DEVELOPMENT OF AN EVOLVING INTRUSION DETECTION ALGORITHM FOR MOBILE AD-HOC NETWORK BASED ON PARTICLE SWARM OPTIMIZATION

A THESIS SUBMITTED TO

SAVITRIBAI PHULE PUNE UNIVERSITY

FOR THE AWARD OF DEGREE OF

DOCTOR OF PHILOSOPHY (PH.D.)

IN THE FACULTY OF SCIENCE AND TECHNOLOGY

BY

BHUSHAN S. CHAUDHARI

UNDER THE GUIDANCE OF

DR. RAJESH S. PRASAD

RESEARCH CENTRE

DEPARTMENT OF COMPUTER ENGINEERING

MATOSHRI COLLEGE OF ENGINEERING AND RESEARCH CENTRE,

NASHIK, INDIA

August 2018

I dedicate every achievement of my life and this thesis to my beloved father...!

Matoshri College of Engineering and Research Centre,

Eklahare, Nashik-422105, India.

Department of Computer Engineering

Certificate

This is to certify that, the work incorporated in the thesis, **“Development of an Evolving Intrusion Detection Algorithm for Mobile Ad-hoc Network based on Particle Swarm Optimization”** is submitted by **Bhushan S. Chaudhari** for the **Doctor of Philosophy (Ph.D)** in Computer Engineering, Savitribai Phule Pune University, has been carried out by the candidate at Department of Computer Engineering, Matoshri College of Engineering and Research Centre Eklahare, Nashik during the period from 02/08/2014 to /08/2018 under the guidance of **Dr. Rajesh S. Prasad.**

.

Dr. V. H. Patil	**Dr. G. K. Kharate**
Head (C.E.) and Research Coordinator	Principal

Faculty of Science and Technology,

Savitribai Phule Pune University,

Pune-411007

Certificate of the Guide

This is to certify that, the work incorporated in the thesis **"Development of an Evolving Intrusion Detection Algorithm for Mobile Ad-hoc Network based on Particle Swarm Optimization"** submitted by **Bhushan S. Chaudhari** was carried out by the candidate for the **Doctor of Philosophy (Ph. D)** degree at Department of Computer Engineering, Matoshri College of Engineering and Research Centre, Eklahare, Nashik during the period from 02/08/2014 to /08/2018 under my direct supervision and guidance.

Date: **Dr. Rajesh S. Prasad**

Place: (Guide)

.

Faculty of Science and Technology,

Savitribai Phule Pune University,

Pune-411007

Certificate

This is to certify that, the viva-voce of **Mr. Bhushan S. Chaudhari** (Ph.D. candidate in Computer Engineering) was conducted in the thesis entitled **"Development of an Evolving Intrusion Detection Algorithm for Mobile Ad-hoc Network based on Particle Swarm Optimization"**, at Savitribai Phule Pune University, Pune on / / .

Guide	**External Referee**
Dr. Rajesh S. Prasad	Dr.

Chairman

Dr.

.

DECLARATION

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Date:

Place: Nashik

Bhushan Shivram Chaudhari

(Eligibility No: 12015232877)

Acknowledgments

This work would not have been possible without the support of many people. First and foremost I wish to express my sincere gratitude to my research advisor **Dr. Rajesh S. Prasad**, for his able guidance and motivating influence throughout the course of my research work. It is the outcome of his gentle encouragement, constructive criticism, and the countless hours he spent in discussions with me, that this thesis has materialized in the present form.

Many thanks to **Dr. G. K. Kharate**, Principal, MCERC, Nashik for his encouragement and support. I am thankful to **Dr. V. H. Patil**, Head, Department of Computer Engineering for her guidance, and cooperation. I take this opportunity to thank my brother **Dr. Pramod D. Patil** for his encouragement and support throughout research work. I am also thankful to officials of Sandip University, Nashik for providing facilities while completing my research work. Many thanks to all officials of SPPU, specially **Mrs. Aparna Chavan**, for their cooperation.

