad hoc networks are more likely to be attacked due to lack of infrastructure and no central management. Security has become one of the major concerns in MANETs. Due to some unique characteristics of MANETs, prevention methods alone are not sufficient to make them secure; therefore, detection should be added as another defense before an attacker can breach the system.

1.1 MANETs and its vulnerabilities

Mobile ad hoc networks (MANETs) are a collection of mobile nodes that communicates over wireless media. According to Internet Engineering Task Force (IETF), MANETs is an autonomous system of mobile routers (and associated hosts) connected by wireless links; the union of which forms an arbitrary graph [25]. A set of mobile hosts carry out the basic networking functions such as routing, packet forwarding, and service discovery. It doesn't require any pre installed infrastructure to establish the network. Nodes are self organized. These are free to move around. All the nodes in the network work as router as well as host at the same time [26][36][37]. Primary concern of the network is to maintain route traffic while connecting devices.

These are sometimes restricted to local area of wireless device or may be connected to Internet. Figure 1.1 shows a MANETs among common wireless devices. Cooperation at the network layer takes place at the level of routing by finding path for packet forwarding. Some other significant properties of MANETs are decentralization of nodes, dynamic topology and openness of media [1][2]. MANETs has emerged as an evolution of wireless technology and it is likely to be an integral part of future communication. Some areas of application of MANETs are disaster relief, battlefield communication, outdoor meeting, ubiquitous peer-to-peer market and multi-person game through Bluetooth [3]. Figure 1.2 depicts a vehicular Ad hoc Network (VANET).

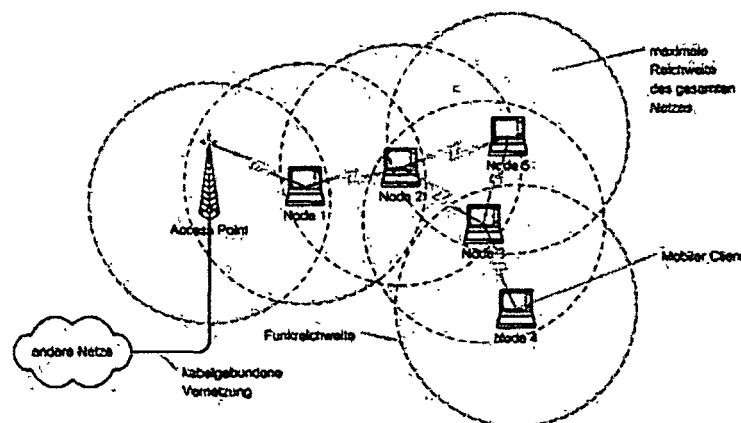


Figure 1.1 Mobile Ad hoc Network (MANETs)

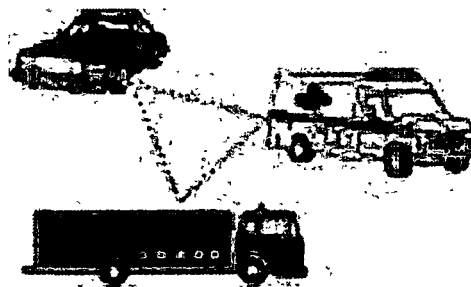


Figure 1.2 Vehicular Ad hoc Network (VANET)

Vulnerabilities of MANETs

Achieving security in wireless ad hoc environment is a very challenging task. Vulnerability is a weakness in security system. MANETs face a number of non-trivial challenges to the security design. MANETs is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

Dynamic topology: There is no fixed topology in MANETs. Nodes are free to move and can be connected dynamically in arbitrary manner. The links of network may vary over time and are based on the proximity of one node to another node.

Lack of centralized management: There is no centralized monitoring system to manage the operation of different nodes. Due to the lack of centralized monitoring system, it is difficult to detect attacks; it is not easy to monitor the traffic in a highly dynamic large scale ad hoc network.

Restricted power supply: Usually nodes in MANETs rely on battery power which is a scarce resource. Adversaries may consider it as a point to inject denial-of-service attacks. The adversary knows that the target node is battery restricted so either it can continuously send additional packets to the target or ask it for routing those additional packets or it can induce the target to be trapped in some kind of time consuming operations. By this, the battery power of target node will be drained and that may result in making the node out of service to all the genuine service requests.

Resource availability: Resource availability is a major issue in MANETs. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

Lack of Secure Boundaries: Nodes in MANETs can freely ride, join and leave the network. There is no secure boundary in MANETs.. As soon as an adversary comes in the radio range of a node, it can communicate with that node due to lack of secure boundaries. MANETs are susceptible to various kinds of attacks. The attacks include

data tampering, message replay, message contamination, eavesdropping, denial of service etc.

Scalability: Scalability is a major issue concerning security in MANETs. Scalability can be defined as whether the network is able to provide an acceptable level of services even when large numbers of nodes are present. In MANETs due to mobility of nodes, the scale of ad hoc network keeps changing all the time.

Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result, a malicious node can easily become a routing agent and disrupt network operation by disobeying the protocol specifications.

Bandwidth constraint: Variable low capacity links exist in MANETs as compared to wired network which are more susceptible to external noise, interference and signal attenuation effects. Wireless links have significantly lower capacity as compared to wired links

Adversary inside the network: Due to lack of restricted boundary, MANETs allow the nodes to join or leave the network at any time. Thus it may contain some adversaries within the network. It is very difficult to detect such adversaries. It leads to some attack. Some of the nodes may compromise with some other nodes to attack the system.

1.2 Packet dropping attack: its remedies & mitigation

In ad hoc networks, a node performs both terminal function and routing functions to form an infrastructure less network. Therefore, a node becomes an integral part of the network that forwards packets towards the destination. When a node does not forward packets for others, but silently or intentionally drops them, then it is called a packet dropping attack (PDA). It is a type of denial of service in which nodes in the network drop the packets instead of forwarding. It is very challenging to detect and prevent [166][167][168], especially when the node becomes compromised due to a number of different causes. In ad hoc networks, packets may be dropped for several other

reasons in addition to genuine causes such as collisions, channel errors, buffer overflows etc.

The PDA in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack.

Firstly, packets are dropped in the situation when a node aims on saving its own resources. This is mainly because, in a wireless environment, the most energy is consumed in the transmit mode. If a node does not forward packets, it does not use its own energy for packet transmission and preserves its energy longer.

Secondly, when a node is trying to save its bandwidth then also packets may be dropped. Bandwidth is also considered as a scarce resource in a wireless environment. To get better service for its own, it tries to save bandwidth by dropping some packets which are not meant for it. In these scenarios, it is categorized as selfish node, it can selectively drop the packets originated from or destined to certain nodes to save its own resources.

The malicious node may intentionally drop all the packets which are supposed to be forwarded. This is called a black hole attack. A special case of black hole attack dubbed gray hole attack is introduced where the malicious node retains a portion of packets (one packet out of N received packets or one packet in a certain time window), while the rest is normally relayed.

The compromised node broadcast the message [168][169] that it has the shortest path towards a destination to initiate packet dropping attack. Hence, all packet transmissions will be directed through the compromised node, and the node is able to drop the packets. If the malicious node attempts to drop all the packets, the attack can be identified through common networking tools. Moreover, when other routers notice that the compromised router is dropping all packets, they will generally begin to remove that router from their forwarding table. Hence, there is no packet transmission through the compromised node. However, it is often harder to detect the packet dropping attack, if the malicious router begins dropping packets on a specific time

period or over every n packet, because some packet transmission still flows across the network.

There are certain other reasons why a node may simply drop data packets. Packets are dropped if a node malfunctions and cannot perform the regular function of forwarding packets. Such node behavior is unpredictable. When a network is congested, packets cannot be forwarded to other nodes and packets are dropped. Congestion in ad hoc networks could occur depending on ad hoc network applications.

Lastly, wireless channels are very unreliable. Burst channel errors due to interference, fading, etc. could occur while a node is sending packets over an open air interface. Like interference, when a network is jammed, data packets cannot be sent or received at any node in a jammed area. Packets from a non-jammed area cannot be sent through the jammed area and these are also dropped. Otherwise, the nodes in the jammed area don't have any intentions to drop packets.

For malicious node mitigation, several techniques had been used. Malicious node mitigation can be classified into two categories,

- (i) Prevention and protection,
- (ii) Detection and response.

A prevention mechanism guards against a malicious node's attack by applying cryptographic mechanisms such as encryption and authentication. However, it cannot guard against insider attacks. A detection and response mechanism detects misbehavior activities and responds to an attack.

A protection mechanism applies cryptographic techniques to secure communications over an ad hoc network in order to prevent any malicious activity. Most research works focus on securing a routing protocol which is a key component for a wireless ad hoc network to operate properly. The two most important security services for a secure a routing protocol are authentication and data integrity services.

Many research works contribute to selfish node mitigation in ad hoc networks. It can be categorized into two approaches namely

- (i) Incentive-based approaches, and

(ii) Reputation-based approaches.

An incentive-based approach aims on discouraging a node from becoming selfish. A reputation-based approach aims on detecting a selfish node and responding with appropriate action. For examples, Watchdog [161] mechanism can be used to avoid selfish node; CORE[162] is another technique which use an average weighted rating to combine direct and indirect reputations to detect and avoid selfish node. CONFIDANT [163] is another methodology through which selfish node can be detected and avoided by using weighted average rating to combine direct and indirect reputations. On detection it generates alarm to the network. TWOACK [164] avoids selfish node path.

1.3 Motivation

MANETs are vastly implemented in several areas where secure communication is mandatory. In such areas due to lack of streamline flow of data, some major problems may take place. Intermittent data flow due to malicious packet dropping may disrupt the communication between source and destination and also corrupt the entire system. Some of the typical application area of MANETs are as follows,

Military battlefield in which it is very difficult to establish infrastructure based network. For some business environments, where collaborative work is required, MANETs can play vital role. In such environment, people need to communicate amongst the group members, need secure communication. Malicious packet dropping in such scenario may disrupt the entire system. Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at conference or classroom. Another local level application might be in home networks where devices can communicate directly to exchange information. In Personal area network and Bluetooth, MANETs are used as a short range, localized network where nodes are usually associated with a given person. Short-range MANETs such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop and a mobile phone.

In commercial purpose, it can be used in emergency/rescue operations for disaster relief efforts, such as in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. In disaster prone area, intermittent data or malicious packet dropping in data flow may lead the system to more dangerous level.

MANETs are vulnerable to different kind of attacks [30][40]. Nodes in MANETs are susceptible to various attack which is influenced by extreme unpredictable nature of MANETs [1][29][30][32][35][38][39]. Some nodes may not cooperate for selfish and malicious reasons. Selfish nodes use system services while taking care to save some of its own resources to the extent of deviating from regular routing and forwarding. Amongst the different kind of attacks, packet dropping attack (PDA) remains a major concern. Malicious node in the network drops packets intentionally which are supposed to be forwarded to reach destination [7][8][9]. Routes that pass through such kind of nodes fail to establish path from source to destination [8]. To send the same kind of packets repeatedly, network has to consume its network resources like bandwidth, computational cost etc. a lot. It affects the entire network performance. Selfish as well as malicious nodes disrupt routing protocol and leads to reduction of network throughput, consequently network performance degrades. Previous protocols were not able to handle all type of security issues. Few protocols emerged with strong cryptographic method [33].

By considering the importance of application of MANETs and its security threat due to PDA, herein lies the motivation of development of a PDA detection methodology having capability to cope with such misbehaving nodes that involved with packet dropping attack.

At the same time, tradeoffs should be considered between the detection effectiveness and efficiency of the detection mechanism. There must be a clear analysis of different performance parameters while implementing algorithm. How does the detection technique work when malicious node deployment is very high or node mobility is

high or pause time is high. In the same network scenario, what is the performance of already existed methodology. All these analysis must be done to show the efficiency of proposed detection methodology.

1.4 Objectives

Several research efforts have been made to secure routing in MANETs [1][3][4]. Several studies that deals with security threats in MANETs [7][8][9][12][13], reveal that few of them addressed packet dropping attack in MANETs as major concern. Of course, indirectly it has been addressed. Most of the research is concerned with trusted authority to issue certificates or cryptographic authentication to routing protocol [12][13]. These methodologies are not directly concerned with network performance parameters. Dynamic nature of the network should be controlled not only by simple preventive system but also by detection system [41] that provides security to the system, without hampering normal routing as well as performance of the network. Of course routing protocol determines the ability to cop with the dynamic topology change and packet forwarding nature of the nodes. Initial protocols are not designed to withstand the malicious nodes, but subsequently different protocol extension as well as some new protocols is proposed to address the security issues of MANETs [27]. MANETs QoS such as throughput, packet delivery ratio, network overhead, end-to-end delay etc. depends on type of protocol used [31].

PDA as major concern have been addressed by [14][15][17] among others. In [14], authors proposed a mechanism to detect and isolate packet dropping attackers in MANETs, which is named as Detection and Isolation Packet Dropped Attackers in MANETs (DIPDAM). It is based on on three ID messages Path Validation Message (PVM) , Attacker Finder Message (AFM) and Attacker Isolation Message (AIM). It is based on End-to-End (E2E) communication between the source and the destination. This methodology is based on only single factor i.e. End-to-End (E2E) and limited to type of packets. In [15], authors proposed a distributed cooperative protocol for detecting PDA which is based cooperative participation of the nodes in a MANETs.

Here, authors utilize the redundancy of routing information to make the scheme to work in presence of transient network partitioning and Byzantine failure of nodes. But this protocol is limited to isolate the malicious nodes from the network. Moreover efficiency of this protocol has been shown only in Random walk model which is less realistic than some other mobility model like Levy walk mobility model. In [17], authors propose mechanism to monitor, detect and safely isolate the misbehaving nodes. The entire procedure is based on five different modules such as monitor, detector, isolator, investigator and witness module. But this is less tolerant with control packets which is also very crucial. Though the process overhead is less when there is no attack, yet it is high while detecting and isolating PDA. This methodology is also not concerned with collusive misbehavior where two nodes collude and conceal the dropping of each other, and node reinsertion after that is justifiable in case of temporary node failure leading to wrong isolation of benign node. Control packets misbehaving is also not handled by this methodology.

None of the methods properly address the PDA detection using collaborative/cooperative framework. The objective of this thesis is to address PDA using coalition game theoretic framework where genuine nodes will collaborate to detect PDA by neutralizing the effects of malicious nodes. Prime concern of this research is to address these issues in packet dropping attack in MANETs. We propose to address this through three different approaches:

- I. *Centralized packet dropping attack detection*: In centralized packet dropping attack detection methodology, it is assumed that all data related to network communication are centrally observed. It is a static offline system. It performs statistical detection methodology. Performance of this method is compared with OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) [173][174] an existing methodology in various network scenarios.
- II. *Distributed packet dropping attack detection*: Analyzing experimental results of centralized PDA detection methodology, it is clear that this methodology is not able to handle the dynamic nature of MANETs. More complicity may arise to the

network if it deploys malicious nodes in it. To address the distributed and dynamic nature of the problem for a network containing malicious nodes that involves packet dropping attack, distributed packet dropping attack detection methodology is proposed to detect and avoid malicious nodes from the network, based on ad hoc rules of cooperation. This methodology is named as NAODV (New Ad hoc on Demand Distance Vector). Simulation for this methodology is done for several network scenarios in Levy Walk Model of mobility and compared with two existing system namely SAODV [85][86][87][88][89][90][103][104] and TAODV [105][106].

III. *Distributed packet dropping attack detection using a game theoretic approach*: MANETs is formulated as coalition game in which all the genuine nodes in the network that cooperate in packet forwarding, will be in one side of the game. Malicious nodes which will try to drop the packets invariably will be in the other side of the game. Coalition is formed amongst the genuine nodes to help routing packets. Selfish nodes, as well as non responders are neither considered under the coalition of genuine node nor considered as opponents. Based on performance of the node, TRUST value of node is either increased or decreased. Accordingly a node is merged into coalition or it is splitted from the coalition. A utility function is defined which is used to measure network utility in terms of performance.

The overall scope of the research is to address the detection of packet dropping attack due to malicious node in an efficient way. Aim is to have a methodology for detection and avoidance of malicious node from the network; where the detection process should not degrade network performance parameters.

1.5 Thesis outline

The thesis is organized in six different chapters. The chapter 1 of this thesis contains introduction to MANETs. Chapter 2 contains literature reviews and general discussion of MANETs. Chapter 3 presents centralized packet dropping attack detection methodology with simulation results and comparison with OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) [173], an existing methodology. Chapter 4 of the thesis contains distributed packet dropping attack

detection methodology with simulation results and comparative study with SAODV and TAODV. Chapter 5 presents a game theoretic approach to distributed packet dropping attack detection. Finally Chapter 6 provides research contribution, limitation of the proposed systems; also discuss possible future enhancements of current research.

Chapter 2: This chapter contains the literature review and general discussion related to different topics relevant to the proposed methodologies. It includes MANETs characteristics. It also includes different mobility models of MANETs. Security issues with respect to existing protocols are also discussed in this chapter. The chapter further contains packet dropping attack, impact of packet dropping attack and packet dropping attack detection methodologies. Then it provides concept on introduction to game theory, Game theoretic approach to detect and isolate packet dropping attack in MANETs and its equilibrium concept is also discussed.

Chapter 3: This chapter contains centralized packet dropping attack detection methodology. It describes the proposed methodology along with system model, its assumptions and different performance measurement parameters of the network. Then, it discusses the simulation environment and simulation results for various parameters and gives a comparative analysis of performance of OCEAN and proposed centralized PDA detection methodology.

Chapter 4: This chapter proposes a distributed PDA detection methodology which is named as NAODV (New Ad hoc on Demand Distance Vector). It starts with proposed system model, assumptions, different performance evaluation parameters and proposed algorithm. Thereafter simulation environment along with simulation results for various performance evaluation parameters are discussed. Simulation is also done for another two existing methodologies namely SAODV and TAODV. The chapter provides a comparative analysis and discussion of three methodologies namely NAODV, SAODV and TAODV.

Chapter 5: This chapter contains a game theoretic approach to distributed PDA detection methodology. The system model, assumptions, game strategy, utility characteristic functions and equilibrium status of proposed methodology is discussed.

Chapter 6: This chapter contains conclusion and future work. It includes research contribution of three different methodologies namely centralized PDA detection methodology, distributed PDA detection methodology and game theoretic approach to distributed PDA detection methodology. Then outlines of some of the future research directions based on the proposed methodology are provided.

The appendix of the thesis contains discussion on the network simulator i.e. NS 2, decision tree algorithm ID5R. and protocol structure for SAODV and TAODV

Chapter 2

Literature Review and General Discussion

2.1 Introduction to MANETs

2.1.1 Characteristics

Mobile ad hoc network (MANETs) is a collection of mobile nodes in which all the nodes are connected via wireless link. These are self configured networks. MANETs contains several characteristics. Because of these intrinsic properties, MANETs becomes special amongst the users. Nodes in MANETs perform in open media that permits the network to work without preinstalled infrastructure.



Figure 2.1 MANETs characteristics

Autonomous nodes of MANETs can play as host as well as router at the same time [144]. Figure 2.1 gives the idea of MANETs. These are not depended on central administration. So, network control and management is distributed amongst the nodes. Nodes must collaborate amongst themselves to avail the features of network [2].

Nodes in MANETs are free to move arbitrarily in any direction in different speeds. This leads to a dynamic network topology i.e. topology may change randomly at any moment in unpredictable fashion [144]. Thus it exhibits flexible network architecture to work with limited wireless connectivity and resources [3][6]. Network must comply with unstable node conditions including traffic and propagation condition as well as mobility pattern of the nodes. So it exhibits seamless interaction and ubiquitous mobile computing environment.

Neighbor discovery in MANETs is another intrinsic property of MANETs [3]. When a new node joins the network, immediately it is identified by the neighbor nodes and starts routing with it. Each node in the network works as intelligent node. Every node must work as DTE (Data Terminal Equipment) and DCE (Data Communication Equipment) [4].

Nodes in MANETs may rely on battery or on any exhaustible power device; So, computation and other activities of MANETs are always concerned with energy conservation [3][5][6].

The channels, over which nodes communicate, are shared by several sessions and hence subject to noise, fading, network interference. The path between any pair of nodes is a heterogeneous path and thus packets follow multiple wireless links to reach destination [2].

Another characteristic of MANETs is computational decentralization, which include independent computations, switching and computation capabilities of nodes [3]. Moreover it can support diversified digital devices such as iPods, PCs, palm handheld computers, smart phones, smart labels, smart sensors, automobile embedded systems etc.

2.1.2 Routing in MANETs

Nodes in MANETs exchange data dynamically within themselves without depending on base station. Routing is done by the routing protocol available for MANETs.

Routing is the process through which user traffic is directed and transported from source to destination. Routing is the most crucial part of implementation of MANETs.

Usually, packets are routed to destination from source via routers as shown in

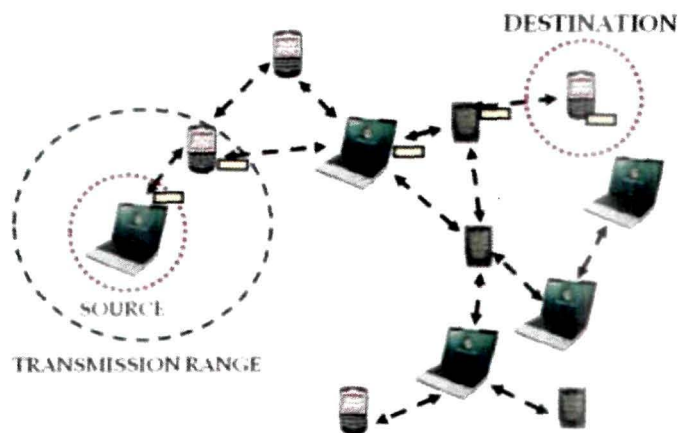


Figure 2.2 Routing in MANETs

Figure 2.2, there is no specific device named as router; all the nodes connected to network are worked as host as well as router at the same time. To complete the routing function effectively, a good routing protocol is required. Routing in MANETs is signified as dynamic optimization task, which includes shortest path routing, optimum bandwidth utilization, and minimum delay in delivering packets. It also complies with minimum battery power and limited capacity of wireless link. Ad hoc network can enhance its performance parameters by utilizing all its nodes by allowing them to participate in packet forwarding as well routing [50][51]. Routing protocol in MANETs must be self organized and manageable. Routing must follow a loop free path while it transmits packets through multi hop path. In spite of dynamic topology change with rapid convergence, it must provide its service. It should be scalable to large network. As shown in the Figure 2.2, to send packets from source to destination,

routing algorithm follows multi hop routing path, at the same time it should look forward the shortest path out of several paths. Ultimate aim of routing in MANETs is to discover a path from source to destination, maintain the path in case of sudden link failure; in such cases it may alter its existing path.

Sometimes routing also provides periodic information to the nodes in MANETs. For routing in MANETs, several routing algorithm had been proposed. Task wise routing can be divided into four different segments such as,

- a. Path discovery: When a node has to establish communication to destination, it will have to discover the shortest path through which data can be sent.
- b. Path selection: During path discovery, if it discovers more than one path, in that case it will have to select the appropriate path based on some criteria provided in the network.
- c. Data forwarding: After selection of path, routing must take the responsibility to forward packets to destination.
- d. Path maintenance: Path maintenance helps to maintain the continuous flow of data in case of link failure that occurs in the network.

Routing in MANETs is limited by several characteristics that include MANET's security, traffic pattern, routing functionality etc. In addition to these, routing in MANETs is also effected by a series of parameters such as multiple route selection, fast route establishment, bandwidth limitation, battery power constraints etc. According to different routing state, such as static, dynamic and quasi static, functionality of routing may vary. Node mobility is another important characteristic which must be considered for routing [49].

Routing in MANETs can be divided into two parts:

- a. Proactive routing or table driven routing, here each node maintains one or more routing table keeping the information of entire network topology. These are updated regularly to keep up to date routing information of the network.
- b. For this topology information needs to be exchanged between the nodes on

regular basis. In this routing, routes are available on request.

- c. Reactive routing or on demand routing: It creates a route on demand when a packet to be sent from source to destination. For highly dynamic ad hoc network, this routing is desirable as it doesn't require periodic updating of routing information as well as topology information.

Apart from these, MANETs has certain characteristics through which it decides the short-hop routing as it gains several benefits including energy saving as well as to reduce higher signal-to-interference ratios [48].

2.1.3 Routing Protocols

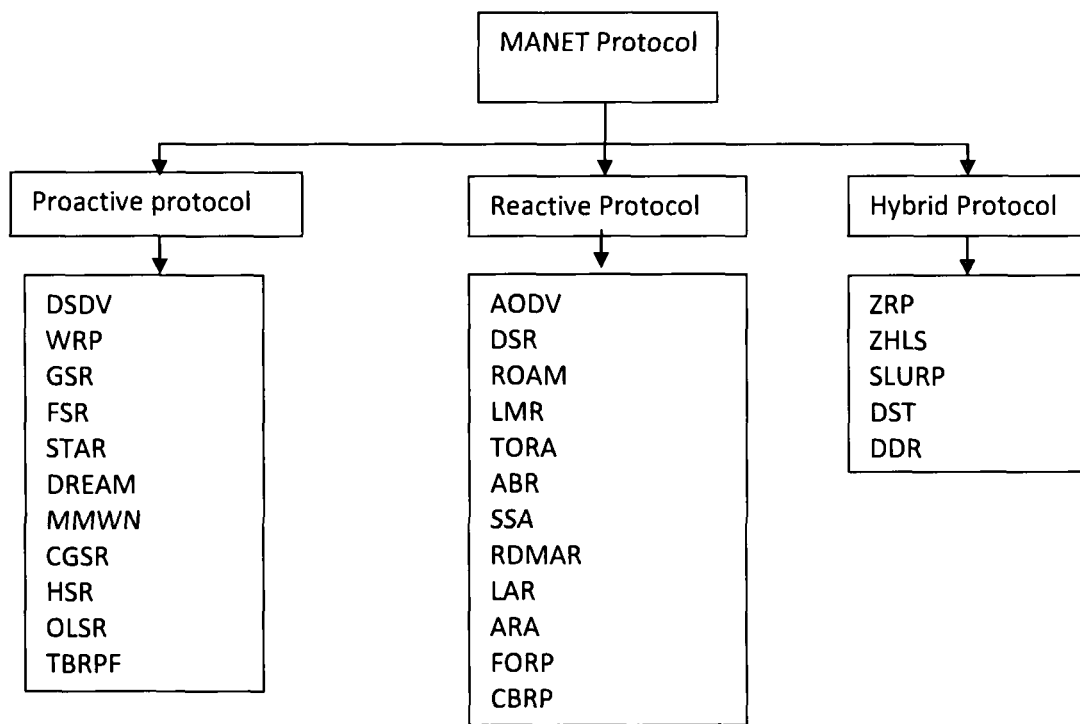


Figure 2.3 MANETs routing protocols

MANETs is a multi hops wireless network where all nodes are responsible for carrying packets from source to destination. To perform routing smoothly, it needs a set of instructions and algorithms. Accordingly, different set of routing protocols are

generated. Basic functions of such protocols are to find a route and deliver the packets to correct destination [52]. Basic properties of routing protocol include distributed nature, quality of service support, efficient bandwidth support, resource management, optimization of network performance matrices. Free from loop and strong security support [55]. The limited resource in MANETs forces the researchers to design an efficient and secure routing strategy to get reliable service [57].

Routing protocols in MANETs are classified into three different table categories as shown in Figure 2.3 based on protocol discussed in the literature [52][53][54][55]. Out of these all, *Ad hoc on Demand Distance Vector (AODV)*, reactive protocol of MANETs, is discussed elaborately because AODV protocol has been taken as base protocol for implementation of proposed methodologies to detect PDA in MANETs in the thesis.

Ad hoc on Demand Distance Vector (AODV)

As shown in Figure 2.3, *AODV* is a reactive protocol in which routing tables are dynamically created when needed. When source node wants to send data to destination, it tries to establish the path through several ways by sending some RREQ packets. When it gets RREP packet containing shortest path, the source sends packets through this shortest path.

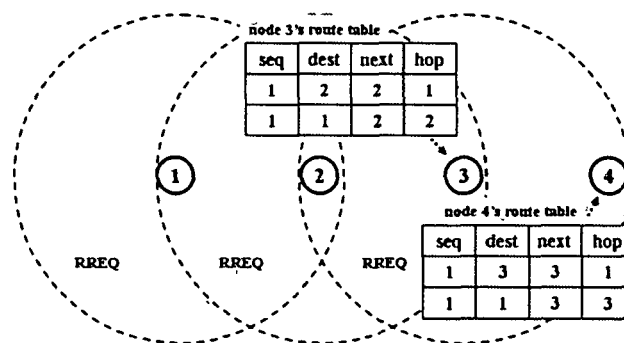


Figure 2.4 Working of AODV

Basic conception of AODV is based on DSR and DSDV protocol [59][60]. So, it copes with on demand route discovery and route maintenance concept of DSR, while from DSDV, it adopts the properties of hop-by-hop routing and maintenance of node sequence numbers. As a result, AODV becomes stronger enough to work in limited

bandwidth and node mobility of ad hoc network [59]. Each node in the network maintains routing table with routing details entries of its neighbor nodes with two counters namely sequence number and a broadcast id. Figure 2.4 shows the basic functionality of AODV. When a node wants to communicate with any other node in the network, it sends RREQ packets containing different fields like *source address*, *source sequence number*, *destination address*, *destination sequence number* and *hop-count*. A RREQ can be uniquely identified by observing the pair (source address, broadcast-id).

It establishes the reverse path back from all the nodes through which RREQ traverse. For any intermediate node, having route entry for destination in its routing table, it compares the destination sequence number in its routing table with that in the RREQ. If the destination sequence number in its routing table is less than that in the RREQ, it rebroadcasts the RREQ to its neighbors. Otherwise, it uncast a route reply packets to its neighbor.

2.1.4 Mobility Models

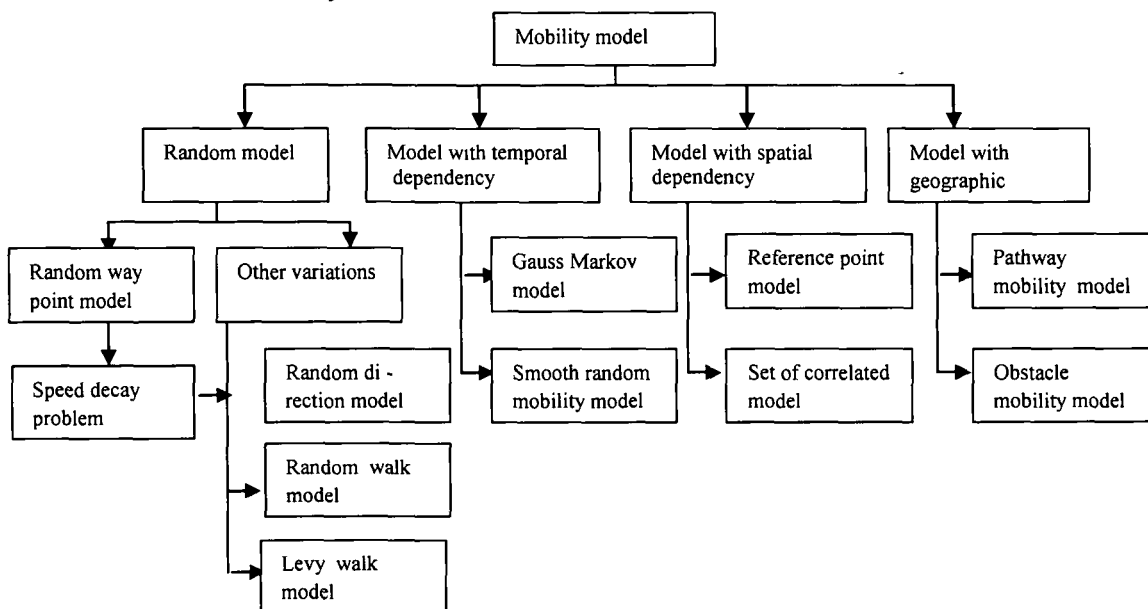


Figure 2.5 Mobility models in MANETs

A mobility model in MANETs is a kind of model which mimics the movement of actual mobile nodes [61]. So, it explains the movement pattern of nodes in MANETs [53]. Mobility model is designed to understand the movement pattern of mobile users in terms of location, velocity and acceleration [64]. In real network, nodes change their direction as well as speed at any time anywhere. The performance of routing protocol is based on duration of interconnection between any two nodes taking part in communication [62]. The mobility of nodes affects the connectivity amongst the nodes. It then affects the performance of routing protocol.

As per spatial and temporal dependency, different mobility models can be found in MANETs. According to *spatial dependency*, two nodes are moving in same direction, implies they have high spatial dependency. *Temporal dependency* is a measure that explains how current velocity is related to previous velocity. Nodes having same velocities have high temporal dependency.

Mobility models in MANETs can be divided into several types as shown in Figure 2.5. Mobility models are divided into several categories as per their mobility characteristics. In temporal mobility model, movement of the mobile node is affected by its movement history. In spatial dependency model, the mobile nodes tend to travel in a correlated manner. Similarly in case of *geographic restriction* model, the movement of nodes are guided and bounded by streets, freeways and obstacles. In case of *random models*, nodes move independently to a randomly chosen destination with random velocity.

2.1.4.1 *Random Model*

In this model, nodes move independently to a randomly chosen directions with randomly selected velocities. Mobile nodes move freely without any restriction. Random model is categorized in two types, such as *random way point model* and *other variations*. Other variations include *random direction model* and *random walk model*. Out of these all, random way point model is vastly used.

2.1.4.1.1 Random Way Point Model

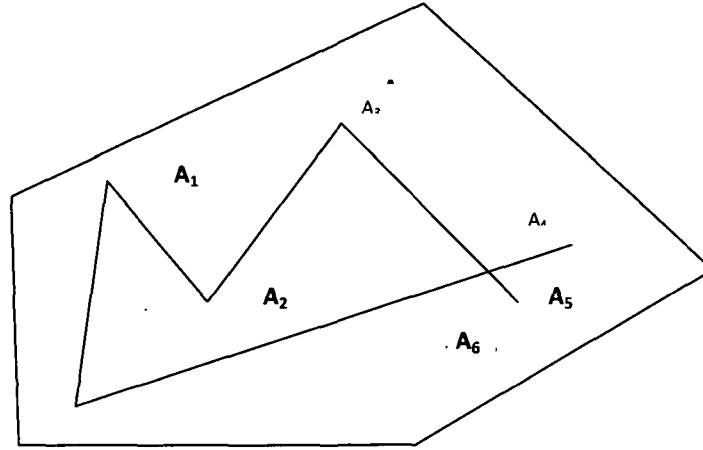


Figure 2.6 Mobility pattern for random way point model

This model was first proposed by Johnson and Maltz [64]. Because of its simplicity and wide availability, this model is used vastly. To generate the node trace of the Random Waypoint model the *setdest* tool from the CMU Monarch group may be used. This tool is included in the widely used network simulator ns-2 [64].

It is a commonly used mobility model for MANETs. It explains the movement pattern of independent nodes in a simplified way as shown in Figure 2.6. It exhibits certain properties like,

- All the nodes move along the zigzag line from the waypoint A_i to A_{i+1} .
- Waypoints are uniformly distributed over the convex area.
- From one point to other, at the starting point, it selects a random velocity drawn from velocity distribution.
- Formally the process is defined by $(A_i, A_{i+1}); (A_{i+1}, A_{i+2}); \dots$
- At each way point, nodes waits for a random pause time
- Random way point model is used as elementary synthetic model for Ad hoc network. These are easier to implement for process simulation with analytical results and analytical results can be used to choose the realistic values for model parameters before the actual process simulation.

2.1.4.2 *Levy Walk Model*

Commonly used mobility models in computer networking research are random way point (RWP) or random walk models. These models are simple enough to be theoretically tractable and at the same time, to be emulated in network simulators in a scalable manner. However, no empirical evidence exists to prove the accuracy of such models. Human walks are not random walks, but the patterns of human walks and Levy walks contain some statistical similarity.

The term Levy walks (LW) was first coined by Schlesinger et al to explain a typical particle diffusion not governed by Brownian motion (BM). BM characterizes the diffusion of tiny particles with a mean free path (or flight) and a mean pause time between flights [172]. The Levy Walk Mobility Model proposed in [171][172] more or less imitates the human mobility behavior in an outdoor condition. Real world human mobility traces are generated at various places that include two different campuses, a metropolitan area and a park or any other places like this by using GPS devices. The word “flight” is used to define movement of an object along a straight line without any change in the direction.

There are certain difficulties in this model. It is difficult to get a human walk flight from the traces as the human seldom walks in a straight line. Also there might not be continuity in a human walk as the person may pause for few minutes or he may change the direction or may move in a vehicle and disappear for few minutes and appear in another location or it is run out of battery service etc. To eliminate some of the errors that it may provoke, three different methods are proposed for analysis.

These are

Rectangular: If there is no pause while moving between the two points, then the distance between any two points is considered as a flight in the rectangular model

Angle: In this model, the length between any two points is a perpendicular length to the point from that position. The angle model takes various flights found out from the rectangular model and combines them in to a single flight provided that there is

no pause between any of the successive flights and the relative angle is less.

Pause based methods: The pause model also combines the flights obtained from the rectangular model. It establishes more trajectories and accordingly represents the more natural human walk.

The Levy Walk Model consists of four variables namely flight length, direction, flight time and pause time. Flight length defines the longest straight-line trip of a particle from one location to another without a directional change or pause. It is characterized by other three variables like direction, flight time and pause time [170].

2.1.4.3 Model with Temporal Dependency

Due to physical constraints such as acceleration, velocity, direction and other factors of mobile entities, the velocity of mobile nodes varies according to previous velocity pattern to avoid abrupt velocity change in the network [61][64]. Initially it was proposed for simulating mobility in personal communication system. Nodes having same velocity have high temporal dependency [62]. Various mobility models are proposed based on temporal dependency as random models are unable to cope with the temporal dependency behavior. *Gauss Markov mobility* model and *Smooth random mobility* model are example of such kind of mobility model.

2.1.4.3.1 Gauss Markov Mobility Model

It was first introduced by Liang and Haas [64]. Here, the velocity of mobile node is assumed to be correlated over time and modeled as a Gauss-Markov stochastic process. It was designed to work with different level of randomness via single tuning parameter. Initially each mobile node is assigned with a current speed and direction. At fixed interval of time, n , movement occurs by updating the speed and direction of each mobile node. The value of speed S_n and direction d_n at the n th instance is calculated using the following equation.

$$S_n = S_{n-1} + \alpha * r_g * S$$

$$d_n = d_{n-1} + \alpha * r_g * \alpha$$

Here S_n =New speed and S_{n-1} =Current speed.

d_n =New direction, d_{n-1} =Current direction

r_g =A random number taken from standard Gaussian distribution.

S = standard deviation of speed for the Gaussian distribution.

Gauss-Markov mobility model can generate movement with smooth curve and mobile nodes are generally stayed away from the edge of simulation area. This mobility model can reduce the sudden stops and sharp turns.

2.1.4.4 Model with Spatial Dependency

The mobile node's movement can be influenced by its neighborhood. In random model, mobile nodes move independently of its neighbor or any other nodes in the network. So, it is assumed that the location, speed, movement and directions are not affected by its neighbor node. As the velocity of different nodes are correlated with the status of neighbor nodes in space, so this specific type of mobility model is call as spatial dependency model [64]. This can be categorized as *Reference point model* and set of *correlated models*.

2.1.4.4.1 Reference Point Group Model

The conception of this mobility model is that mobile nodes in MANETs tend to coordinate their movements. Accordingly a new concept of spatial mobility model i.e. *reference point group mobility (RPGM)* model is proposed just like a number of soldiers move together in a group or platoon. In this model, each group has a group leader. So, the group leader decides the mobility pattern of group members [64]. The members of the group follow the leader's mobility closely, with some deviation. As shown in Figure 2.7, multiple groups can move together in the network according to different mobility pattern of respective group with their group leader in the centre. Node mobility for each node is assigned with a reference point that follows the group movement.

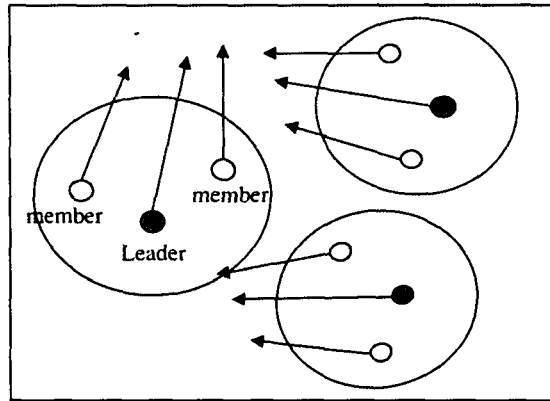


Figure 2.7 Group Mobility in RPGM: Multiple Groups

Node mobility for each node is assigned with a reference point that follows the group movement. Each mobile node can be placed randomly in their neighborhood upon this reference point. RPGM model is able to emulate different type of mobility behaviors such as in-place mobility model, overlap mobility model, convention mobility model.

2.1.4.5 Model with Geographic Restriction

Geographic restrictions: Most of the realistic situation regarding application of MANETs in urban areas, the movement of a mobile node may be bounded by obstacles, buildings, streets or freeways. Random waypoint model and its variants are not able to handle those situations of mobility with specific characteristics. Thus, several other mobility models like obstacle mobility model or pathway mobility model were proposed. These are defined for the objects with some geographical points. Obstacle mobility model of geographic restriction model includes the movement path through which mobile nodes can pass through. The obstacle and paths are generated with the help of a tool called *tergen*. This tool is restricted to creation of rectangle shaped object but by changing the coordinate position of the corner of obstacle, some advance shapes can be created.

2.1.4.5.1 Path Way Model

This is an example of a geographic model which increases the probability for the

object to travel within some specified paths. The geographic model is sometimes used for map matching. These mobility models are then used by a particle filter or a Kalman filter sequentially with the incoming position measurements. So to integrate geographic constraints with mobility model, node movement can be restricted to the pathways in the map. The map can be predefined in the simulation as *city section model*, *city map model*, *obstacle mobility model*.

2.1.5 Security Issues in MANETs

2.1.5.1 Introduction

Due to intrinsic properties of MANETs such as open medium, lack of central monitoring and controlling system, dynamic network topology, autonomous terminal, distributed operations, multi hop routing, easy access of network etc., security becomes a major issues in MANETs [70][71][72][73]. Due to *wireless link* of MANETs, the network is susceptible to some attack such as active interference. As shown in Figure 2.8, all the nodes are allowed to access the wireless link without any central monitoring system. That makes the network vulnerable to attack. Due to dynamic topology of the network, nodes can easily enter or leave the network independently. So, there is no restriction to simply discard the malicious nodes from the network. Cooperative nature of the network also makes it vulnerable to attack. MANETs does not have any clear line of defense. Attacker can enter into the system at any time from any end. There is no clear line that separate the inside network from outside world.

Flexibility of operation in MANETs creates several security issues in MANETs in different layers of the network. In application layer of the network, security issues occur due to detecting and preventing viruses, malicious codes, application faults etc. In transport layer of the network, security issues occur in authenticating and securing end-to-end communication through data encryption. Issue of protecting ad hoc routing protocol in MANETs comes under network layer. Similarly link layer expects security issues in MAC sub layer. Security issues in physical layer are occurred in terms of signal jamming DoS attack [66].

Security issues in MANETs lead to some security goals such as *authentication, integrity, confidentiality, availability, access control* and *non-repudiation* [68].

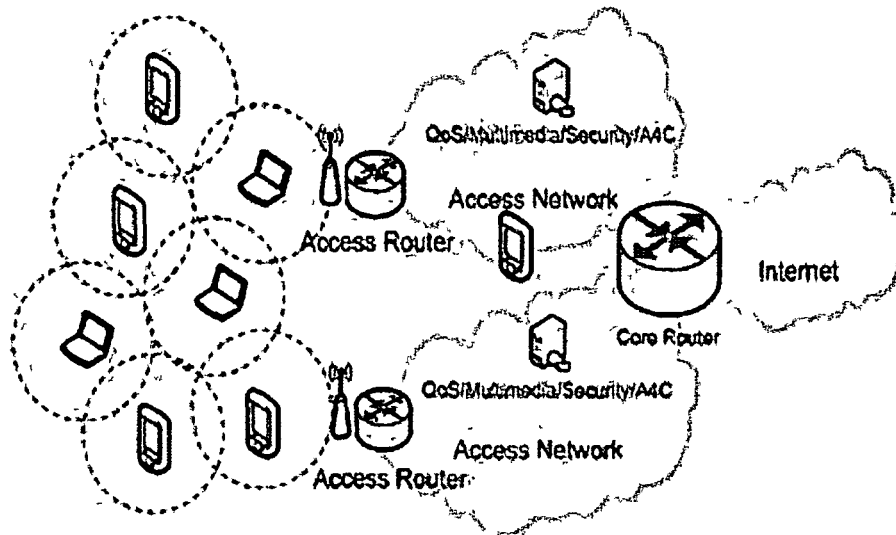


Figure 2.8 Security issues in MANETs

Open peer-to-peer architecture of MANETs, creates security issues [73]. Since all the nodes in MANETs work as router and forward packets to next hop for destination, so presence of any vulnerable node may create security threat to the whole network. Moreover the wireless network is easily accessible to both genuine node as well as malicious node. Portable devices along with security information are vulnerable to attack. So, attacker can easily enter into the network with the help of these weaker devices as well as software.

The security solutions which are used for wired networks are ineffective and insufficient for highly dynamic network like MANETs.

2.1.5.2 Types of Attacks on MANETs

Mobile ad hoc network is vulnerable to different kind of attacks. Figure 2.9 shows categories of attack based on literature [74][75][76][77].

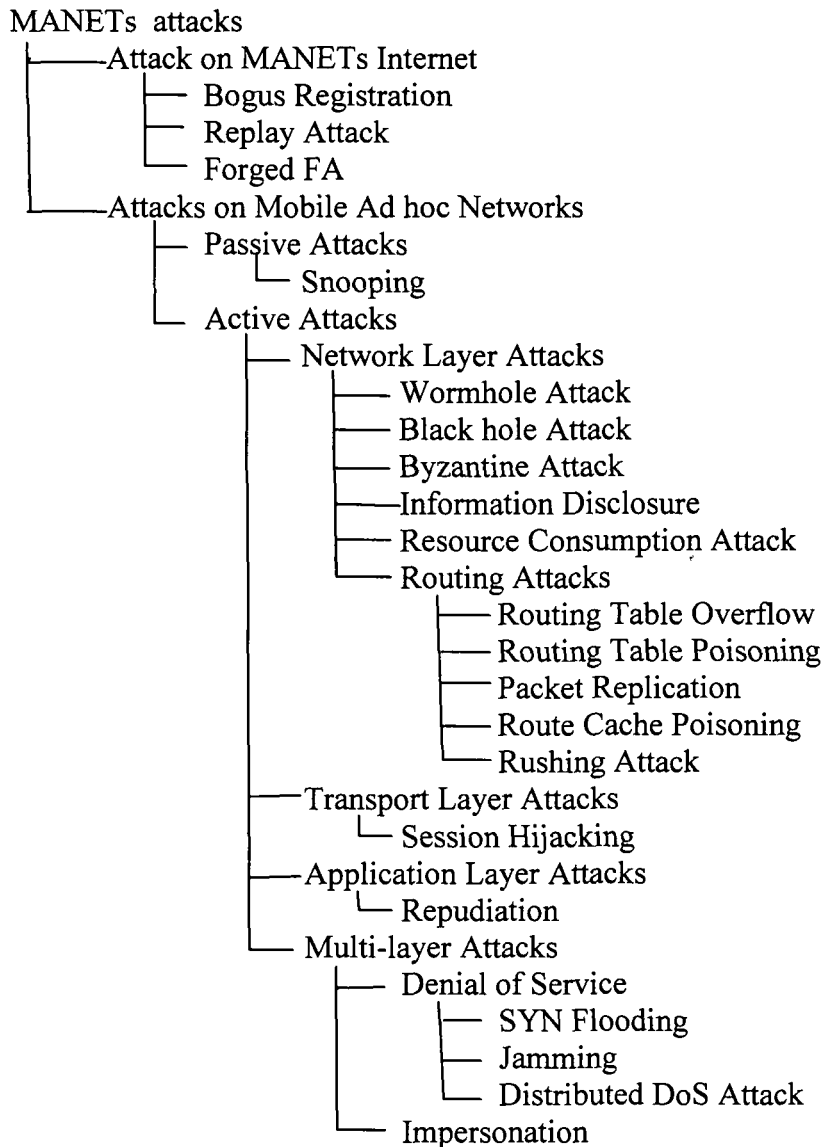


Figure 2.9 Types of attack on MANETs

Attack on MANETs includes different attacks like Bogus registration, Replay attack and forged FA. In bogus registration, an attacker registers itself with bogus registration. An attacker may advertise itself as genuine node to the mobile nodes (MN) in such a way that MN starts registering the bogus node and shares its confidential information. In replay attack, valid data transmission is maliciously repeated or delayed by the malicious nodes present in the network. Forged FA is a

form of network attack in which a node advertises itself as a fraudulent FA then MN under the coverage of the forged FA may register with it. As a result, forged FA can capture the sensitive network data and may disturb the proper functioning of the network. Simply monitors the data exchanged in the network without disturbing the normal function of the network. At some point, the attacker also starts interpreting the data gathered through snooping, as a result confidentiality of network information leak out. An example of such kind of attack is snooping in which an attacker tries to access the unauthorized information from other MN.

In active attack, an attacker disrupts the normal functioning of the network by altering or destroying the original data. Again this kind of attack can be classified as external attack and internal attack. In external attack, malicious nodes are outside of the network. On the other hand internal attacks are carried out by the nodes which are part of the network. So, these are more severe kind of attack than the external attack.

Active attack may activate in different layers of the network as shown in Figure 2.9. Wormhole is a kind of network layer attack in which a malicious node tunnels the received packets from one location of the network to another location. This tunnel between two colluding attackers is referred to as a wormhole [79].

Attack on Mobile Ad hoc network includes both passive as well as active attack. Passive attack doesn't disturb the proper operation of the network. Here, the attacker Routing in the network is severely disrupted when control packets are tunnels by this attack.

Black hole attack is a kind of network layer attack in which attacker listens to RREQ packets. Accordingly it responds to the sender by RREP, packets by showing the shortest path to the destination by altering sequence number. In response to this, when the sender sends packets through this attacker nodes, it consumes all the packets without forwarding these to destination [78][79].

In Byzantine attack, compromised intermediate nodes work together to create routing loops, forwarding packets through non-optimal path, selectively dropping packets as

well as maliciously dropping packets. As a result, network performance parameters degrade abruptly.

According to information disclosure, confidential information of the network such as network topology, geographic location of nodes or optimal routes may disclose to unauthorized users by the attacker.

Resource consumption attack helps the attacker to consume network resources such as battery power of MN, bandwidth, and computational power, which are limited to an ad hoc network.

Routing attack of active attack in MANETs is normally on the routing protocol of the network and disrupts the normal operations of the network. Routing table overflow is an example of such kind of attack in which attacker creates some unnecessary routes entry in the routing table, thus preventing the entry of new genuine routes in the table. Another example is the routing table poisoning. In this attack, malicious nodes present in the network, create fictitious routing updates in the table and thus mislead the sender to send packets. In case of packet replication, an attacker replicates the stale packets, thus consumes additional bandwidth of the network. In route cache poisoning, an attacker may modify the route cache to mislead the sender for forwarding packets. In rushing attack, an attacker quickly flooded the RREQ packets in to the network adversely; as a result, when the legitimate packets are flooded in the network, these are discarded by the MN by assuming these as duplicate packets.

Session hijacking is an example of transport layer attack. In this attack, it gives an opportunity to the malicious node to behave as a genuine node. Since the entire authentication for the MN is done at the beginning of the session so, adversaries can take the advantage of attacking the system. Repudiation is a kind of attack which may occur in the application layer of the network.

Similarly application layer attack contains repudiation attack. Multi-layer attack take place in any layer of network protocol stack. One example of such kind of attack is a kind of Denial of service attack in which attacker may prevent genuine MN from the services offered by the network. In SYN flooding attack, malicious node sends a

large number of SYN packets to victim node and then spoofing the return address. One of the severe attacks in MANETs is DDoS in which several adversaries are distributed throughout the network and they prevent the genuine nodes from accessing network services.

In impersonation attack, an adversary may become a part of network management and start changing the internal configuration of the network

2.1.5.3 Security Goals

Security issues in MANETs lead to some security goals such as *authentication, integrity, confidentiality, availability, access control* and *non-repudiation* [68].

In authentication, it is expected that nodes in MANETs must authenticate each other to communicate amongst themselves. While communicating, it must ensure that there should not be any third party which interfere the communication. Authentication can be provided by different methodologies such as cryptographic hash function, digital signature and issuing of certificate.

Due to flexibility of MANETs, all types of MN are allowed to enter into the network. Malicious nodes may compromise with one another to mislead the genuine node and thus it may modify the original message or it may drop the packets without delivering these to destination. , according to the concept of integrity, the original message must be in take. It should not be modified or dropped.

Another security goal of MANETs can be explained as confidentiality, which can be explained by the fact that any unauthorized persons are not allowed to view the message in original. It can be achieved by different encryption policies so that unauthorized persons are restricted from viewing the original messages.

Irrespective of state of the network, it must provide streamline service to the network. This fact can be explained by the concept of availability. According to non-repudiation, sender and receiver should not deny the receiving of message.

2.1.5.4 Vulnerabilities in Existing Protocol

MANETs is vulnerable to different kind of attacks due to its flexibility of uses.

Vulnerabilities in routing protocol implies the attacks against routing protocols to violate the rules of MANETs, insertion of erroneous routing information, attempting to disturb routing algorithm [82][83]. MANETs protocols are suffered from impersonation, fabrication etc. Attacks may come from any end. As mentioned in section 2.1.5.2, attacker may attack MANETs in different layer of the network such as application layer, transport layer, network layer, data link layer and physical layer.

Some of the draw backs of MANETs protocols are,

- a. Lack of central monitoring system
- b. Lack of central point of entry
- c. Unable to handle high mobility of the nodes
- d. Limited resources like battery power, bandwidth
- e. Lack of clear line of defense and secure communication
- f. Easy authorization of MN
- g. Unable to handle distributed nature of attack

Due to vulnerabilities of protocol, a malicious router may inject packets with same identification information into the network by collecting source IP and sequence number of any packet [81]. So, destination accepts the invalid packets and discards the valid packets. Apart from these, different kind of attacks such as blackhole attack, wormhole attack, Byzantine attack, information disclosure attack, resource consumption attack, routing table overflow attack, routing table poison attack, packet replication attack and many other attacks are caused due to lack of security in MANETs protocol.

Again, as mentioned in section 2.1.5.3, security goals of MANETs can be achieved in terms of availability of service, integrity, confidentiality, authentication, non repudiation, authorization and anonymity etc. A malicious node which exhibit in the network maliciously and shows its presence in the network by packet dropping, battery drainage, bandwidth consumption, buffer overflow, stale packets, delay of

packets, link break, message tampering, fake routing, stealing information and session capturing [80].

Routing protocol in MANETs should be designed in such a way that it must meet the security goals to protect the network from attacks.

2.1.5.5 Security Mechanism

As mentioned in section 2.1.5.4, MANETs protocols are vulnerable to different kind of attacks. Adversaries compromise with network functions by attacking different layers of the network [84]. So, significant research efforts must be made to provide secure mechanism in such a way that it should increase the survivability of MANETs and protect MANETs from different attacks. It can be done either by developing secure routing protocol or by improving the robustness of MAC layer protocol [84].

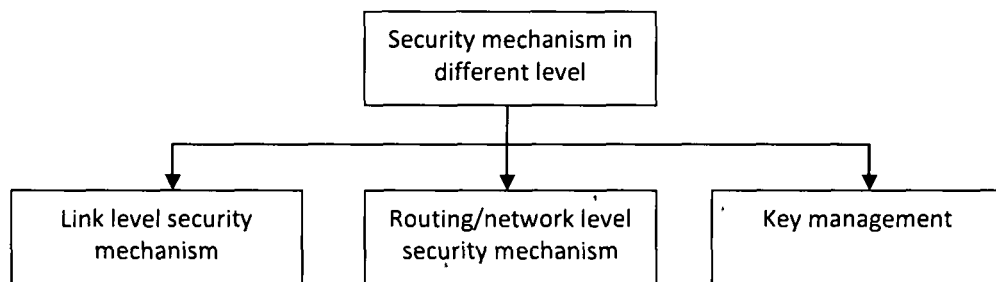


Figure 2.10 Security mechanisms in MANETs

Security mechanisms in different levels are as follows:

Link level security: It specifies the data transfer security between two nodes. In ad hoc wireless network links are not secure. Adversaries can enter into the network at any time to intercept the packets. So, there need a secure mechanism in this level in such a way that MN can trust each other to establish secure communication amongst them. Third party is not allowed to view information. To protect data, encryption and decryption policy of cryptography can be implemented. Certification authority is another kind of secure mechanism which can be applied as link level security in

MANETs. But certification mechanism creates network overhead and sometimes these are compromised with malicious nodes to consume confidential information from the network.

Network level security: Since all the nodes are worked as router in MANETs, so routing within the network is more vulnerable as adversaries are also worked as parts of network. Security mechanism in this level of the network is very challenging. Basic purpose of this security is to provide secure data transmission from source to destination. This kind of security mechanism should monitor the network in such a way that there should not be any modification or dropping of packets due to malicious node present in the network. Moreover, it should able to determine the presence of selfish node in the network. So, development of a proper intrusion detection system is an example of such kind of secure mechanism. It can be achieved by IPSec, self issuing of certificate, extending the existing routing protocol, application of multi agent system, game theoretic approach etc.

Key management: This is also another kind of secure mechanism, in which cryptographic keying mechanisms are used to provide security. It comprises of key generation, key distribution and key maintenance. Some key management techniques are symmetric key management such as OFT, Logical key hierarchy, asymmetric key management, mobile certification authority etc.

2.1.5.6 Secure Routing Protocol

Due to specific characteristics of MN of MANETs as router, mobile node that takes part in communication, have the right to work with data packets. Any intruder, which is also a part of network, may misuse the packets by its malicious activities. Most of the routing protocols are lacking behind the security. It assumes that all the nodes in MANETs are trustable. Secure routing protocols are derived as an extension of existing routing protocol. Security extensions are either cryptographic or trust based system [101]. Main security service of routing protocol is the authorization. Authorization is done by two different processes, first, when the routing updates come

from outside, router should decide whether it will make necessary change in it or not. It is named as import authorization. Another authorization known as export authorization may carry out whenever it receives a request for routing information. Authorization is related with another two terminologies such as authentication and integrity [100][102]. Routing protocol generates two kinds of messages, as data message and routing message.

Table 2.1: Security extension of some of MANETs routing protocol

Reactive protocol	Proactive protocol	Hybrid protocol
Extension of DSR protocols: 1. SQoS Route Discovery 2. Ariadne 3. Confidant	Extension of DSDV: 1. SEAD	Extension of ZRP : 1. SRP
Extension of AODV : 1. CORE 2. SAODV 3. TAODV 4. SAR	Extension of OLSR: 1. SLSP	
Others 1. SPREAD 2. ARAN		

Data message can be protected by point-to-point security system as these are point-to-point in nature. But routing messages are normally processed or modified or resent by the immediate node, so immediate node must provide the power of authentication to process the routing message. Implementation of secure routing protocol is getting more challenging in MANETs to protect the network from intruders. Some examples of extension of existing protocols for secure routing are shown below in Table 1.

Data message can be protected by point-to-point security system as these are point-to-point in nature. But routing messages are normally processed or modified or resent by the immediate node, so immediate node must provide the power of authentication to process the routing message. Implementation of secure routing protocol is getting more challenging in MANETs to protect the network from intruders. Some examples of extension of existing protocols for secure routing are shown below in Table 1.

Following Table 2 shows the comparison of some of the secure routing protocols [101].

Table 2.2: Comparison of the best known secure routing protocols.

Secure Protocol	Background Protocol	Type of Attack				
		Modification	Impersonation	Fabrication	Wormhole	Selfish
Ariadne	DSR	Yes	Yes	Yes	Yes	No
Confidant	DSR	No	No	No	No	Yes
SAODV	AODV	Yes	Yes	Yes	No	No
TAODV	AODV	Yes	No	Yes	No	Yes
SAR	AODV	Yes	Yes	Yes	No	No
ARAN	Reactive	Yes	Yes	Yes	No	No
SEAD	DSDV	Weak	Yes	Yes	No	No
SLS	OLSR	Yes	Yes	Yes	No	No
SRP	ZRP	Yes	Yes	Yes	No	No

2.1.5.6.1 SAODV

The Secure Ad hoc On-Demand Distance Vector (SAODV) routing protocol is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism by providing security features like integrity and authentication. It uses the cryptographic method to secure AODV protocol [85][86][87] [88][89][90] [103][104].

Digital signature is used to authenticate non-mutable fields of the messages and hash chains to secure the hop count information, as for non-mutable information, authentication can be performed in a point-to-point manner. But for mutable information, same kind of technique cannot be used. Since router error messages are some big mutable messages. Hence, some other techniques are used [85]. SAODV can use the Simple Ad hoc Key Management (SAKM) as a key management system. In these extension messages, there is a signature of the AODV packet with the private key of the original sender of the Routing message (not of the intermediate nodes that just forward it).

Concerning to RREQ and RREP messages there are two alternatives. In case of first one, only final destinations are allowed to reply a RREQ,

- When a RREQ is sent, the sender signs the message. Intermediate nodes verify the signature before creating or updating a reverse route to that host. Reverse route is preserved only if the signature is verified and found fine.
- The actual destination node signs the RREP with its private key.
- Intermediate and final nodes, again verify the signature before creating or updating a route to that host, and then store the signature with the route entry.

In case of second one there is no such limitation

- When a RREQ is sent, the sender signs the message. Intermediate nodes verify the signature before creating or updating and if the signature is fine they store the reverse route.
- The RREQ message has a second signature that is always stored with the reverse route. This second signature is needed to be added in the RREPs of that RREQ and in regular RREPs to future RREQs that the node might reply as intermediate nodes.
- An intermediate node that wants to reply a RREQ needs not only the correct route, but also the signature corresponding to that route to add it in the RREP, the 'Lifetime' and the 'Originator IP address' fields that work with that signature. If these are fine and correct, it generates the RREP.

If a node wants to reply as an intermediate node for a route to a node that has been added due to a RREQ or to a RREP, it has to store the 'RREQ Destination' or 'RREP Originator' IP address, the lifetime and the signature. And use them as the 'Signature', 'Old Lifetime', and 'Old Originator IP address' fields in the RREP-DSE message.

2.1.5.6.2 TAODV

TAODV (Trusted AODV) is a secure routing protocol which is an extension of AODV protocol. It is based on trust model. It uses trust relationship among the nodes for routing. It employs a trust model derived from subjective logic. Here signing and verification of digital signature at each routing message is not required. It consists of basic four different parts as [105][106],

- Basic routing protocol i.e. AODV
- Trust model that define the algorithms or rules to combine, judge, and update trust information based on subjective logic [142]
- Trusted routing protocol
- Self-organized key management mechanism that generate a *{secret, public}* key pair for each node and distribute public keys in a secure self-organized way

Modules of trusted routing protocol includes the following

- Trust recommendation
- Trust combination
- Trust judgment
- Trust update
- Signature authentication
- Trust authentication

When a node A wants to establish a route to any other node B, initially the uncertainty elements in A towards other node such as B is 0.5 or more. So, A may be in confusion whether it will believe B or not. So it will try to implement either a) cryptographic scheme as applied in SAODV or b) Any other scheme for route discovery. After consecutive communication, gradually A will try to implement the “Trust updating algorithm” for other nodes. After establishment of trust amongst the different nodes in the network, then the nodes will be relied on trusted routing protocol.

Now, node A will try to gather all trust information about node B from different neighbors and then calculate the trust for node B.

Node A now will utilize the trust recommendation protocol to exchange trust information about a node, B, from its neighbors, then use the trust combination algorithm to combine all the recommendation opinions together and calculate a new option towards B.

Framework for TAODV is as shown in Figure 2.11 below.

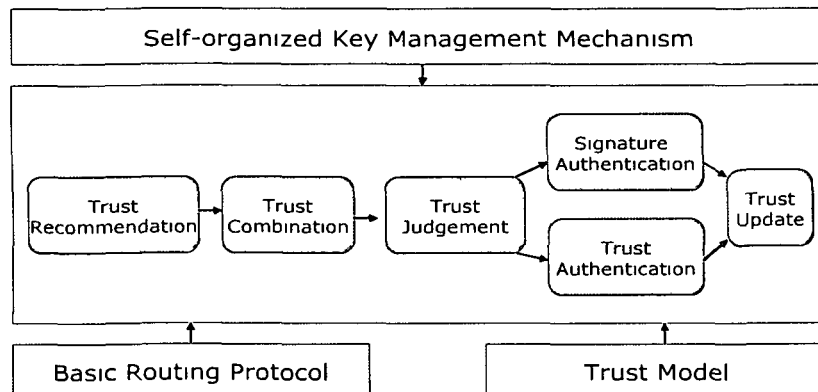


Figure 2.11 Framework for TAODV

Routing Table Extension takes place in TAODV implementation; original routing table includes another three fields as [142]

- Positive events are the successful communication times between two nodes.
- Negative events are the failed communication ones
- Opinion: It is the nodes believe towards another node's trustworthiness

Similarly routing message extension also takes place by adding new fields for trust information. These are denoted as TRREQ (trusted routing request) and TRREP (trusted routing reply).

Trust updating policy updates the trust dynamically. It consists of some steps as follows::

- a. Whenever positive events occurred in A while communicating to B, immediately B's number of successful events in A will be increased by 1.
- b. Likewise each time a negative event occurs while communicating from node A to node B, immediately B's number of failed events in A will be increased by 1.
- c. Each time when the field of successful and failed events is changing, the corresponding value of opinion will be recalculated.

- d. Whenever a new opinion is obtained, the corresponding number of successful or failed events will be mapped back with the help opinion space to the evidence space.
- e. The positive event implies successful data or routing packets forwarding, keeping message integrity and passing cryptographic verification.

The trust recommendation protocol consists of three types of messages such as Trust Request Message (TREQ), Trust Reply Message (TREP), and Trust Warning Message (TWARN).

Trust Routing Step at a node is as shown in Figure 2.12.

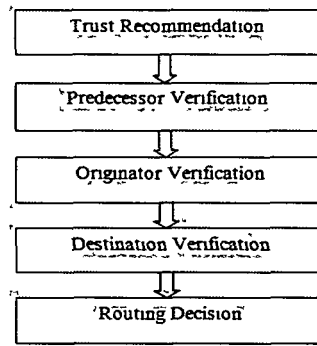


Figure 2.12 Trusted routing step at a node

2.1.5.6.3 *Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN)*

The objective of OCEAN [173] is to avoid this trust-management machinery and see how far it can get simply by using direct first-hand observations of other nodes' behavior.

In OCEAN, a node makes routing decisions based solely on direct observations of its neighboring nodes exchanges with it. This eliminates most trust management complexity, although at a cost of less information with which to make decisions about node behavior.

OCEAN is using the same concepts deployed in the Watchdog and Pathrater but it also punishes the selfish and misbehaving nodes in order to force them to cooperate in the network.

OCEAN is a layer that resides between the network and MAC layers of the protocol stack, and it helps nodes make intelligent routing and forwarding decisions. Principle of OCEAN can be implemented in any routing protocol of MANETs [174].

OCEAN analyses the routing misbehavior according to misleading and selfish behavior. If a node takes part in routes discovery but does not forward a packet, then such kind of nodes are known as misleading nodes. On the other hand, if a node does not participate in routes finding, it is considered as a selfish node. In order to discover misleading routing behaviors, after a node forwards a packet to its neighbor, it saves the packet in its cache and monitors the neighboring node for a given period of time. It then produces a positive or negative event as its monitoring results in order to update the rating of neighboring node. If the rating is lower than faulty threshold, neighboring node is added to the list of problematic nodes and also added to RREQ as an avoid-list. As a result traffic will not use this problematic node. This node is given a specific time to return to the network because it is possible that this node is wrongly accused of misbehaving or if it is a misbehaving node, then it must improve in this time period.

OCEAN [173] is composed of five components to discover malicious nodes:

1. **Neighbor Watch:** It observes the behavior of the neighbors of a node.
2. **Route Ranker:** It holds the nodes ratings for the neighbor nodes.
3. **Rank-based Routing:** It applies the information from Neighbor Watch in the actual selection of routes.
4. **Malicious Traffic Rejection:** It performs the straightforward rejection of traffic from nodes that are considered misleading.
5. **Second Chance Mechanism:** It is intended to consider the nodes that were previously considered misleading to become useful again.

OCEAN attempts to mitigate selfish routing behavior in ad hoc networks. The general idea is to punish nodes for their selfish behavior by rejecting their traffic, in the hopes that this threat will force them to cooperate. OCEAN relies only on direct observations of interactions with neighbors to measure their performance.

But OCEAN is more sensitive to some parameter settings. It doesn't punish misbehaving node as severely as systems using full blown reputation information. OCEAN is not a guaranteed service. It doesnot guarantee whether a packet is successfully received by the destination or not [173]. Sometimes trade based system like OCEAN may suffer from deadlock problem where two nodes may not forward packets for each other for a long time. Addressing scheme for addressing this problem also consumes extra overhead. Chippoint scheme of OCEAN to detect selfish node provides a solution but decreases the network throughput [173][174].

2.2 Packet Dropping Attack in MANETs

In MANETs, node cooperation for forwarding packets from one node to another is the most essential characteristics. Initially all the nodes that participate in network communication are assumed to be trustable. All the nodes are worked as router. So, all the nodes are supposed to forward packets to their next hops in normal operation of MANETs. Instead of that, some adversaries that take part in MANETs communication are intentionally dropped packets instead of forwarding them to next hop. Such kind of attack is known as packet dropping attack. Packet dropping attack can be considered as one of the vulnerable attacks in MANETs. Malicious node in the network drops packets intentionally which are supposed to be forwarded to reach destination [107][108][109][110][113]. Routes that pass through such kind of nodes fail to establish path from source to destination [8]. As a result, network performance degrades abruptly. In ad hoc network, packets may drop due to several reasons. Some nodes are selfish nodes. Selfish nodes use system services while taking care to save some of its own resources to the extent of deviating from regular routing and forwarding some of the nodes are working as malicious node which can drop packets

intentionally in the network to reduce network performance parameters abruptly. Some packets may be dropped due unsteadiness of the medium such as network contention, congestion and corruption in the medium. Sometimes packet dropping is caused by genuineness of the node such as overflow of the transmission queue [107]. All these causes are not considered as packet dropping attack.

2.2.1 Types of Packet Dropping Attack

2.2.1.1 Selective Packet Dropping Attack

MANETs communication is a multi-hop communication and each node in the network forwards packets to its next hop for delivering packets to destination. Without the node's cooperation, MANETs is not able to provide service. More the nodes are cooperative to transfer traffic; network becomes more powerful and reliable. Route discovery and packet forwarding by the nodes in MANETs consumes resources including local CPU time, network bandwidth, memory and most importantly energy of MN. Selfish nodes in MANETs are kind of node which wants to utilize the network resources for its own profit but not willing to provide service to other nodes [114][115][116][117][118]. As a result, any packet that comes for its own is consumed by such node, while any other packets which are supposed to be forward are dropped to maximize their benefits. They are assumed to behave rationally [119]. Nodes are strongly motivated to accept any packets which are meant for them and deny any other packets which are supposed to forward to next hop for destination [118]. Some advantages of having selfish node is that it can reduce the total rebroadcast traffic during flooding based route discovery [114]. Detected selfish nodes should be avoided from the network; thereby it helps to increase network performance parameters [116]. Selfish nodes don't damage the other nodes in MANETs directly. But indirectly it harms the network by its non cooperative nature to forward the packets. Selfish nodes can be classified in two different categories [115].

Active selfish node: This kind of nodes participates in network communication, any packets which are meant for them are received by them, and rests of the packets are dropped by these nodes to save their resources.

Passive selfish node: These kinds of nodes don't participate in network communication. They stay silent and they don't contribute to any of the activities like forwarding, receiving, route discovery and network maintenance.

Selfish nodes may possibly diminish the network services and thereby decrease the whole data accessibility in the network [117]. So, the overall performance of MANETs gets affected.

2.2.1.2 Malicious Packet Dropping Attack

Malicious packet dropping attack is a kind of DoS attack in which malicious node that presents in the network, drops packets instead of forwarding these to next hop [91][92][93][95][96][97]. Such kinds of nodes disrupt the usual network services with an intention to drain other node's resources [94].

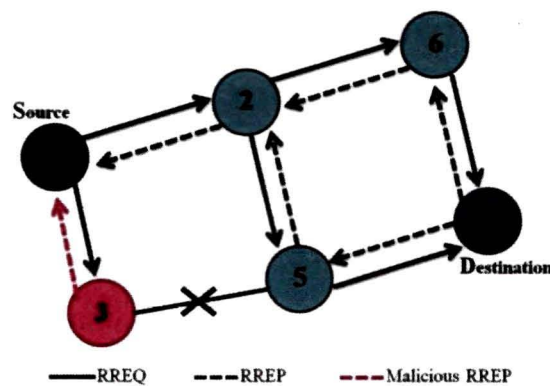


Figure 2.13 A single example of packet dropping attack

DoS attack may affect the network in two different ways, DoS attack on routing traffic and DoS attack on data traffic. An attacker can drop packets in the network for both kind of traffic in different ways. As for example, in case of blackhole attack, data traffic may be captured by advertising shorter distance and then drop the attracted packets. In another case, data traffic may not flow through routing paths and some of

them may drop due to network congestion. In such situation, an attacker avoids some traffic or redirects the traffic to other nodes by advertising routing update message. An attacker may mislead some of the nodes to update their routing tables with invalid paths so that if any traffic flows through such path will eventually drops packets. Malicious nodes can inject huge amount traffic into the network to clog the network, so that due to congestion in the network, genuine packets are also dropped along with malicious packets to reduce congestion. Malicious nodes join the network and compromise with genuine nodes to participate in communication; then it silently drops some or all the packets which are supposed to be forwarded. Malicious packet dropping attack is a serious threat to MANETs, which is very easy to deploy but very difficult to detect and avoid [95]. Most of the routing protocols in MANETs are vulnerable to different kind of attacks including packet dropping attack [91].

As shown in Figure 2.13, node 3 is the malicious node who replies the RREQ packet sent from source node and sends a false RREP packet by mentioning that it has the shortest route to destination. As a results source starts sending the packets via the erroneous node. It then drops the packets instead of forwarding packets to destination.

2.2.2 Mitigation of Impact of PDA in MANETs

2.2.2.1 Selfish Node Mitigation

Security is the primary concern of MANETs. Selective packet dropping attack or selfish packet dropping attack is also kind of unlawful activity in MANETs as mentioned in section 2.2.2.1. Because of this activity, normal function of MANETs gets disrupted. So, many researches are going on to mitigate such kind of attack in MANETs. Few examples are given below,

In [98], it tries to identify potential threats in MAC layer introduced by selfish nodes, mainly the “smart” attack which can cross the boundaries of existing detection and reaction system against MAC layer selfish behavior. So, they propose a *Predictable Random Backoff (PRB)* algorithm that is capable of mitigating the impact of these vulnerabilities. In [99], it is believed that frequent elimination of such misbehaving

nodes never allows a faster growth of MANETs. So, authors propose a mathematical model which is based on time division technique to minimize the malicious behavior of node, instead of repeated elimination of such nodes. In [119], it investigates the security mechanism which is proposed for selfish node attack, shared root node attack and control packet attack in MANETs. It is done with the help of Multicast Ad hoc On Demand Distance Vector (MAODV). Here, security solution is evaluated with the help of delivery ratio, control overhead and total overhead. In [120], authors addressed the behavior based anomaly detection technique which is inspired by biological immune system to enhance performance of MANETs in spite of presence of misbehaving node like selfish node. So, they use the intelligent learning techniques that learn and detect each node by false alarm and negative selection approach.

2.2.2.2 Malicious Node Mitigation

Nodes in MANETs usually cooperate and forward each other's packets in order to carry smooth running of communication. All the nodes that work as a host are also work as router at the same time. Initially every node is trusted by every other. By taking this as an advantage, adversaries which are also represented themselves as a part of communication device, start dropping packets intentionally to disrupt the normal function of MANETs. To mitigate packet dropping attack in MANETs, several methodologies are used. These can be categorized as *Centralized methodology*, *distributed* and *game theoretic based* methodology. In *centralized methodology*, it is assumed that all data related to network communication are centrally observed. It is a static offline system. Details of this method are discussed in Chapter 3 of this thesis. In *distributed methodology*, detection of packet dropping attack is done based on cooperative participation of nodes in MANETs. Chapter 4 of this thesis contains detail discussion of this methodology. In *game theoretic based* methodology, MANETs can be formulated as coalition game in which all the genuine nodes in the network that cooperate in packet forwarding, should be in one side of the game.

Malicious nodes which will try to drop the packets invariably will be in the other side of the game. Details of this methodology are discussed in Chapter 5 of this thesis. Apart from these, several solutions are proposed for mitigating the routing attack including packet dropping attack. But most of them isolate malicious node based on binary decision taken for severity in attack. This causes additional damage to the network, so, risk mitigating technique is considered as one of the important technique [122]. In [97], authors address packet dropping attack in wireless ad hoc network by post routing detection methodology called as side channel monitoring (SCM). Basic idea behind the technology is to use the nodes which are adjacent to data communication path, to monitor the message forwarding nature of the nodes en route. These nodes constitute a directional side channel towards source which is parallel to the backward route. As and when it discovers abnormality in MANETs due to some malicious nodes, they issue an alarm packet to the source node through both the channel. Then analytical methods are used to identify number of malicious nodes and their activities. In [121], authors propose a trust based security protocol based on MAC layer approach, which attains confidentiality and authentication of packets in both routing and link layer of MANETs. First phase of the protocol contains trust based packet forwarding scheme for detecting and isolating the malicious nodes using routing layer information. They use a trust counter for each node. A node is punished or rewarded based on trust value of the counter. If the trust counter value falls below a trust threshold, then the respective node will be identified as malicious node. In [123], authors propose a security mechanism that provides message integrity, mutual authentication and two hop authentication mechanism without the help of online certification authority. This mechanism provides identity impersonation, replay attacks and enable node to regulate the behavior of its neighbors to resist active attack.

2.3 PDA Detection Methodology

Observing the severity of PDA, several methodologies have been proposed. These are broadly classified as centralized PDA detection methodology, distributed PDA detection methodology and game theoretic approach for PDA detection. In normal operation of MANETs, packets sent from source to destination must be reached in proper order. Of course sometimes due to network congestion or any other reasons except malicious activities, some of the packets may be dropped. But when an exceptional numbers of packets are dropped in the network, a PDA detection methodology must work in the network for detection and avoidance of malicious nodes so that it can continue its service. At the same time, any PDA detection methodology should not hamper the normal operation of MANETs; thereby its security goals like *authentication, integrity, confidentiality, availability, access control* and *non-repudiation* must be fulfilled as mentioned in section 2.1.5.3.

2.3.1 Categories of PDA Detection Methodology

Packet dropping attack can be addressed by following methods,

- (a) Credit-based systems [175, 176, 178, 177]
- (b) Reputation-based systems [181, 182, 189,186, 180, 188,187, 185]
- (c) Acknowledgment-based systems [189, 190,191]

Credit-Based Systems:

In this system, incentives are provided for forwarding packets. In [175][176], authors proposed a system in which nodes receive credit for each packet they forward, and spend their accumulated credit to transmit their own packets. A counter named as *nuglet* is used. The nuglet counter is incremented each time the node forwards a packet, and decremented each time the node transmits its own packet. The nuglet counter has some restriction like it cannot take on a negative value and cannot be arbitrarily changed by the node. To enforce this rule, the nuglet counter is implemented in a tamper-proof hardware module, called the security module. The security module is assumed to provide universal protection from both software and physical attacks.

In [177], authors proposed *Sprite*, in which nodes collect receipts for the packets that they forward to other nodes. For a packet sent from a source to a destination, each node along the path records a hash of the packet as the receipt, and forwards the packet to its next hop. When the node has a high-speed link to a Credit Clearance Service (CCS), it uploads its receipts. The CCS determines the value of the receipts and provides credit in exchange. Credit is only granted if the destination reports a receipt verifying reception of the packet and if the node was on the routing path. After verification, credit is removed from the sources account and given to each node who participated in packet forwarding. Thus nodes that transmit their own packets but do not cooperate in packet forwarding will incur a debt at the CSS. Misbehavior implies debt accumulation beyond a certain threshold is interpreted as

A scheme has been proposed in [178], which not only rewards nodes for participating in packet forwarding with credit, but takes into account congestion. When sending a packet, the source computes a congestion price, which is a metric defined by the required power for transmission and the available bandwidth. It then compares this price to its personal willingness-to-pay parameter, which the source continually adjusts based on its personal observations. By taking into consideration bandwidth in computing the cost (credit) is required to send a message to the destination, the scheme avoids overwhelming low cost routes, as they would increase in costs as they become saturated. Power and bandwidth metrics are dynamically updated based on shared information among nodes.

While credit-based systems motivate selfish nodes to cooperate in packet forwarding, they provide no incentive to malicious nodes. Such nodes have no incentive to collect credit and receive no punishment for non-cooperation. Furthermore, tamper-proof hardware as mentioned in [179] is currently too expensive to integrate in every network device, while providing an unverifiable level of security. *Sprite* removes this requirement, at the expense of requiring the presence of a CCS. Lastly, credit-based systems lack a mechanism for identifying the misbehaving node(s), allowing them to remain within the network indefinitely.

Reputation-Based Systems: Reputation-based systems use neighborhood monitoring techniques to identify misbehaving nodes. In [180], authors proposed a scheme which relies on two modules, the watchdog and the pathrater. The watchdog module monitors the node's behavior of their next hop node by operating their radio in promiscuous mode. Once a node forwards a packet to the next hop, the node overhears to verify that the next hop node faithfully forwarded the packet. The scheme is based on the assumption that links between nodes are bi-directional and nodes utilize omni-directional antennas. A cache is used to store packets that wait for verification. If packets remain in the cache longer than a threshold period, the watchdog makes an accusation of misbehavior. The pathrater module uses the accusations generated to choose a path that will most likely avoid misbehaving nodes. CONFIDANT, which is built upon the watchdog/pathrater model, is proposed in [181][182]183] Here, they proposed a scheme, nodes perform neighborhood monitoring using their radios in promiscuous mode while selecting paths that attempt to avoid misbehaving nodes. Whereas authors proposed using only the previous hop for monitoring, CONFIDANT requires all neighboring nodes to operate in promiscuous mode for monitoring, thus relying on a neighborhood watch. In addition, monitoring nodes notify other nodes of detected misbehavior through the broadcast of alarm messages. Instead of including a proof of the misbehavior in the alarm message, a scheme based on Pretty Good Privacy (PGP) [184] is implemented to determine the trust level of the alarm message.

In [185], a reputation-based scheme is proposed which is consisting of four modules: a Monitor, a Opinion Manager, a Reputation Manager, and a Routing/Forwarding Manager. The Monitor module monitors the nodes neighbors via the watchdog model, verifying that neighboring nodes faithfully participate in packet forwarding. Based on observations from the Monitor, the Opinion Manager formulates opinions of the nodes behavior and periodically advertises them to neighboring nodes. The Reputation Manager accepts these opinions and processes them to arrive

at a trust metric for a specific node. When establishing a routing path to a destination, the Routing/Forwarding Manager uses these trust metrics to avoid including untrustworthy (misbehaving) nodes.

In [186], authors present similar work on how to derive reputation rankings using beta probability functions based on feedback of behavior of neighboring node.

In [187], it proposed a reputation-based scheme which also relies on first and second-hand information. However the authors propose two different methods for nodes to acquire the second-hand information, i.e., the reputation information originating from neighboring nodes. In the first method, as soon as a node witnesses misbehavior, defined according to a threshold number of packet drops, the node immediately broadcasts the accusation. Thus the proactive transmitting of reputation information allows all nodes in the network to have up-to-date behavioral information about their neighbors. However, since the proactive broadcasting of information may require unacceptable bandwidth requirements, thus diminishing the networks functionality, nodes can also acquire second-hand information in an on demand manner. In much the same way that on demand routing protocols request route information.

Another proposal in [188], proposed CORE, in which nodes create a composite reputation rating for a given node by combining the nodes subjective reputation, its indirect reputation and its functional reputation. The subjective reputation is calculated from direct observation of the nodes behavior, using a weighted average of both current and past observations. The indirect reputation is a value calculated based on second-hand observations made by other nodes in the network. A node's functional reputation is based on task-specific behavior. Thus it is computed based on its reputation in packet forwarding, routing, etc. Denial-of-service attacks based on misbehaving nodes broadcasting negative ratings for honest nodes are prevented by preventing nodes from broadcasting negative behavior. Thus when sharing reputation metrics, node are restricted to sharing only positive ratings.

Acknowledgment-Based Systems: Acknowledgment-based systems rely on the reception of acknowledgments to verify that a message was forwarded to the next

hop. Authors proposed a scheme called TWOACK in [189], where nodes explicitly send 2-hop acknowledgment messages(TWOACK) to verify cooperation. For every packet a node receives, it sends a TWOACK along the reverse path, verifying to the node 2-hops upstream that the intermediate node faithfully cooperated in packet forwarding. Packets that have not yet been verified remain in a cache until they expire. A value is assigned to the quantity/frequency of un-verified packets to determine misbehavior.

TWOACK is improved in [190] by proposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments (2ACK) to verify cooperation. To reduce overhead, 2ACK allows for only a percentage of packets received to be acknowledged. It uses a one-way hash chain to allow nodes to verify the origin of packets they are acknowledging, thus preventing attacks in which a misbehaving node drops the original packet and forwards a spoofed packet.

Similarly, another method had been proposed in [191] to identify the link on which misbehavior is occurring.

Since acknowledgment-based systems are proactive, hence it incurs message overhead regardless of the presence of misbehavior. 2ACK provides a method to reduce message overhead by acknowledging only a fraction of the packets, with the tradeoff of increased delay in misbehavior detection.

2.3.2 Existing Detection Methodologies

Some of existing works related to distributed PDA detection as well as game theoretic approach to detect PDA are discussed below,

Distributed PDA detection approach, based on end-to-end connection is proposed in [124]. This detection and isolation mechanism of packet dropping attacks is based on three ID messages like path validation message (PVM) that enables E2E feedback loop between the source and the destination, attacker finder message (AFM) which will find the attacker node from the routing path and attacker isolation message (AIM) is used to isolate the attacker from routing path and update the black list and then

trigger to neighbors with updated information. Another cooperative PDA detection mechanism has been proposed in [125], which is based on cooperative participation of nodes in MANETs. It is a collaborative distributed protocol which involves cryptographic key distribution and intrusion detection activity for detection of malicious packet dropping attack. Key distribution requires a trust management scheme to dynamically bind the trust relationship between the key distribution servers and the clients. Initial security to intrusion detection mechanism is provided by LLCs (location limited side channels). Thereafter a dynamic trust management scheme for key distribution is provided. A reputation based approach to detect and isolate the misbehaving nodes has been proposed in [126], which can be integrated with routing protocol. It is based on sending acknowledgement packets and counting the data packets on an active path. It has basic three steps like detection of malicious group, identification of particular misbehaving node, isolation and mitigation of misbehaving node. A solution is proposed in [127] to monitor, detect and isolate misbehaving nodes that participates in packet dropping attack. It suggests a social-based approach to approve detection and isolation of malicious nodes to reduce false positive rate of detection. This methodology fails to analyze collusive dropping of packets. It has limitations to handle continuous packet dropping as well as detection of selective misbehavior. Detection is delayed because of Bayesian approach for judgment. A novel simplified IDS for detecting packet dropping attack in MANETs is proposed in [128]. Here mobility aspects are considered explicitly by means of a heuristics which considers the forwarding operation at each node. In [129], a homographic linear authentication based public auditing architecture is proposed which assist the packet dropping attack detector to detect the attack accurately by verifying the truthfulness of packet loss information reported by nodes.

Game theoretic approaches to distributed PDA detection have been explored. In [130], IDS is handled by an elected leader node for a cluster of node. A unified framework has been proposed in this paper to increase the lifetime of the cluster, detect and punish the misbehaving leaders through checkers. To analyze the

hop. Authors proposed a scheme called TWOACK in [189], where nodes explicitly send 2-hop acknowledgment messages(TWOACK) to verify cooperation. For every packet a node receives, it sends a TWOACK along the reverse path, verifying to the node 2-hops upstream that the intermediate node faithfully cooperated in packet forwarding. Packets that have not yet been verified remain in a cache until they expire. A value is assigned to the quantity/frequency of un-verified packets to determine misbehavior.