I am thankful to **Dr. A. K. Dwivedi**, **Dr. A. D. Potgantwar**, **Dr. Pawan Bhaladhare** and **Dr. Geetanjali Kale** for their help in providing valuable inputs for this research work. I must thank **Dr. D. V. Patil** and **Dr. Vivek Waghmare** who helped me in solving problems in Latex. I sincerely acknowledge to all my colleagues for their support.

I am eternally grateful for the support of my wife **Suvarna**. She relieved me from my maximum responsibilities. Many thanks to my beloved daughter, **Vedika** who made it possible to keep the environment joyful, in spite that I could not spare more time with her. Finally, I thank the god for his grace without which I would never have been to this stage.

BHUSHAN S. CHAUDHARI

Abstract

Mobile Ad-hoc Network (MANET) is a self-configured, infrastructure-less and self-controlled wireless network consisting of heterogeneous mobile nodes. Dynamic topology formation in MANET has brought revolution in the field of wireless networks and internet technology. Every node in MANET is able to relay traffic and acts as a router as well as end host. Major application areas of MANET are sensor networks, military rescue operations, business community conferences etc. Major challenges in MANET are limited resources like battery power, bandwidth, scalability and shared medium. Ever increasing multi-objective and multi-layered advanced attacks have made MANET, an elementary field for researchers. An Intrusion Detection System (IDS) is a software or hardware used for security management system. The primary role of IDS is to report unauthorized and malicious events in the network. Although some of the IDS models so far proposed, claims to have achieved greater accuracy in attack detection, none of the systems is claimed to be the de-facto standard.

This thesis presents a simple, cost-effective and robust IDS algorithm for MANET, based on one of the swarm intelligence algorithms, called particle swarm optimization (PSO). Since this algorithm proposes cooperative cognizance by birds for decision making, it best suits to effective routing requirement of MANET. PSO parameters such as sociality and individuality are effectively used in this IDS agent-based approach. Each IDS agent keeps track of packet signatures received from neighboring nodes as well as communication among any two nearboring nodes. Looking at unavailability of standard dataset for attack detection in MANET, an audit set containing attack signatures of five major MANET attacks is proposed through this research. The same can further extended for other attack types. This research claims minimum false alarm rate and optimum accuracy. Greater accommodation level for performance parameters and effective routing are key points of this model.

Table of Contents

List of Tables

List of Figures

Nomenclature

ACK	Acknowledgement Packet
ACC	Ant Colony Clustering
ACO	Ant Colony Optimization
AODV	Ad-hoc On-Demand Distance Vector Routing
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CONFIDANT	Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTwork
CGSR	Clusterhead Gateway Switch Routing
CMN	Speedup obtained
CORE	COllaborative Reputation
DoS	Denial of Service
DSDV	Destination-Sequenced Distance-Vector Routing
DSR	Dynamic Source Routing
EAACK	Enhanced Adaptive ACKnowledgment
EIGRP	Enhanced Interior Gateway Routing Protocol
FAR	False Alarm Rate

FNR	False Negative Rate
FPA	Flower Pollination Algorithm
FPR	False Positive Rate
FTP	File Transfer Protocol
HIDS	Host IDS
HTTP	Hypertex Transfer Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organisation for Standardisation
LAN	Local Area Network
LMR	Lightweight Mobile Routing
MANET	Mobile Ad-hoc Network
MINLP	Mixed Integer Non-Linear Problem
MRA	Message Authentication Report
NAM	Network Animator
NIDS	Network IDS
OCEAN	Observation-based Cooperation Enforcement in Ad hoc Networks
Otcl	Object Tool Command Language
OLSR	Optimized Link State Routing

PLR	Packet Loss Ratio
PSO	Particle Swarm Optimization
PRNET	Packet Radio NETwork
QoS	Quality of Service
RIDAN	Real-time Intrusion Detection for Ad hoc Networks
RREP	Route Reply
SARN	Survivable Adaptive Radio Network
SNR	Signal to Noise Ratio
TCL	Tool Command Language
TCP/IP	Transmission Control Protocol/ Internet Protocol
TPR	True Positive Rate
TNR	True Negative Rate
TORA	Temporally Ordered Routing Algorithm
TWOACK	TWO network-layer ACKnowledgment-based scheme
VANET	Vehicular Ad-hoc Network
WAN	Wide Area Network
WPR	WayPoint Routing
Wi-Fi	Wireless Fidelity
WAP	Wireless Application Protocol
WoT	Web of Trust
WSN	Wireless Sensor Network