TWOACK is improved in [190] by proposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments (2ACK) to verify cooperation. To reduce overhead, 2ACK allows for only a percentage of packets received to be acknowledged. It uses a one-way hash chain to allow nodes to verify the origin of packets they are acknowledging, thus preventing attacks in which a misbehaving node drops the original packet and forwards a spoofed packet.

Similarly, another method had been proposed in [191] to identify the link on which misbehavior is occurring.

Since acknowledgment-based systems are proactive, hence it incurs message overhead regardless of the presence of misbehavior. 2ACK provides a method to reduce message overhead by acknowledging only a fraction of the packets, with the tradeoff of increased delay in misbehavior detection.

2.3.2 Existing Detection Methodologies

Some of existing works related to distributed PDA detection as well as game theoretic approach to detect PDA are discussed below,

Distributed PDA detection approach, based on end-to-end connection is proposed in [124]. This detection and isolation mechanism of packet dropping attacks is based on three ID messages like path validation message (PVM) that enables E2E feedback loop between the source and the destination, attacker finder message (AFM) which will find the attacker node from the routing path and attacker isolation message (AIM) is used to isolate the attacker from routing path and update the black list and then

trigger to neighbors with updated information. Another cooperative PDA detection mechanism has been proposed in [125], which is based on cooperative participation of nodes in MANETs. It is a collaborative distributed protocol which involves cryptographic key distribution and intrusion detection activity for detection of malicious packet dropping attack. Key distribution requires a trust management scheme to dynamically bind the trust relationship between the key distribution servers and the clients. Initial security to intrusion detection mechanism is provided by LLCs (location limited side channels). Thereafter a dynamic trust management scheme for key distribution is provided. A reputation based approach to detect and isolate the misbehaving nodes has been proposed in [126], which can be integrated with routing protocol. It is based on sending acknowledgement packets and counting the data packets on an active path. It has basic three steps like detection of malicious group, identification of particular misbehaving node, isolation and mitigation of misbehaving node. A solution is proposed in [127] to monitor, detect and isolate misbehaving nodes that participates in packet dropping attack. It suggests a social-based approach to approve detection and isolation of malicious nodes to reduce false positive rate of detection. This methodology fails to analyze collusive dropping of packets. It has limitations to handle continuous packet dropping as well as detection of selective misbehavior. Detection is delayed because of Bayesian approach for judgment. A novel simplified IDS for detecting packet dropping attack in MANETs is proposed in [128]. Here mobility aspects are considered explicitly by means of a heuristics which considers the forwarding operation at each node. In [129], a homographic linear authentication based public auditing architecture is proposed which assist the packet dropping attack detector to detect the attack accurately by verifying the truthfulness of packet loss information reported by nodes.

Game theoretic approaches to distributed PDA detection have been explored. In [130], IDS is handled by an elected leader node for a cluster of node. A unified framework has been proposed in this paper to increase the lifetime of the cluster, detect and punish the misbehaving leaders through checkers. To analyze the

interaction of checkers, a cooperative game theoretic model has been proposed in such a way that it is able to reduce false positive rate. To maximize the probability of detection, a zero-sum non-cooperative game between the leader and intruder is formulated. It also helps the leader to use its optimal sampling strategy during intrusion detection. A throughput characteristic function is defined in [131] which is meant for maximal throughput and reliable traffic. Nodes are enforced to form coalition based on this function. It is also used to imply quantification of security function. Thus, it creates a threatening mechanism to the nodes to join the network. Shapley value is used in this method to fair payoff distribution inside the coalition. This method can be integrated with any routing protocol for wireless network. In [132], a game theoretic frame work is proposed to analyze regular as well as malicious nodes. Individual strategy of nodes in terms of cost and gain are generated based on Bayesian signaling game. Regular nodes update their belief based on the behavior of opponent while malicious nodes evaluate their risk of being caught. A Game-Theoretic Adaptive Multipath Routing (GTAMR) protocol is proposed in [134] to detect and punish malicious node as well as selfish node that drops packets. In this scheme, more than one node coordinates their misbehavior and can be used in the network in which wireless network use directional antennas. ERTFT, a game theoretic strategy, allows the nodes to promote their cooperation for detection. Security and QoS, both are considered together in Service Level Specification (SLSs) in [24]. A game theoretic approach is proposed to make the system in such a way that a service level agreement (SLA) can be established with user to establish security and QoS parameters for the user.

2.3.3 Desirable Properties of Detection Methodology

Desirable properties of any PDA detection methodology can be summarized as below,

1. Implementation of PDA detection methodology should not create another weakness in the MANETs.

2. The methodology should be an autonomous system and it must be transparent to the system as well as to the users.
3. It must use very less system resources to perform its goal; otherwise system overhead will be high. So, excessive communication amongst the nodes or run complex algorithm is not desirable.
4. It must be fault-tolerant so that it is able to recover itself automatically during system crashes. It should not loss any of its previous information and should work from that point onward. It must be same with its objective during life time of its work [135].
5. Apart from normal detection and isolation of malicious nodes, the system should save itself from intruder so that it should not compromise with intruder and take part in malicious activities in the network.
6. The system must generate very less false positive and false negative rate so that its accuracy remains high.
7. Implementation of such system should not degrade network performance in terms of some parameters such as throughput, packet delivery ratio etc.
8. It should interoperate with other existing systems to collaboratively detect intrusions.
9. It should isolate the malicious nodes from the system

2.4 Game Theoretic Approach

2.4.1 Introduction

Game theory can be identified as mathematical model of conflict and co-operation amongst intelligent rational decision makers [140]. Though game theory is basically a part of mathematics and it is used vastly in economics, it can also be used in other field of application. It is an interactive decision situation which is represented by mathematical model. Game theory can be modeled to MANETs nodes which are autonomous but interdependent of rational decision makers.

The work can be represented either as non-cooperative security game between attacker and detector or as model of cooperation amongst the various nodes that are involved in detecting malicious activities in MANETs. These models of cooperation can be classified as credit based model and trust model. Credit based model is based on economic incentive while trust based model is based on reputation [157]. The concept can also be explained by the fact that to encourage the nodes, two basic mechanisms are followed. One is reputation based mechanism and other is price-based mechanism. In reputation based mechanism, any node keeps a record of its neighbour's reputation. The more cooperative a node is the better reputation it gains. In price-based mechanisms, the loss that a cooperative node makes is compensated by some kind of virtual money. The price of relaying a packet may be different for each node. Therefore, an effective price-based mechanism should be supplemented by a technique which determines these prices accurately

Non cooperative game theory can be applied to forward decision by autonomous nodes, they also involve with cooperation aware routing [158]. A non cooperative game may contain the elements such as number of players, objective function of each player for which it tries to optimize utilities, preference, utility, actions, strategies etc [138].

Normally a game may contain the following Components:

- players
- actions
- strategies
- information
- outcomes
- payoffs
- Equilibrium concept

Goals of players are articulated by utility functions and utility is defined over outcomes. Actions and strategies can be defined as follows:

- Any plan or steps for performing some actions are known as strategy.

- In some cases, actions and strategies are taken as equivalent.
- But in some cases both actions and strategies are granted differently. In such cases strategies are recognized as primary choice of actions.
- The payoff for each player depends on the combined actions of all players.

Characteristics of game theory

Strategic game consists of three main basic components

A set players ($N = \{1, 2, \dots, n\}$) where $N \geq 2$

A set of actions for each player ()

Utility function for each player ()

2.4.2 Game Theoretic Approach to PDA Detection in MANETs

It can be considered as cooperative or coalition game because it considers the cooperative actions of number of players and then analyze the results accordingly. It is also a kind of strategic game, as all the players have the idea about their strategies; they make the outcome of the game based on their decision. Solution of a strategic game is either Nash equilibrium or stability. It is the point from which no other players want to deviate unilaterally.

Due to the De-centralized nature of nodes, they can independently adapting its operation based on perceived or measured statistics. Similarly, due to interactive decision makers of the nodes, decision taken by one node affects and influences the other nodes.

MANETs is very much vulnerable to attack due to decentralized nature of nodes, open topology and dependency of each node on others for packet forwarding etc. Hence to detect vulnerabilities, either we may follow centralized detection methodology or distributed detection methodology. But from several performance evaluation processes, it is observed that distributed detection methodology is found better. Game theory can be used to study the different decision made by the players (i.e. network nodes) in a distributed way to reach the goal.

MANETs components can be set as equivalent game components as follows:

Player Set: Player sets in MANETs implies different nodes that participated in communication in the network including attacker and genuine node.

Action set: Nodes may act as,

- a. Source i.e. sender
- b. Destination i.e. receiver
- c. Forwarder
- d. Packet dropper
- e. Malicious packet dropper detector etc.

Utility function

- a. Utility function is a kind of function which can be implemented to network to determine the network status at a time whether it is dominated by genuine nodes or attacker.
- b. Based on node's performance, incentives can be paid in terms of trust , ; it can be categorized under "Credit exchange", "Optimal equilibrium inducing mechanisms" of game theory.
- c. To win game by genuine node, utility function's value must be increased.

A game with complete information implies that each player knows the facts about the game such as set of players, strategies and utility functions. Of course set of complete information always doesn't mean that these are complete information.

2.4.3 Equilibrium Concept

The concept of equilibrium in game theoretic approach can be understood by the fact that no players that participate in the game is able to earn any other extra benefit by changing their strategies. So, it is a state in which opposing forces or influences are balanced. Equilibrium selection implies identification of desired Nash equilibrium [159] or stability achieved by the system.

2.4.4 Nash Equilibrium

NASH EQUILIBRIUM is an important concept in game theory, It occurs when each

Chapter 3

Centralized PDA Detection

3.1 Introduction

In this Chapter, a centralized PDA detection methodology has been proposed. Architecture is presented. Performance of this methodology has been compared with AODV protocol using random way point mobility model. Proposed methodology is also compared with OCEAN [173] using Levy walk mobility model.

In Centralized PDA detection methodology, nodes in the network provide their gathered information to a central entity in the network. The central entity analyzes the information received from the nodes individually in order to detect the PDA at a particular node. Data ship to a central location for analysis. It is a static offline system. It performs statistical detection methodology. It scrutinizes data from a single host. A centralized detection methodology is not scalable, because under heavy network load, the system suffers from the inefficient capacity of central analyzer [143]. Centralized PDA detection methodology is able to detect malicious node from centrally collected data. It needs relatively small numbers of components to keep running.

It has some disadvantages. As state of malicious node detection is centrally stored, if any of the component under the system does not work then the whole system will collapse. Minor change in the network needs the whole system to run once again. Size of centralized PDA detection methodology is limited to fixed number of components.

3.2 The Architecture

3.2.1 Assumptions

In the system model, low rates of packet loss or any other packets drop other than malicious packet drop are assumed as *threshold* packet drop. When packet drop is more than the threshold packet drop than PDA is suspected. PDA is confirmed in certain node based on some network performance parameters such as packet delivery ratio as well as throughput of the network. It is assumed that packets are forwarded in a hop-by-hop fashion in on demand ad hoc way. The communication links are assumed to be bi-directional and there is no wireless channel error. All nodes use Omni-directional antennas for bidirectional communications. Neighbor discovery protocol is assumed to work in such a way that every node can understand its neighbors.

It is assumed that all the nodes in MANETs have the capability to understand packet drop in them. Thus it has the ability to understand the threshold packet drop as well as malicious packet drop. Promiscuous mode of node is enabled with source routing. A malicious node can drop packets continuously or selectively. Here collusion of more than one node is not considered so that malicious node can monitor each other and collude and mask the misbehavior of each other.

3.2.2 System Model

It is assumed that in addition to regular nodes, MANETs also has the following different kind of nodes:

Malfunctioning node: These nodes are suffering from hardware failure or software errors.

Malicious node: These nodes are active nodes that utilizes their resources to participate in network communication in established routes of the nodes in such a way that they force the other nodes to adopt the malicious route for packet forwarding and

thereby drop the packets maliciously which are supposed to be forwarded. Such nodes are acquainted with regular routing information so that it can attract the packets towards it and drop the packets.

Selfish node: These nodes refuse to forward the packets to their next hop for delivering it to destination to save their resources. Thus packets are dropped in such kind of nodes. At the same time they are accepting the packets which are meant for them.

Misbehaving nodes drop packets intentionally to reduce network performance. A misbehaving node also drops packets to conserve its energy. Malicious node drops any packet that comes to it for forwarding to its neighbor. When packets are dropped beyond certain amount by the neighbor then an attack is suspected. Packet dropping is considered for RREQ, RREP and data packets. Of course, it does not consider the coalition formation of attackers for this network model,

Generally routing protocol performs two kinds of activities like routing function and data forwarding function. By data forwarding function it forwards packets to destination through established route. Routing and data forwarding function of routing protocol is affected when the activity of malicious node is going on. Trusted environment is expected by the routing protocol to work perfectly on routing and forwarding of packets. Presence of malicious nodes in the network, affects both the services of routing protocol.

The proposed system model is established as an informed, abstracted and traditional model of MANETs with deployment of attacker capabilities.

Router can be traffic faulty by maliciously dropping packets. After implementation of centralized PDA detection methodology, the network shows better performance by detecting and avoiding malicious nodes from the network. That is observed in different simulation environments and results are shown in the later part of this chapter.

Packets may be dropped in the network due to any other reasons such as collision, link failure etc. apart from malicious packet drop. Any other packet drop in the network, excluding malicious packet drop, are represented by *threshold* packet drop. In MANETs, all the nodes are connected via wireless link. It consists of different types of nodes as mentioned earlier. After implementation of centralized PDA detection methodology, malicious nodes are detected and isolated from the network. Thereby, it improves the network performance.

3.2.3 Proposed Methodology

Proposed centralized PDA detection methodology consists of the following modules,

1. Data Collection module
2. Data Classifier
3. Data Comparator
4. PDA Recognition
5. PDA intimation
6. Communicator

Schematic diagram of the proposed methodology is depicted in Figure 3.1

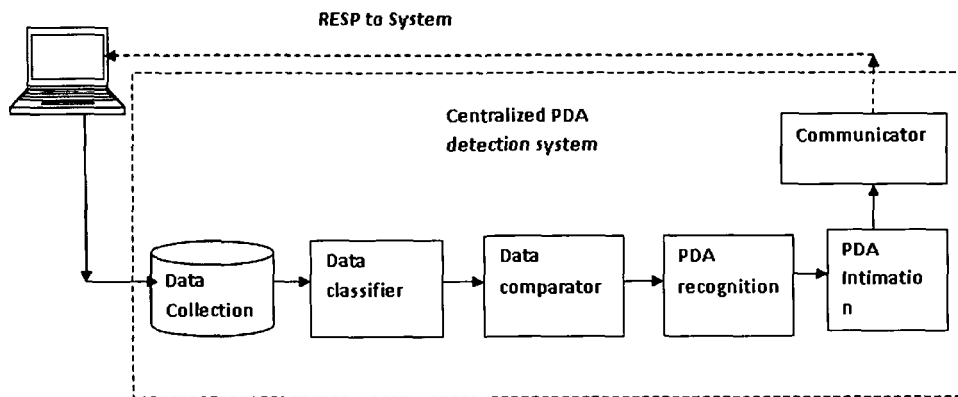


Figure 3.1. Schematic diagram of proposed centralized packet dropping attack detection methodology

(1) Data Collection: It is like a data gathering centre in which network data are collected centrally for PDA detection. It analyses the network traffic and local activities including user and system activities with other associated nodes. It collects

the various traffic patterns from the collected data. Collected data must include all relevant information including types of traffic, end-to-end delay, packet sequence number, TTL value of packets, packet size etc. If the packet dropping attack persists in the network, the node may have to put some extra effort to get back the lost packets. It also keeps track of network as well as node resources such as bandwidth, computational cost etc. If it consumes much bandwidth or more energy then there is a chance of having packet dropping attack. But this module doesn't determine that packet drop happened in the network is really an attack or it is because of other causes including network congestion or hardware/software fault or protocol fault etc. It simply gathers all relevant data.

(2) **Data Classifier:** Collected data consists of network traffic details including routing updates and packet headers. This module classifies the data according to variation of behavior during communication. Packets are segregated according to packet type such as sent packets, received packets and dropped packets with respect to nodes. Then it calculates total number of packets sent, received and dropped at different nodes. From this, it identifies total number of packets that is dropped in the RTR level of nodes in the network.

(3) **Data Comparator:** This module involves in determination of threshold value for packet drop d_{th} . There may be several reasons of packet drop in MANETs. Out of these all, congestion is identified as major cause of packet drop in MANETs. However, wireless characteristics such as interference of radio signal, radio channel contention and low bandwidth can lead wireless link unreliable. Link failure mostly occurs when mobile node which forms a route launches to move out of its neighborhood's transmission range. In addition, battery depletion can make link breakage. Hence, in addition to congestion, link failure and wireless channel error have significant contribution in generating loss in MANETs. Such kind of packet loss in the network are identified as threshold packet loss i.e. d_{th} . Setting of a threshold value for packet loss in the network is very crucial.

This module compares dropped packets d_r with threshold packet drop d_{th} . If d_r is more than d_{th} for any node then the node is kept in suspected malicious node list.

(4) PDA Recognition: Excessive packet drop in the network may not be the concrete reason for identifying the malicious packet drop. The previous module compares packet drop in the network d_r with threshold packet drop for identifying malicious packet drop in the network. It can be justified more precisely once it evaluates the following,

- a. Network performance in terms of packet drop ratio (PDR) and throughput (T).
- b. If it finds that PDR is very high and throughput is very low then it confirms the suspected malicious packet dropping as packet dropping attack.

(5) PDA Intimation: Based on the results generated by the module *PDA Recognition*, it confirms the suspected malicious node as malicious node.

(6) Communicator: This module broadcasts alarm in the network to notify other nodes in the network about the malicious node so that it can be avoided by the other nodes while forwarding or sending their data. Broadcast notification about malicious node is restricted to few hop away from the node for which anomaly has been detected as the most promising node that may involve in intrusion may lie in neighbor circle or few hops away from neighbor.

Algorithm 3.1 Algorithm for Centralized PDA detection methodology

Input: Packet details of N , T_{th} , D_{th} { $*$ N is the number of nodes, T_{th} is the minimum throughput and D_{th} is the threshold packet drop for a network, $*$ }

Output: *malicious_node_ID*, *ALARM* message

1. Data Classification: **for all** (i in N) **do**
2. Find TS_i , TR_i , TD_i
 { $*$ TS_i is the total number of packet sent from i , TR_i is the total number of packet received at i , TD_i is the total number of packet dropped in i $*$ }
3. **end for**
4. Data Comparator: **for all** (i in N) **do**
5. **if** ($TD_i > D_{th}$) **then**
6. PDA is suspected for i { $*$ PDA is the packet dropping attack $*$ }

7. Update N_s { * N_s is the data structure to maintain suspected malicious node list * }
8. **end if**
9. **end for**
10. PDA recognition: **for all** (i in N_s) **do**
11. $PDR_i := \frac{\sum \text{No.of packets sent}}{\sum \text{No.of packets receive}}$ { * PDR_i is the packet drop ratio for a node i * }
12. $T_i := \frac{y}{t}$ { * T_i is the Throughput and y is the numbers of packets delivered within t times for a node i * }
13. **if** ($(PDR_i > PDR_{th})$ AND $(T_i < T_{th})$) **then** { * PDR_{th} is the threshold packet drop ratio for a node i * }
14. Update N_{PDA} { * N_{PDA} is the data structure to keep malicious node that involved in PDA * }
15. **End if**
16. **End for**
17. PDA intimation and communicator: **for all** (i in N_{PDA}) **do**
18. PDA is confirmed for node i
19. Generate $ALARM_i$ { * $ALARM_i$ is the broadcast message containing details of malicious node i to avoid the node for further communication * }
20. **End for**

3.2.4 Performance Parameters

Detection rate: Detection rate of the proposed methodology can be determined by the following formulae,

$$\text{Detection rate} = \frac{\text{Number of true positive}}{\text{Number of true positive} + \text{number of false negatives}}$$

False positive rate: It is measured as percentage of the ratio of total number of genuine nodes but detected as malicious nodes to Total number of genuine nodes.

$$\text{FPR} = \frac{\text{Total number of genuine nodes but detected as malicious nodes}}{\text{Total number of genuine nodes}} \times 100$$

Throughput of the network: It can be calculated by number of packets delivered per unit time slot.

$$\text{Throughput} = \frac{\text{Total number of delivered data packets}}{\text{Total simulation time}}$$

Packet Delivery Ratio (PDR): It is determined as the ratio between the numbers of packets received by the destination to the number packets generated by the application that are sent from the source to destination.

$$\text{Packet Delivery Ratio} = \frac{\text{number of packet received at the destination}}{\text{Number of packet sent from source}}$$

Normalized Routing Load (NRL): It measures the number of routing packets transmitted per data packet delivered. It signifies the importance of efficiency of routing protocol.

$$\text{NRL} = \frac{\text{Total number of routing packets}}{\text{Total number of delivered packets}}$$

End-to-end Delay: It is the time difference for a packet to reach from source to destination. It includes all type of delays in all the intermediate hop due to any reason through which packet should pass. It is normally affected by different types of calculation or security measures done by intermediate hop from source to destination, route discovery latency, queuing at interface queue, retransmission delay etc.

Round Trip Time: It is the amount of time that is required to get back the acknowledgement from destination to the source after sending the packet from the source node. When an acknowledgement received by the sender exceeds the RTT time limit, then the data packet is accounted as a lost packet.

3.3 Performance Evaluation

Network simulator NS 2 is used for simulation purpose to evaluate the performance of proposed centralized PDA detection methodology. Initially proposed methodology is compared with AODV protocol using random way point mobility model. As random way point mobility model is simple enough, hence to get more realistic results, proposed methodology is compared with OCEAN [173] using levy walk mobility model.

3.3.1 Centralized PDA Detection vs. AODV ((RWP)

Simulation Environment

Table 3.1: Simulation Environment (RWP Model)

Animation area	1000m X 1000m
Mobility model	Random way point (RWP)
Channel type	Wireless
No. of nodes	100
Simulation time	600 sec
Pause time	10-70 sec
Node Speed	10-70 m/s
Data rate	100 kbps
Transmission range	100 m
Packet size	512 byte
Traffic type	CBR
Routing protocol	AODV

Simulation Results

Simulations are performed with following criteria:

- a. When percentage of malicious node is increasing, we keep node speed and pause time as constant/fixed
- b. When node speed is increasing, we keep malicious node percentage and pause time as constant/fixed
- c. When pause time is varying, we keep node speed and percentage of malicious node as constant/fixed

3.3.1.1 Detection Rate

In Figure 3.2, it is observed that when number of malicious node is increasing, detection rate is gradually decreasing. Since, it is a static offline system and due to lack of scalability to detect malicious node dynamically, its performance degrades. Any time, any node that has been identified as malicious node, may quit from the network, on the other hand new nodes may enter to the network and work as malicious or malicious node may not drop packet at the time of analysis but later it

shows its malicious activity. As the state of PDA detection is centrally stored, hence it is difficult to monitor the ongoing system state that leads to degradation of detection rate.

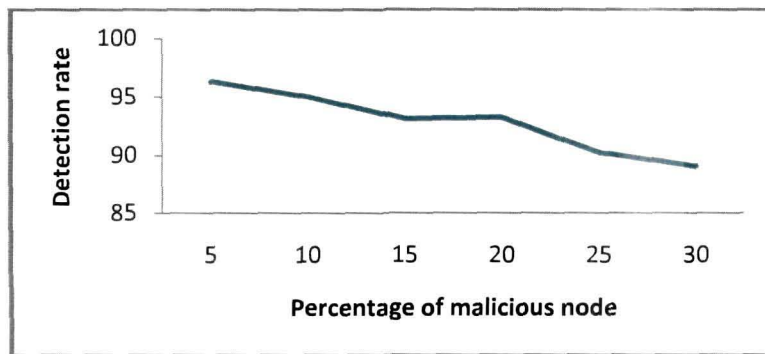


Figure 3.2 Effect of increase of malicious node on detection rate (RWP model)

In Figure 3.3, detection rate of the algorithm decreases with increased node mobility. In high node mobility, these are in transit state, they lose connectivity frequently. Probability for a path break is more and services tend to be available for a shorter period. Due to non linked path, packets are dropped frequently. Some packets will be lost due to collision resultant from high mobility. Static nature of detection methodology does not help to handle the packet dropping attack dynamically, that leads to high false negative rate and ultimately it decreases the detection rate of the algorithm.

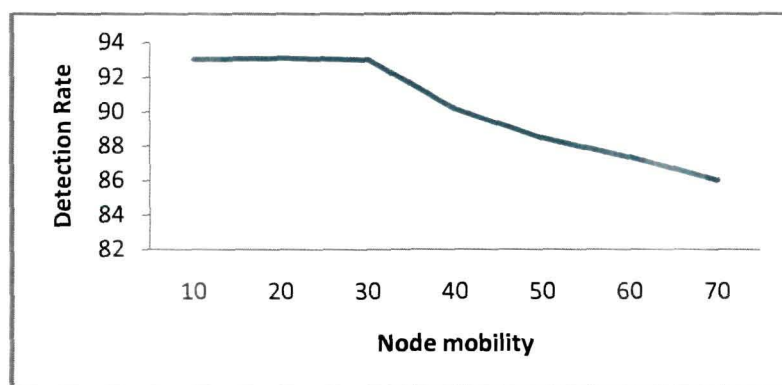


Figure 3.3 Effect of node mobility in detection rate (RWP model)

In Figure 3.4, it is observed that detection rate is increasing with increased pause time, as high pause time implies more stable network that leads to long lived service and stable network. Though it is a static offline system, still it shows better performance in a stable network.

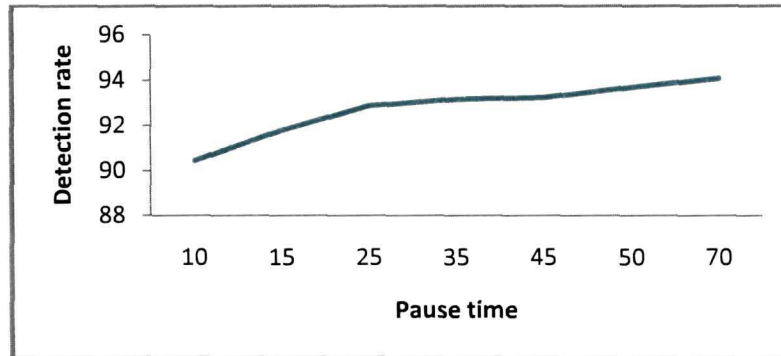


Figure 3.4 Effect of pause time in detection rate (RWP model)

3.3.1.2 *False Positive Rate*

In Figure 3.5, it is observed that as the number of malicious node is increasing, it shows a mixed response. Due to static property of detection methodology, initially when the number of malicious nodes increases in the network, the algorithm is unable to handle the malicious node as they may be out of range or new node enters to the network which may work as malicious. All the time malicious nodes may not show their malicious activities. So, static detection methodology shows mixed response.

In Figure 3.6, False positive rate increases with increase number of node mobility. Higher node mobility is the significance of higher failure of connectivity and frequent change of topology, so packets from source to destination are not able to deliver, so it will apparently drop the packet. Even the packets are dropped because of collision. So nodes may be falsely accused of packet drop attack, thus it will increase the false positive rate. In low node mobility, routing table will have less dynamic changes, so it will be easier to characterize the node activities to detect malicious packet drop attack, which results in low false positive rate.

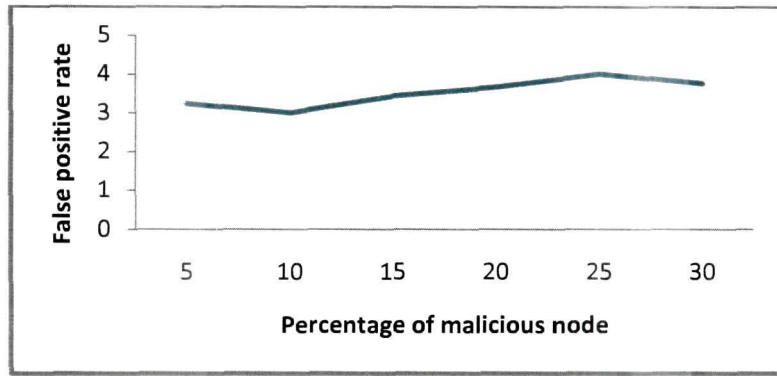


Figure 3.5 Effect of increase number of malicious node in false positive alarm (RWP model)

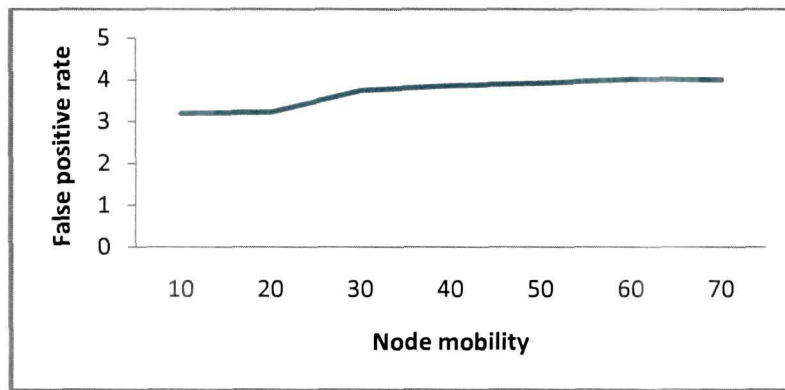


Figure 3.6. Effect of node mobility in false positive alarm (RWP model)

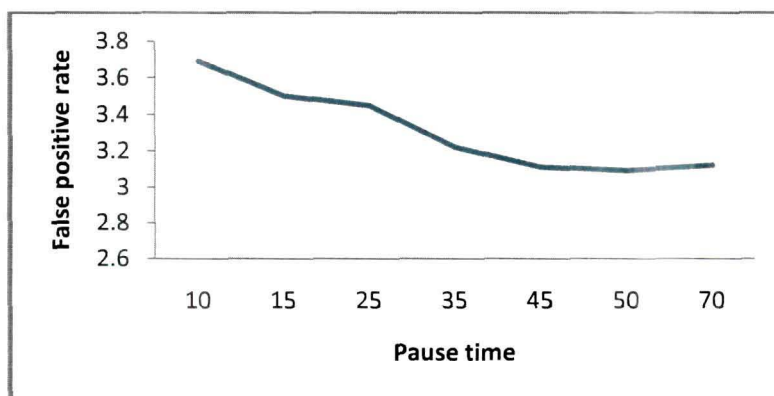


Figure 3.7 Effect of pause time in false positive alarm (RWP model)

But Figure 3.7 shows that high pause time implies low false positive rate. This can be explained by the fact that centralized detection process is very much sensitive to the collected data. Small changes to the network may cause an abrupt decision to the process as it is not a dynamic process. Since high pause time gives more stability to the network and less changes over the routing table, so detection process works more accurately. As a result, false decoration of node as malicious will be less. Thus false positive rate will be less.

3.3.1.3 *Throughput Analysis*

In Figure 3.8, when the percentage of malicious node is increasing, throughput in the network is gradually decreasing for AODV. Since throughput of the network depends on number of delivered packets and malicious nodes intentionally drop the packets instead of forwarding the packets to destination, so increase number of malicious nodes in the network will deliberately decrease the throughput of the network. But the presence of centralized packet drop attack detection methodology shows better performance than AODV.

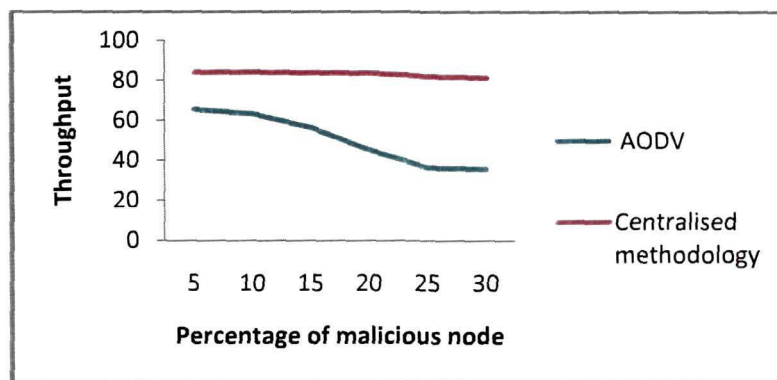


Figure 3.8 Effect of increase number of malicious node in throughput (RWP model)

In Figure 3.9, it is observed that as node mobility is increasing with fixed number of malicious node, throughput is degrading gradually in AODV. It is because of the fact that due to high node mobility, node will lose the connection repeatedly and reinitiate

the route between source and destination. As a result some packets are also dropped in addition to packet drop due to malicious nodes. Graph for Centralized PDA detection methodology is found better in comparison to AODV but its value is degrading as node mobility is increasing. Centralized PDA detection methodology can control PDA partially, but packet loss due to mobility will be still there. More over due to centralized static behavior, some nodes may be falsely accused of malicious or some non malicious node may also behave as malicious which again causes packet drop in the network.

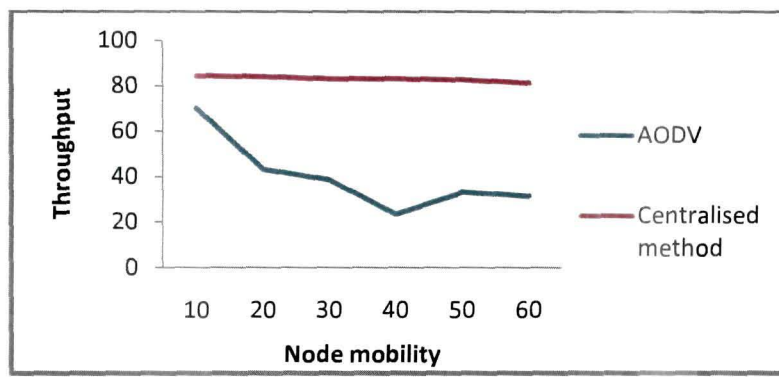


Figure 3.9 Effect of node mobility in throughput (RWP model)

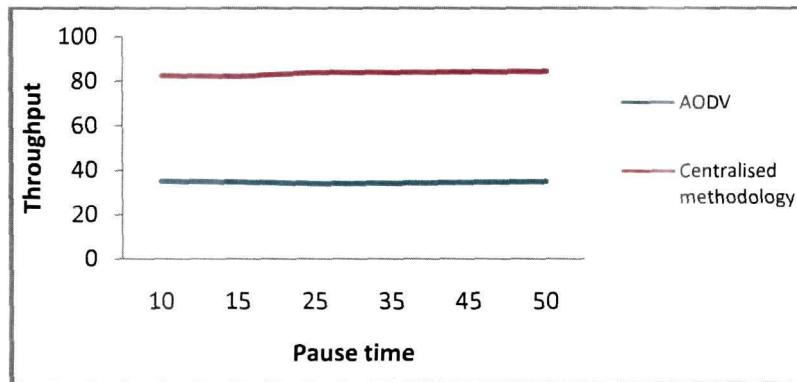


Figure 3.10 Effect of pause time in throughput (RWP model)

In Figure 3.10, there is a big difference of throughput between AODV and centralized PDA detection methodology. Both the graphs are stable. It reflects the fact that as pause time is increasing, network becomes more stable, and nodes are behaving

regularly. Change in routing table information will be less. Network topology is not changing frequently. So, once some packets are dropped because of some malicious node, it will be almost constant, hence it will reflect a constant throughput in AODV. Application of centralized PDA detection methodology gives an extra impact to the network for controlling PDA in comparatively stable network.

3.3.1.4 Packet Delivery Ratio Analysis

In Figure 3.11, in AODV, PDR is decreasing with increased number of malicious nodes as malicious nodes were invariably dropping the packets or not forwarding the packets. Moreover, AODV is not capable of resisting the malicious packet drop in the network. Once the centralized PDA detection methodology is applied to the network, it will identify the malicious node and avoid those nodes from the network for packet forwarding; automatically PDR will be increased compared to AODV. But when the percentage of malicious nodes is increasing then PDR is falling down in centralized method due its non scalability and non capability to detect malicious node dynamically. Due to dynamic nature of MANETs, nodes may change their status, they may quit from the range, then they again come to the range with different IP, centralized PDA detection methodology is unable to handle new status of routing table as well as node characteristics.

In Figure 3.12, PDR is gradually decreasing with increased node mobility in AODV while the centralized PDA detection methodology is able to maintain better PDR in comparison to AODV but still it is decreasing with increase node mobility. When node mobility is increasing, path breakage from source to destination will be more, thus change of routing information will be high. Nodes change their status frequently. Collision of packets will be high. As a result, some extra packets will be dropped in addition to malicious packet drop. Similarly, in case of centralized method, it is not able to handle the packet delivery during high mobility for the frequent change of routing information in the network as it performs PDA detection statically.

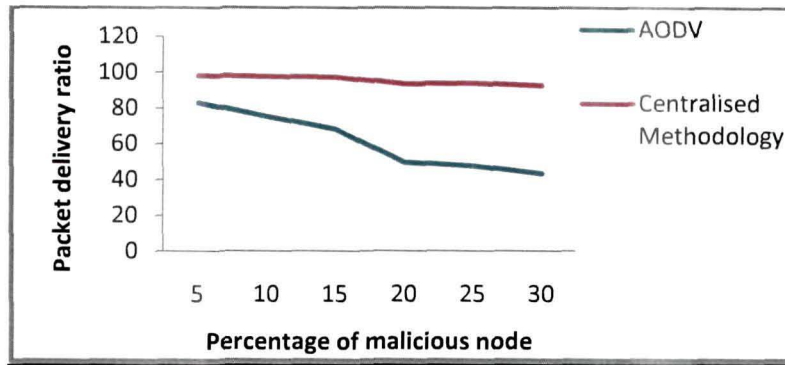


Figure 3.11 Effect of increase number of malicious node in PDR (RWP model)

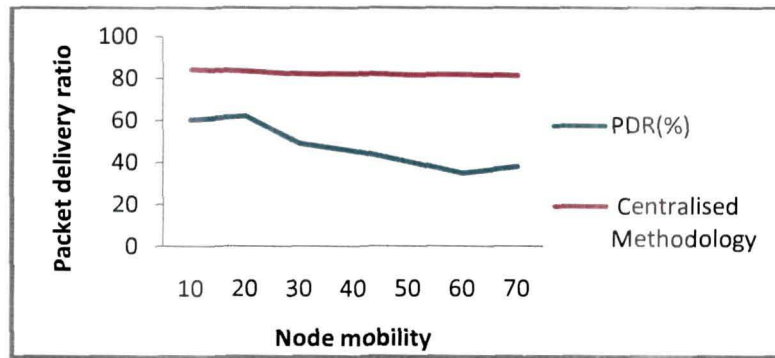


Figure 3.12 Effect of node mobility in PDR (RWP model)

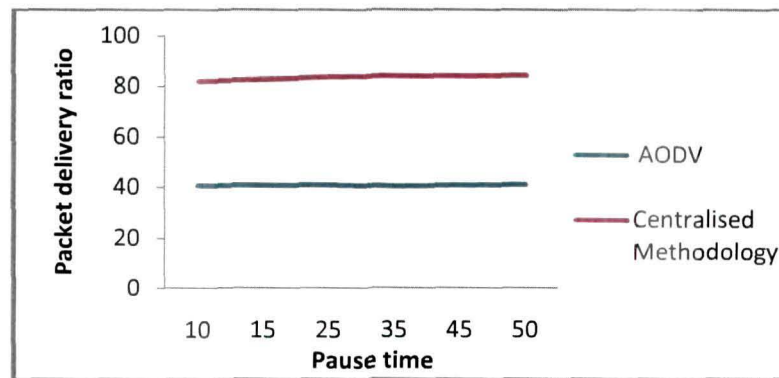


Figure 3.13 Effect of pause time in PDR (RWP model)

In Figure 3.13, when pause time is varying, both AODV and proposed methodology

maintain almost a constant ratio but there is a difference between both AODV and proposed methodology. PDR is far better than that of AODV as AODV is not able control PDA by itself. Increase of pause time gives more stability to the network. Nodes are not exposed to frequent change of status, thus routing table information are almost regular. So, centralized PDA detection methodology is able to show better performance.

3.3.1.5 Normalized Routing Load (NRL) Analysis

In Figure 3.14, it is clear that with increased number of malicious nodes in the network, NRL is gradually increasing in case of AODV. Since NRL is the ratio between total numbers of routing packets to total numbers of delivered packets, therefore when the network contains more malicious nodes, it will drop more packets, Further, due to its inability to deliver packets to destination, it will generate more routing packets. Therefore, NRL will be gradually increasing. In case of proposed methodology, it controls and avoids malicious nodes. Hence, NRL is comparatively low though it is increasing initially, but after a while it maintains a constant level.

As shown in Figure 3.15, when there is a constant number of malicious nodes (i.e. 20% of total nodes) with variable node mobility then also performance is found to be better in case of proposed methodology. But in both cases it is observed that NRL is gradually increasing with increased node speed. Due to high node mobility, packets will be deliberately dropped as it breaks the linkage between source and destination frequently. This will be an add-on to total packet drop due to malicious nodes. Since the centralized PDA detection methodology tries to minimize malicious packet drops, so NRL is comparatively low for the system.

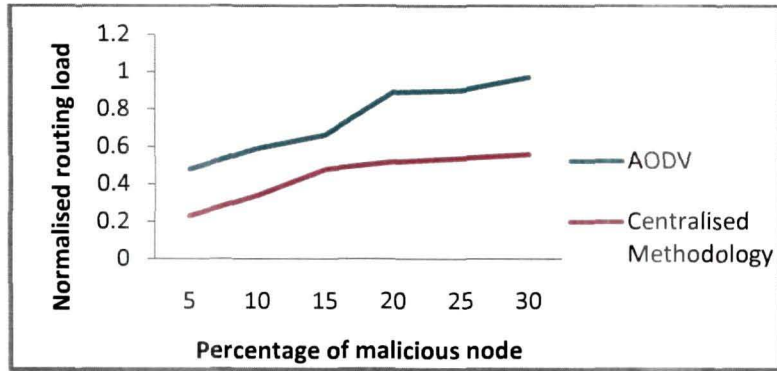


Figure 3.14 Effect of increase number of malicious node in NRL (RWP model)

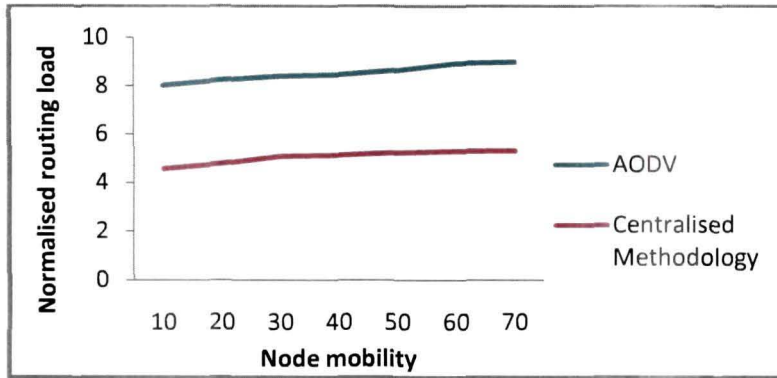


Figure 3.15 Effect of node mobility in NRL (RWP model)

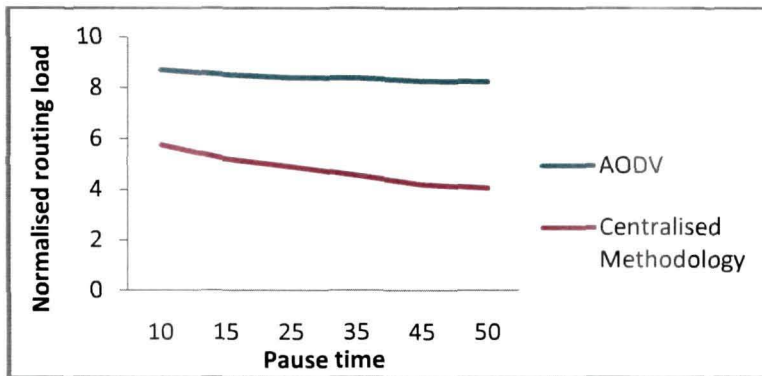


Figure 3.16 Effect of pause time in NRL (RWP model)

In Figure 3.16, with increased pause time in the network, NRL is decreasing for both AODV and proposed centralized PDA detection methodology. This is because of the

network stability which indicates regular and stable behavior of nodes. Therefore additional packet drop due to highly dynamic node will be reduced. It also helps the centralized method to reduce malicious packet drop by identifying the malicious nodes.

3.3.1.6 End-to-end Delay Analysis

In Figure 3.17, it is observed that though there is a difference between AODV and proposed methodology in terms of end-to-end delay, but still for both cases end-to-end delay is increasing with increased number of malicious node. In MANET, end-to-end delay is the delay encountered by a packet right from sending the packets from source up to the time that it receives ACK from destination. The packet delay consists of the queuing delay experienced at the source node, the queuing delays incurred at the intermediate nodes as well as MAC delay observed at the source and intermediate nodes. Presence of malicious node in AODV will invariably drop packets due to which sender will have to wait for long time to get ACK packets from the receiver. As the number of malicious nodes increase, end-to-end delay will also increase in the network. In presence of centralized PDA detection methodology, end-to-end delay is lower. But the static centralized PDA detection method is not able to handle the end-to-end delay in the network entirely.

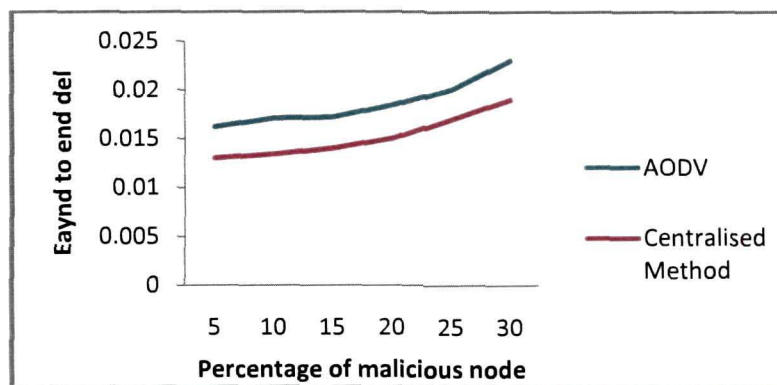


Figure 3.17 Effect of increase number of malicious node in End-to-End delay (RWP model)

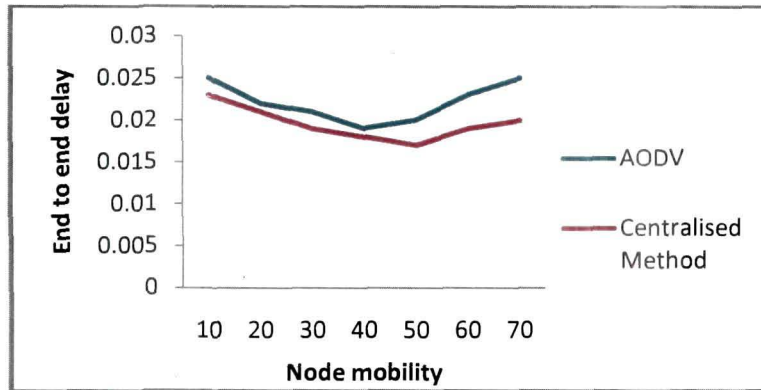


Figure 3.18 Effect of node mobility in End-to-End delay (RWP model)

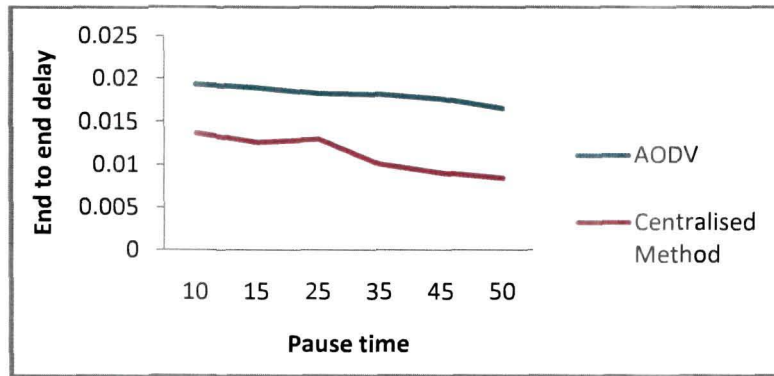


Figure 3.19 Effect of pause time in End-to-End delay (RWP model)

In Figure 3.18, as node speed is increasing, end-to-end delay is decreasing. It is because of active route timeout. A breakage link is not detected until the connection to a node along the route expires. So, AODV will try to send traffic to a node for the duration of the active route timeout irrespective of the node non-reach ability. Of course due to existence of malicious node in the network, end-to-end delay will be suppressed over the normal end-to-end delay. On the other hand, in case of high node mobility, with constant number of malicious node, centralized PDA detection process initially decreases the end-to-end delay, but after some time it starts increasing it. This is because of the fact that though the centralized process statically identifies the malicious nodes, and then tries to regularize the performance, but due to dynamic

nature of MANET, state and characteristics of nodes may change, even in high mobility, nodes can change their characteristic frequently. Thus packets from source to destination may not reach on time or end-to-end delay may increase.

In Figure 3.19, when the pause time is more, due to network stability, in both the cases end-to-end delay is gradually decreasing.

3.3.1.7 Round Trip Time (RTT) Analysis

From the Figure 3.20, it is clear that as the number of malicious node is increasing in the network, RTT is also gradually increasing for AODV due to increase number of malicious packet drop in the network as AODV itself is not able to control the same. In case of proposed methodology also it is observed that though it is comparatively low, still it is gradually increasing. The proposed methodology detects and avoids malicious nodes from the network, but static nature of detection is unable to control dynamic nature MANET. As a result, some new nodes may act as malicious node or existing malicious node may work actively that increases packet drop in the network.

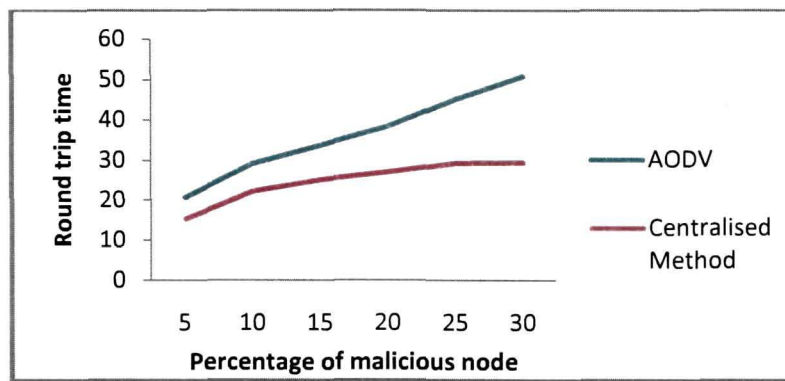


Figure 3.20 Effect of increase number of malicious node in RTT (RWP model)

Increase of node speed doesn't affect RTT much in proposed methodology. There is a difference between AODV and proposed methodology as shown in Figure 3.21. Since high mobility is the significance of more unstable network, frequent breakage of links; as the node speed increases, packet delivery time will also increase, thus it takes

much time to get ACK packet from destination to source after sending packet from source. Relatively low RTT in case of proposed methodology signifies the detection capability of the proposed methodology.

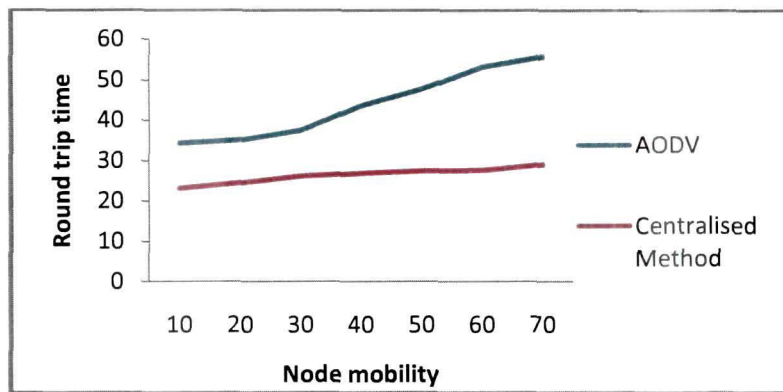


Figure 3.21 Effect of node mobility in RTT (RWP model)

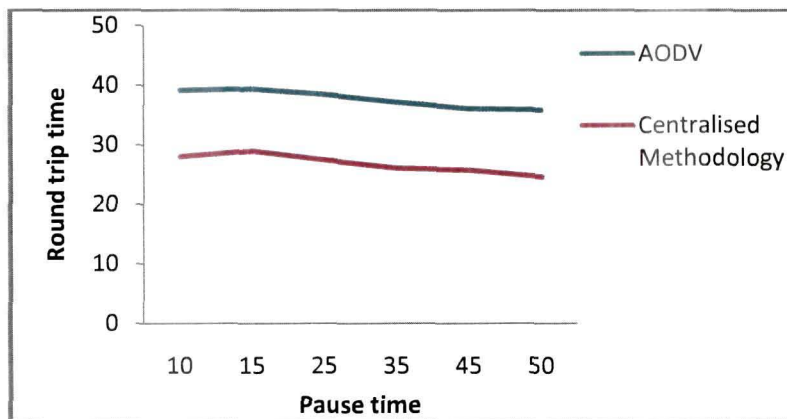


Figure 3.22 Effect of pause time in RTT (RWP model)

But in Figure 3.22, when pause time is increasing, for both the cases, RTT is gradually decreasing. Still due to the ability of detection and avoidance of malicious node, RTT is comparatively low in case of proposed methodology. When the pause time in the network is more, it indicates more stable network, thus node characteristics also remained constant. Hence the probability of frequent link breakage will be low. Packets deliver to destination on time, source gets ACK packets

on time, and hence RTT is getting low. In case of proposed methodology, it tries to control and avoid malicious nodes from the stable network, so it gives more impact on RTT.

3.3.2 Centralized PDA Detection Vs. OCEAN(LWM)

In the following section, the proposed centralized PDA detection methodology has been compared with an existing methodology namely OCEAN [173] using *Levy Walk* mobility model. Proposed methodology is a standalone PDA detection methodology. OCEAN is also a standalone system that considers two kind of routing misbehavior as mentioned below.

Firstly, node misleading, in which a node may respond positively to route request but failed to forward packets and it leads to PDA. Thereby, it handles malicious nodes that drops packets in MANETs. Secondly, selfish behavior, in which a node may not even respond to route requests but may nonetheless send its own traffic through the network, unfairly preserving its resources while exploiting others. Centralized PDA detection methodology is also designed to handle PDA in MANETs. Hence, proposed methodology is compared with OCEAN [173].

However, instead of taking random way point model, Levy walk mobility model has been considered. Random way point model is simplest mobility model of MANETs. Moreover, human walks are seldom similar with random way point mobility model. But human walks are statistically more similar with Levy walk mobility model. Hence to get more realistic results, Levy walk mobility model has been considered for comparison of proposed centralized PDA detection methodology with OCEAN.

Simulation Environment

Table 3.2: Simulation Environment (LWM)

Animation area	1000m X 1000m
Mobility model	Levy Walk Model(LWM)
Channel type	Wireless
No. of nodes	100
Simulation time	600 sec
Pause time	10-70 sec
Node Speed	1-3 m/s
Data rate	100 kbps
Transmission range	100 m
Packet size	512 byte
Traffic type	CBR
Routing protocol	AODV

Simulation Results

Simulations are performed with the following criteria:

- d. When the percentage of malicious node keeps on increasing, then the node speed and pause time are kept as constant
- e. When node speed keeps on increasing, then both the malicious node percentage and pause time are remained constant
- f. When the pause time is varying, then the node speed and percentage of malicious node are kept as constant

3.3.2.1 Detection Rate

In Figure 3.23, it is observed that as the number of malicious node is increasing, detection rate is gradually decreasing for both the methodologies namely OCEAN [173] and proposed centralized PDA detection methodology. Proposed methodology is a static offline system and due to lack of scalability to detect malicious node dynamically, its performance degrades as the percentage of malicious node increases. Similarly, in OCEAN also rate of detection decreases gradually as number of malicious node increases. OCEAN [doesn't provide any guaranteed service, second

chance mechanism of OCEAN may sometimes effect the detection mechanism. Being a trade based system, OCEAN may suffer from deadlock problem. It affects the detection methodology [173].

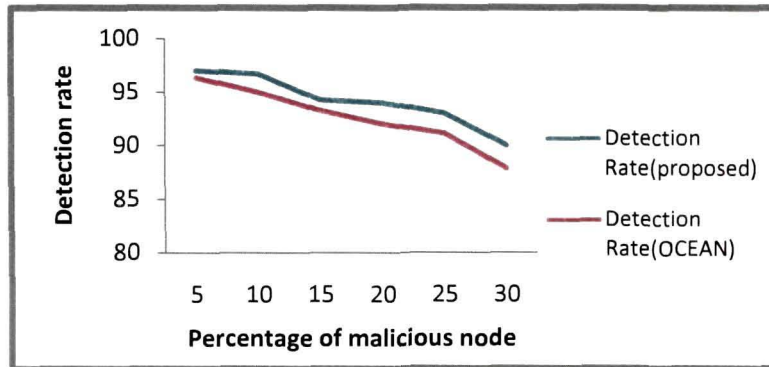


Figure 3.23 Effect of increase of malicious node on detection rate (LWM)

In Figure 3.25, it is observed that detection rate is increasing with increased pause time, as high pause time implies more stable network that leads to long lived service and stable network. Though it is a static offline system, still it shows better performance in a stable network.

As seen in Figure 3.24, detection rate of the proposed algorithm as well as OCEAN [173] is falling down as the node mobility is gradually increasing. In high node mobility, these are in transit state, they lose connectivity frequently. Probability for broken path is more and services tend to be available for a shorter period. Due to non linked path, packets are dropped frequently. Some packets are lost due to collision resultant from high mobility. Static nature of detection methodology does not help to handle the packet dropping attack dynamically, that leads to high false negative rate and ultimately it decreases the detection rate. OCEAN indeed relies on direct observation of interaction with neighbor to measure their performance [173]. But due to high mobility, it loses the track to keep direct observation. It finally affects the detection rate.

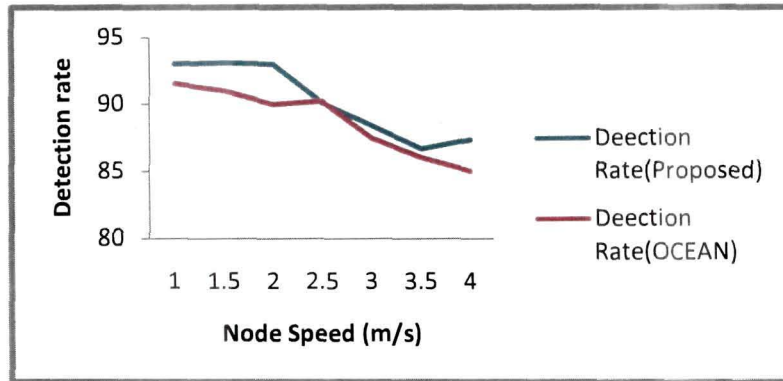


Figure 3.24 Effect of node mobility in detection rate (LWM)

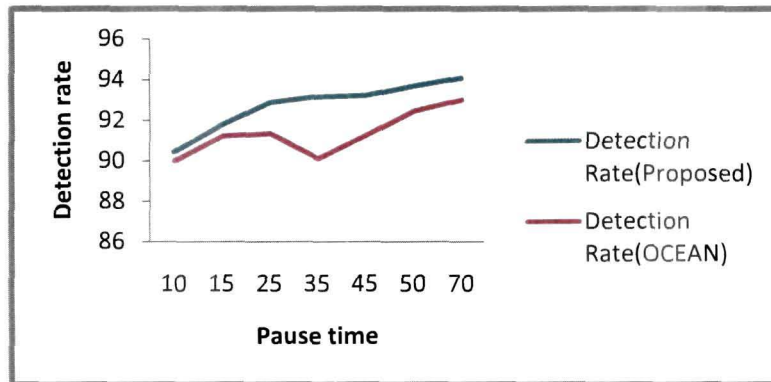


Figure 3.25 Effect of pause time in detection rate (LWM)

3.3.2.2 *False Positive Rate*

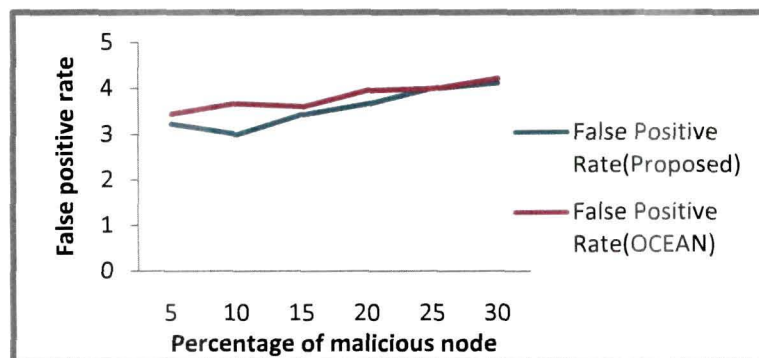


Figure 3.26 Effect of increase number of malicious node in false positive alarm (LWM)

In Figure 3.26, it is observed that as the number of malicious node is increasing, it gives a mixed response. Due to static nature of detection methodology, as the number of malicious node increases, initially false positive rate comes down but it again increases with increase number of malicious nodes. In case of OCEAN [173], it shows mixed result of false positive rate. But at a point when the number of malicious nodes is more, false positive rate of both the methodologies become almost same. Due to static nature of detection methodologies, OCEAN and the proposed centralized methodology show the mixed response. Still the performance of proposed methodology is better when the number of malicious nodes in the network is less.

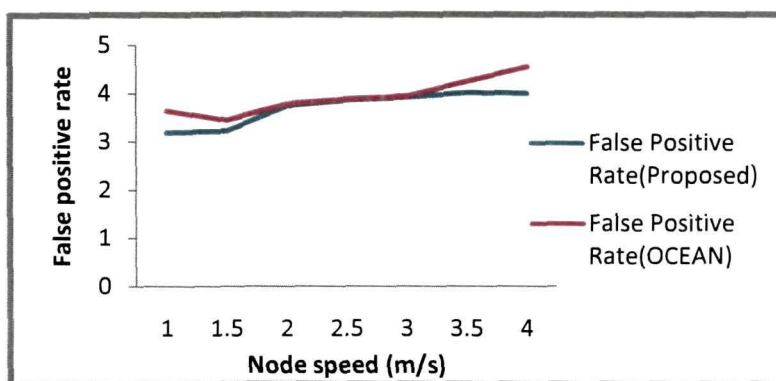


Figure 3.27. Effect of node mobility in false positive alarm (LWM)

In Figure 3.27, initially, false positive rate of the proposed methodology is increasing with increased node mobility. High node mobility doesn't affect the false positive rate much. it maintains a constant level of false positive rate. In case of OCEAN initially the false positive rate is increasing, then it becomes almost same as that of proposed methodology. But in high node mobility, again false positive rate of OCEAN is increasing [173]. Higher node mobility is the significance of higher failure of connectivity and frequent change of topology, so packets are not delivered to destination properly; it will apparently drop the packets. Packets are also dropped because of collision. So nodes may be falsely accused of packet dropping attack.

But in Figure 3.28, observation shows that high pause time implies low false positive rate for both the methodologies. This can be explained by the fact that centralized detection process is very much sensitive to the collected data. Small changes in the network may cause an abrupt decision to the process as it is not a dynamic process. Since high pause time gives more stability to the network and less changes over the routing table, so detection process works more accurately. As a result false accusation of node as malicious will be less. Thus false positive rate will be less.

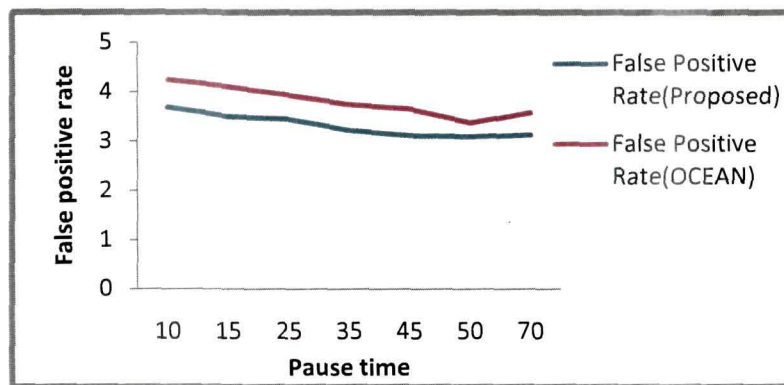


Figure 3.28 Effect of pause time in false positive alarm (LWM)

3.3.2.3 Throughput Analysis

In Figure 3.29, when the percentage of malicious node is increasing, throughput of both the methodologies is decreasing gradually due to static offline nature of detection of packet drop attack. Throughput of the network depends on number of delivered packets in certain time. Malicious nodes intentionally drop the packets instead of forwarding the packets to destination, so increased number of malicious nodes in the network will deliberately decrease the throughput of the network. The performance of proposed methodology is better in comparison to OCEAN [173] because *chippoint* scheme to detect malicious node in OCEAN decreases network throughput.

In Figure 3.30, it is observed that as the node mobility is increasing, throughput is degrading gradually in both proposed methodology and OCEAN. Due to high node

mobility, nodes lose the connection repeatedly and reinitiate the route between source and destination. As a result some packets are also dropped in addition to malicious packet drop. Performance of Centralized PDA detection methodology is found better in high node mobility. Moreover, malicious traffic rejection policy of OCEAN effects the throughput of the system [173].

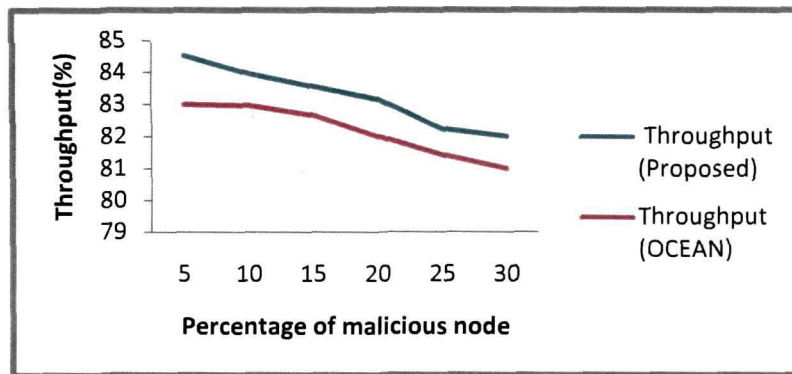


Figure 3.29 Effect of increase number of malicious node in throughput (LWM)

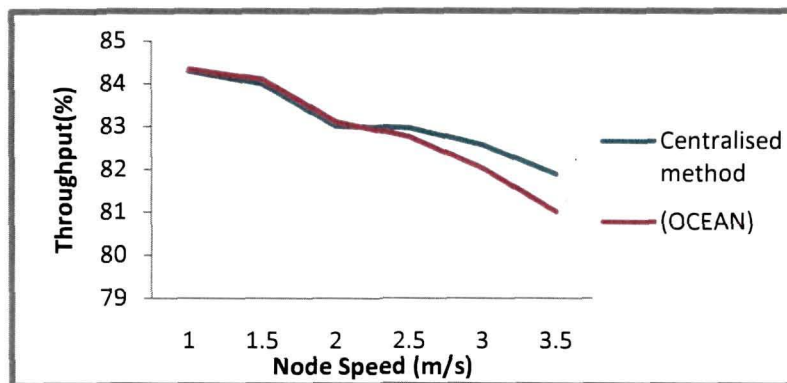


Figure 3.30 Effect of node mobility in throughput (LWM)

. In Figure 3.31, there is a difference of throughput between proposed methodology and OCEAN [173]. As the pause time is increasing, throughput of the network is also increasing. It reflects that high pause time results more stable network, thus nodes behavior become more regular. Change in routing table information will also be less. Network topology is not changing frequently. Performance of centralized PDA

detection methodology is better due to its simplicity in detecting PDA. But in OCEAN due to its complexity in detection of malicious nodes, throughput of the network is less in comparison to proposed methodology

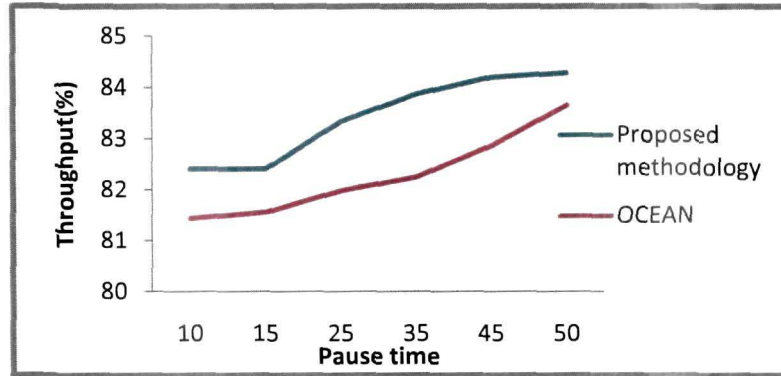


Figure 3.31 Effect of pause time in throughput (LWM)

3.3.2.4 Packet Delivery Ratio Analysis

In Figure 3.32, the PDR for proposed methodology is decreasing with increasing order of malicious node as malicious nodes invariably drop packets or not forwarding the packets. PDR is gradually decreasing with increase order of malicious node in OCEAN [173] as well. For both the cases it generates zigzag graph. Of course, Performance of proposed methodology is better than the performance of OCEAN. In both the approaches, PDR is falling down due to its non scalability and non capability to detect malicious node dynamically. Due to dynamic nature of MANETs, nodes may change their status, they may quit from the range, then they again come to the range with different ID, both the methodologies are unable to handle new status of routing table as well as node characteristics.

In Figure 3.33, PDR is gradually decreasing with increased node mobility in both OCEAN as well as in proposed methodology. The centralized PDA detection methodology is able to maintain better PDR in comparison to OCEAN. When node mobility is increasing, path breakage from source to destination will be more, thus change of routing information will be high. Nodes change their status frequently.

Collision of packets will be high. As a result, some extra packets will be dropped in addition to malicious packet drop. Due to static offline nature of detection process, it is not able to maintain high PDR during high mobility. Frequent change of routing information effects PDR of the network.

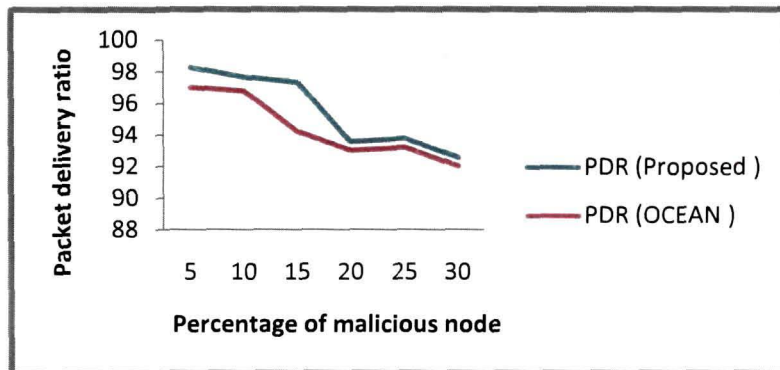


Figure 3.32 Effect of increase number of malicious node in PDR (LWM)

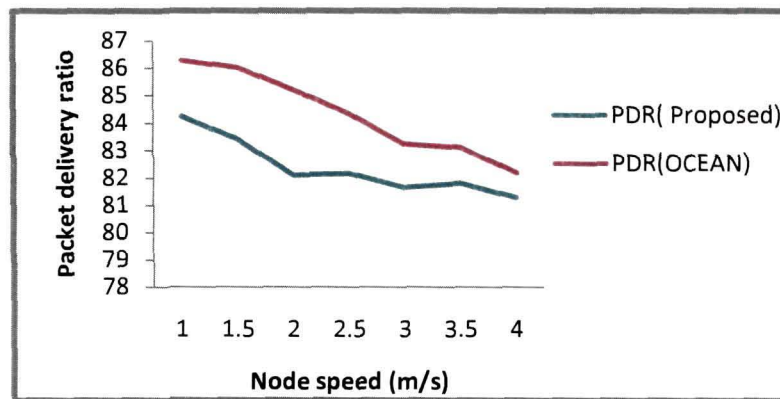


Figure 3.33 Effect of node mobility in PDR (LWM)

In Figure 3.34, when Pause time is varying, initially both OCEAN [173] and proposed methodology maintain almost same PDR. But as the pause time is gradually increasing, both the methodologies maintain high PDR. Still there is a difference between OCEAN and proposed methodology. PDR is far better than that of OCEAN in proposed methodology as OCEAN is not a guaranteed service. Even it doesn't

guarantee whether a packet is successfully delivered to destination or not. Increasing order of pause time gives more stability to the network. Nodes are not exposed to frequent change of status, thus routing table information are almost regular. So, centralized PDA detection methodology is able to show better performance

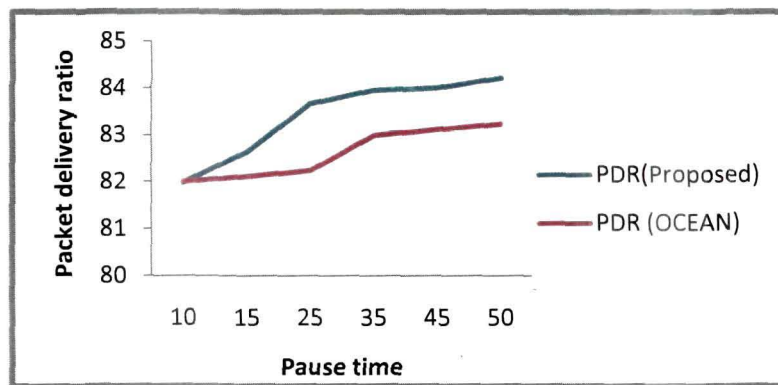


Figure 3.34 Effect of pause time in PDR (LWM)

3.3.2.5 Normalized Routing Load (NRL) Analysis

In Figure 3.35, it is clear that with increased number of malicious nodes in the network, NRL is gradually increasing in case of OCEAN [173] as well as in case of proposed methodology. Initially, proposed methodology bears more NRL than OCEAN but later on during high deployment of malicious nodes, performance of proposed methodology becomes better than OCEAN. Since NRL is the ratio between total number of routing packets to total number of delivered packets, therefore when the network contains more malicious nodes, it will drop more packets, Further, due to its inability to deliver packets to destination, it will generate more routing packets. Therefore, NRL will be gradually increasing. In case of proposed methodology, it controls and avoids malicious nodes with less complexity, while OCEAN detects malicious node with several processes including *neighbor node observation*, *route ranker*, *malicious traffic rejection* and *second chance mechanism*. It initiates more NRL in OCEAN during high deployment of malicious node.

As shown in Figure 3.36, with constant percentage of malicious nodes (i.e. 20% of total nodes) and constant pause time but varying node mobility, observation shows that performance of proposed methodology is better than performance of OCEAN, though the NRL is gradually increasing in both cases. Due to high node mobility, packets are dropped deliberately as it breaks the linkage between source and destination frequently. This will be an add-on to total packet drop due to malicious nodes.

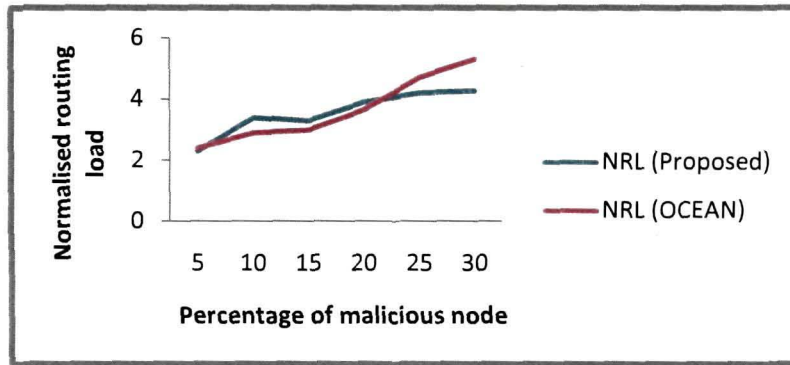


Figure 3.35 Effect of increase number of malicious node in NRL (LWM)

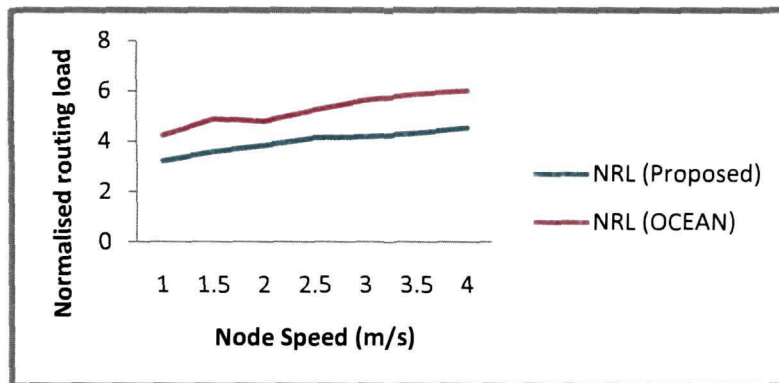


Figure 3.36 Effect of node mobility in NRL (LWM)

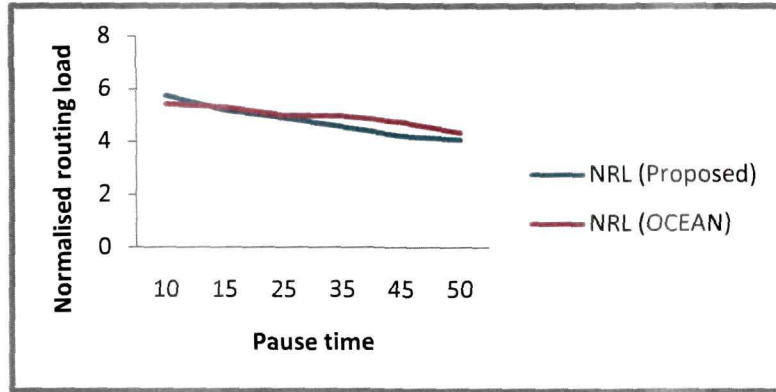


Figure 3.37 Effect of pause time in NRL (LWM)

In Figure 3.37, with increased pause time in the network, NRL is decreasing for both OCEAN [173] and proposed centralized PDA detection methodology. This is because of the network stability which indicates regular and stable behavior of nodes. Therefore additional packet drop due to highly dynamic node will be reduced. From observation it is clear that initially NRL is higher in case proposed methodology but later on during high pause time, performance of proposed methodology becomes better.

3.3.2.6 End-to-end Delay Analysis

In Figure 3.38, it is observed that though there is a slight difference between OCEAN [173] and proposed methodology in terms of end-to-end delay, but still for both cases end-to-end delay is increasing with increased number of malicious node. In MANETs, end-to-end delay is the delay encountered by a packet right from sending the packets from source up to the time that it receives ACK from destination. The packet delay consists of the queuing delay experienced at the source node, the queuing delays incurred at the intermediate nodes as well as MAC delay observed at the source and intermediate nodes. Presence of malicious node in the network will invariably drop packets due to which sender will have to wait for long time to get ACK packets from the receiver. As the number of malicious nodes increase, end-to-end delay also increase. Due to scalability and limitation of static offline system, end-

to-end delay is not controlled by both the system completely during high percentage of malicious nodes.

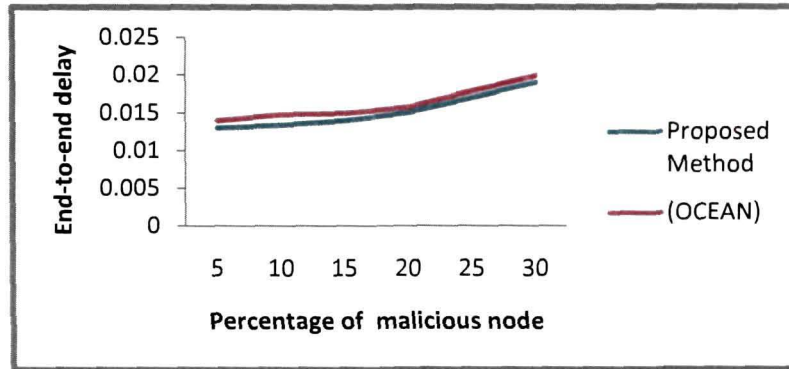


Figure 3.38 Effect of increase number of malicious node in End-to-End delay (LWM)

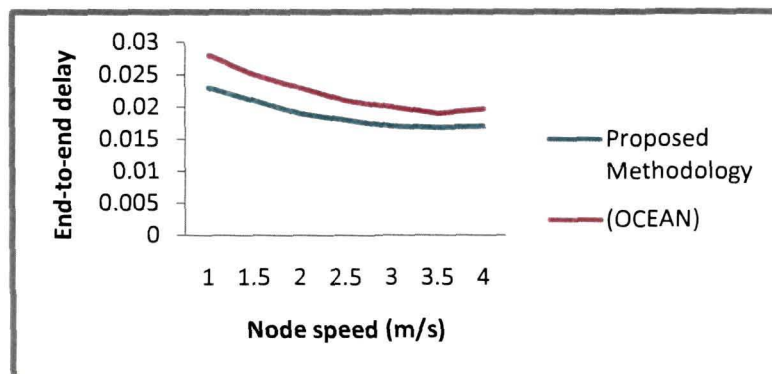


Figure 3.39 Effect of node mobility in End-to-End delay (LWM)

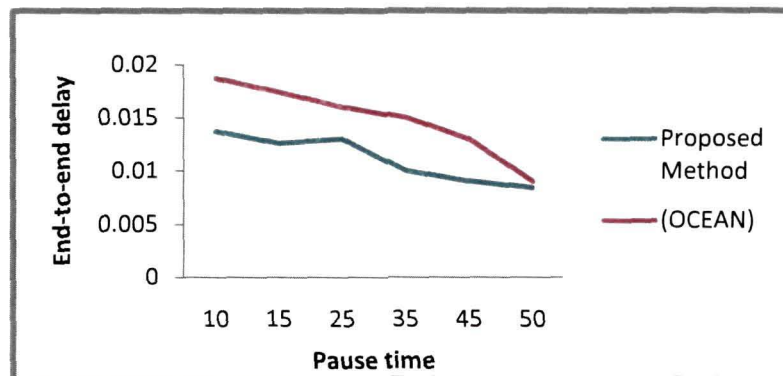


Figure 3.40 Effect of pause time in End-to-End delay (LWM)

In Figure 3.39, with increased node mobility, end-to-end delay is decreasing in both methodologies. It is because of active route timeout. A breakage link is not detected until the connection to a node along the route expires. So, routing protocol will try to send traffic to a node for the duration of the active route timeout irrespective of the node non-reach ability. Of course due to existence of malicious node in the network, end-to-end delay will be suppressed over the normal end-to-end delay. On the other hand, in case of high node mobility, with constant number of malicious node, centralized PDA detection process initially shows low end-to-end delay, but after some time it starts increasing.. This is because of the fact that though the centralized process statically identifies the malicious nodes, and then tries to regularize the performance, but due to dynamic nature of MANETs, state and characteristics of nodes may change, even in high mobility, nodes can change their characteristic frequently. Thus packets from source to destination may not reach on time or end-to-end delay may increase. On the other hand, due to maintenance of different steps including neighbor node observation, route ranker, malicious traffic rejection and second chance mechanism, end-to-end delay is more in OCEAN [173].

But in Figure 3.40, when the pause time is more, due to network stability, in both the cases end-to-end delay is gradually decreasing though at certain point during high pause time, both methodologies bear almost same end-to-end delay.

3.3.2.7 Round Trip Time (RTT) Analysis

From the Figure 3.41, it is clear that as the number of malicious node is increasing in the network, RTT is also gradually increasing for OCEAN [173] as well as in proposed methodology though it is comparatively low. The proposed methodology detects and avoids malicious nodes from the network, but the static nature of detection is unable to control dynamic nature of MANETs with malicious node deployment. As a result, some new nodes may act as malicious node or existing malicious node may work actively to the network that increases packet drop in the network. Thus it effects RTT.

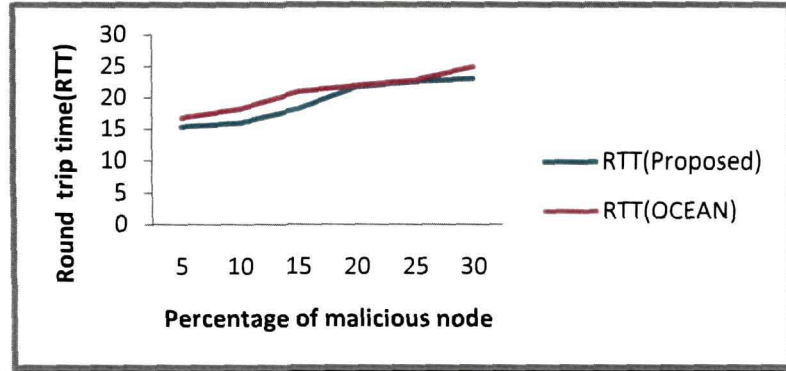


Figure 3.41 Effect of increase number of malicious node in RTT (LWM)

Increase of node speed doesn't effect RTT much in proposed methodology as well as in OCEAN [173]. There is a very slight difference between OCEAN and proposed methodology as shown in Figure 3.42. Since high mobility is the significance of more unstable network, frequent breakage of links; as the node speed increases, packet delivery time will also increase, thus it takes much time to get ACK packet from destination to source after sending packet from source. Relatively low RTT in case of proposed methodology signifies the detection capability of the proposed methodology.

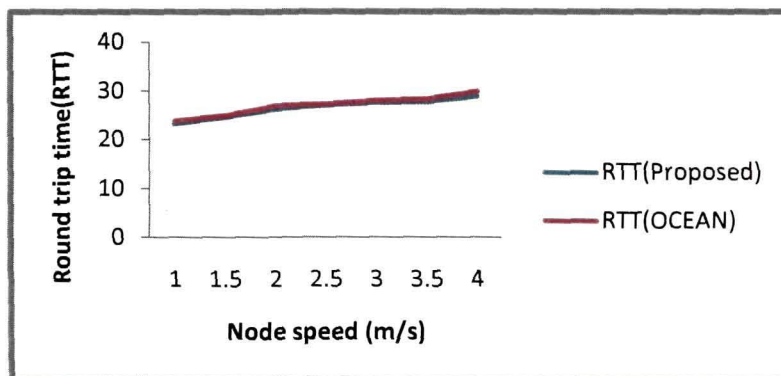


Figure 3.42 Effect of node mobility in RTT (LWM)

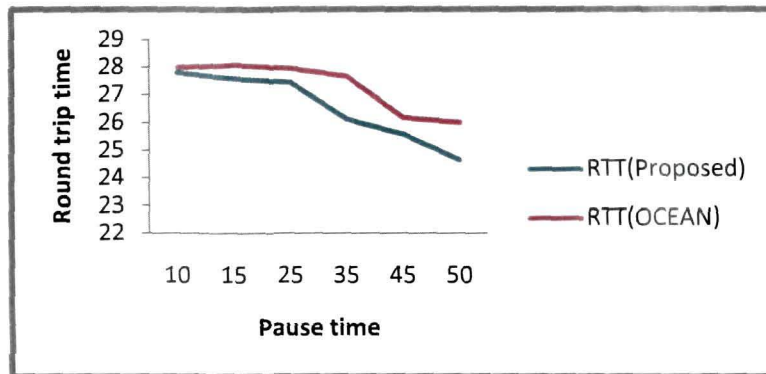


Figure 3.43 Effect of pause time in RTT (LWM)

But in Figure 3.43, when pause time is increasing, for both the cases, RTT is gradually decreasing. Still due to the ability of detection and avoidance of malicious node, RTT is comparatively low in case of proposed methodology. When the pause time in the network is more, it indicates more stable network, thus node characteristics are also remained constant. Hence the probability of frequent link breakage will be low. Packets deliver to destination on time, source gets ACK packets on time, and hence RTT is getting low. In case of proposed methodology, it tries to control and avoid malicious nodes from the stable network, so it gives more impact on RTT.

3.4 Discussion

Centralized PDA detection methodology has been implemented in two mobility models of MANETs such as *Random way point* model and *Levy walk* mobility model. In case of *Random way point* mobility model, proposed methodology is compared with AODV protocol. Using *Levy walk* mobility model, the proposed methodology is compared with OCEAN .

From the various analysis it is clear that centralized PDA detection methodology is able to detect malicious node from some audited data. It is better than AODV.

From the various results and analysis, it is clear that performance of proposed centralized PDA detection methodology is better than the OCEAN with respect to detection rate, false positive rate and other network performance parameters as mentioned above. Of course both the methodologies are able to detect malicious node from some audited data, so it needs relatively small numbers of components to keep running. In centralized PDA detection methodology, use of resource is less. The entire process in proposed methodology is less complex than OCEAN [173] .