WWW	World Wide Web
ZRP	Zone Routing Protocol

Chapter 1

Introduction

Advent of wireless technology have made our livelihood more progressive and productive. Unlike traditional structured networks, wireless networks do not require conventional media for communication. With the minimum cost of installation, computing nodes are able to communicate with each other in wireless networks. Move over, infrastructure-less networks have laid the foundation of the fastest and cost-effective communication. Flexibility is one of the great advantages of wireless network. To fulfill needs of temporary scenarios, ad-hoc networks are in great demands. Devices such as laptops, smartphones, and tablet computers have changed our daily routines greatly [1].

Forms of currently used ad-hoc networks are Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET) and Wireless Sensor Network (WSN). Each type of ad-hoc network has its own application areas. With the help of VANET, it has become easier to track traffic congestion by forming a network between moving vehicles [2]. Connecting different electronic gadgets for accessing and monitoring is possible through WSN. Even though MANET has proved its usefulness in emergency operations and conferences, privacy of communication is difficult to maintain. Its topology-free environment and dynamic nature of independent nodes makes it vulnerable to security attacks [3]. In initial days of MANET invention, encryption techniques helped security experts to ensure a secure environment. Over the period of time, it is proved that encryption alone is not sufficient as a security measure [4]. To achieve authenticity, researchers are also significantly tried to strenthen the routing protocol. Still, in various aspects, researchers'contributions could not address all the security and routing problems in MANETs using conventional techniques.

1.1 Motivation

Mobile Ad-hoc Network (MANET) is an upcoming technology. The advent of wireless and mobile devices has provided a new paradigm of computing. Ubiquitous computing and mutual data exchange without any existing infrastructure have become more and more important. Business, safety, and military applications already exist but the demand for higher data rates, better security, and more convenient connection establishment are a driving force in the development of new ad-hoc networking technologies.

The characteristics of mobile ad-hoc networks make the QoS support a very complex process unlike in traditional networks. The nodes in the mobile ad-hoc network have limited battery power and limited bandwidth. They are prone to failure due to the lack of battery power. Dynamic behavior of nodes like low signal quality or node failure leads to changes in topology as well. It may lead to frequent path breaks. To secure MANET communication against ever-increasing, advanced and multi-objective attacks have become need of time. Most of the Intrusion Detection Systems (IDS) found in literature are relying on conventional routing protocols. Limitations of these routing protocols provided gateway for attackers to breach the security. Despite consistent efforts by researchers in minimizing IDS limitations, performance parameters such as accuracy and false alarm rate need significant improvements.

1.2 Problem Statement and Research Objectives

This research intends to the rigorous study of different security attacks over MANET and to analyze MANET behavior under various attacks. That, in turn, will result in the identification of efficient techniques for analysis of intrusive signatures and an efficient solution over major attacks. Problem statement for our research work is, “Development of an Evolving Intrusion Detection Algorithm for Mobile Ad-hoc Network based on Particle Swarm Optimization”.

Objectives of this research are as follows:

1. To study different security attacks and their effects on MANET communication.

2. To review different existing intrusion detection models in Mobile Ad-hoc Networks and to identify potential research gaps.

3. To propose an IDS Model based on Particle Swarm Optimization algorithm.

4. To implement the PSO-based IDS model and to compare and analyze its performance with existing models.

5. To validate the results.

1.3 Research Contributions

The core idea underlying all the aforementioned work is to provide a comprehensive and cost-effective intrusion detection model to detect advanced types of security attacks. Looking at the significance of routing strategy in securing network communication, a novel anomaly type PSO based model is claimed in this research work. The main contributions of this thesis are summarized as follows:

1. This thesis presents state of the art survey of challenges in MANET and types of threats associated with it. MANETs and their limitations are also identified and described in the illustrated manner.

2. MANET advanced attacks and their effects on specific performance parameters are identified in this research. Due to diversified nature of these attacks, most of the existing IDS models are failed to address them simultaneously. The same has resulted in parameter-specific and attack-specific IDS models. This thesis proposes the model where each node acts as IDS agent and is evaluated for most of the desired performance attributes viz. energy optimization, minimum end-to-end delay, minimum packet loss and optimum route bandwidth.