But state of malicious node detection is centrally stored, so if any of the components under the system doesn't work then the whole system will collapse. Moreover due to lack of dynamic nature of the detection methodology, a minor change in the network needs the whole system to run once again. Size of centralized PDA detection methodology is limited to fixed number of components, so as and when the number of nodes increase in the network, system will have to recompute to cover all the new components. In between network have to suffer from some unexpected results in terms of network performance parameters. It is distinguished mostly when the node mobility is increasing. Similarly, with increased node mobility, the methods don't show very good results for throughput, packet delivery ratio, normalized routing load, end-to-end delay and round trip time. From this it can be concluded that though the centralized PDA detection methodology is better than OCEAN, still these are not capable of handling high node mobility.

Due to non scalability of the system, detection rate is gradually decreasing when number of malicious node is increasing. Similarly, false positive rate also shows mixed response. Throughput of the network is also gradually decreasing with increase number malicious node. Since the detection methodologies are static methodologies, so all the time these will not be able to detect the malicious node due to high dynamic nature of the network. Due to non scalable centralized property, PDR in the network is gradually decreasing. So such methods are not capable of handling high rate of malicious nodes. For end-to-end delay also it doesn't show full positive response with increased number of malicious node. RTT is also not as expected in case of

centralized PDA detection methodology as well as in OCEAN with increased number of malicious node.

Centralized PDA detection for an open, dynamic network like MANETs, is not a reliable process to detect malicious node responsible for PDA. This emphasizes to work with another automated detection process which should be distributed in nature. In the next chapter, distributed PDA detection methodology is proposed.

Chapter 4

Distributed PDA Detection

4.1 Introduction

Various results and analysis of centralized PDA detection methodology in chapter 3 shows that centralized PDA detection methodology is not suitable for a highly dynamic network with malicious node deployment.

Intrusion detection is normally based on collection and analysis of system and network audit data [11]. Apart from this, it also depends on cooperation of neighbor nodes [145][146][147][148]. Distribution is restricted to data collection. A distributed PDA detection methodology is proposed which is named as “*New Ad hoc on Demand Distance Vector (NAODV)*”. PDA is detected and confirmed not only by the node which has been suffering but also confirmed by other nodes participating in the network. It is not limited to data collection and detection, but also generates alarm to avoid malicious nodes from the network. One of the primary goals of detection methodology is to identify the misbehavior and implement detection methodology in such a way that it should raise less alarm [149]. It is assumed that intelligent agents are supposed to adapt decision making by cooperation with other nodes participating in the network.

4.2 The Architecture

4.2.1 Assumption

In the system model, low rates of packet loss or any other packets drop other than

malicious packet drop are assumed as *threshold* packet drop. When packet drop is more than the *threshold* packet drop then PDA is suspected. PDA is suspected in certain node based on the different network performance parameters such as *packet delivery ratio* as well as *throughput* of the network. It is assumed that packets are forwarded in a hop-by-hop fashion in on demand ad hoc way. The communication links are assumed to be bi-directional and there is no wireless channel error. All nodes use unidirectional antennas for bidirectional communications. Neighbor discovery protocol is assumed to work in such a way that every node can understand its corresponding neighbor.

It is assumed that all the nodes in MANETs have the capability to understand packet drop in them. Thus it has the ability to understand the *threshold* packet drop as well as *malicious* packet drop. Promiscuous mode of node is enabled with source routing. A malicious node can drop packets continuously or selectively. Here collusion of more than one node is not considered, so that malicious node can monitor each other and collude and mask the misbehavior of each other.

It is assumed that intelligent *agent* are supposed to adapt decision making by the cooperation with other nodes. Activity of the agent is dependent on the network performance matrices such as:

- a. Delay in Delivery of the Packet
- b. Response Time
- c. Quality of Service Provider
- d. Packet Forwarding Misbehavior

Accordingly in every node, local agent calculates the following to suspect packet drop misbehavior i.e.:

$$\text{Packet Drop Ratio} = \frac{\sum \text{No. of packets sent}}{\sum \text{No. of packets received}}$$

$$\text{Throughput} = \frac{y}{t} \quad \text{i.e. } y \text{ numbers of packets are delivered within } t \text{ times at a node.}$$

If for a particular node Packet Drop Ratio (PDR) is very high and throughput is very low then that node is suspected of malicious activity. It is assumed that nodes are communicating to one another in wireless channel and there is some amount of packet

drop due to congestion, overload or for media interference. Flow of traffic will be observed by each node that participated in communication. Agents will perform local analysis of packet drop in every node.

4.2.2 System Model

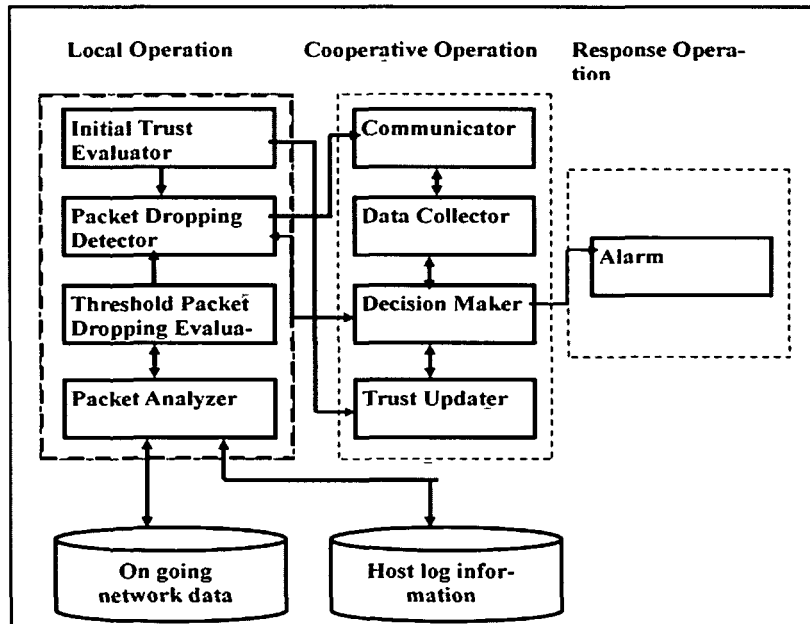


Figure 4.1: Schematic diagram of distributed PDA detection methodology (NAODV)

Proposed distributed PDA detection methodology New Ad hoc on Demand Distance Vector (NAODV) is based on cooperation of different nodes available within the network. Data, collected from different nodes are analyzed to detect PDA. Upon detection, message will be distributed amongst the nodes in terms of alarm to avoid the malicious nodes for packet forwarding. The system is unique in comparison to existing system in several points. Unlike the other TRUST evaluation procedure, While sending *PROB REQ*, it takes care to avoid feed back or to receive duplicate packets. Use of *CONFIDENCE* level to determine the *TRUST* level of a node is also a unique process. It generates more accurate result. Calculation of adaptive time for collecting *PROB RESP* based on four different conditions, randomly generating the

option is also unique. Use of incremental order decision tree algorithm ID5R, increases the accuracy of the system to evaluate *TRUST* level of the suspected malicious node. The entire system is an automatic, self manageable process. Data, collected from various node's host level audit system like "system log", are analyzed by the system.

Local Operation

Local operation runs on each node to detect PDA locally. Then these will collaborate with other modules to confirm PDA in the network.

Packet analyzer: It analyzes the packet stream with various fields in the packets and stores the content according to the specified logic. Packet analyzer will legitimately be used to analyze each packet that comes to every node to identify any suspected malicious packet drop in the network.

Threshold packet drop evaluator: It determines the threshold value of packet drop due to any reason except malicious packet dropping.

Initial trust evaluator: When a node first time joins the network, its trust value is evaluated by this module in cooperation with neighbor nodes according to algorithm 4.3.

Packet drop detector: It compares the dropped packets that are evaluated by packet analyzer with threshold packet drop. Once the number of dropped packets is more than the threshold packet drop then packet dropping attack is suspected. It communicates to "*cooperative operation*" module for confirmation of packet dropping attack.

Cooperative Operation

Communicator: This module is activated after getting signal from "*packet drop detector*" module that some packets are dropped beyond the threshold packet drop due to some suspected malicious node. Then it sends the *PROB REQ* message to all its neighbors to know *TRUST* and *CONFIDENCE* level of the suspected malicious node within the adaptive time.

Data collector: *PROB RESP*, which are sent in response to *PROB REQ* are collected by this module within the adaptive time. Adaptive time is based on either of the following conditions, randomly generating the options:

- a. Number of node scanned (% of total nodes)
- b. Number of Responses expected(% of total nodes)
- c. Fixed amount of time to forward *PROB REQ* and to get *PROB RESP*
- d. Number of level crossed

Decision Maker: This module dynamically evaluates the *TRUST* level of a node. *PROB RESP* that is collected from various neighbors containing *TRUST* and *CONFIDENCE* level of suspected malicious node, are analyzed to confirm whether the suspected malicious node is really a malicious node or not. To analyze dynamically, incremental decision tree algorithm ID5R [18][19][20][21] is used.

Trust updater: It dynamically updates the *TRUST* level of the nodes according to Algorithm 4.2

Response Operation

Alarm generator: If the “*Decision Maker*” confirms that suspected malicious node is a confirmed malicious node then alarm will be broadcasted in the network to avoid the malicious node for packet forwarding.

4.2.3 Algorithm of the Proposed System (NAODV)

Algorithm 4.1 Algorithm for distributed PDA detection methodology

Input: *PDR*, T_{th} , D_{th} , Receive packets, Sent Packets, Drop packrts, Node *IP* , adaptive_time

Output: malicious Node *IP*, *alarm*

1. Initialize the value of T_{th} { * T_{th} is the minimum throughput for a network * }
2. Initialize the value of D_{th} { * D_{th} is the threshold packet drop in a network * }
3. **if** (node *IP* = new node *IP*) **then** { * If a node joins as new node. Node *IP* means *IP* address of a node * }
4. evaluate initial *TL* { * As in Algorithm 4.3 * }
5. create *LOG* file and save *TL* in *LOG* file
6. **end if**
7. $PDR := \frac{\sum No.of\ sent}{\sum No.of\ receive}$ { * *PDR* is the packet drop ratio * }

8. $T := \frac{y}{t}$ { * T is the Throughput and y is the numbers of packets delivered within t times at a node.* }
9. **if** ($PDR > D_{th}$) AND ($T < T_{th}$) **then**
10. print *suspected_malicious_node*
11. broadcast *PROB REQ* { * *PROB REQ* is the REQ packet which is sent to all neighbors of the node that suspects PDA* }
12. **end if**
13. **do**
14. neighbor checks its “*LOG file*” for relevant data
15. **if** (*TRUE*)
16. send *PROB RESP* to *original_sender* in step 11
17. **else**
18. forward *PROB REQ* to their neighbors
19. **end if**
20. collect *PROB RESP* from the neighbors
21. forward *PROB RESP* to *original_sender*
22. generate decision tree to identify *confirm_malicious_node* { * Decision tree is generated as per logic of ID5R * }
23. **while** (*adaptive_time*) **goto** step 12 { * Till *adaptive_time*, sender accepts *PROB RESP* * }
24. **if** (*suspected_malicious_node* == *confirm_malicious_node*) **then**
25. GD:=”malicious” { * GD is the global decision of all neighbors to confirm PDA
26. * }
27. print “*Confirm_malicious_node IP*”
28. Generate and broadcast “*alarm*” to avoid the malicious node for packet forward
29. **else**
30. GD:=”non malicious”
31. **end if**

Activity diagram for the Algorithm 4.1 is shown in Figure 4.2.

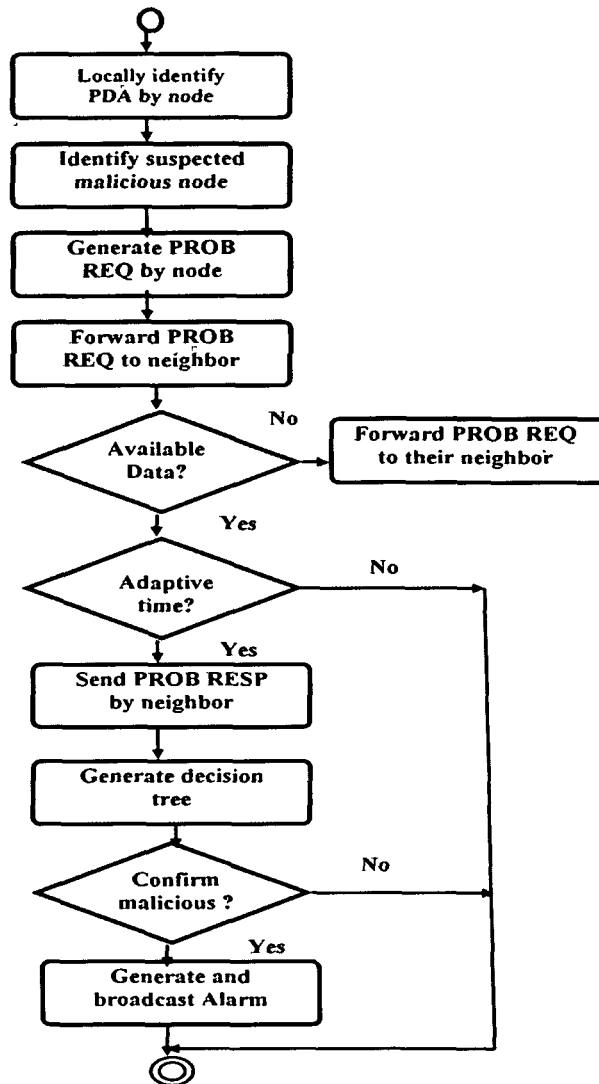


Figure 4.2: Activity diagram of distributed PDA detection methodology (NAODV)

The “*LOG file*” contains the following fields in it.

Node *IP* : *IP* address of its neighbors

Confidence level (*CL*) : Confidence level of node

Trust level (*TL*) : Trust level of node

PROB REQ contains the following fields,

Req_from: *IP* address of the node that sends *PROB REQ*

Req_to: *IP* address of the node to whom it sends *PROB REQ*

Mal_node: IP address of the suspected malicious node

Neighbor list: List of neighbor nodes of the sender to avoid feedback which may occur due to duplicate *PROB REQ* that may be sent from the receiver.

Adaptive_time: It is time within which node should respond to sender, Adaptive time is based on either of the following conditions, randomly generating the options:

- Number of node scanned (% of total nodes)
- Number of *PROB RESP* expected(% of total nodes)
- Fixed amount of time to forward *PROB REQ* and to get *PROB RESP*
- No. of level crossed

In **Algorithm 4.1**, *PROB RESP* contains the following fields,

Req_from: IP address of the sender

Suspected_mal: IP address of suspected malicious node

Response_to : IP address of the node where it will send the response

Confidence_level: Confidence level of the suspected malicious node

Trust_level: Trust level of the suspected malicious node

In **Algorithm 4.1**, Condition of **No Response** may occur due to following reasons, if

- There is no neighbor to forward the request.
- If adaptive time “t” is over
- If the node is in out of range from the network after getting request
- If any node is a co-operative malicious node with the suspected malicious node
- If a node is not communicating due to selfish behavior or to save its resources
- If link failure occurs

Following Algorithm 4.2 shows the dynamic TRUST evaluation process of nodes based on their cooperative participation in detection process.

Algorithm 4.2 Algorithm to update TRUST level of node

Input: TL_m, GD

Output: TL_c

```
1: get  $TL_m$  { *  $TL_m$  is the TRUST level of suspected_malicious_node send by  $n$  *}
2: get  $GD$  { *  $GD$  is the Global decision generated by decision tree for suspected
malicious node in algorithm 4.1 *}
3: If ( $GD = "malicious"$ ) then
4:     If ( $TL_m = "high"$ ) then
5:          $TL_c := low$  { *  $TL_c$  is the TRUST level of node  $n$  that sends PROB RESP
*}
6:     else
7:          $TL_c := high$ 
8:     end if
9: end if
10: If ( $GD = "non\ malicious"$ ) then
11:     If ( $TL_m = low$ ) then
12:          $TL_c := low$  ;
13:     else
14:          $TL_c := high$  ;
15:     end if
16: end if
```

In Algorithm 4.3, Initial *TRUST LEVEL* (TL) evaluation algorithm is given. *Trust Level* (TL) for a node can be defined according to behavior of the node. It can be defined either as *TRUST* or *DISTRUST*. *TRUST* is assumed as "1" and *DISTRUST* as "0". To assign initial TL to a node, it follows a distributed cooperative process. It not only depends on the node which wants to assign TL but also depends on the other neighbors of that node according to Algorithm 4.3.

Algorithm 4.3 Algorithm to find initial TRUST evaluation of a node

Input: TL_i, n, i

Output: TL

```
1:  $i := 1$ 
2: for all ( $i$  in  $n$ ) do { *  $n$  is the number of neighbors of a new node for which initial
TRUST to be evaluated *}
3:     send TRREQ { * TRREQ is the trust request send to all neighbors of a node to
send TRUST level for which TRUST to be evaluated *}
4:     if ( $TL(i) = 1$ ) then { *  $TL_i$  is the TRUST level sent by neighbor  $i$  *}
5:          $TOT\_TRUST := TOT\_TRUST + 1$  ; { *  $TOT\_TRUST$  is the Total number of
nodes that assign TRUST value as "HIGH" *}
6:     else
7:          $TOT\_DISTRUST := TOT\_DISTRUST + 1$  ; { *  $TOT\_DISTRUST$  is the Total
```



```

      number of nodes that assign TRUST value as “LOW” *}
8:   end if
9: end for
10:  $p := (2/3)*n$ 
11: if ( $TOT\_TRUST >= p$ ) then
12:    $TL := HIGH$  { *  $TL$  is the  $TRUST$  level of the new node *}
13: else
14:    $TL := LOW$ 
15: end if

```

4.2.4 Performance Parameters

Network performance parameters which are used to measure network performance before and after implementation of proposed detection methodology, NAODV are same as mentioned in section 3.2.4 of Chapter 3.

4.3 Multi Agent System for Proposed Methodology

4.3.1 Introduction

Multi agent system is a system that consists of several autonomous agent involved with different activity with common objective. These are computational systems work asynchronously with respect to other agents [155]. They can interact, cooperate or exchange data with other agents so that their common effort helps to attain the goal. Due to flexible problem solving approach of multi agent system, these are in high demand to address the challenges faced by MANETs. In MANETs, capability of nodes to forward packets and to participate in routing process, directly affects the network characteristics [150][153]. Moreover, intrusion detection in MANETs, that carried out in a mobile agent based system has the advantages of overcoming different challenges of MANETs such as network latency, reducing network load, autonomous execution, platform independency, dynamic adaptation and scalability [151][152][156]. Mobile agents are alternative to the client-server distribution model. Such autonomy system can generate decision, distribute decision automatically, but limited to the specification provided in the design.

4.3.2 Multi Agent Architecture for Proposed Algorithm

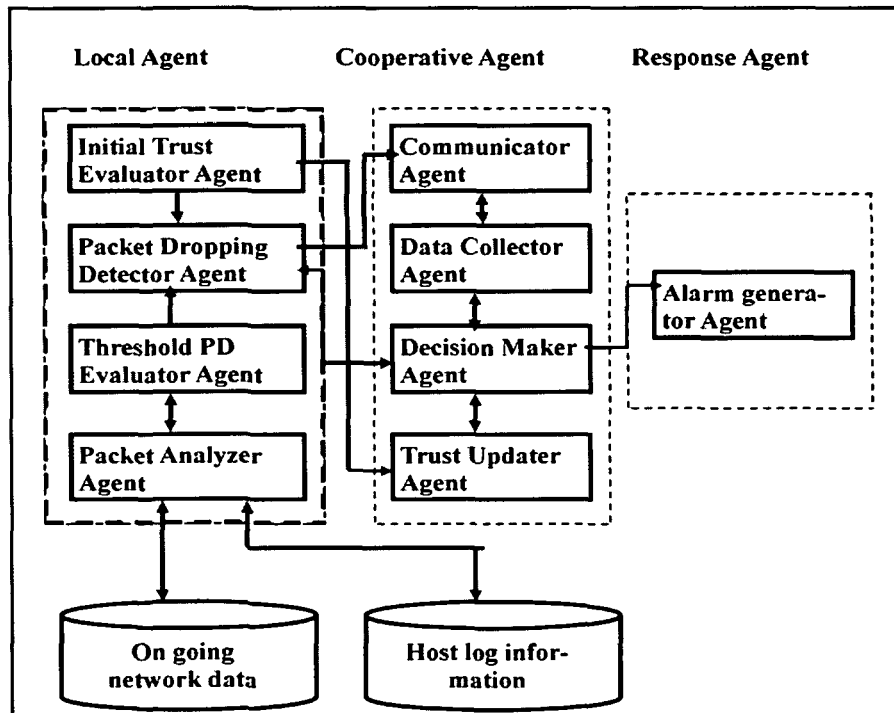


Figure 4.3: Schematic diagram of multi agent system of distributed PDA detection

Proposed distributed packet dropping attack detection methodology can relate with multi agent system in which several agents as mentioned below should work actively to set a common goal that is packet dropping attack detection.

According to Figure 4.3, the multi agent system consists of the following agents:

Local Agent: Local agent will run on each node to suspect packet dropping attack locally. Then these will collaborate with other agent to confirm packet dropping attack in the network. Based on the type of functions, it contains the following agents under it.

- Packet Analyzer
- Threshold Packet drop evaluator
- Initial trust evaluator

- Packet Drop Detector

Co-operative Agent: Cooperative agents involve with collaboration of other categories of agents such as Local agent and Response agent. It also contains following agents under it.

- Communicator agent
- Data collector agent
- Decision Maker agent
- Trust updater agent

Response Agent: This agent generates and distributes alarm to the network when decision taken by cooperative agents with respect to malicious packet dropping attack is positive.

4.3.3 Collaboration-Multi Agent System

The proposed PDA detection methodology is based on collaborative functions of different independent agents. Agents are well understood about their functions. Automated agents work independently in the network and then correlate or exchange their data with other agents to generate a common decision.

As shown in Figure 4.3, the proposed multi agent system is a combination of three groups of agent namely *Local agent*, *Cooperative agent* and *Response agent*. They collaborate with one another to take mutual decision of packet dropping attack in MANETs.

Local agent is implemented in every system in the network, which gathers information about its own system. It analyzes the packet dynamically to compare the packet drop in the network with threshold packet drop. If it finds number of packet drop is more than the threshold packet drop than it communicates with cooperative agent for distributed cooperative decision for PDA.

Communicator agent communicates with neighboring nodes to send specified data to *data collector agent* of *cooperative agent*.

Data collector agent is implemented with detection methodology to provide specified data to *decision maker agent* to decide the PDA in MANETs. *Trust updater agent* of *cooperative agent* dynamically updates TRUST of nodes based on cooperative participation of nodes.

If the *Cooperative agent* confirms malicious packet dropping in the network, then it communicates with *response agent* to broadcast an alarm to the network to avoid the malicious node from further communication.

4.4 Performance Evaluation of the Detection Mechanism

4.4.1 NAODV using Random Way Point Model

Simulation Environment

Table 4.1: Simulation Environment (RWP Model)

Animation area	1000m X 1000m
Mobility model	Random way point (RWP)
Channel type	Wireless
No. of nodes	100
Simulation time	600 sec
Pause time	10-70 sec
Node Speed	10-70 m/s
Data rate	100 kbs
Transmission range	100 m
Packet size	512 byte
Traffic type	CBR
Routing protocol	AODV, SAODV, TAODV, NAODV

Simulation Results

Simulations are performed for three different methodologies namely SAODV, TAODV and proposed NAODV with following criteria:

- a. When percentage of malicious node is increasing, then constant node speed and pause time is maintaining
- b. When node speed is increasing, then constant malicious node percentage and pause time is maintaining
- c. When pause time is varying, then constant node speed and percentage of malicious node is maintaining

4.4.1.1 *Detection Rate (NAODV, SAODV, TAODV)*

Figure 4.4 shows the detection rate of all the three different methodologies with increased number malicious nodes. Similarly, Figure 4.5 shows the detection rate with increased node mobility, while Figure 4.6 shows the detection rate with increased pause time. It is observed that NAODV shows the best performance in all the three cases.

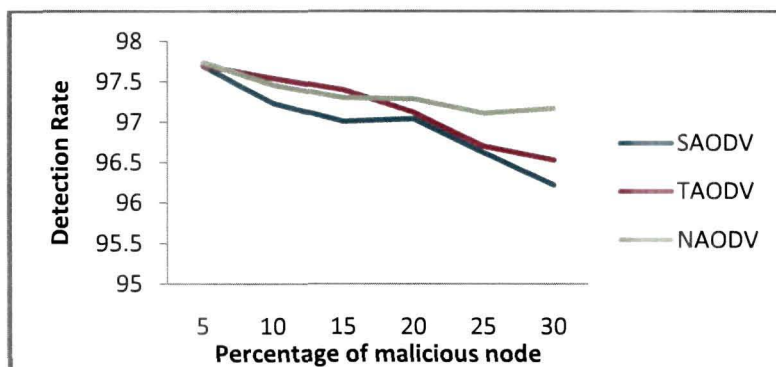


Figure 4.4. Effect of increase of malicious node on detection rate (RWP Model)

It can be explained by the fact that in NAODV, malicious node detection and avoidance is completely based on cooperation of neighbors. Global decision is taken based on decision tree algorithm. Accordingly TRUST level of the node is dynamically updated. On the other hand, TAODV is a trusted routing protocol that cooperates with a self organized key management mechanism. Moreover it performs trusted routing in a self-organized way. In SAODV, signature is verified by both source node and intermediate node and then only routing table is updated. Malicious

node cannot generate signature of destination node, hence it will not be able to impersonate destination node.

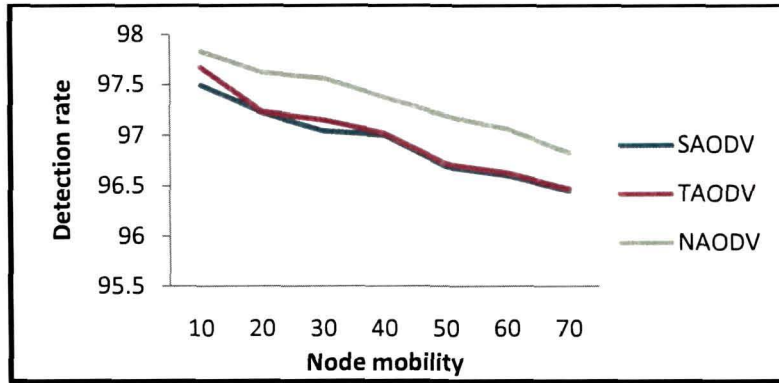


Figure 4.5. Effect of increase of node mobility on detection rate (RWP Model)

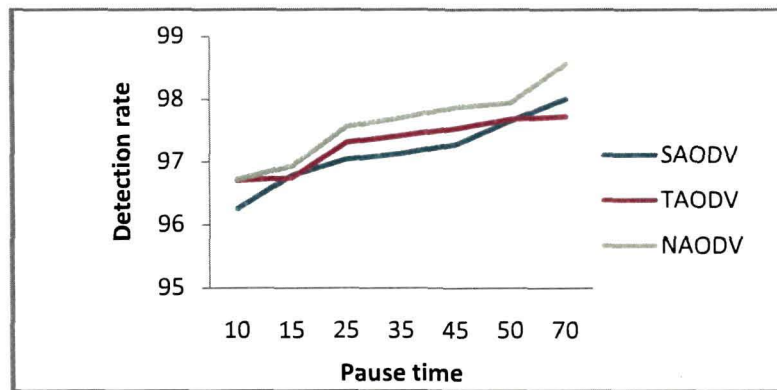


Figure 4.6. Effect of increase of pause time on detection rate (RWP Model)

4.4.1.2 *False Positive Rate (NAODV, SAODV, TAODV)*

Figure 4.7, Figure 4.8 and Figure 4.9 compare the false positive rate of three different methodologies with respect to increased number of malicious node, increased node mobility and increased pause time. SAODV is not designed to resist the DoS attacks like packet dropping attack. It provides a cryptographic support to secure the routing protocol. It shows the vulnerabilities to packet dropping attack.

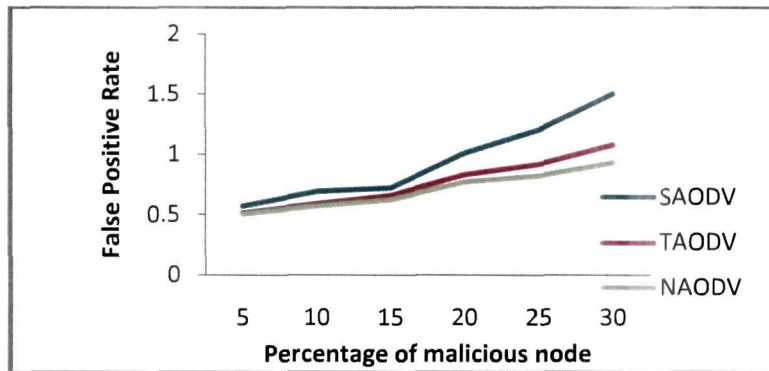


Figure 4.7 Effect of increase of malicious node on false positive rate (RWP Model)

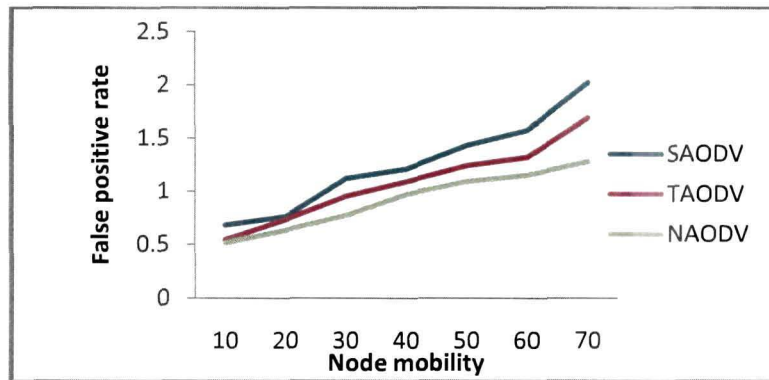


Figure 4.8 Effect of increase of node mobility on false positive rate (RWP Model)

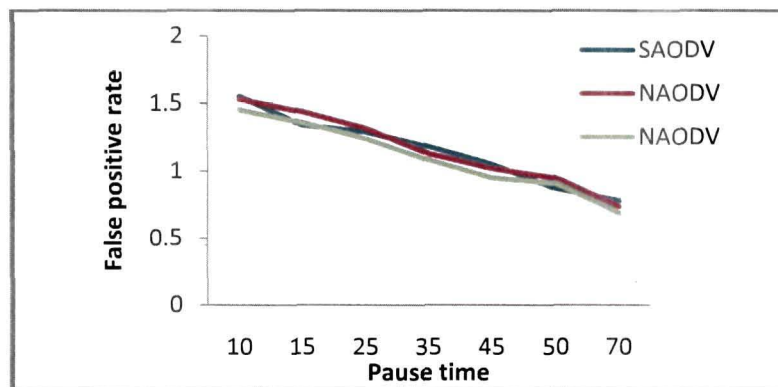


Figure 4.9 Effect of increase of pause time on false positive rate (RWP Model)

TAODV facilitates trusted routing, not directly involve with PDA detection. On the other hand, in NAODV, detection of malicious packet dropping is done in distributed cooperative way, after confirmation only it generates an alarm to avoid the malicious nodes for further packet forwarding, hence false positive rate will be comparatively less.

4.4.1.3 Throughput Analysis (NAODV, SAODV, TAODV)

Throughput of the network is compared for three methodologies as shown in Figure 4.10, Figure 4.11 and Figure 4.12.

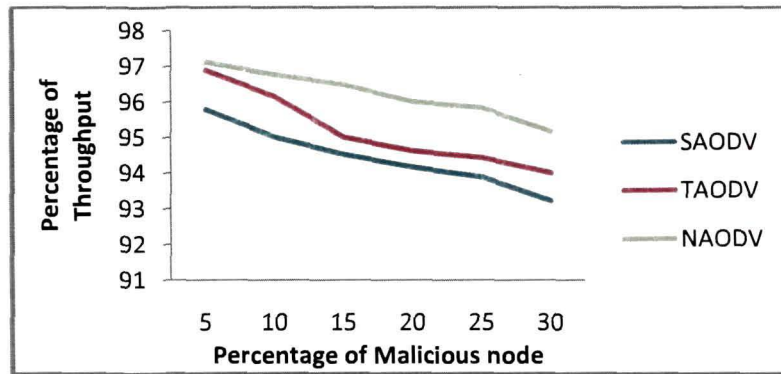


Figure 4.10 Effect of increase of malicious node on throughput (RWP Model)

In SAODV, it takes some extra time for computation and verification of security fields during route discovery process. It always prefers safest path instead of shortest path. These all consume some extra time. Since throughput depends on total number of packets delivered in specified time, hence it comes down. TAODV also consumes extra time for updating TRUST by evidence & opinion, exchange and authentication. But NAODV doesn't consume much time for route discovery and there are not so complex security measures during route discovery, so it delivers more packets in specified time. This implies more throughputs.

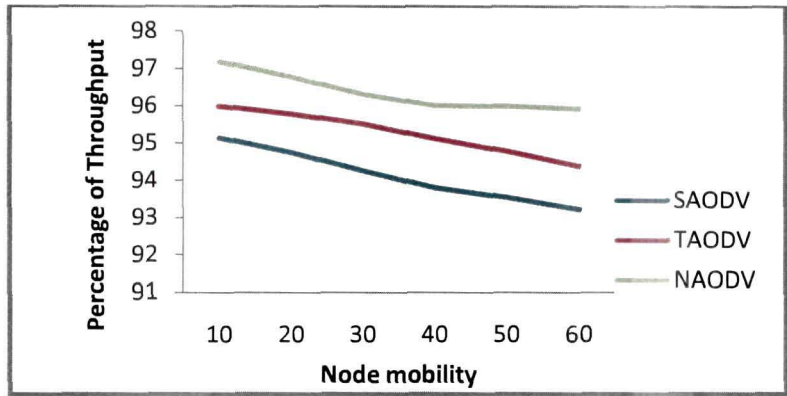


Figure 4.11 Effect of increase of node mobility on throughput (RWP Model)

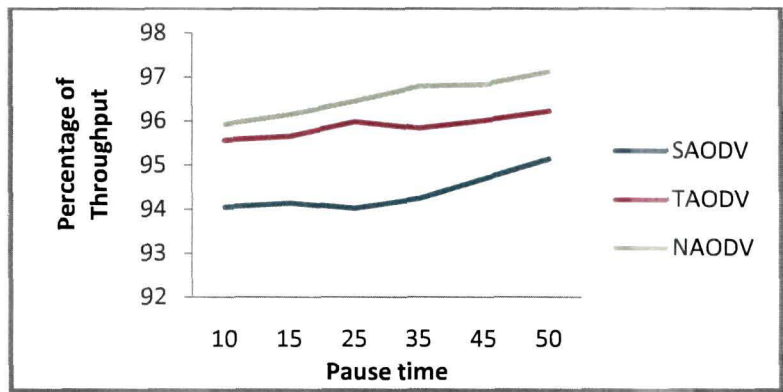


Figure 4.12 Effect of increase of pause time on throughput (RWP Model)

4.4.1.4 Packet Delivery Ratio Analysis (NAODV, SAODV, TAODV)

Figure 4.13, Figure 4.14 and Figure 4.15, compare the packet delivery ratio of NAODV, SAODV and TAODV.

In all the three cases, NAODV performs the best. NAODV is simply meant for packet dropping attack detection. So, for any network, it tries to detect malicious node in distributed cooperative way and avoid the same for further packet forwarding. By this it decreases packet drop ratio and oppositely it increases packet delivery ratio.

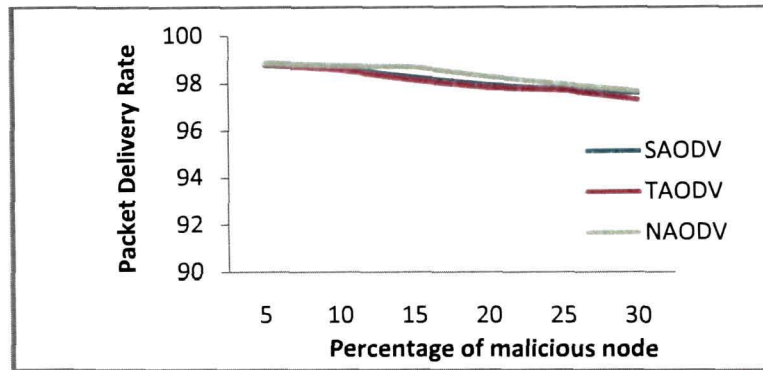


Figure 4.13 Effect of increase of malicious node on packet delivery ratio (RWP Model)

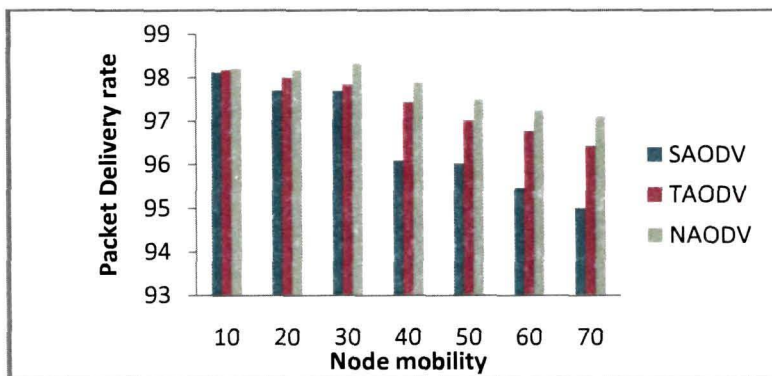


Figure 4.14 Effect of increase of node mobility on packet delivery ratio (RWP Model)

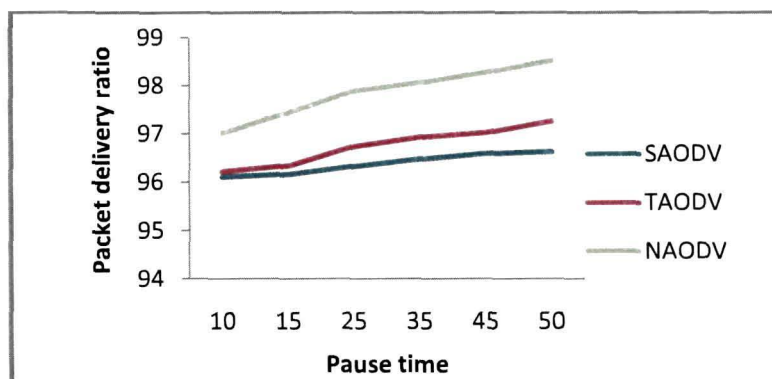


Figure 4.15 Effect of increase of pause time on packet delivery ratio (RWP Model)

When the node mobility is higher, it signifies the high failure of connectivity and frequent change of topology. As a result, packets drop ratio will be more. Nodes may

be falsely accused of malicious. It is more in case of SAODV than TAODV, while less in case of NAODV. SAODV chooses the safest path instead of shortest path and tries to eliminate the malicious nodes in the way, so the average path length is longer. As the node mobility is higher, the network topology will break frequently and it will not be able to deliver the packets on time. Moreover high security application of SAODV will resist the path more.

4.4.1.5 Normalized routing load Analysis (NAODV, SAODV, TAODV)

NRL is the ratio between total numbers of routing packets to total number of delivered packets. A network contains more malicious nodes means it will drop more packets. NRL is inversely proportional to PDR. In presence of malicious node, NAODV shows better performance in comparison to other two methodologies such as SAODV and TAODV as shown in Figure 4.16.

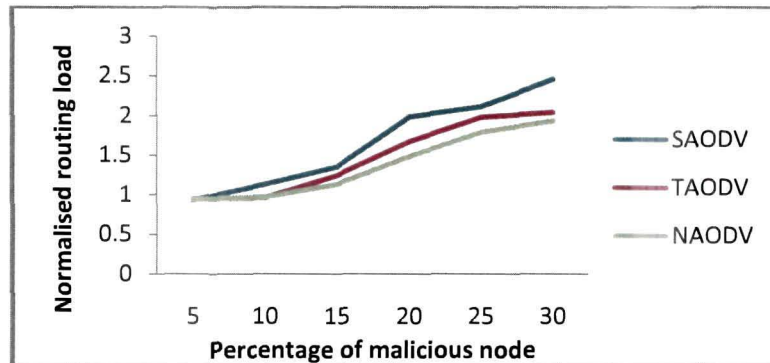


Figure 4.16 Effect of increase of malicious node on normalized routing load (RWP Model)

In presence of malicious nodes in the network, it forces SAODV to use hash chain and digital signature to provide secure routing process. That leads to slow PDR, thus it creates more NRL in the network. Similarly, in TAODV, system performance is improved in comparison to SAODV by avoiding generating and verifying digital signatures at every routing hop.

According to Figure 4.17, in case of SAODV, NRL is found to be more than that of TAODV and NAODV due to its intensity to find the safest path. In high mobility of node, network topology change and link failure occurs frequently. Network becomes unstable for all the time. As a result, SAODV is unable to find the safe path for routing. PDR is decreasing, thus NRL is increasing. In TAODV, a node does not request and verify certificates continuously. So, computation overhead is reduced greatly. At the same time, in TAODV, the whole system provides security to the system up to certain level, not directly involved in PDA detection. NAODV is directly involved with PDA detection and avoidance in distributed way, hence controlling of PDA in NAODV, leads to high packet delivery ratio. So, NRL is less in comparison to other two systems.

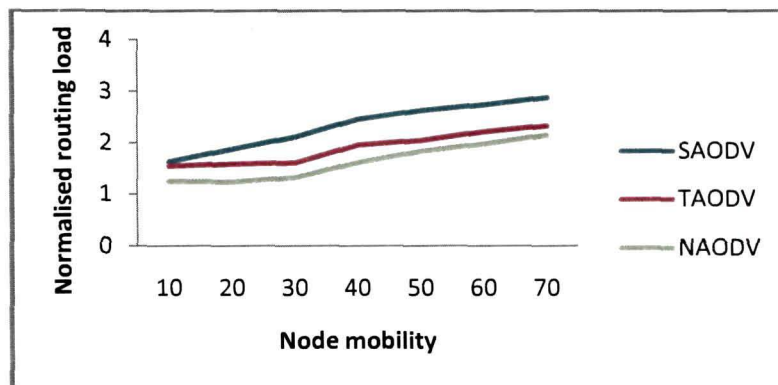


Figure 4.17 Effect of increase of node mobility on normalized routing load (RWP Model)

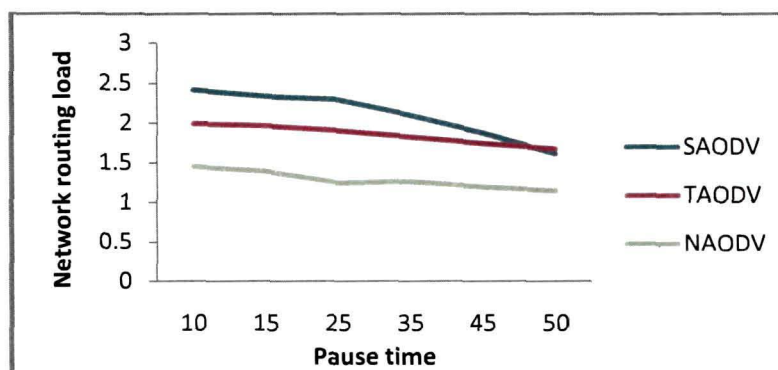


Figure 4.18 Effect of increase of pause time on normalized routing load (RWP Model)

According to Figure 4.18, with increase number of pause time in the network, NRL is gradually decreasing in all the methodologies such as SAODV, TAODV and NAODV. When pause time is increasing network is getting more stable which indicate regular and stable behavior of nodes. So, additional packet drop due to highly dynamic node will be reduced.

4.4.1.6 *End-to-end Delay Analysis (NAODV, SAODV, TAODV)*

In Figure 4.19, it is observed that end-to-end delay is increasing with increased number of malicious in all the three different methodologies. In MANETs, end-to-end delay is the delay encountered by a packet right from the generation of the packet from the source and till it gets back the ACK from destination. The packet delay consists of the queuing delay experienced at the source node, the queuing delays incurred at the intermediate nodes as well as MAC delay observed at the source and intermediate nodes. Presence of increased malicious node in MANET will invariably drop packets. In SAODV and TAODV, due to high security measures during route discovery from source to destination, end-to-end delay is more. As number of malicious nodes is increasing it consumes more time, thus end-to-end delay is also more.