3. Most of the IDS systems discussed so far in the literature are independent of routing protocol used for MANET communication. It leads to the less secure environment. It can also be easily compromised. This thesis proved that the packet signatures obtained from routing protocol are helpful in identifying threats in the network and in ensuring secure

packet delivery. Synonymously it is claimed that effective routing strategy in MANET contributes to intrusion detection.

4. This thesis proposes a modified PSO-based routing strategy where cooperative nature of MANET is effectively used for securing communication and achieving common performance parameters. The same is proved by comparing it with existing routing algorithms such as Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector Routing (AODV) routing.

5. On execution of experimental setup, parameter specific node traces are obtained. Such an experiment is never claimed so far in the literature. Ever changing node behavior can be observed using these traces which helps in the estimation of node fitness.

6. Most of the IDS models discussed so far in literature are attack specific and rarely aimed at finding robust security system against multiple active attacks. Through experimentation, an audit training set for most common active attacks is generated. The same model can be generalized to obtain packet signatures for desired existing MANET attacks.

7. Very few attempts at achieving Host IDS (HIDS) and Network IDS (NIDS) in the same model are observed in the literature. This thesis proposes a novel IDS algorithm capable of monitoring neighboring nodes (NIDS) and its own network traffic (HIDS). Cooperative nature of PSO is effectively used for achieving the same.

8. This thesis also proved that higher node density contributes to secure communication in MANET provided that, the efficiency of MANET routing protocol is optimum.

9. Experimentation done in this research identified the effect of varying node size over packet loss.

10. Finally, thesis proved the effectiveness of the combination of PSO based routing and an agent-based novel IDS model for minimizing false alarm rate and improving the accuracy of intrusion detection.

1.4 Organization of Thesis

The major issue with MANET is that there is no central access point for communication. The node dependency makes it easy to breach the security and inject attacks in the network. Intrusion detection approaches so far published needs improvement in terms of cost-effectiveness, communication overhead, algorithm complexity etc. The aim of this research is to provide an improved intrusion detection algorithm to improve accuracy and minimize false alarm rate.

The thesis is organized into six sections which are further divided into multiple subsections. An overview of chapters presented in this thesis goes as follows:

The goal of **Chapter 1** is to discuss problem statement of this thesis. It also presents research objectives and aims. The major contributions of this research are also briefed in this chapter.

Chapter 2 focuses on MANET and its properties. The layer structure of MANET and OSI varies in terms of the protocol stack. The same is also discussed in this chapter. This chapter also presents MANET attacks, routing protocols, and related discussion. This chapter also presents state of the art survey on category wise existing intrusion detection models discussed so far by researchers. It also comments on limitations and challenges of existing MANET IDS models and routing protocols.

Chapter 3 discusses existing IDS models based on PSO and their limitations. The same chapter also presents MANET and IDS performance attributes used so far by researchers. It also discusses attributes used for a novel IDS model discussed in this thesis. MANET routing attacks and their influence on selected performance attributes is a key point of this chapter.

Chapter 4 is a most important chapter of this thesis where we presented architecture of an IDS agent, modified PSO parameter mapping for MANET routing and an evolving IDS algorithm for attack detection. It also discusses on NS2 simulation tool used for experimentation. NS2 simulation environment and parameter initialization are presented in this chapter in a detailed manner.

Chapter 5 illustrates experimentation done on our IDS model based on PSO parameters. This chapter discusses results and graphs plotted in the NS2 simulation tool. Comparison of results of PSO based IDS model against existing IDS models namely Enhanced Adaptive AC-

Knowledgement (EAACK) and Watchdog algorithms are discussed in detail. The comparison is mainly based on two performance parameters namely accuracy and false alarm rate. Graphs obtained through NS2 presents efficiency of PSO-based algorithm in terms of accuracy and false alarm rate.

Conclusion of any research is the most useful for further improvements in any domain. **Chapter 6** presents conclusion and future scope of this research. Guidelines provided in this chapter will help guide researchers who are working for the betterment of security in mobile ad-hoc networks.