In Figure 4.20, in case of high node mobility, with deployment of malicious node, both SAODV and TAODV show the instability in end-to-end delay. Due to dynamic nature of nodes in MANET, state and characteristics of nodes may change, even in high node mobility; nodes can change their characteristic frequently. Thus packets from source to destination may not reach on time or end-to-end delay may increase. In case of SAODV and TAODV, high security measures during path delivery as well as acket delivery, causes the high end-to-end delay. On the other hand NAODV shows almost a stable and low end-to-end delay in spite of increased number of node speed. In Fig 4.21, when the pause time is more, due to network stability, in all the three cases end-to-end delay is gradually decreasing. Still it is more in case of SAODV and

TAODV because of their computational overhead during security measure during packet delivery.

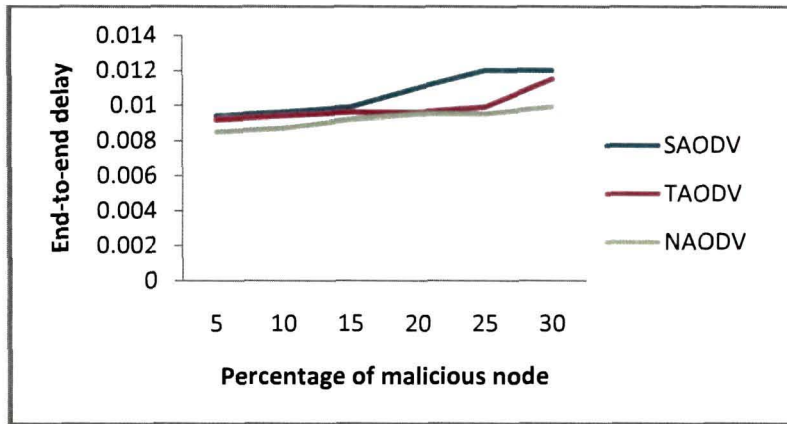


Figure 4.19 Effect of increase of malicious node on end-to-end delay (RWP Model)

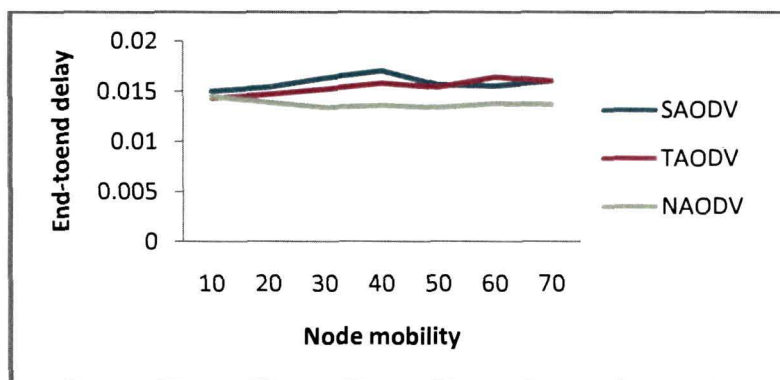


Figure 4.20 Effect of increase of node mobility on end-to-end delay (RWP Model)

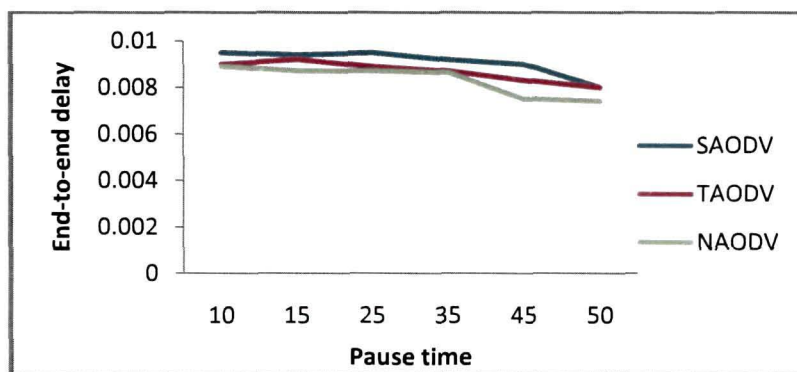


Figure 4.21 Effect of increase of pause time on end-to-end delay (RWP Model)

4.4.1.7 Round trip time (NAODV, SAODV, TAODV)

From the Figure 4.22, it is clear that as the number of malicious node is increasing in the network, NAODV consumes less RTT in comparison to other two methodologies. In SAODV, it measures the generation and validation of nodes that switch between signing, verifying and hash chain operations rapidly in case of both send and receive message. Each message is validated before any further processing takes place. So, each RREQ and RREP gets delayed by some amount of time at each hop through which message should be forwarded. When the number of malicious nodes is increasing, due to complex security measures, SAODV shows more RTT in comparison to other two methodologies. TAODV shows comparatively less amount of time. But in TAODV, due to its simplicity in comparison to SAODV, there is much less pre-packet overhead. The main overhead that incurred in TAODV is the overhead related to R ACK packets which is a new kind of packet rather than packet extension.

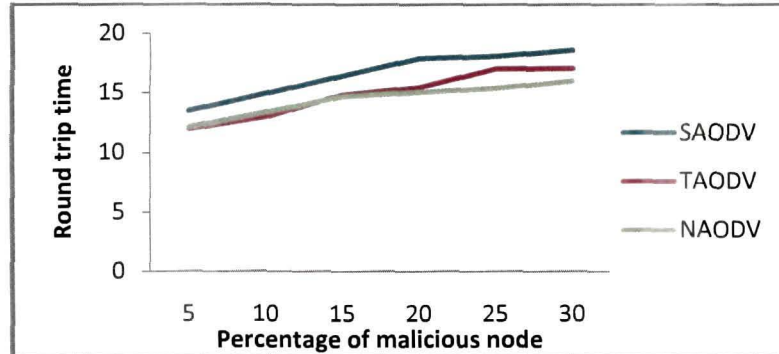


Figure 4.22 Effect of increase of malicious node on round trip time (RWP Model)

As in Figure 4.23, when the node speed is increasing with malicious node deployment, RTT is increasing in all the three cases, though it is lowest in case of NAODV. High mobility is the significance of more unstable network, frequent breakage of links etc, as a result packet delivery time will also be increased, and thus it takes much time to get ACK packet from destination to source after sending packet

from source. On the other hand, in case of SAODV and TAODV, it is affected more because of their complexity in computation.

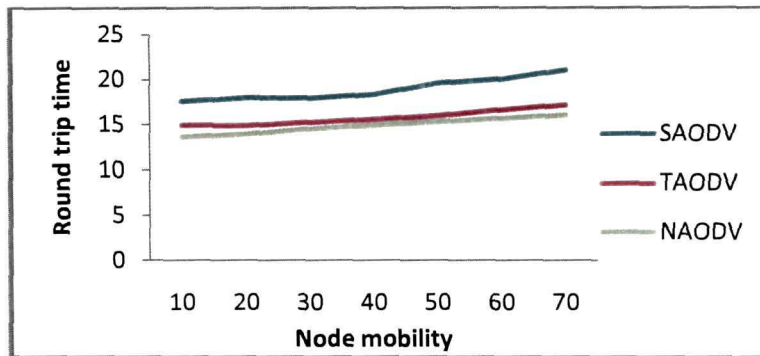


Figure 4.23 Effect of increase of node mobility on Round trip time (RWP Model)

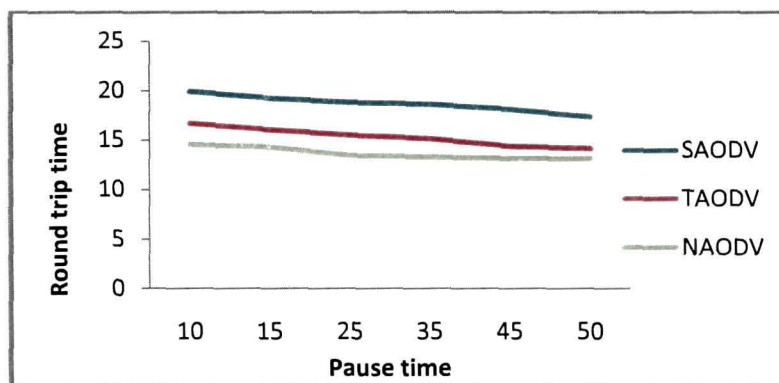


Figure 4.24 Effect of increase of pause time Round trip time (RWP Model)

In Figure 4.24, as the pause time is increasing, for all the three cases, RTT is gradually decreasing. When the pause time in the network is more, it indicates more stable network, thus node characteristics are also remained constant. Probability of frequent link breakage will be low. Packets may deliver to destination on time, source also gets ACK packet on time. Hence, RTT is getting low. In SAODV and TAODV, it is more than that of NAODV, because of additional time consumption for security measures during packet delivery.

4.4.2 NAODV using Levy Walk Model

Simulation Environment

Table 4.2: Simulation Environment (LWM)

Animation area	1000m x 1000m
Mobility model	Levy walk model (LWM)
Channel type	Wireless
No. of nodes	100
Simulation time	600 sec
Pause time	10-70 sec
Node Speed	1- 4 m/s
Data rate	100 kbs
Transmission range	100 m
Packet size	512 byte
Traffic type	CBR
Routing protocol	AODV, SAODV, TAODV, NAODV

Simulation Results

Simulations are performed for three different methodologies namely SAODV, TAODV and proposed NAODV with following criteria:

- d. When percentage of malicious node is increasing, then constant node speed and pause time is maintaining
- e. When node speed is increasing, then malicious node percentage and pause time is maintained as constant.
- f. When pause time is varying, then constant node speed and constant percentage of malicious node is maintaining

4.4.2.1 Detection Rate (NAODV, SAODV, TAODV)

Figure 4.25 shows the detection rate of all the three different methodologies with increased number of malicious nodes. Similarly, Figure 4.26 shows the detection rate

with increased node mobility, while Figure 4.27 shows the detection rate with increased pause time. It is observed that NAODV shows the best performance in all cases except detection rate with increased pause time. In this case, initially SAODV shows the best performance. Mixed response is shown by the SAODV and TAODV in malicious node deployment. In this scenario, detection rate of NAODV is almost stable irrespective of increase of malicious node.

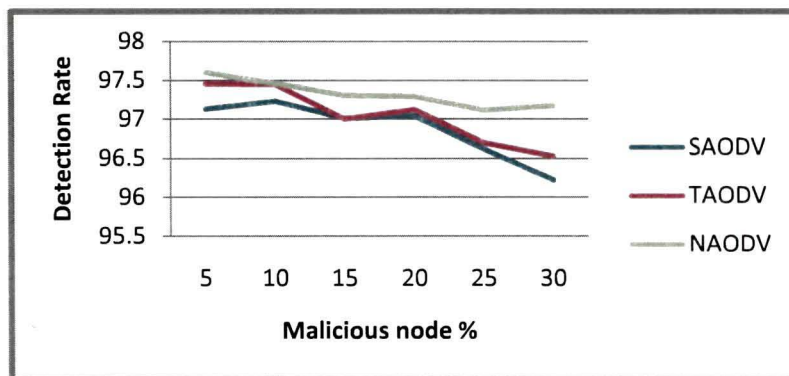


Figure 4.25. Effect of increase of malicious node on detection rate (LWM)

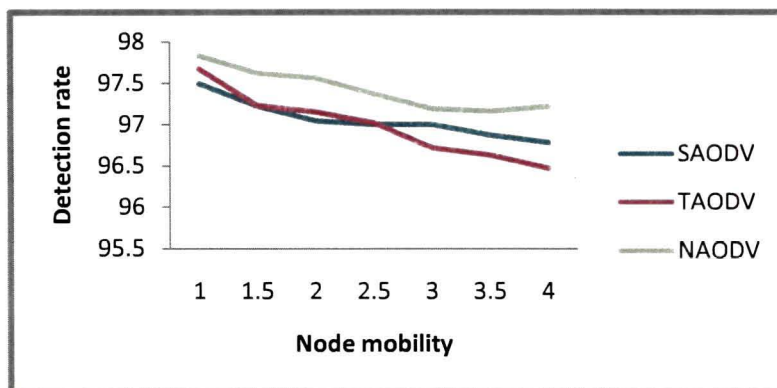


Figure 4.26. Effect of increase of node mobility on detection rate (LWM)

It can be explained by the fact that in NAODV, malicious node detection and avoidance is completely based on cooperation of neighbors. Global decision is taken based on incremental order decision tree algorithm. Accordingly TRUST level of the node is dynamically updated. On the other hand, TAODV is a trusted routing protocol

that cooperates with a self organized key management mechanism. Moreover, it performs trusted routing in a self-organized way. In SAODV, signature is verified by both source node and intermediate node and then only routing table is updated. Malicious node cannot generate signature of destination node, hence it will not be able to impersonate destination node.

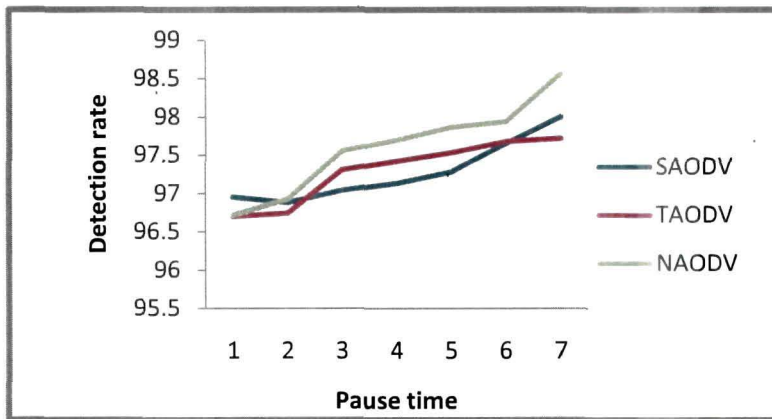


Figure 4.27. Effect of increase of pause time on detection rate (LWM)

4.4.2.2 False Positive Rate (NAODV, SAODV, TAODV)

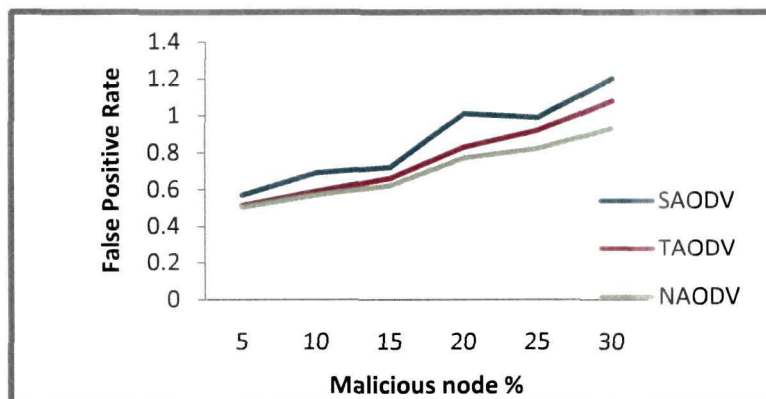


Figure 4.28 Effect of increase of malicious node on false positive rate (LWM)

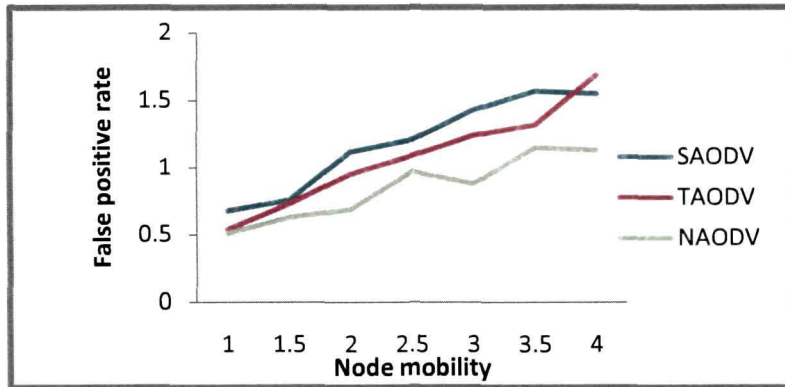


Figure 4.29 Effect of increase of node mobility on false positive rate (LWM)

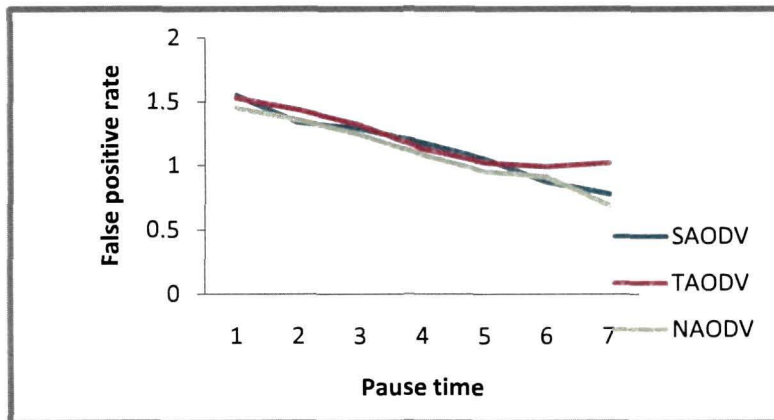


Figure 4.30 Effect of increase of pause time on false positive rate (LWM)

Figure 4.28, Figure 4.29 and Figure 4.30 compare the false positive rate of three different methodologies with respect to increased number of malicious node, increased node mobility and increased pause time. Initially, the false positive rate of TAODV is slightly differed from NAODV, but as the number of malicious node is increasing, false positive rate of TAODV and SAODV is also increasing, it is less in case of TAODV compared to SAODV. Observation from Figure 4.29, it is clear that NAODV shows mixed response with increase node mobility. Still its performance is better. At certain point with high node mobility, false positive rate of TAODV is more than SAODV. But in Figure 4.30, as the pause time is increasing, there is very less difference in performance amongst SAODV, TAODV and NAODV, though at high pause time NAODV shows better performance. SAODV partially resists the DoS

attacks like packet dropping attack. It provides a cryptographic support to secure the routing protocol. Hence It shows vulnerabilities to packet dropping attack. TAODV facilitates trusted routing rather than PDA detection. On the other hand, in NAODV, detection of PDA is based on distributed cooperative way and it generates alarm to avoid the malicious nodes for further packet forwarding after getting confirmation from all neighbors. As a result, false positive rate is comparatively less.

4.4.2.3 Throughput Analysis (NAODV, SAODV, TAODV)

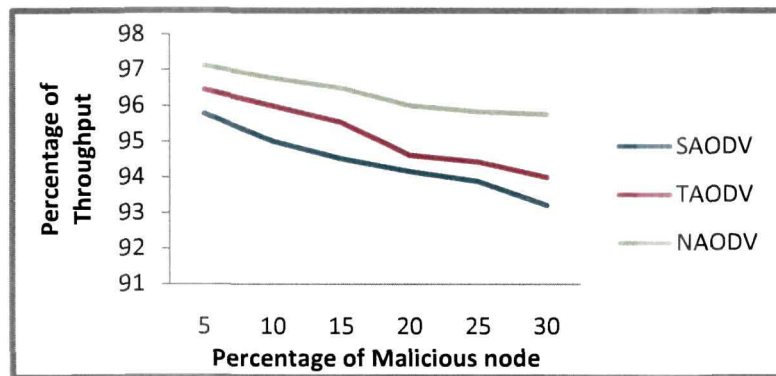


Figure 4.31 Effect of increase of malicious node on throughput (LWM)

Throughput of the network is compared for three methodologies as shown in Figure 4.31, Figure 4.32 and Figure 4.33.

In SAODV, it takes extra time for computation and verification of security fields during route discovery process. It always prefers safest path instead of shortest path. These all consume some extra time. Due to this throughput comes down as it depends on total number of packets delivered in specified time. TAODV also consumes extra time for updating TRUST by evidence & opinion, exchange and authentication. But NAODV doesn't consume much time for route discovery and there is not much complex security measures during route discovery, so it delivers more packets in specified time. This implies more throughputs. When node mobility is high, at some point, throughput of SAODV and TAODV are almost equal but later on during high

node mobility, performance of TAODV becomes better though its performance is quite low in comparison to NAODV.

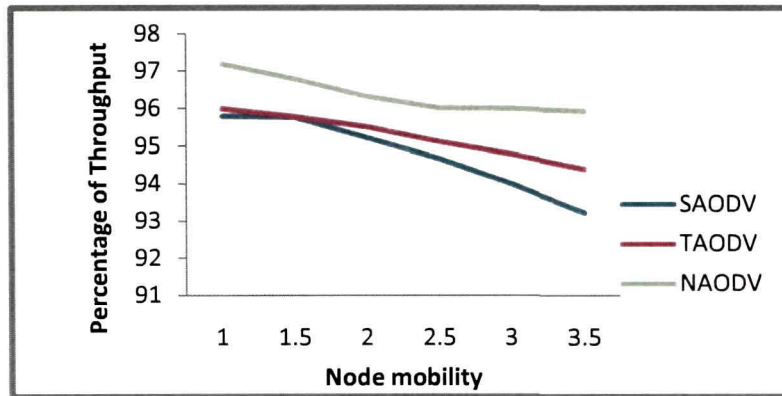


Figure 4.32 Effect of increase of node mobility on throughput (LWM)

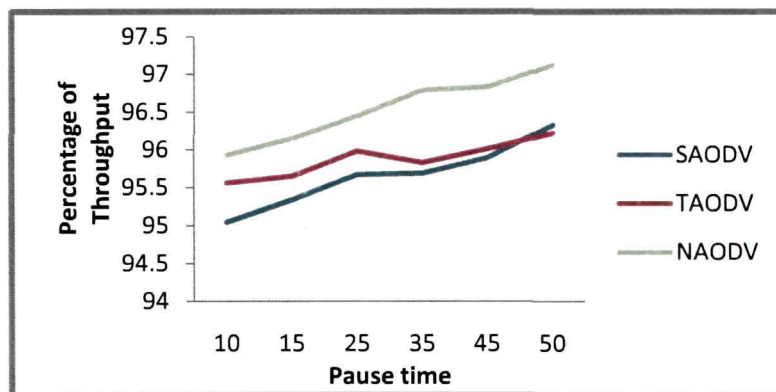


Figure 4.33 Effect of increase of pause time on throughput (LWM)

4.4.2.4 Packet Delivery Ratio Analysis (NAODV, SAODV, TAODV)

Figure 4.34, Figure 4.35 and Figure 4.36, compare the packet delivery ratio of NAODV, SAODV and TAODV.

In all the three cases, NAODV performs the best. NAODV is simply meant for packet dropping attack detection while other two methodologies partially detect PDA. NAODV detects malicious node from the network in cooperative distributed way and

avoid such nodes for packet forwarding. By this it reduces packet drop ratio and oppositely increases packet delivery ratio.

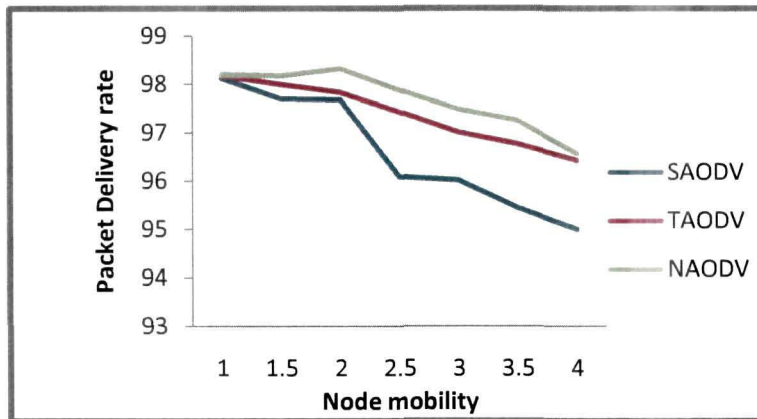


Figure 4.34 Effect of increase of malicious node on packet delivery ratio (LWM)

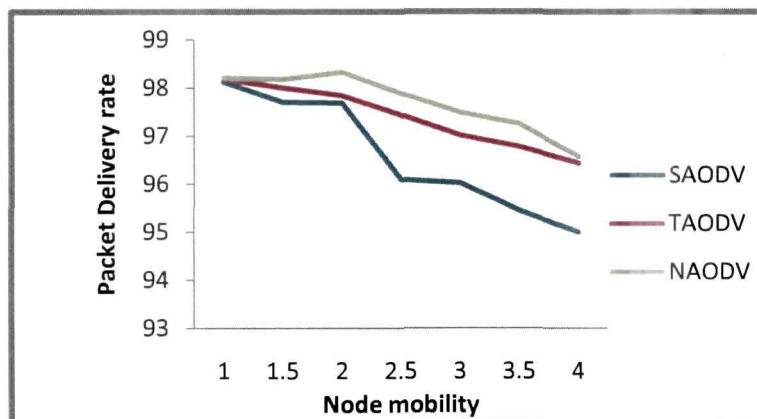


Figure 4.35 Effect of increase of node mobility on packet delivery ratio (LWM)

When the node mobility is higher, it signifies the high failure of connectivity and frequent change of topology. As a result, it drops more packets. Nodes may be falsely accused of malicious. It is more in case of SAODV than TAODV, while less in case of NAODV. SAODV chooses the safest path instead of shortest path and tries to eliminate the malicious nodes in the way, so the average path length is longer. When the node mobility is higher, the network topology breaks down frequently and it is not

be able to deliver the packets on time. Moreover high security application of SAODV resists the path more.

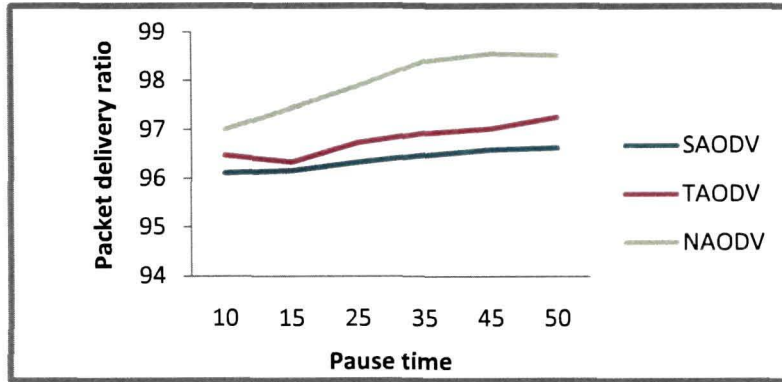


Figure 4.36 Effect of increase of pause time on packet delivery ratio (LWM)

4.4.2.5 Normalized routing load Analysis (NAODV, SAODV, TAODV)

Normalized Routing Load (NRL) is the ratio between total numbers of routing packets to total number of delivered packets. A network contains more malicious nodes means it drops more packets. NRL is inversely proportional to PDR. In presence of malicious node, NAODV shows better performance in comparison to other two methodologies such as SAODV and TAODV as shown in Figure 4.37. Of course at certain point NRL of NAODV and TAODV becomes almost same. But after that NRL of NAODV is getting down irrespective of more malicious node deployment.

In presence of malicious nodes in the network, it forces SAODV to use hash chain and digital signature to provide secure routing process. That leads to less packet delivery ratio, thus it generates more NRL in the network. But in TAODV, system performance is improved in comparison to SAODV by avoiding generating and verifying digital signatures at every routing hop.

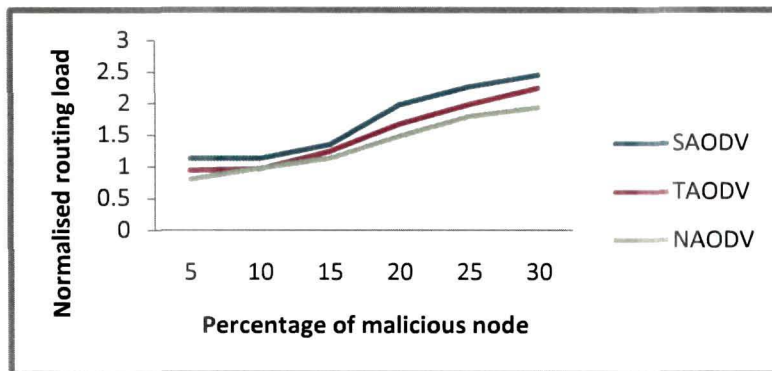


Figure 4.37 Effect of increase of malicious node on normalized routing load (LWM)

According to Figure 4.38, in case of SAODV, NRL is found to be more than that of TAODV and NAODV due to its intensity to find the safest path. During high node mobility, network topology changes frequently. That results in frequent link failure. Network becomes unstable for all the time. As a result, SAODV is unable to find the safe path for routing. PDR is decreasing, thus NRL is increasing. In TAODV, a node does not request and verify certificates continuously. So, computation overhead is reduced greatly in comparison to SAODV. At the same time, TAODV provides security to the system up to certain level, thus it decreases packet delivery ratio to some extent. Due to direct involvement of NAODV for PDA detection and avoidance of malicious node, its packet delivery ratio is higher in comparison to SAODV and TAODV. Thus, it results in low NRL.

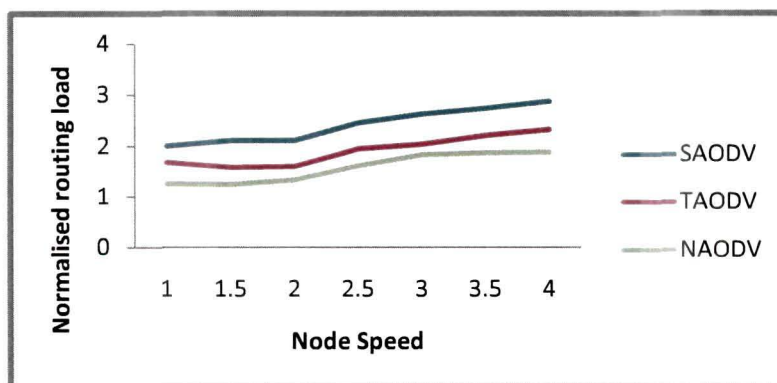


Figure 4.38 Effect of increase of node mobility on normalized routing load (LWM)

According to Figure 4.39, NRL is gradually decreasing in all the three different methodologies as the pause time is gradually increasing. High pause time implies more stable network, which indicate regular and stable behavior of nodes. So, additional packet drop due to highly dynamic node is controlled

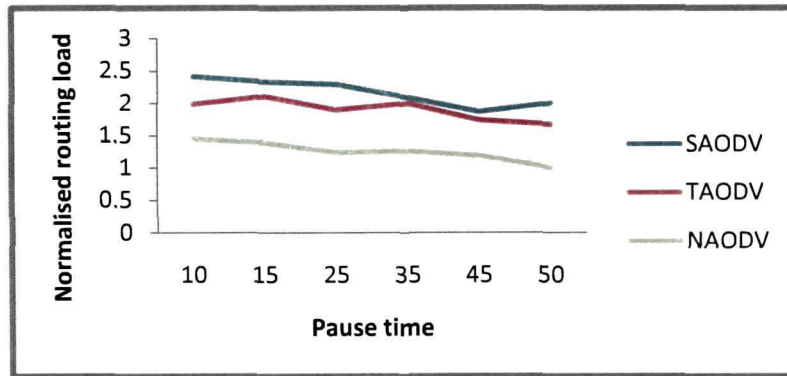


Figure 4.39 Effect of increase of pause time on normalized routing load (LWM)

4.4.2.6 End-to-end Delay Analysis (NAODV, SAODV, TAODV)

In Figure 4.40, it is observed that end-to-end delay is increasing with increased number of malicious nodes in all the three different methodologies. In MANETs, end-to-end delay is the delay encountered by a packet right from the generation of the packet from the source and till it gets back the ACK from destination. The packet delay consists of the queuing delay experienced at the source node, the queuing delays incurred at the intermediate nodes as well as MAC delay observed at the source and intermediate nodes. Presence of increased malicious node in MANETs invariably drops packets. In SAODV, end-to-end delay is gradually increasing with increasing order of malicious node. But, TAODV shows mixed response. At some point, end-to-end delay of NAODV is same as that of TAODV but due to simplicity of operation of NAODV, end-to-end delay is getting down in comparison to TAODV and SAODV.

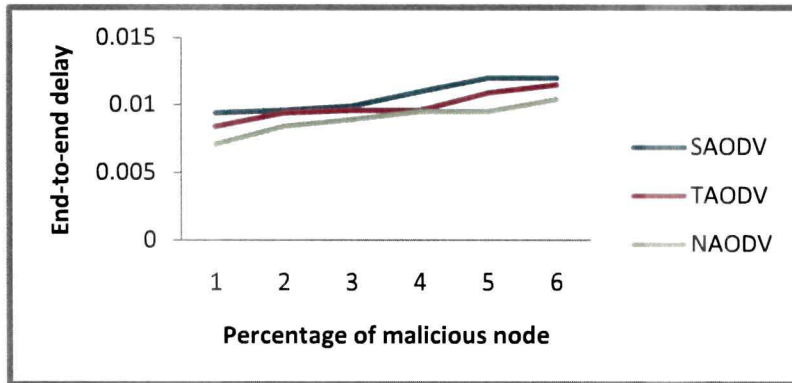


Figure 4.40 Effect of increase of malicious node on end-to-end delay (LWM)

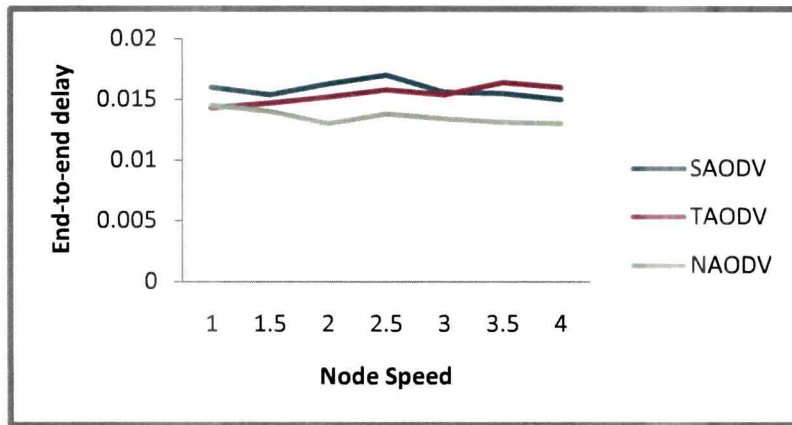


Figure 4.41 Effect of increase of node mobility on end-to-end delay (LWM)

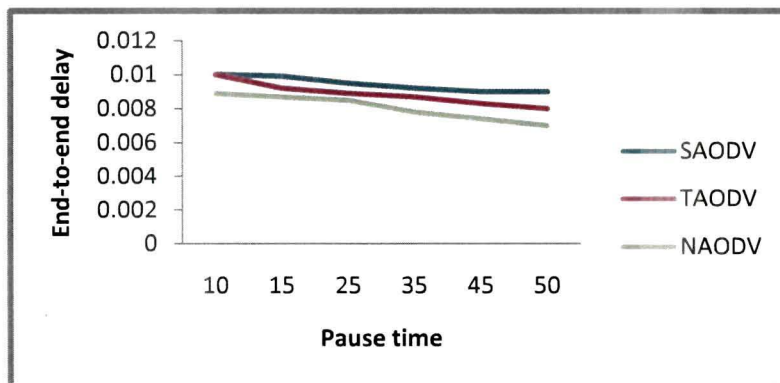


Figure 4.42 Effect of increase of pause time on end-to-end delay (LWM)

In Figure 4.41, in case of high node mobility, with deployment of malicious node, both SAODV and TAODV show the instability in end-to-end delay. Due to dynamic nature of nodes in MANETs, state and characteristics of nodes may change. Nodes can change their characteristic frequently. Thus packets from source to destination may not reach on time or end-to-end delay may increase. Techniques that provide security used by SAODV and TAODV are more complex in comparison to NAODV; it results in high end-to-end delay. On the other hand, NAODV shows almost a stable and low end-to-end delay in spite of high node mobility

In Fig 4.42, when the pause time is more, due to network stability, in all the three cases end-to-end delay is gradually decreasing. Still it is more in case of SAODV and TAODV because of their computational overhead during security measure in packet delivery.

4.4.2.7 Round trip time (NAODV, SAODV, TAODV)

From the Figure 4.43, it is clear that as the number of malicious node is increasing in the network, NAODV consumes less RTT in comparison to other two methodologies. In SAODV, it measures the generation and validation of nodes that switch between signing, verifying and hash chain operations. Each message is validated before any further processing takes place. So, each RREQ and RREP packet is delayed by some amount of time at each hop through which message should be forwarded. When the number of malicious nodes is increasing, due to complex security measures, SAODV takes more RTT in comparison to other two methodologies. TAODV takes comparatively less time. But in TAODV, due to its simplicity in comparison to SAODV, there is much less pre-packet overhead. The main overhead that incurred in TAODV is the overhead related to R ACK packets which is a new kind of packet rather than packet extension.

As in Figure 4.44, when the node speed is increasing with malicious node deployment, RTT is increasing in all the three cases, though it is lowest in case of NAODV. High node mobility is the significance of more unstable network. Due to

frequent breakage of links, packet delivery time also be increases, and thus it takes much time to get ACK packet from destination to source after sending packet from source. On the other hand, in case of SAODV and TAODV, it is affected more because of their complexity in computation.

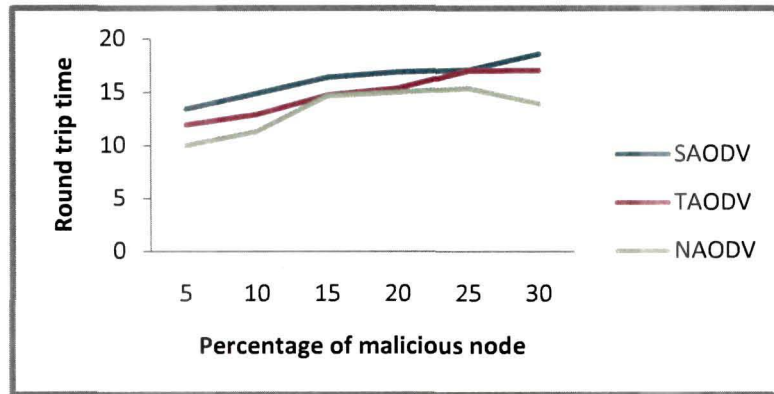


Figure 4.43 Effect of increase of malicious node on round trip time (LWM)

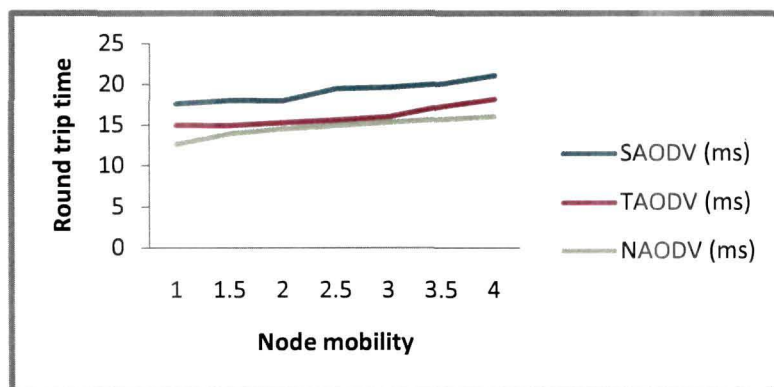


Figure 4.44 Effect of increase of node mobility on Round trip time (LWM)

In Figure 4.45, as the pause time is increasing, for all the three cases, RTT is gradually decreasing. When the pause time in the network is more, it indicates more stable network, thus node characteristics are also remained constant. Probability of frequent link breakage will be low. Packets may deliver to destination on time, source also gets ACK packet on time. Hence, RTT is getting low. In SAODV and TAODV,

it is more than that of NAODV, because of additional time consumption for security measures during packet delivery.

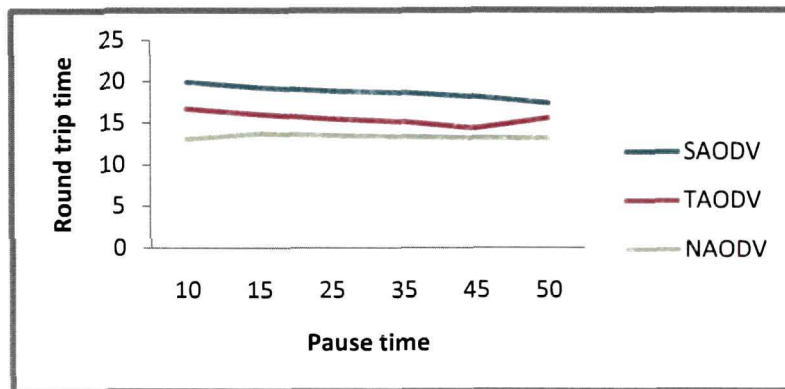


Figure 4.45 Effect of increase of pause time Round trip time (LWM)

4.5 Discussion

From various simulation results for two different mobility models such as *Random way point mobility* model and *Levy walk* mobility model, it is found that distributed PDA detection methodology is more appropriate than centralized PDA detection methodology. Static, offline, centralized PDA detection methodology is not suitable to handle dynamic unstable nodes of MANETs. Distributed cooperative decision making process, dynamic TRUST evaluation of nodes; detection and avoidance of malicious nodes, makes the distributed PDA detection methodology efficient. Different simulation results that is generated for SAODV, TAODV and NAODV, for different network performance parameters, it is found that NAODV shows the best results.

TAODV is a trusted routing protocol with a self organized key management mechanism that follows the self organized way. SAODV indirectly handles PDA by providing cryptographic support to secure the routing protocol. NAODV detects PDA in distributed cooperative way. After confirmation of PDA, it generates alarm to the system to avoid malicious nodes from further communication. For computation and verification of security fields, SAODV takes some extra time to discover route and

deliver packets to destination. TAODV also needs some extra time for TRUST updates by evidence and opinion, exchange and authentication. NAODV computes and updates TRUST dynamically for PDA detection purpose and it doesn't consume much time for route discovery and there is a not much complex security measure during route discovery so it delivers more packets in specified time.

High node mobility signifies the high failure of connectivity and frequent change of topology. Nodes may be falsely accused of malicious. From results, it is confirmed that it is more in SAODV and TAODV in comparison to NAODV.

SAODV uses the hash chain and digital signature to provide secure routing process. But the other two methodologies avoid generating and verifying digital signature at every routing hop.

Performance of all the three different methodologies degrade in case of increased node mobility, while it upgrades during increased number of pause time. It is because of the unsteadiness of the network during high node mobility and stability of the network during high pause time. Performance of NAODV is still better in comparison to the other two methodologies, because of simplicity of computation and dedication of service for PDA detection.

Chapter 5

Game Theoretic Approach

5.1 Introduction

In chapter 4, from various simulation results it is clear that distributed packet dropping attack detection methodology (NAODV) is an efficient method to detect and isolate malicious packet dropping in MANETs. But to remove some of the arbitrariness of this methodology, game theoretic approach to distributed packet dropping attack detection methodology is proposed.

As mentioned in section 2.4, the concept of game theory can be applied. It deals with strategic interactions among the different players of the game [138]. Each player tries to maximize the utility of the game based on own concept. Performance of MANETs is dependent on node cooperation. MANETs node must cooperate with each other to accomplish certain goal. Thus, malicious nodes that maliciously drop packets introduce several problems to MANET. Specifically it degrades network performance in terms of performance parameters such as throughput and packet delivery ratio of the network.

In this work, MANETs is assumed as game space, in which one side of the game is occupied by coalition of genuine node and other side of game is occupied by attacker i.e. malicious nodes which invariably drop packets.

Node cooperation is the most desirable property of MANETs to communicate amongst them. Non cooperative nodes create anomalies to the network. So, formulating MANETs as cooperative game increases the utility of the network by restricting the non cooperative malicious nodes. Cooperative game theory deals with the formation of cooperative group which is known as coalition. By this each player

can strengthen their position by cooperative participation in the game and thereby increasing overall utility of the coalition. Two main parameters of coalition game theory, namely value of a coalition and payoff received by a player, are shown very distinctly in the proposed methodology. Here, payoff received by independent players are represented by *trust* value assigned to the players depending on their cooperation. This approach in proposed methodology is a kind of non-transferable utility game as the *payoff* i.e. *trust* obtained by each player under coalition is not distributed to other nodes in the coalition. As a result, it encourages the nodes to show their cooperation for their existence in the coalition. Otherwise, if their *trust* value falls below threshold *trust*, then these will be splitted from coalition.

Packet dropping attacks by malicious nodes can be detected using a distributed PDA detection technique as discussed in Chapter 4. However, the efficacy of the detection performance can be further improved with a framework of interaction among the nodes in the network, which can be formulated using a game theoretic model. Here, for the sake of simplicity, we assume that there is a set of malicious nodes in the network which try to disrupt the network operations by dropping packets which otherwise are supposed to be forwarded by them towards the destinations. In order to mitigate this type of unexpected behavior of the network, the genuine nodes will try to form coalitions among themselves. The Goal of coalition formation by genuine nodes is to increase the network utility by detecting the malicious nodes which launch attacks to decrease the network utility in terms of data rate. Here, we assume that the term genuine node represents node which behaves in trustworthy way within the network.

Depending on the stated problem, the formation of coalition occurs with following mechanism:

- Initially each individual node is a single node coalition (termed as singleton coalition).
- Each coalition performs merge operation with other coalitions. The merge operation will take place with either non-singleton coalitions (i.e. coalition

having more than one genuine node and utility greater than zero) or other singleton coalitions to form a larger coalition whereby improving the utility provided taking a decision about malicious behavior of a node.

It is assumed that the nodes in the network acquire the initial trust value computed by distributed PDA detection methodology as discussed in the Chapter 4.

5.2 Game Model

The proposed problem can be modeled using game theory as a coalitional game with non-transferable utility as each of the players (node) has their own utility in terms of the initially assigned trust value to them. Let the game for malicious node detection be represented by $G = \langle N, V \rangle$, where N is the set of nodes and V is the characteristic function devised by the utility of the game.

Let N be the numbers of nodes in a coalition S and T be the trust value of the node. We assume that each of the nodes in a coalition maintain two vectors that are described below.

- a. Each node $i \in S$, maintains a vector of trust values denoted by symbol $Z_{i,T}$ which consists of addresses of all other nodes and their corresponding trust values with respect to node i and can be given by,

$$Z_{i,T} = \{(j, T_j)\} \forall j \in S, j \neq i \quad \text{----- (1)}$$

where,

j = represents id of j^{th} node in the coalition S

T_j = represents the trust value of j^{th} node with respect to i^{th} node

For example, for a coalition S of size m , the vector can be represented as follows,

$$U = \{Z_{1,T}, Z_{2,T}, \dots, Z_{m,T}\}, \text{ where } Z_{i,T} = \{(j, T_j)\} \forall j \in S, j \neq i$$

- b. Each node $i \in S$ maintains a vector of suspected node denoted as $E_{i,T}$ which consists of address of the nodes and corresponding trust values and can be given by

$$E_{i,T} = \{(j, T_j)\} \text{ where node } j \text{ is suspected as malicious and } j \in S \quad \text{----- (2)}$$

The purpose of keeping the vector $E_{i,T}$ is that if the network utility is degraded, the game will first determine the behavior of nodes available in $E_{i,T}$ in order to detect the malicious nodes. Otherwise it consumes more network resources including bandwidth, computational cost, time etc.

5.3 The proposed framework

- Any node, that wants to join in genuine node coalition, will broadcast its *trust* value. The *trust* value of a new node will be verified against a threshold *trust* value denoted by T_{TH} , which is computed dynamically by averaging the *trust* values of the genuine nodes within the coalition. If it is within the range of T_{TH} , then it allows the node to be a part of coalition. All the nodes in the network will update their *trust* vector by an entry containing new node's address and its *trust* value.
- In a stable coalition S if any node $k \in S$ suspects any other node $l \in S$ as malicious then
 - node k broadcasts a message to all other nodes of coalition S asking about latest trust value of the suspected node l .
 - All other nodes of coalition S i.e. $\forall i \in S, i \neq l, i \neq k$ reply with the latest trust value of the suspected node l to the node k .
 - Then node k receive all the reply and generate a temporary opinion vector $O_{k,T}$, given by

$$O_{k,T} = \{(l, T_{i,l})\}, \quad \forall i \in S, i \neq l, i \neq k, l \in S$$
 where
 $l =$ Suspected node
 $T_{i,l} =$ represent the *trust* value of the suspected node computed by the i^{th} node in the coalition S .

- node k recomputes the *trust* value of suspected node l by taking average of *trust* from $O_{k,T}$. i.e.

$$T_{k,l} = \frac{\sum_{i=j}^S T_{i,l}}{|O_{k,T}|} \quad \forall j \in S, j \neq l, j \neq k$$

- If the newly computed *trust* value i.e. $T_{k,l}$ for the suspected node is less than the T_{TH} , then the suspected node will be split out from the coalition and marked as malicious.
- But if $T_{k,l}$ greater than or equal to T_{TH} , then node k computes network utility according to equation (3) given below. If it finds that network utility is within desirable range then it assumes that suspected node may be a malicious or may not be malicious. At this point, the suspected node will remain in the coalition because it may happen that the *trust* value of node l is degraded due to packet loss or so other than malicious packet dropping such as network congestion etc. But node k makes an entry for node l on its suspected node vector $E_{k,T}$.
- At any time, if the network utility is degraded then a message with an alert is broadcasted in the network to compute *trust* value of all the nodes available in suspected node vector $E_{i,T}, \forall i \in S$ independently. Then all nodes share the newly computed *trust* value for the suspected nodes available in their corresponding suspected node vectors. From the shared *trust* value, a decision will be taken by computing the average of the value of the suspected node.
- If it finds that for any suspected node, the newly computed *trust* value is less than T_{TH} , then it splits the node from the coalition. Otherwise it merges the node into coalition by removing its entry from suspected node vector $E_{i,T}, \forall i \in S$.

5.4 Design of Utility function

Average utility per node in a coalition can be given by the following utility function

$$V(S) = f(T, C) \text{-----(3)}$$

Where $f(T, C) = \sum_{i=1}^{|S|} v(n_i)$. The $v(n_i)$ represent the utility of the i^{th} node in the coalition S which is given by following equation,

$$v(n_i) = T_{avg, i} * C \text{-----(4)}$$

Where, $T_{avg, i}$ is the average of *trust* value of the *trust* vector $Z_{i,T}$ for the node $i, i \in S$ and C represents the capacity of the channel given by the Shannon's formula $C = B \log_2 (1 + SNR)$ where B is the bandwidth of the channel (which is considered as uniform for all nodes during a time frame in the network) and SNR is the Signal to Noise ratio (which is also considered as constant for the network).

5.5 Coalition stability

The stability of the proposed game G can be achieved while the coalition formation occurs according to Pareto order condition.

5.6 Definition of Pareto order[192]

Consider two collections of coalitions $\hat{R} = \{R_1, \dots, R_l\}$ and $\hat{S} = \{S_1, \dots, S_m\}$ that are partitions of the same subsets $A \subseteq \mathcal{K}$ (same player in \hat{R} and \hat{S}). For a collection $\hat{R} = \{R_1, \dots, R_l\}$, let the utility of a player j in a coalition $R_j \in \hat{R}$ be denoted by $\phi_j(\hat{R}) = \phi_j(R_j) \in V(R_j)$. \hat{R} is preferred over \hat{S} by Pareto order, written as $\hat{R} \triangleright \hat{S}$, iff

$$\hat{R} \triangleright \hat{S} \Leftrightarrow \{\phi_j(\hat{R}) \geq \phi_j(\hat{S}) \forall j \in \hat{R}, \hat{S}\}$$

with at least one strict inequality ($>$) for a player k .

5.7 Coalition rules

The game has two operations *merge* and *split* for formation of coalition.

Merge: Two coalitions with situations, non-singleton and non-singleton, non-singleton and singleton, singleton and singleton, singleton and non-singleton etc. may

form a larger coalition through merge if the average utility per node of the newly formed coalition is greater than or equal to either of the two participant component coalitions. Suppose two coalition S_i and S_j merge to form a larger coalition $S_{i,j}$ iff

$$S_{i,j} \triangleright S_i \text{ and } S_{i,j} \triangleright S_j \text{ which yield } \{S_i, S_j\} \rightarrow S_{i,j}$$

Split: A large coalition may split into smaller ones if the average utility of the newly formed coalitions through split is greater than the initial larger coalition. Suppose a large coalition $S_{i,j}$ splits into one small sub non-singleton coalition S_i and one singleton coalition S_j iff

$$S_i \triangleright S_{i,j} \text{ which yield } S_{i,j} \rightarrow \{S_i, S_j\}$$

Property 1: The game has non-transferable utility

Proof: Each node within the coalition S has its own trust vector which contains the trust values of all the other node of the coalition S . Also each node has its own utility according to its trust values. Since the value of trust vector and the utility of each individual node cannot be arbitrarily distributed among the other nodes in the coalition; the proposed game has a non-transferable utility.

5.8 Stability condition

A non-singleton coalition is said to be stable if it consists of only genuine node with maximum trust value having optimum utility within a desirable range and no-more split operation is required.

Algorithm 5.1: Coalition Based Malicious Node Detection (CBMND) algorithm.

Input: T of N nodes

Output: Coalition of genuine node

1. **for all** (i in N) **do** { * N is the number of nodes in the network* }
2. $S_i = i$ { * S_i is a singleton coalition with node i 's individual trust value* }.
3. node i computes $Z_{i,T}$ and $E_{i,T}$ { * $Z_{i,T}$ contain trust values of all $N-1$ nodes with respect to node i and $E_{i,T}$ contain the ids of the suspected nodes* }
4. **end for**
5. **for all** (i, j in N) **do**

6. **if** ($T_i > T_{TH}$) **then** { $*$ T_{TH} is the threshold trust value and T_i is the trust value of node i }
7. goto step 11.
8. **else**
9. Node i will not be allowed to take part in coalition.
10. **end if**
11. Merge: **if** ($V(S_{i,j}) \geq S_i$) and $V(S_{i,j}) \geq V(S_j)$) **then**
12. Two coalitions S_i and S_j merges to form a large coalition $S_{i,j}$.
13. **end if**
14. **end for**
15. **do**
16. **if** ($V_{i2}(S_j) \leq V_{i1}(S_j)$) **then** { $*$ $V_{i1}(S_j)$ and $V_{i2}(S_j)$ represents utility of coalition S_j at time $t1$ and $t2$ respectively } }
17. node i verifies the entry in $E_{i,T}$ to find out the suspected nodes.
18. Split: **if** ($V(S_{i,k}) \geq V(S_{i,k,j})$) **then** { $*$ it will check if the removal of suspected node increase the utility of coalition then split operation is performed to split the coalition in order to remove malicious node }
19. A coalition $S_{i,j,k}$ splits into coalition $S_{i,k}$ and S_j . i.e. the node j has been removed from the coalition $S_{i,j,k}$.
20. update $Z_{i,T}$ and $E_{i,T}$ accordingly.
21. **end if**
22. **end if**
23. **until** coalition become stable.

5.9 Simulation and results

We use MATLAB 2010b for the simulation and analysis of the proposed game model. The parameters those are used during simulation are listed in the table below.

Parameter	Value
SNR (Signal to Noise ratio)	10 dB
C (capacity of channel)	20 Hertz

For simulation, we have assumed that each and every single node in the network has been assigned a *trust* value by the distributed PDA detection methodology as in Chapter 4. We assumed that the trust value for the genuine node ranges from 0.8 to 0.95 and for a malicious its ranges from 0 to 0.8. To perform simulation, we generate trust vector for all the genuine nodes and malicious node randomly depending upon their ranges.

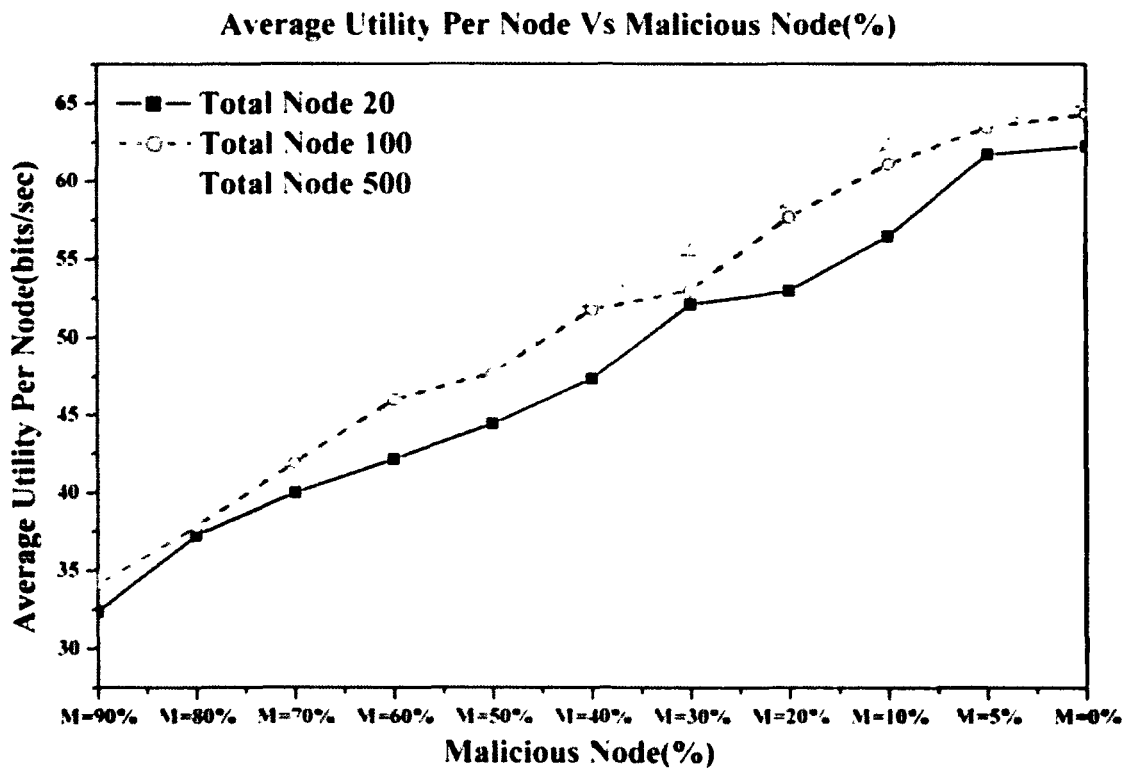


Figure 5.1: Average Utility Per Node vs. Malicious Node (%)

The Figure 5.1, plots the scenario of Average Utility Per Node versus Malicious node (%). The graph shows the percentage of malicious nodes in the X-axis and Average Utility per node along Y-axis. Simulation is performed for three different type of networks: small scale, medium scale and large scale network having total number of node equal to 20,100 and 500 respectively. From the Figure 5.1, it has been observed that how the elimination of malicious node within the coalition increases the utility significantly.

The Figure 5.2, plots the scenario of Average Utility per node versus Number of Malicious node (M). Malicious nodes are plotted along X-axis and Average Utility per node are plotted along Y-axis. Initially, it is assumed that there are 15 nodes in the coalition out of which 10 nodes are genuine and 5 nodes are malicious. From the Figure 5.2, it has been observed that the proposed game model detects the malicious node and split it out from the coalition which eventually increases the average utility per node of the coalition. It has also been observed that after detection and removal of all malicious nodes from the coalition, the utility reach to a optimum and stable range for that coalition since the coalition contain only genuine node.

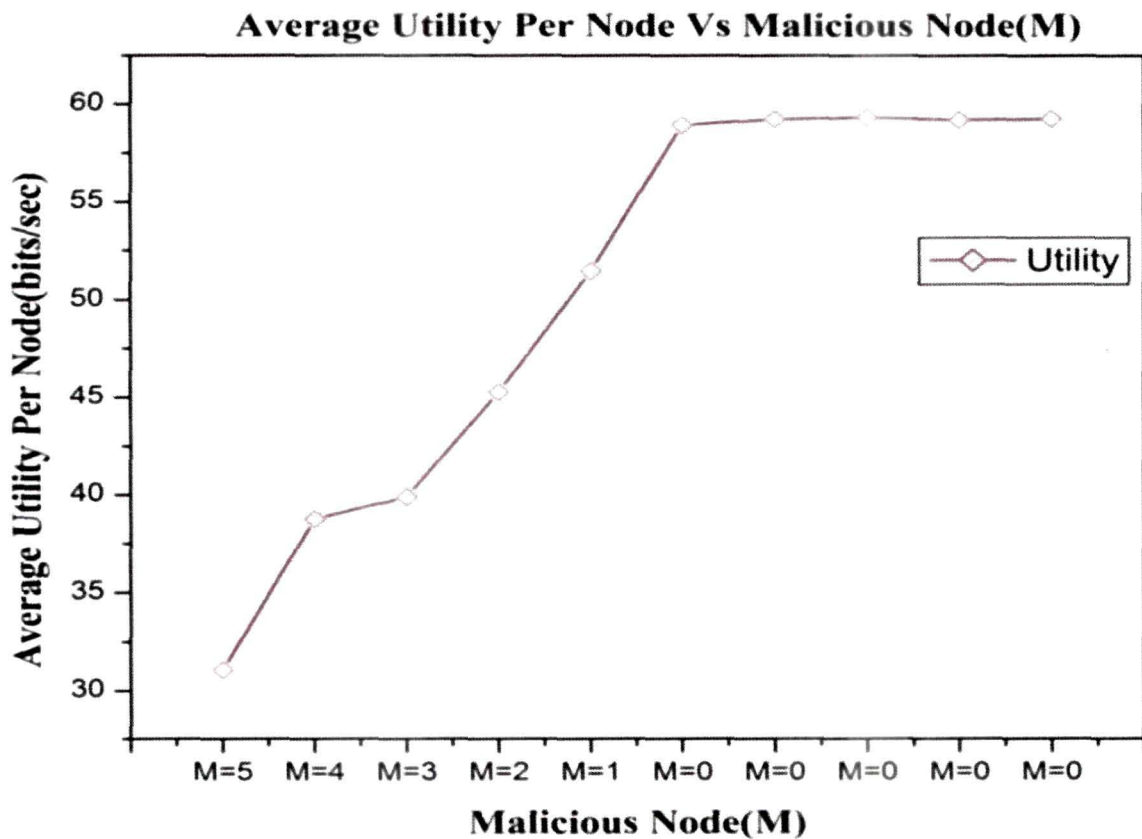


Figure 5.2 Average Utility per node vs. Number of Malicious node (M)

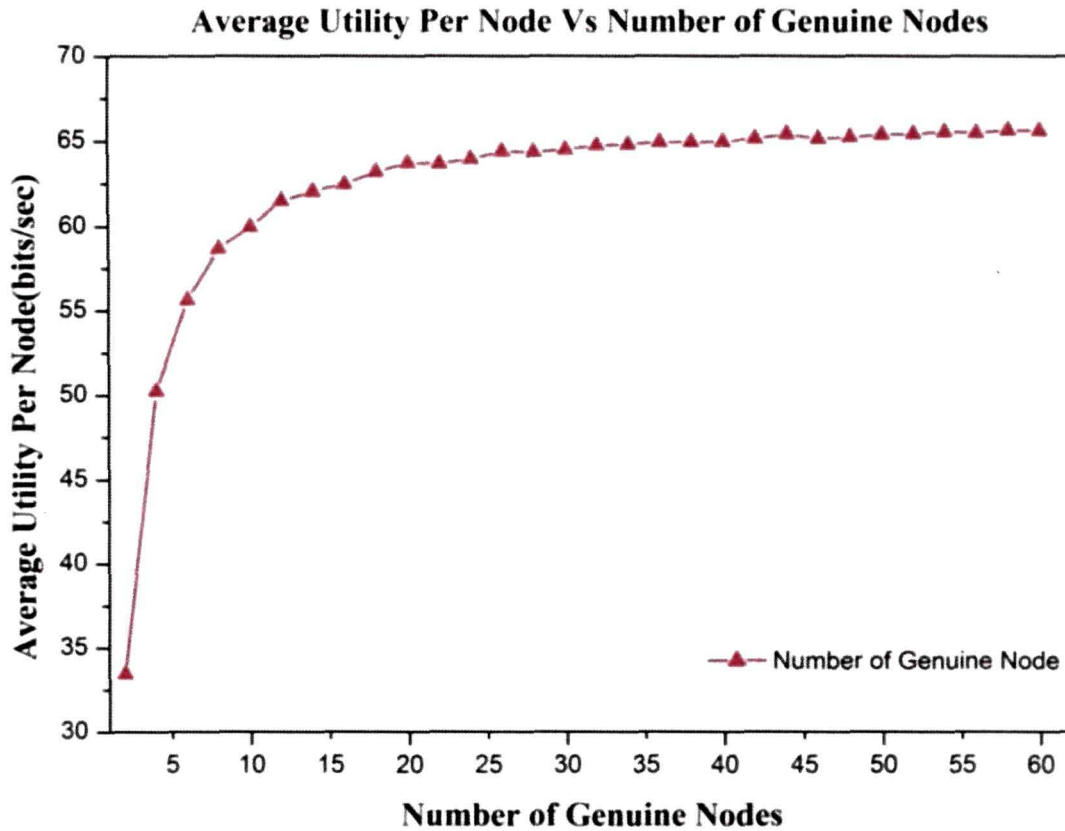


Figure 5.3 Average Utility Per Node vs. Number of Genuine Nodes

Figure 5.3, plots the scenario of Average Utility Per Node versus Number of Genuine Nodes. Genuine nodes are plotted along X-axis and Average Utility per node are plotted along Y-axis. Initially, it is assumed that there are only 2 nodes in the coalition. From the Figure 5.3, it has been observed that the increasing number of genuine node within a coalition increases the average utility of that coalition. From the same figure, it can also be observed that after a sufficient number of genuine node within a coalition, the utility of the coalition reaches to an optimum and stable range.

5.10 Discussion

The proposed methodology is an approach to detect malicious nodes, which are responsible for PDA, from MANETs by game theoretic approach. Here, all the genuine nodes in the network form a coalition to detect and avoid malicious nodes and thereby increase the average utility per node. All the nodes inside the coalition try to increase their *trust* value by their participation in the network communication. If the *trust* value of any node goes below the threshold *trust* value, then such kind of node is spilt out from the coalition. Evaluation of threshold *trust* value itself is a dynamic process. Predefined static *trust* value may sometimes create some arbitrariness to the methodology by increasing false positive rate of the detection methodology.

Simulation has been done for three different scenarios. Elimination of malicious node within the coalition increases the utility significantly. The proposed game model detects the malicious node and split it out from the coalition which eventually increases the average utility per node of the coalition. It has also been observed that after detection and removal of all malicious nodes from the coalition, the utility reach to a optimum and stable range for that coalition since the coalition contain only genuine node. Genuine node within a coalition increases the average utility of that coalition. It is also be observed that after a sufficient number of genuine nodes within a coalition, the utility of the coalition reaches to an optimum and stable range.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

This dissertation has primarily focused on detection of packet dropping attack (PDA) in MANETs and many aspects concerning PDA in MANETs has been investigated. Consequently, the thesis makes three contributions for detection of packet dropping attack (PDA) in MANETs namely, centralized packet dropping attack detection methodology, distributed packet dropping attack detection methodology and game theoretic approach to distributed packet dropping attack detection. In this chapter, we summarize the main contribution made in this dissertation and provide direction for future works.

6.1.1 *Centralized PDA Detection*

As security is a vital part in the MANET and is often very cumbersome. In Chapter 3 we have proposed a centralized packet dropping attack detection methodology in order to detect the PDA centrally. In this methodology, each node in the network provides its gathered information to a central entity in the network. The central entity analyzes the information received from the nodes individually in order to detect the PDA at a particular node. From the extensive simulation results that are illustrated in Chapter 3, it has been observed that, the performance significantly degrades when the node mobility in a network is quite high. The system gets initialized for every change in the network topology. Thus the proposed methodology is incapable of detecting

PDA in highly dynamic networks like MANET. Failure of the central entity will lead to the failure of the whole network as well.

6.1.2 *Distributed PDA Detection*

Centralized packet dropping attack detection methodology is incapable of detecting PDA in highly dynamic networks. In Chapter 4, we have proposed a distributed PDA detection methodology based on cooperative participation of nodes in MANETs. In distributed PDA detection methodology, PDA at a node is detected and confirmed by not only using the node's information but also from the information received from its neighbors. It is assumed that intelligent agents are supposed to adapt decision making by cooperation with other nodes in the network. Here, TRUST and CONFIDENCE level of nodes are utilized along with an efficient decision tree algorithm namely; ID5R to handle the dynamic network information to detect PDA in MANETs. From the simulation results, it has been observed that the proposed distributed methodology outperforms the centralized PDA detection methodology in terms of accuracy in detecting and segregating the malicious nodes in MANETs.

6.1.3 *Game Theoretic Approach*

To eliminate the arbitrariness in distributed PDA detection methodology, game theoretic based distributed PDA detection methodology has been proposed in Chapter 5. In MANETs, node cooperation is the most desirable property to communicate amongst them. As the non cooperative nodes create anomalies to the network, hence, MANETs has been formulated as cooperative game to increase the utility of the network by restricting the non cooperative malicious nodes. Coalition is formed by all the genuine nodes. Thereby, each player in the coalition tries to strengthen their position by cooperative participation in the game to increase the overall utility of the network. Value of a coalition and payoff received by a player, the main parameters of coalition game theory, are shown very distinctly in the proposed methodology. Here, payoff received by independent players are represented by *trust* value assigned to the players depending on their cooperation.

This approach in proposed methodology is a kind of non-transferable utility game as the *payoff* i.e. *trust* obtained by each player under coalition is not distributed to other nodes in the coalition. Thereby, it encourages the nodes to show their cooperation for their existence in the coalition. Otherwise, if their *trust* value falls below threshold *trust* , then these will split out from coalition.

6.2 Future Research Direction

In this section, we outlined some of the possible avenues for future research works in this field of research. Few of the research directions are listed below:

- The performance of the proposed distributed PDA detection methodology under various networking environments are evaluated using Network Simulator 2 (NS-2). Performance evolution of the proposed methodology in a real time network setup is left as a part of future works.
- The Utility characteristic function of the game theoretic approach based distributed PDA detection methodology has been investigated in a simplified way. Incorporation of other parameters like residual energy of a node, computational overhead and different mobility models needs further investigation, which is left as a part of future works.
- The proposed methodologies are mainly concerned in dealing with malicious nodes in the MANET only. Further enhancing methodologies in order to efficiently detect the selfish nodes in the MANET is also left as a part of the future works.
- In our work, it presumed that the malicious nodes introduce the attack individually. Hence, schemes to deal with cooperative malicious coalition packet dropping attack is yet to be investigated and left as a part of future works.

Appendix A

Network Simulator 2

A.1 Introduction

NS (Version 2) is an open source network simulation tool. It is an object oriented, discrete event driven simulator written in C++ and Otcl. The primary use of NS is in network research to simulate various types of wired/wireless local and wide area networks; to implement network protocols such as TCP and UDP, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and many more.

Ns2 is written in C++ and Otcl to separate the control and data path implementations. The simulator supports a class hierarchy in C++ (the compiled hierarchy) and a corresponding hierarchy within the Otcl interpreter (interpreted hierarchy).

In ns2, C++ is used for detailed protocol implementation and in general for such cases where every packet of a flow has to be processed. Using C++ , any one can implement new queuing discipline. Otcl is suitable for configuration and setup. Otcl runs quite slowly, but it can be changed very quickly making the construction of simulations easier. In ns2, the compiled C++ objects can be made available to the Otcl interpreter. The ready-made C++ objects can be controlled from the OTcl level.

Some of the important classes are:

The Class Tcl contains the methods that C++ code will use to access the interpreter. The class Tcl encapsulates the actual instance of the OTcl interpreter, and provides the methods to access and communicate with that interpreter.

The class provides methods for the following operations:

- obtain a reference to the Tcl instance;
- invoke OTcl procedures through the interpreter;
- retrieve, or pass back results to the interpreter;
- report error situations and exit in an uniform manner; and
- store and lookup “TclObjects”.
- acquire direct access to the interpreter

Class TclObject is the base class for most of the other classes in the interpreted and compiled hierarchies. Every object in the class TclObject is created by the user from within the interpreter. An equivalent shadow object is created in the compiled hierarchy. The two objects are closely associated with each other.

The class TclClass defines the interpreted class hierarchy, and the methods to permit the user to instantiate TclObjects.

This compiled class (class TclClass) is a pure virtual class. Classes derived from this base class provide two functions: construct the interpreted class hierarchy to mirror the compiled class hierarchy; and provide methods to instantiate new TclObjects. Each such derived class is associated with a particular compiled class in the compiled class hierarchy, and can instantiate new objects in the associated class.

The class TclCommand is used to define simple global interpreter commands. This class provides just the mechanism for *ns* to export simple commands to the interpreter, that can then be executed within a global context by the interpreter. There are two functions defined in `~ns/misc.cc`: `ns-random` and `ns-version`. These two functions are initialized by the function `init_misc (void)`, defined in `~ns/misc.cc`; `init_misc` is invoked by `Tcl_AppInit(void)` during startup.

The class EmbeddedTcl contains the methods to load higher level built in commands that make configuring simulations easier. *ns* permits the development of functionality in either compiled code, or through interpreter code, that is evaluated at initialization. As example, the scripts `~tclcl/tcl-object.tcl` or the scripts in `~ns/tcl/lib`. Such loading and evaluation of scripts is done through objects in the class EmbeddedTcl.

The class `Inst Var` contains methods to access C++ member variables as OTcl instance variables.

This class defines the methods and mechanisms to bind a C++ member variable in the compiled shadow object to a specified OTcl instance variable in the equivalent interpreted object. The binding is set up such that the value of the variable can be set or accessed either from within the interpreter, or from within the compiled code at all times

A.2 NS 2 for Wireless Network

NS 2 can be used to simulate wireless ad hoc network. A mobile node consists of network components like Link Layer (LL), Interface Queue (IfQ), MAC layer, the wireless channel nodes transmit and receive signals from etc.

nam is used to visualize the following output of a wireless network script,

- Mobile node position
- Mobile node moving direction and speed
- Control the speed of playback

A Simple wireless example in NS 2 is given below,

```
#Define Global Variables
```

```
set ns_ [new Simulator]
```

```
# Create a topology
```

```
set topo [new Topography]
```

```
# Define area 670x670
```

```
$topo load_flatgrid 670 670
```

```
#Define standard ns/nam trace
```

```
set tracefd [open 694demo.tr w]
```

```
$ns_ trace-all $tracefd
```

```
set namtrace [open 694demo.nam w]
```

```
$ns_ namtrace-all-wireless $namtrace 670 670
```

```
#Create "God"
```

#God is used to store an array of the shortest number of hops required to reach from one node to another.

```
set god_ [create-god 3]
```

#Define how a mobile node should be created

```
$ns_ node-config -adhocRouting DSDV\  
    -llType LL \  
    -macType Mac/802_11\  
    -ifqLen 50 \  
    -ifqType Queue/DropTail/PriQueue \  
    -antType Antenna/OmniAntenna \  
    -propType Propagation/TwoRayGround \  
    -phyType Phy/WirelessPhy \  
    -channelType Channel/WirelessChannel \  
    -topoInstance $topo  
    -agentTrace ON \  
    -routerTrace OFF \  
    -macTrace OFF
```

#Create a mobile node and attach it to the channel

```
set node [$ns_ node]
```

Disable random motion

```
$node random-motion 0
```

#Use “for loop” to create 3 nodes

```
for {set i < 0} {$i<3} {incr i} {  
    set node_($i) [$ns_ node]
```

#Define node movement model

```
source movement-scenario-files
```

#Define traffic model

```
source traffic-scenario-files
```

```

#Define node initial position in nam
    for {set i 0} {$i < 3 } { incr i} {
        $ns_ initial_node_position $node_($i) 20

#Simulation stop time
    $ns_ at 200.0 "$ns_ nam-end-wireless 200.00"
#Start simulation
    $ns_ at 200.00
    $ns_ halt
    $ns_ run
#Mobile Movement Generator
    setdest -n <num_of_nodes> -p pausetime -s <maxspeed> -t <simtime> -x
    <maxx> -y <maxy>
#Random movement
    $node start
    Source: See ns-2/indep-utils/cmu-scen-gen/setdest/
#Generating traffic pattern files
#CBR traffic
    ns cbrgen.tcl [-type cbf[tcp]] [-nn nodes] [-seed seed] [-mc connections] [-rate]
#TCP traffic
    ns tcpgen.tcl [-nn nodes] [-seed seed]

```

A.3 Running A New Routing Protocol

A new routing protocol for ns-2 has to be coded in C/C++. The output for this file can be incorporated into the simulator by specifying the file name in the Makefile and building ns-2 again. If the routing protocol involves a different packet format than what is defined in packet.h, this must also be specified in the header file.

Post Analysis

Post analysis is one of the important steps to analyze. After the simulation, it gives the trace file which contains the packet dump from the simulation. The format of this trace file for ad hoc wireless networks is as follows:

- N: Node Property
- I: IP Level Packet Information
- H: Next Hop Information
- M: MAC Level Packet Information
- P: Packet Specific Information

Event	Abbreviation	Flag	Type	Value
Wireless Event	s: Send r: Receive d: Drop f: Forward	-t	double	Time (* For Global Setting)
		-Ni	int	Node ID
		-Nx	double	Node X Coordinate
		-Ny	double	Node Y Coordinate
		-Nz	double	Node Z Coordinate
		-Ne	double	Node Energy Level
		-NI	string	Network trace Level (AGT, RTR, MAC, etc.)
		-Nw	string	Drop Reason
		-Hs	int	Hop source node ID
		-Hd	int	Hop destination Node ID, -1, -2
		-Ma	hexadecimal	Duration
		-Ms	hexadecimal	Source Ethernet Address

		-Md	hexadecimal	Destination Ethernet Address
		-Mt	hexadecimal	Ethernet Type
		-P	string	Packet Type (arp, dsr, imep, tora, etc.)
		-Pn	string	Packet Type (cbr, tcp)

Depending on the packet type, the trace may log additional information. The trace file is used to analyze different network performance parameters such as packet delivery ratio, throughput, end-to-end delay, round trip time etc.

Appendix B

Decision tree algorithm – ID5R

B.1 Introduction

Intrusion detection technology is found to be more effective. once an efficient decision tree algorithm can be applied to the system, as decision tree can be converted into respective rules and can be utilized under knowledge base for intrusion detection. Decision tree is a fast classification method with top down divide and rule, starting from root, ability to learn classification intelligently is another behavior of decision tree. In case of decision tree, selecting test attributes and then to divide the sample set is very crucial. If the size of the sample set is very large then obviously branches and layers of the generated tree will also be large, as a result some unnecessary branches as well as abnormal result may generate, so these sort of branches should be pruned. Of course if there are several number of categories, then accuracy of decision tree is reduced

For a set of data, which is increasing significantly, where non incremental decision tree algorithm cannot be applied, some incremental decision tree algorithm such as ID5R should be applied. Incremental algorithm is capable of building the concept step wise in a systematic manner as and when new training instances are available.

B.1.1 Introduction to ID5R

ID5R is an extension of ID3 algorithm, which maintains sufficient information to compute E-score for attribute at a node, based on lowest E-score, one of the attribute is selected as root node. Since it is an incremental decision tree algorithm, so instead

of discarding the sub tree every time after receiving new instance to the system it adopts the following:

- Re-structure the tree instead of rebuilding the tree.
- Pull up instead of simply deleting sub trees

Likewise, Leaf nodes contain a set of instance descriptions, Non-leaf nodes (decision nodes) contain set of potential candidate tests, each with positive and negative counts for each possible outcome and branches contain positive and negative counts for this outcome.

B.1.2 Algorithm of ID5R

- Start with empty tree n
1. If n is empty:
 - create leaf
 - set leaf class to class of instance
 - set of instances: singleton set consisting of instance
 2. If n is a leaf and instance is of the same class:
 - Add instance to the set of instances
 3. Otherwise:
 - a) If n is a leaf: expand it one level (choose test arbitrary)
 - b) for all candidate tests at node n : update counts
 - c) if the current test is not the best one among all candidate tests:
 - i. Restructure tree n so that the best test is now at root (Pull-Up)
 - ii. Recursively reestablish best test in each sub tree (ignore path of instance)
 - (d) Recursively update tree t along the path instance goes. Grow the branch if necessary.

To restructure the tree, the pull up algorithm is as follows

Pull-Up a test attribute A

1. If the test A is already at the root, do nothing
2. Otherwise:

(a) Recursively pulls up A to the root of each immediate sub tree

(If necessary, expand leaves)

(b) Transpose the tree so that A is now in the root and the old root attribute is now in the roots of all immediate sub trees.

It uses the following to measure the information gain:

$$\text{Gain}(S,A)=\text{Entropy}(S)-\sum_{v \in \text{values}(A)} \frac{|S_v|}{|S|} \text{Entropy}(S_v)$$

$$\text{Entropy}(S)= -\frac{|S^+|}{|S|} \log_2 \frac{|S^+|}{|S|} - \frac{|S^-|}{|S|} \log_2 \frac{|S^-|}{|S|}$$

S: trainings set, A: test

S⁺ (S⁻): set of all positive (negative) examples in S

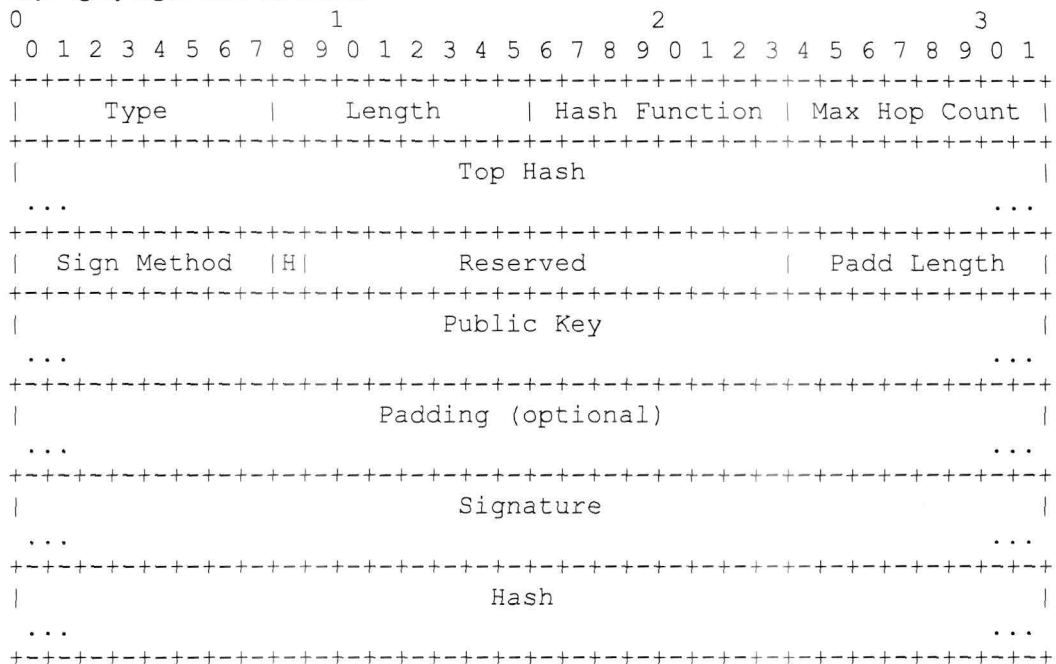
S_v :subset of all examples in S for which test A has value v

Appendix C

Protocol stack for TAODV and SAODV

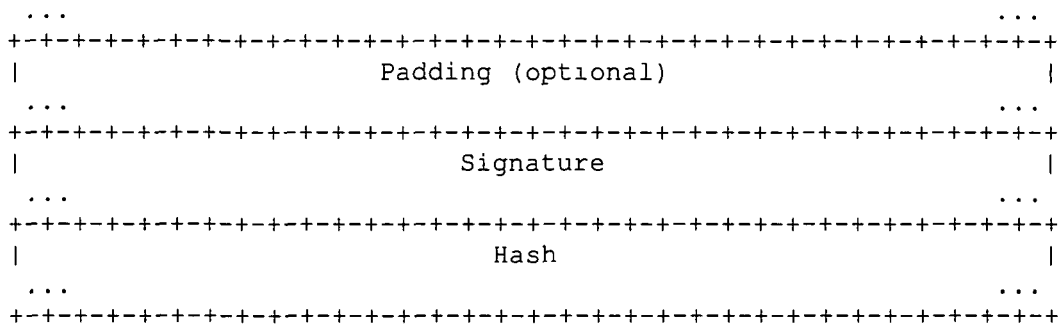
Protocol format for SAODV:

RREQ (Single) Signature Extension

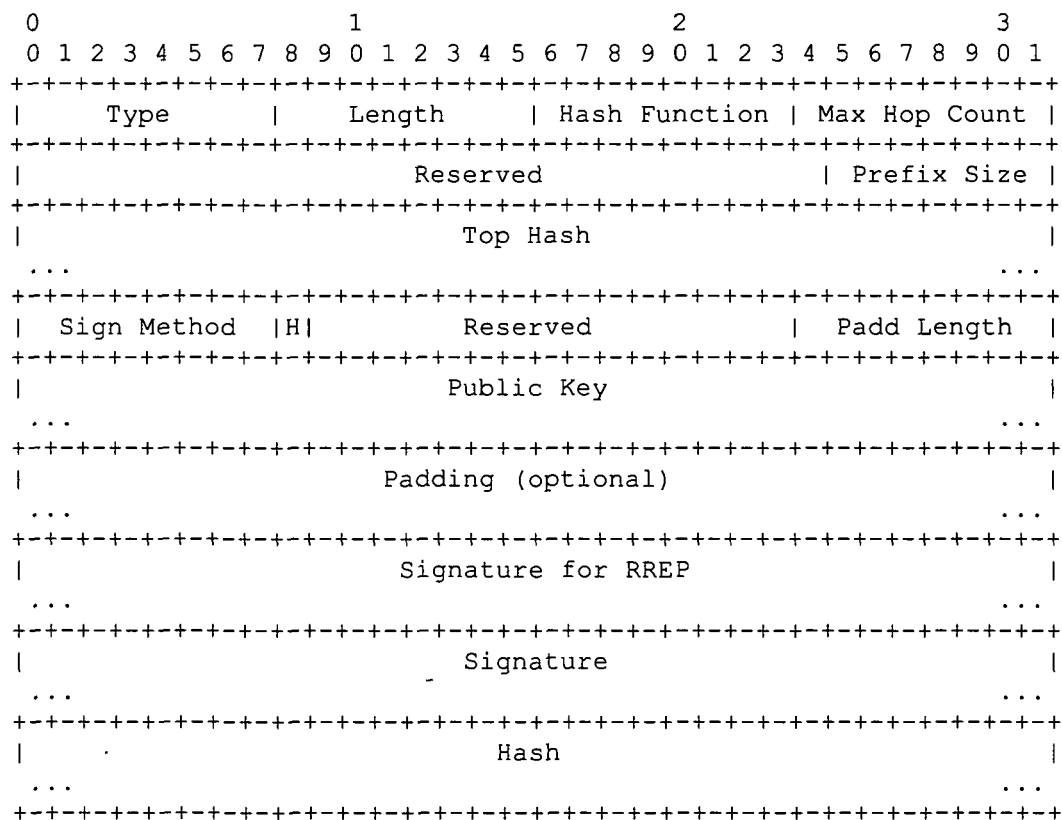


RREP (Single) Signature Extension

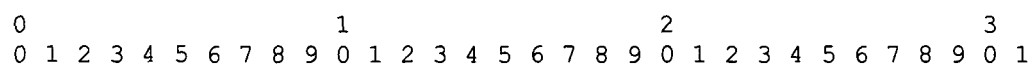




RREQ Double Signature Extension



RREP Double Signature Extension



```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type       |   Length     | Hash Function | Max Hop Count |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Top Hash                                     |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Sign Method  |H|           Reserved           | Padd Length  |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Public Key                                     |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Padding (optional)                           |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Signature                                       |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Old Lifetime                                       |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     ' Old Originator IP address                       |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Sign Method 2 |H|           Reserved           | Padd Length 2 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Public Key 2                                       |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Padding 2 (optional)                             |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Signature of the new Lifetime and Originator IP address |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Hash                                               |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

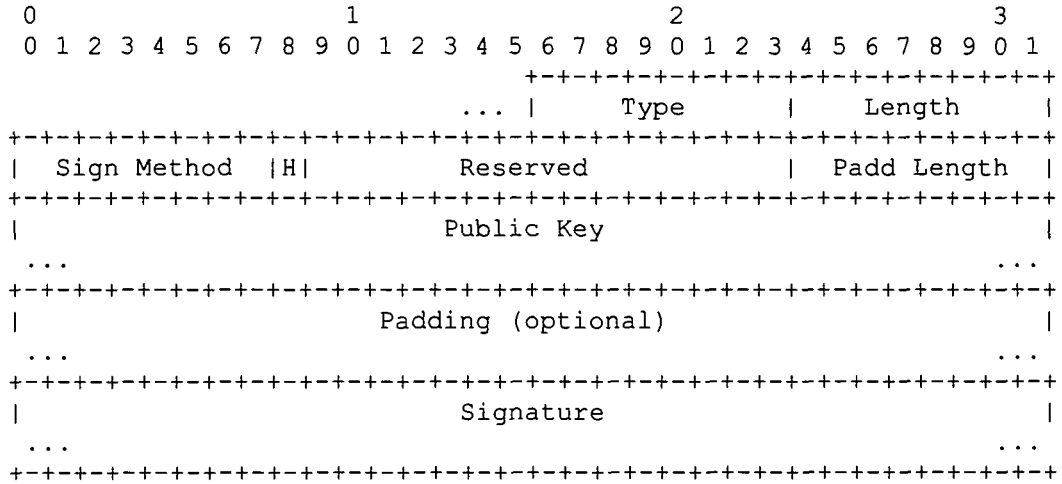
RERR Signature Extension

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type       |   Length     |           Reserved           |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Sign Method  |H|           Reserved           | Padd Length  |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Public Key                                       |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Padding (optional)                             |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Signature                                       |
|   ...                                               ...   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

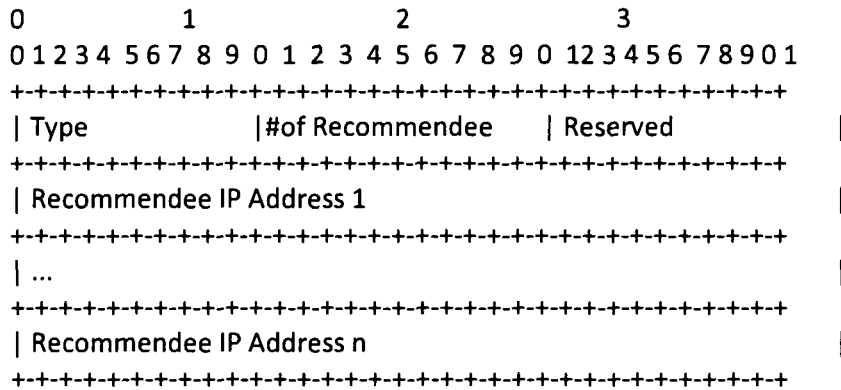
```

RREP-ACK Signature Extension

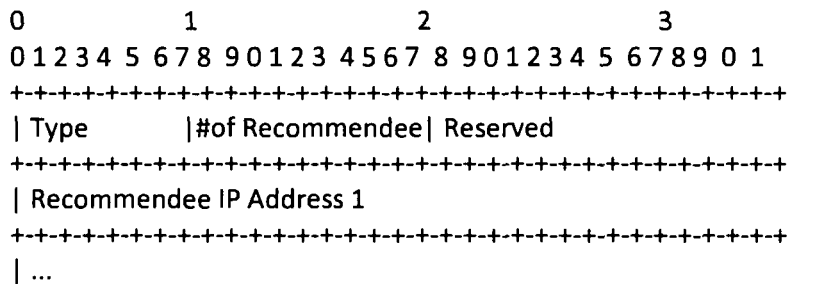


Protocol format for TAODV

Trust Request (TREQ) Message Format



Trust Reply (TREP) Message Format



```
+++++
| Recommender IP Address n
+++++
| Opinion about Recommender 1
+++++
| ...
+++++
| Opinion about Recommender n
+++++
```

Bibliography

- [1] Stephan Eichler and Christian Roman, "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC," *Mobile Adhoc and Sensor Systems(MASS), 2006 IEEE International Conference*, Page(s):481–484, E-ISBN:1-4244-0507-6, Print ISBN:1-4244-0507-6
- [2] Sharma, Y., Sharma, A., Sengupta, J., "Performance evaluation of Mobile Ad hoc Network routing protocols under various security attacks," *Methods and Models in Computer Science (ICM2CS), 2010 International Conference*, pages117 – 124, Print ISBN: 978-1-4244-9701-0
- [3] Nishu Garg and R.P.Mahapatra, "MANET Security Issues," *IJCSNS International Journal of Computer Science and Network Security(2009)*, VOL.9, No.8
- [4] Milanovic, N. Malek, M. Davidson, A. and Milutinovic, V., "Routing and Security in Mobile Ad Hoc Networks," *IEEE Computer Society (2004)*, Vol.: 37, Issue: 2, Page(s):61– 65, Issue: 2, ISSN :0018-9162
- [5] Hoang Lan Nguyen and Uyen Trang Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks, " *Ad Hoc Networks 6 (2008) Elsevier*, page(s) 32–46
- [6] K.P.Manikandan , Dr.R.Satyaprasad and Dr.K.Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks, " (*IJACSA) International Journal of Advanced Computer Science and Applications(2011)*, Vol. 2, No.3
- [7] Muhammad Zeshan, Shoab A.Khan, Ahmad Raza Cheema and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks," *Future Information Technology and Management Engineering*.

2008. FITME '08. International Seminar(2008 IEEE), Page(s):568 – 572,
Print ISBN:978-0-7695-3480-0

- [8] Soufiene Djahel, Farid Nat-abdesselam and Zonghua Zhang, "Mitigating Packet Dropping Problem in Mobile AdHoc Networks: Proposals and Challenges," *IEEE communications surveys & tutorials(2011)*, vol. 13, No. 4
- [9] Julian Benadit.P, Sharmila Baskaran and Ramya Taimanessamy, "Detecting Malicious Packet Dropping Using Statistical Traffic Patterns," *IJCSI International Journal of Computer Science Issues(2011)*, Vol. 8, Issue 3, No. 2, ISSN (Online): 1694-0814
- [10] Charles E Perkins and Elizabeth M. Royer, "Adhoc On-Demand Distance Vector Routing," *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop*, Page(s):90 – 100, Print ISBN:0-7695-0025-0
- [11] Tanapat and Anusas-amornkul, "On Detection Mechanisms and Their Performance for Packet Dropping Attack in Ad Hoc Networks," *Doctoral Dissertation (2008)*, University of Pittsburgh, ISBN: 978-0-549-89437-7
- [12] S.Madhavi, K.Duraiswamy, B.Kalaavathi and S.Vijayaragavan, "Performance Analysis of SAODV with DOS Attack," *International Journal of Electronics Communication and Computer Engineering*, Vol.3, Issue:2, ISSN 2249 –071X
- [13] Xiaoqi Li, Michael R. Lyu and Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," *Aerospace Conference, 2004. Proceedings. 2004 IEEE* , Vol.2, Page(s):1286 – 1295, ISSN :1095-323X, Print ISBN:0-7803-8155-6
- [14] Ahmed Mohamed Abdalla, Ahmad H. Almazeed, Imane Aly Saroit and Amira Kotb, "Detection and Isolation of Packet Dropping Attacker in MANETs," *(IJACSA) International Journal of Advanced Computer Science and Applications 2013*, Vol. 4, No.4

- [15] Jaydip Sen, M. Girish Chandra, P. Balamuralidhar, Harihara S.G. and Harish Reddy, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks," *ICT-MICC 2007. IEEE International Conference*, Page(s):75 – 80, E-ISBN :978-1-4244-1094-1, Print ISBN:978-1-4244-1094-1
- [16] Aishwarya Sagar Anand Ukey and Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET," *IJCSI International Journal of Computer Science Issues 2010*, Vol. 7, Issue 4, No 1, ISSN (Online): 1694-0784, ISSN (Print): 1694-0814
- [17] Djamel Djenouri and Nadjib Badache, "On eliminating packet droppers in MANET: A modular solution," *Elsevier, Ad Hoc Networks(2009)*, Vol:7, Issue 6, Pages 1243-1258
- [18] Leovigildo Sánchez-Casado, Gabriel Mací-Fernández and Pedro Garcia-Teodoro, "An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs," In *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Pages 231-238, ISBN: 978-0-7695-4745-9
- [19] Tao Shu and Marwan Krunz, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing," In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks 2012*, Pages 87-98, ISBN: 978-1-4503-1265-3
- [20] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A game theoretic intrusion detection model for mobile ad hoc networks," *Computer Communications, Elsevier Science Publishers*, vol. 31, Issue 4, page:708–721, 2008.
- [21] Xiaoqi Li Michael R. Lyu, "A Novel Coalitional Game Model for Security Issues in Wireless Networks," *IEEE GLOBECOM 2008. IEEE*, Page(s):1–6, ISSN :1930-529X, Print ISBN:978-1-4244-2324-8

- [22] F. Li, Y. Yang, and J. Wu, "Attack and flee: Game-theory-based analysis on interactions among nodes in manets," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions* 2010, Vol.40 , Issue: 3, pp. 612 –622
- [23] Tootaghaj, D.Z , Farhat, F., Pakravan, M.-R. and , "Game-theoretic approach to mitigate packet dropping in wireless Ad-hoc networks," *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, Page(s): 163 – 165, Print ISBN:978-1-4244-8789-9
- [24] Zubair Md. Fadlullah, Athanasios V. Vasilakos, and Nei Kato, "A Game Theoretic Approach to Integrate Security with Quality of Service," *IEEE International Conference on Communications (ICC 2012), Ottawa, Canada, Jun. 2012.*
- [25] Lakshmi P.S., Pasha Sajid² and Ramana M.V, "Security and Energy efficiency in Ad Hoc Networks," *Research Journal of Computer and Information Technology Sciences* 2013, Vol. 1(1), page(s): 14-17
- [26] Chun-Ta Li,"A secure routing protocol with node selfishness resistance in MANETs," *Int. J. Mobile Communications*, Vol. 10, No. 1, 2012 103
- [27] R.Balakrishna, U.Rajeswar Rao, G.A.Ramachandra, M.S.Bhagyashekar, "Trust-based Routing Security in MANETS," (*IJCSE*) *International Journal on Computer Science and Engineering* 2010, Vol. 02, No. 03, page(s): 547-553
- [28] B.Praveen Kumar, P.Chandra Sekhar, N.Papanna, B.Bharath Bhushan, "A Survey On Manet Security Challenges And Routing Protocols," *Int.J. Computer Technology & Applications*, Vol. 4 (2), page(s):248-256
- [29] Durgesh Wadbude, Vineet Richariya, "An Efficient Secure AODV Routing Protocol in MANET," *International Journal of Engineering and Innovative Technology (IJEIT)* 2012), Vol. 1, Issue 4
- [30] Aarti and Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks," *International Journal of Advanced*

- [31] Ashish Bagwari, Raman Jee, Pankaj Joshi and Sourabh Bisht, "Performance of AODV Routing Protocol with Increasing the MANET Nodes and Its Effects on QoS of Mobile Ad Hoc Networks Published," *Communication Systems and Network Technologies (CSNT) 2012, International Conference on*, Page(s):320–324, Print ISBN:978-1-4673-1538-8
- [32] Dharma P. Agrawal and Lakshmi Venkatraman, "Strategies for enhancing routing security in protocols for mobile ad hoc networks," *Journal of Parallel and Distributed Computing 2003*, Vol.63, Issue 2, Page(s): 214–227
- [33] Jared Cordasco and Susanne Wetzels, "Cryptographic Versus Trust-based Methods for MANET Routing Security," *Proceedings of the 3rd International Workshop on Security and Trust Management 2008*, Vol.197, Issue 2, Page(s): 131–140
- [34] Hamed Janzadeh, Kaveh Fayazbakhsh, Mehdi Dehghan and Mehran S. Fallah, "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains," *Future Generation Computer Systems, Elsevier 2009*, Vol.25, Issue:8, Page(s): 926–934
- [35] Wenjia Li, James Parker and Anupam Joshi, "**Security Through Collaboration and Trust in MANETs**," *Mobile Networks and Applications, Springer June 2012*, Vol. 17, Issue 3, Page(s):342-352
- [36] Praveen Joshi, "Security issues in routing protocols in MANETs at network layer," *World Conference on Information Technology, 2011*, Vol. 3, Page(s): 954–960
- [37] Shakshuki, E.M., Nan Kang and Sheltami, T.R., "Intrusion-Detection System EAACK—A Secure for MANETs," *Industrial Electronics, IEEE Transactions on March 2013*, Vol. 60 , Issue: 3, Page(s):1089 – 1098, ISSN :0278-0046

- [38] Ahmod Alomari, "Security Authentication of AODV Protocols in MANETs," *Network and System Security 2013, Lecture Notes in Computer Science*, LNCS 7873, pp 621-627
- [39] Chauhan K.K., Sanger A.K.S., Kushwah V.S., "Securing On-Demand Source Routing in MANETs," *Computer and Network Technology (ICCNT) 2010*, Page(s): 294 – 297, E-ISBN :978-1-4244-6962-8, Print ISBN:978-0-7695-4042-9
- [40] Sheikh, R., Singh Chande, M. and Mishra, D.K., "Security issues in MANET: A review," *Wireless And Optical Communications Networks (WOCN), 2010*, Page(s):1–4, Print ISBN:978-1-4244-7203-1
- [41] Giovanni Vigna Sumit Gwalani Kavitha Srinivasan, Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks," *20th Annual Computer Security Applications Conference (ACSAC'04)*, Page(s): 16-27, ISSN :1063-9527
- [42] "Mobile Ad Hoc Networks (MANETs) Are Not A Fundamentally Flawed Architecture," <http://citeseer.uark.edu:8080/citeseerx/viewdoc/summary?doi=10.1.1.136.1446>
- [43] "Mobile Ad-hoc Network (MANET) properties and spectrum needs at node," @Oxford university press
- [44] Pravin Ghosekar, Girish Katkar, Dr. Pradip Ghorpade, "Mobile Ad Hoc Networking: Imperatives and Challenges," *IJCA Special Issue on "Mobile Ad-hoc Networks MANETs, 2010*
- [45] Carlos de Morais and Dharma P. Agarwal, "Mobile Adhoc Networking," <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.8559>
- [46] Aarti and Dr. S. S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks," *International Journal of Advanced Research in Computer Science and Software Engineering 2013*, Vol. 3, Issue 5, ISSN: 2277 128X

- [47] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks," *International Journal of Innovation, Management and Technology* 2010, Vol. 1, No. 3
- [48] Martin Haenggi and Daniele Puccinelli, "Routing in Ad Hoc Networks: A Case for Long Hops," *IEEE Communications Magazine* 2005
- [49] Stephen Mueller, Rose. Tsang, and Dipak Ghosal, "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges," *This research was funded in part by a grant from Sandia National Laboratories, CA, USA.*
- [50] Sergio Marti, T.J. Giuli, Kevin Lai and Mary baker, "Mitigating routing Misbehavior in Mobile Ad hoc Networks," *Proceeding MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking*, Page(s):255-265
- [51] James P., G. Sterbenz, "Mobile wireless networking-MANET routing algorithm and protocol," <http://www.ittc.ku.edu/~jpgs/courses/mwnets>
- [52] Hui Xu , Xianren Wu and Hamid R. Sadjadpour, "A Unified Analysis of Routing Protocols in MANETs," *IEEE Transactions On Communications* 2010, Vol. 58, No. 3
- [53] Huda Al Amri, "Enhancing the scalability of heterogeneous MANET routing protocol," *A dissertation submitted in fulfillment of Doctor of Philosophy*, University of Wollongong
- [54] Jatin Gupta Ishu Gupta, "A review of evaluation of the Routing Protocols in MANETs," *International Journal of Advanced Research in Computer Science and Software Engineering* 2013, Vol. 3, Issue 5, ISSN: 2277 128X
- [55] Anju Gill, Chander Diwaker, "Comparative Analysis of Routing in MANET," *International Journal of Advanced Research in Computer Science and Software Engineering* 2012, Vol. 2, Issue 7, ISSN: 2277 128X
- [56] Robinpreet Kaur and Mritunjay Kumar Rai, "A Novel Review on Routing Protocols in MANETs," *Undergraduate Academic Research Journal (UARJ)* 2012, ISSN : 2278 – 1129, Vol.1, Issue 1

- [57] Mehran Abolhasan, Tadeusz Wysocki and Eryk Dutkiewicz , “A review of routing protocols for mobile ad hoc networks,” *Elsevier, Ad Hoc Networks 2 (2004)*, page(s):1–22
- [58] Nidhi Gupta, Keshawanand Singh and Keshav Goyal, “A Review On MANET Routing Protocol Categories,” *International Journal of Engineering Research & Technology (IJERT) 2013*, Vol. 2 Issue 6, ISSN: 2278-0181
- [59] Krishna Gorantala, “Routing Protocols in Mobile Ad-hoc Networks,” *Master’s Thesis in Computing Science 2006*, Umea University, SWEDEN
- [60] Kute D.S., Patil A.S., Pardakhe N.V. and Kathole A.B., “A Review: Manet Routing Protocols And Different Types Of Attacks In Manet,” *International Journal of Wireless Communication 2012*, Vol. 2, Issue 1, pp.-26-28., ISSN: 2231-3559 & E-ISSN: 2231-3567
- [61] Yogesh Chaba, R. B. Patel, Rajesh Gargi, “ANALYSIS OF MOBILITY MODELS FOR MOBILE AD HOC NETWORKS,” *Voyager- The Journal of Computer Science and Information Technology 2007*, Vol. 6, No. 1, July-Dec. 2007 page(s):50-55, ISSN 0973-4872
- [62] Bhavyesh Divecha, Ajith Abraham, Crina Grosan and Sugata Sanyal, “Impact of Node Mobility on MANET Routing Protocols Models,” *Journal of Digital Information Management. 2007*, Vol. 5 Issue 1, page(s):19-24
- [63] Gang Lu, Gordon Manson and Demetrios Belis, “Mobility Modeling in Mobile Ad Hoc Networks with Environment-Aware,” *Journal Of Networks 2006*, Vol. 1, No. 1
- [64] Fan Bai and Ahmed Helmy, “A Survey Of Mobility Models in Wireless Adhoc Networks,” URL: <http://www.cise.ufl.edu/~helmy/papers/Survey-Mobility-Chapter-1.pdf>
- [65] Jens Khristoffersson, “Obstacle Constraint Group Mobility Model,” *Master’s thesis, Lulea University of Technology, Sweden*

- [66] Hao Yang, haiyun Iuo, Fan Ye, Songwu lu, and Lixia Zhang , “Security In Mobile Ad Hoc Networks: Challenges And Solutions,” *IEEE Wireless Communications, February 2004*
- [67] Vesa Kärpijoki, “Security in Ad Hoc Networks,” *HUT TML 2000 Tik-110.501 Seminar on Network Security*
- [68] Sweta Kaushik, Manorma Kaushik, “Analysis of MANET Security, Architecture and Assessment,” *International Journal of Electronics and Computer Science Engineering*, Vol. 1, Issue 2
- [69] Hang Zhao, “Security for Ad Hoc Networks,” <https://www.cs.columbia.edu/~smb/classes/s09/l26.pdf>
- [70] Sheikh R., Singh Chande M., Mishra D.K., “Security issues in MANET: A review,” *Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On IEEE*, Page(s):1 – 4, Print ISBN:978-1-4244-7203-1, INSPEC Accession
- [71] Noman Islam, Zubair Ahmed Shaikh, “Security Issues in Mobile Ad Hoc Network,” *Signals and Communication Technology 2013, Wireless Networks and Security*, page(s): 49-80
- [72] Aziz, M. and Al-Akaidi, M., “Security Issues in Wireless Ad Hoc Networks and the Application to the Telecare Project,” *Digital Signal Processing, 2007 15th International Conference*, Page(s):491–494, E-ISBN :1-4244-0882-2, Print ISBN:1-4244-0882-2,INSPEC Accession Number:9855678
- [73] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, “Security in mobile ad hoc networks: challenges and solutions,” *Wireless Communications, IEEE 2004*, Vol. 11, Issue 1, Page(s):38 – 47, SSN :1536-1284, INSPEC Accession Number:7943665
- [74] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication,” *International Journal of Computer Science and Security (IJCSS)*, Vol. (4): Issue 3

- [75] Rusha Nandy and Rusha Nandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme," *Int. J. Advanced Networking and Applications 2011*, Vol. 03, Issue 01, Page(s):1035-1043
- [76] Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks," *International Journal of Computer Science and Security*, vol. 2 Issue 3
- [77] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," *WIRELESS/MOBILE NETWORK SECURITY*, 2006, Springer
- [78] Hoang Lan Nguyen and Uyen Trang Nguyen, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," *Advanced Computing & Communication Technologies (ACCT)*, 2012, Page(s):535 – 541, Print ISBN:978-1-4673-0471-9, INSPEC Accession Number:12616450
- [79] P.Visalakshi and S.Anjugam, "Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey," *International Journal of Computational Engineering Research (IJCER)*, ISSN: 2250-3005, Page(s):189
- [80] Jiazi Yi, Thomas Clausen and Ulrich Herberg, "Vulnerability Analysis of the Simple Multicast Forwarding (SMF) Protocol for Mobile Ad Hoc Networks," *INRIA 2011*, version 1
- [81] R. Puttini, R. De Sousa, L. M'e , "On the Vulnerabilities and Protection of Mobile Ad Hoc Network Routing Protocol," URL:<http://www.rennes.supelec.fr/ren/perso/lme/PUBLI/PMS04a.pdf>
- [82] Jatinder Pal Singh and Anuj Kr. Gupta, "Protocol Stack based Security Vulnerabilities in MANETs," *International Journal of Computer Applications (0975 – 8887)* 2013, Vol. 69, Issue 21
- [83] Lee Guang and Chadi Assi, "Vulnerabilities of ad hoc network routing protocols to MAC misbehavior," *Wireless And Mobile Computing*,

- Networking And Communications, 2005. (WiMob'2005)*, IEEE International Conference, Vol. 3, Page(s):146-153, Print ISBN:0-7803-9181-0, INSPEC Accession Number:8747033
- [84] R.Balakrishna, U.Rajeswar Rao, Dr.Geethanjali and M.S.Bhagyashekar, "Comparisons of SAODV and TAODV, DSR Mobile ad hoc network Routing Protocols," *Int. J. Advanced Networking and Applications* 445 2010, Vol. 2, Issue 1, Page(s): 445-451
- [85] S. Madhavi, K. Duraiswamy, B. Kalaavathi, S.Vijayaragavan, "Performance Analysis of SAODV with DOS Attack," *International Journal of Electronics Communication and Computer Engineering*, Vol. 3, Issue 2, ISSN 2249 –071X
- [86] Latha Tamilselvan and Dr. V. Sankaranarayanan, "Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks," *IJCSNS International Journal of Computer Science and Network Security* 2007, Vol. 7, Issue 3
- [87] Er. Gurjeet Singh, "Performance and Effectiveness of Secure Routing Protocol in Manet," *Global journal of computer science and technology* 2012, Vol. 12, Issue 5
- [88] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong and Joo-Han Song, "Experimental Comparisons between SAODV and AODV Routing Protocols," *WMuNeP'05*
- [89] S. Madhavi, K. Duraiswamy, B. Kalaavathi and S. Vijayaragavan, "Performance Analysis of SAODV with DOS Attack," *International Journal of Electronics Communication and Computer Engineering*, Vol. 3, Issue 2, ISSN 2249 –071X
- [90] Mike Just, Evangelos Kranakis, Tao Wan, "Resisting Malicious Packet Dropping in Wireless AdHoc Networks," *Research supported in part by NSERC (Natural Sciences and Engineering Research Council of Canada), MITACS (Mathematics of Information Technology and Complex Systems)*

and OCIPEP (Office of Critical Infrastructure Protection and Emergency Preparedness)

- [91] Ashok M. Kanthe, Dina Simunic and Ramjee Prasad, "The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad-hoc Networks," *International Journal of Recent Technology and Engineering (IJRTE)* 2012, Vol. 2, Issue 2, ISSN: 2249-8958
- [92] Djamel Djenouri, Othmane Mahmoudi, Mohamed Bouamama, David Llewellyn-Jones and Madjid Merabti, "On Securing MANET Routing Protocol Against Control Packet Dropping," *Pervasive Services, IEEE International Conference on*, Page(s):100 – 108, E-ISBN :1-4244-1326-5, Print ISBN:1-4244-1325-7
- [93] Venkatesan Balakrishnan, Vijay Varadharajan and Udaya Kiran Tupakula, "Fellowship: Defense against Flooding and Packet Drop Attacks in MANET," *Network Operations and Management Symposium, 2006*, Page(s):1 - 4 , ISSN :1542-1201, Print ISBN:1-4244-0142-9
- [94] Sonali Gaikwad and Dr. D. S. Adane , "Mitigating Packet Dropping Attack in Mobile Ad Hoc Networks using 2-ACK scheme and Novel routing Algorithm," *International Journal of Engineering Research & Technology (IJERT)* 2013, Vol. 2, Issue 9, ISSN: 2278-0181, IJERTV2IS90586
- [95] Soufiene Djahel, Farid Naït-abdesselam, and Zonghua Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges," *Communications Surveys & Tutorials IEEE 2011*, Vol. 13 , Issue 4, Page(s):658–672, ISSN:1553-877X, INSPEC Accession Number: 12359780, Digital Object Identifier :10.1109/SURV.2011.072210.00026
- [96] Xu Li, Rongxing Lu, Xiaohui Liang, Xuemin Shen. "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks," *Communications (ICC), 2011 IEEE International Conference*, Page(s):1–5, ISSN :1550-3607, E-ISBN :978-1-61284-231-8, Print ISBN:978-1-61284-232-5, INSPEC Accession Number:12143071

- [97] Lei Guang and Chadi Assi, "Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks," *WiMob, IEEE*, (2006), page: 116-123
- [98] Syed S. Rizvi and Khaled M. Elleithy, "A New Scheme for Minimizing Malicious Behavior of Mobile Nodes in Mobile Ad Hoc Networks," (*IJCISIS*) *International Journal of Computer Science and Information Security* 2009, Vol. 3, Issue 1
- [100] Manel Guerrero Zapata, N. Asokan, "Securing Ad hoc Routing Protocols", *WiSe '02*, Atlanta, Georgia, USA.
- [101] Jonny Karlsson, Laurence S dooley and Gauran pulkkis, "Routing Security in Mobile Ad-hoc Networks," *Issues in Informing Science and Information Technology*, Vol. 9, 2012
- [102] Jaspal Kumar, M. Kulkarni, M. Kulkarni, Daya Gupta, "Secure Routing Protocols In Ad Hoc Networks: A Review," *International Conference [ICCT-2010], Special Issue of IJCCT 2010*, Vol. 2, Issue 2
- [103] Durgesh Wadbude and Vineet Richariya, "An Efficient Secure AODV Routing Protocol in MANET," *International Journal of Engineering and Innovative Technology (IJEIT)*, 2012," Vol. 1, Issue 4
- [104] Manel Guerrero and Zapata, "Secure Ad hoc On-Demand Distance Vector Routing," *International Journal of Engineering and Innovative Technology (IJEIT)* 2012, Vol. 1, Issue 4
- [105] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," *IEEEAC 2004*, paper # 1150
- [106] Mrs. P.Vigneswari, R.Anusha, D.Preethi, R.Jayashree, V.Nandhini, "Comparative Analysis of and Trusted AODV (TAODV) in MANET", *International Journal of Advanced Information Science and Technology (IAIST)* 2013, ISSN: 2319:2682 Vol.10, Issue 10
- [107] Venkatesan Balakrishnan and Vijay Varadharajan, "Packet Drop Attack-A Serious Threat To Operational Mobile Ad Hoc Networks,"

- [108]Mike Just, Evangelos Kranakis, Tao Wan, “Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks,” *In Proceedings of 2nd International Conference on AD-HOC Networks and Wireless*, Montreal, Canada. October 2003
- [109]Jaydip Sen, M. Girish Chandra, P. Balamuralidhar, Harihara S.G., Harish Reddy, “A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks,” *In Proceedings of the International Conference on Telecommunications and Malaysian International Conference on Communications (ICT-MICC'07)*
- [110]AikateriniMitrokotsa, Rosa Mavropodi, Christos Douligeris, “Intrusion Detection of Packet Dropping Attacks inMobile Ad Hoc Networks,” *Ayia Napa*, Cyprus 2006
- [111]Julian Benadit.P, Sharmila Baskaran and Ramya Taimanessamy, “Detecting Malicious Packet Dropping Using Statistical Traffic Patterns,” *International Journal of Computer Science Issues (IJCSI) 2011*, Vol. 8, Issue 3, page(s): 121-126
- [112]Ahmed Mohamed Abdalla, Ahmad H. Almazeed, Imane Aly Saroit, Amira Kotb, “ Detection and Isolation of Packet Dropping Attacker in MANETs,” *(IJACSA) International Journal of Advanced Computer Science and Applications 2013*, Vol. 4, Issue 4
- [113]Djamel Djenouri, Nadjib Badache, “On eliminating packet droppers in MANET: A modular solution,” Elsevier, *Ad Hoc Networks 7* (2009), page(s): 1243–1258
- [114] Qi Zhang and Agrawal D.P., “Impact of selfish nodes on route discovery in mobile ad hoc networks,” *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, Vol. 5, Page(s): 2914 – 2918, Print ISBN: 0-7803-8794-5
- [115]Manoj Kumar Mishra, Binod Kumar Pattanayak, Alok Kumar Jagadev, Manojranjan Nayak, “Measure of Impact of Node Misbehavior in Ad Hoc

- Routing: A Comparative Approach,” *IJCSI International Journal of Computer Science Issues* 2010, Vol. 7, Issue 4, No 8, ISSN (Online): 1694-0784 ISSN (Print): 1694-0814 10
- [116] Reshma Lill Mathew and Prof. P. Petchimuthu, “Detecting Selfish Nodes in MANETs Using Collaborative Watchdogs,” *International Journal of Advanced Research in Computer Science and Software Engineering* 2013, Vol: 3, Issue 3, ISSN: 2277 128X
- [117] N.R.Suganya and S.Madhu Priya, “Detecting Selfish Nodes in a MANET through Fragmentation in Distributed Environment,” *International Journal of Science, Engineering and Technology Research (IJSETR)* 2013, Vol. 2, Issue 6, ISSN: 2278 – 7798
- [118] Frank Kargl, Andreas Klenk, Stefan Schlott and Michael Weber, “Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks,” URL: <http://medien.informatik.uni-ulm.de/forschung/publikationen/esas2004.pdf>
- [119] J.Sengathir and R.Manoharan, “Security Algorithms for Mitigating Selfish and Shared Root Node Attacks in MANETs,” *International Journal of Computer Network & Information Security; Aug 2013*, Vol. 5, Issue 10
- [120] T.V.P.Sundararajan and Dr. A.Shanmugam, “Behavior Based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET,” *International Journal of Computer Science and Security (IJCSS)*, Vol. 3, Issue. 2
- [121] A.Rajaram and Dr. S. Palaniswami, “Malicious Node Detection System for Mobile Ad hoc Networks,” (*IJCSIT*) *International Journal of Computer Science and Information Technologies* 2010, Vol. 1, Issue. 2, Pages.77-85
- [122] P.J Sweetlin Subha1 and Jeban Chandir Moses2, “A Survey of Various Risk Mitigating Techniques in MANET Environment,” *International Journal of Scientific and Research Publications* 2013, Vol. 3, Issue 2

- [123]Sanjeev Rana and Manpreet Singh, “Performance Analysis of Malicious Node Aware Routing for MANET using Two-Hop Authentication,” *International Journal of Computer Applications 2011*, Vol. 25, Issue 3
- [124]Ahmed Mohamed Abdalla, Ahmad H. Almazeed, Imane Aly Saroit and Amira Kotb, “Detection and Isolation of Packet Dropping Attacker in MANETs,” (*IJACSA*) *International Journal of Advanced Computer Science and Applications 2013*, Vol. 4, Issue 4
- [125]Jaydip Sen, M. Girish Chandra, P. Balamuralidhar, Harihara S.G. and Harish Reddy, “A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks,” *Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference*, Page(s): 75 – 80, E-ISBN :978-1-4244-1094-1, Print ISBN:978-1-4244-1094-1
- [126]Aishwarya Sagar, Anand Ukey and Meenu Chawla, “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET,” *IJCSI International Journal of Computer Science Issues 2010*, Vol. 7, Issue 4, No 1, ISSN (Online): 1694-0784, ISSN (Print): 1694-0814
- [127]Djamel Djenouri and Nadjib Badache, “On eliminating packet droppers in MANET: A modular solution,” *Elsevier, Ad Hoc Networks(2009)*, Vol. 7 Issue 6, Page(s):1243-1258
- [128]Leovigildo Sánchez-Casado, Gabriel Mací-Fernández and Pedro Garcia-Teodoro, “An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs,” *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Page(s): 231-238, ISBN: 978-0-7695-4745-9
- [129]Tao Shu and Marwan Krunz, “Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing,” *Proceedings of the fifth ACM conference on Security and Privacy in*

- Wireless and Mobile Networks 2012*, Page(s): 87-98, ISBN: 978-1-4503-1265-3
- [130]H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A game theoretic intrusion detection model for mobile ad hoc networks," *Computer Communications, Elsevier Science Publishers*, vol. 31, Issue 4, page(s): 708–721, 2008.
- [131]Xiaoqi Li and Michael R. Lyu, "A Novel Coalitional Game Model for Security Issues in Wireless Networks," *Global Telecommunications Conference, 2008, IEEE GLOBECOM 2008. IEEE.* Page(s):1– 6, ISSN :1930-529X, Print ISBN:978-1-4244-2324-8
- [132]F. Li, Y. Yang, and J. Wu, "Attack and flee: Game-theory-based analysis on interactions among nodes in manets," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions* 2010, Vol. 40 , Issue 3, page(s): 612–622
- [133]Tootaghaj, D.Z , Farhat, F., Pakravan, M.-R. and Aref, M. "Game-theoretic approach to mitigate packet dropping in wireless Ad-hoc networks," *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, Page(s): 163 – 165, Print ISBN:978-1-4244-8789-9
- [134]Zubair Md. Fadlullah, Athanasios V. Vasilakos, and Nei Kato, "A Game Theoretic Approach to Integrate Security with Quality of Service," *IEEE International Conference on Communications (ICC 2012), Ottawa, Canada, Jun. 2012.*
- [135]Frank Kargl, Stefan Schlott and Michael Weber, "Identification in Ad hoc Networks," *Proceedings of the 39th Hawaii International Conference on System Sciences – 2006*
- [136]Nishu Garg and R.P.Mahapatra, "MANET Security Issues," *IJCSNS International Journal of Computer Science and Network Security 2009*, VOL:9, No.:8
- [137]Chiranjeeb Buragohain, "Game Theory in Ad Hoc Networks,"

- [138] Tamer Basar, "Lecture Notes on Non-Cooperative Game Theory 2010"
- [139] Vivek Srivastava, James Neel, Allen B. Mackenzie, Rekha Menon, Luiz A. Dasilva, James E. Hicks, Jeffrey H. Reed, and Robert P. Gilles, "Using Game Theory To Analyze Wireless Ad Hoc Networks," *IEEE Communications Surveys & Tutorials, Fourth Quarter 2005*
- [140] Luiz A. DaSilva and Allen B. MacKenzie, "Game Theory and MANETs: A Brief Tutorial"
- [141] Mark Felegyhazi and Jean-Pierre Hubaux, "Game Theory in Wireless Networks: A Tutorial"
- [142] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," *IEEEAC 2004*, paper : 1150
- [143] Emmanouil A. PANAOUSIS and Christos POLITIS, "Non-Cooperative Games Between Legitimate Nodes and Malicious Coalitions in MANETs," *Future Network and Mobile Summit 2011 Conference Proceedings, Paul Cunningham and Miriam Cunningham (Eds), IIMC International Information Management Corporation, 2011*
- [144] Ningrinla Marchang and Raja Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks," *Ad Hoc Networks 6 (2008)*, Pages:508–523
- [145] Azadeh Omrani and Mehran S. Fallah, "A Game-theoretic Cooperation Stimulus Routing Protocol in MANETs," *IAENG International Journal of Computer Science*. 2008, Vol. 35 Issue 1, page(s):174-181.
- [146] Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt and J. Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs", *Proceedings of the Third IEEE International Workshop on Information Assurance, IEEE Computer Society Washington, DC, USA ©2005*, Page(s): 57-70, ISBN:0-7695-2317-X

- [147] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer and Richard A. Kemmerer, “An Intrusion Detection Tool for AODV-based Adhoc Wireless Networks”, *Computer Security Applications Conference 2004*, Page(s):16 – 27, ISSN : 1063-9527, Print ISBN:0-7695-2252-1
- [148] Jaydip Sen, “A Distributed Trust Management Framework for Detecting Malicious Packet Dropping Nodes In A Mobile Adhoc Network”, *International Journal of Network Security & Its Applications (IJNSA) 2010*, Vol. 2, Issue 4
- [149] Chin- Yang Henry Tseng, “Distributed Intrusion Detection Models for Mobile AdHoc Networks”, *Dissertation Submitted in partial satisfaction of the requirements for the degree of Doctor Of Philosophy in Computer Science in the office of graduate studies of the University of California Davis*
- [150] J. Arokia Renjit and K. L. Shunmuganathan, “Distributed and cooperative multi-agent based intrusion detection system”, *Indian Journal of Science and Technology 2010*, Vol.3, Issue 10 ISSN: 0974- 6846
- [151] Yasir Abdelgadir Mohamed, Azween B. Abdullah, “Security Mechanism For Manets,” *Journal of Engineering Science and Technology, 2009*, Vol. 4, No. 2, page(s): 231 – 242
- [152] J. Arokia Renjit and K. L. Shunmuganathan, “Distributed and cooperative multi-agent based intrusion detection system,” *Indian Journal of Science and Technology 2010*, Vol. 3, Issue 10
- [153] Martin Rehak, Michal Pechoucek, Pavel Celeda, Vojtech Krmıcek, Pavel Minarik, and David Medvigy, “Collaborative Attack Detection in High-Speed Networks,” *Springer-Verlag Berlin Heidelberg 2007*, page(s): 73–82
- [154] Yian Huang and Wenke Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, In *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*

- [155] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya And J. K. Kalita, "Detecting Distributed Denial Of Service Attacks: Methods, Tools And Future Directions," *The Computer Journal* 2012
- [156] Victor R. Lesser, "Cooperative Multiagent Systems: A Personal View of the State of the Art," *IEEE Transactions On Knowledge And Data Engineering* 1999, Vol. 11, No. 1
- [157] Ricardo Puttini, Ludovic Mé, Jean-Marc Percher and Rafael de Sousa, "A Fully Distributed IDS for MANET," *Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on 2004*, Vol. 1, Page(s):331-338, Print ISBN:0-7803-8623-X, INSPEC Accession Number:8230035
- [158] Marcela Mejiaa, Nestor Penaa, Jose L. Munozb, Oscar Esparzab and Marco A. Alzatec, "A Game Theoretic Trust Model for On-Line Distributed Evolution of Cooperation in MANETs," *Preprint submitted to Journal of Network and Computer Applications (JNCA)*
- [159] Luiz A. DaSilva and Allen B. MacKenzie, "Cooperation in Ad Hoc Networks: A Game-theoretic Approach," *WICAT Workshop on Cooperative Communications New York, NY – 21 October 2005*
- [160] Mark Felegyh'azi, Jean-Pierre Hubaux and Levente Buttyan, "Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks," *IEEE transactions on mobile computing*
- [161] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *The 6th ACM International Conference on Mobile Computing and Networking*, 2000.
- [162] P. Michiardi and R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *CMS'2002, Communication and Multimedia Security 2002 Conference, September 26-27, 2002, Portoroz, Slovenia* Also published in the book : *Advanced Communications and Multimedia Security* , Borka Jerman-Blazic & Tomaz

- Klobucar, editors, Kluwer Academic Publishers, ISBN 1-4020-7206-6, August 2002 , 320 pp, August 2002.*
- [163] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks," in *MOBIHOC'02*, 2002.
- [164] K. Balakrishnan, J. Deng, and P. K. Varshney, "Twoack: Preventing selfishness in mobile ad hoc networks," in *IEEE Wireless Communications and Networking Conference (WCNC'05)*, 2005.
- [165] A. Perrig, R. Canetti, D. Song, and J. Tygar, "The tesla broadcast authentication protocol," in *CryptoBytes*, 2002, pp. 2{13.
- [166] S. Djahel, F.N. Abdesselam, Zonghua Zhang, "Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks : Proposals and Challenges," *IEEE Communications Surveys & Tutorials*, Vol.13, No.4, Fourth Quarter 2011.
- [167] E. Hernandez, M.D. Serrat, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog," *IEEE Communications Letters*, Vol.16, No.5, May 2012.
- [168] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.
- [169] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
- [170] Injong Rhee, Minsu Shin et al., "On the Levy-Walk Nature of Human Mobility", *IEEE/ACM TRANSACTIONS ON NETWORKING*, VOL. 19, NO. 3, JUNE 2011
- [171] Seongik Hong, Injong Rhee et al., "Routing Performance Analysis of Human Driven Delay Tolerant Networks Using the Truncated Levy Walk Model", *ACM SIGMOBILE International Workshop on Mobility Models for Networking Research (Colocated with MobiHoc 08)*, Hong Kong, 2008.

- [172] Hemal Shah, Yogeshwar Kosta and Darshana Patel, "Characterization & Evaluation of Mobility Metrics for Levy walk using MobiSim," *Ganpat University Journal Of Engineering & Technology* 2011, VOL.-1, ISSUE-1
- [173] Sorav Bansal, Mary Baker "Observation-based Cooperation Enforcement in Ad hoc Networks," *[cs.NI]* 6 Jul 2003
- [174] Ghandar, Eman Shabaan and Zaky Fayed "Performance Analysis of Observation Based Cooperation Enforcement in Ad Hoc Networks," *IJCSI International Journal of Computer Science Issues* 2011, Vol. 8, Issue 6, No 2
- [175] L. Buttyan and J. Hubaux. Nuglets "A virtual currency to stimulate cooperation in self-organized mobile ad hoc networks." *ICCA, Swiss Federal Institute of Technology, 2001.*
- [176] Buttyan and J.-P. Hubaux "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM/Kluwer Mobile Networks and Applications, 8(5), 2003.*
- [177] S. Zhong, J. Chen, and Y. R. Yang. Sprite "A simple cheat-proof, credit-based system for mobile ad-hoc networks," *In Proceedings of INFOCOM 2003*, pages 1987-1997
- [178] D. Boneh, C. Gentry, B. Lynn, and H. Shacham "A survey of two signature aggregation techniques," *CryptoBytes, 6(2) 2003*
- [179] V. Gligor, ' Handling new adversaries in secure mobile ad-hoc networks,' *In ARO Planning Workshop on Embedded Systems and Network Security (ESNS '07), 2007.*
- [180] S. Marti, T. Giuli, K. Lai, and M. Baker, " Mitigating routing misbehavior in mobile ad hoc networks," *In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000)*, pages 255-265, 2000.
- [181] S. Buchegger and J.-Y. L. Boudec, " Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," *In*

- Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing (EUROMICRO-PDP'02)*, pages 403-410, 2002.
- [182] M. Jakobsson, J.-P. Hubaux, and L. Buttyan, "A micropayment scheme encouraging collaboration in multi-hop cellular networks," *In Proceedings of Financial Crypto 2003*, 2003.
- [183] S. Buchegger and J.-Y. L. Boudec, "Self-policing mobile ad-hoc networks by reputation systems," *IEEE Communications Magazine* 2005, pages 101-107
- [184] P. Zimmermann, "The Official PGP User's Guide," *MIT Press*, 2005.
- [185] S. Soltanali, S. Pirahesh, S. Niksefat, and M. Sabaei, "An Efficient Scheme to Motivate Cooperation in Mobile Ad hoc Networks," *In Proceedings of the Third International Conference on Networking and Services* 2007, pages 88-98, 2007.
- [186] A. J. Sang and R. Ismail, "The beta reputation system," *In Proceedings of the 15th Bled Electronic Commerce Conference* 2002, pages 324-337.
- [187] Y. Rebahi, V. Mujica, and D. Sisalem, "A reputation-based trust mechanism for ad hoc networks," *In Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC05)*, pages 37-42.
- [188] P. Michiardi and R. Molva. Core, "A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks.," *In Proceedings of the Sixth IFIP Conference on Security Communications and Multimedia (CMS02)*
- [189] K. Balakrishnan, J. Deng, and P. K. Varshney. Twoack: Preventing selfishness in mobile ad hoc networks. In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'05), 2005.
- [190] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment based approach for the detection of routing misbehavior in manets," *IEEE Transactions on Mobile Computing* 2007, Pages: 536-550

- [191] V. N. Padmanabhan and D. R. Simon, "Secure traceroute to detect faulty or malicious routing," *SIGCOMM Computer Communication Review*, 2003, 33(1)
- [192] Ekram Hossain, Dong In Kim and Vijay K. Bhargava "Cooperative Cellular Wireless Networks"

Publications

1. Bobby Sharma Kakoty and Shyamanta M. Hazarika, "General Survey on Intrusion Detection in MANETs," *International Conference on High Performance Computing, Networking and Communication Systems (HPCNCS-09)*, Publisher: ISRST, ISBN: 978-1-60651-011-7
2. Bobby Sharma Kakoty, S. M. Hazarika and N. Sarma, "NAODV-Distributed Packet Dropping Attack Detection in MANETs," *International Journal of Computer Applications 2013*, Volume 83 - Number 11