Chapter 2

Literature Review

2.1 Introduction

MANET is a self-organized temporary wireless network with the peer-to-peer organization. Cooperative nature of nodes is the key to this network. An environment where setting up a structured network is expensive and time-consuming, MANETs are most useful. In military scenarios and rescue operations, where installation of access points and towers is almost impossible, MANET can play a vital role. Unlike wired networks, there is no central coordinator in MANETs. Each device acts as host as well as router and has an equal responsibility to forward packets if the source and destination nodes are not in one hop communication. Nodes keep track of presence of other nodes, available services in network and topology formation and maintenance. The figure 2.1 shows the architecture of simple MANET containing seven nodes. Unlike infrastructure-based networks, MANET nodes are connected by wireless links.

MANET was developed in 1990 to connect movable computing nodes with each other. Before the development of MANET, two generations of ad-hoc networks such as Packet Radio Network (PRNET) and Survivable Adaptive Radio Network (SARN) were in existence [5]. MANET provides packet switching without structured infrastructure. Wireless links in MANET are more susceptible to noise and suffers from obstacles in between. Major challenges faced by MANET are as follows [6]:

1. Limited bandwidth with wireless computing devices makes the communication unreli-

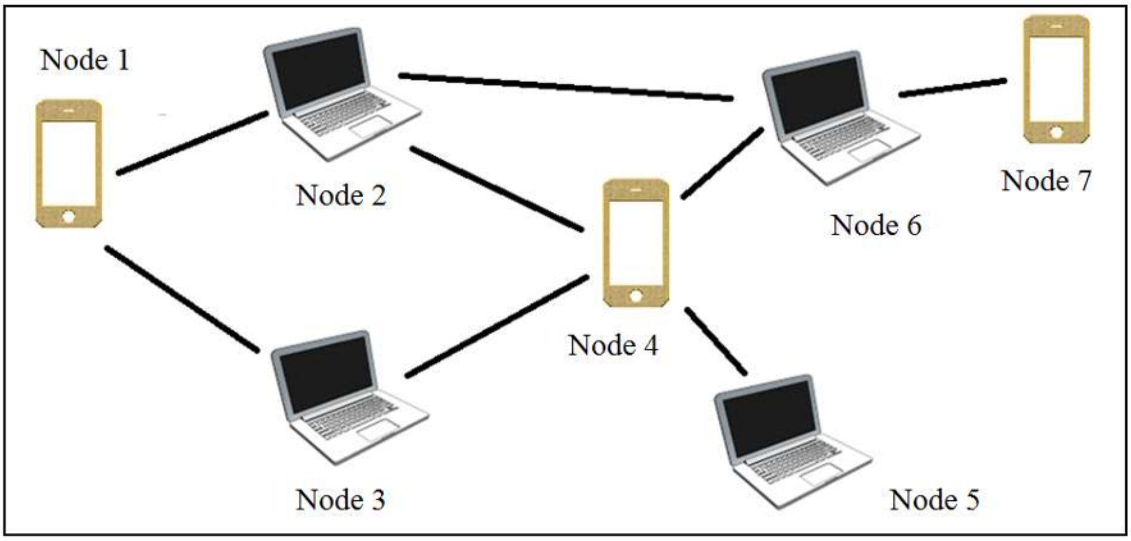


Figure 2.1: MANET General Architecture

able.

2. The energy-constrained environment in MANET may result in frequent link breaks.
3. Wireless links suffer from noise which leads to frequent communication topology change.
4. Arbitrary nature of MANET nodes often gives gateway for vulnerabilities.
5. Scalability is another issue since node size depending on the desired application area.
6. Some nodes in MANET may not participate in communication (hidden terminal). On the contrary, a node may get over flooded with packets called exposed terminal phenomena. These phenomena deteriorate MANET performance.
7. Privacy protection is critical in MANET and requires robust countermeasures.

Intrusion detection systems in MANET have gained the attention of researchers due to aforementioned challenges.

2.2 MANET Protocol Stack

Lack of consistency is observed in choosing appropriate routing protocol for MANET. This may be the reason behind poor routing performance of MANETs so far. The protocol stack of

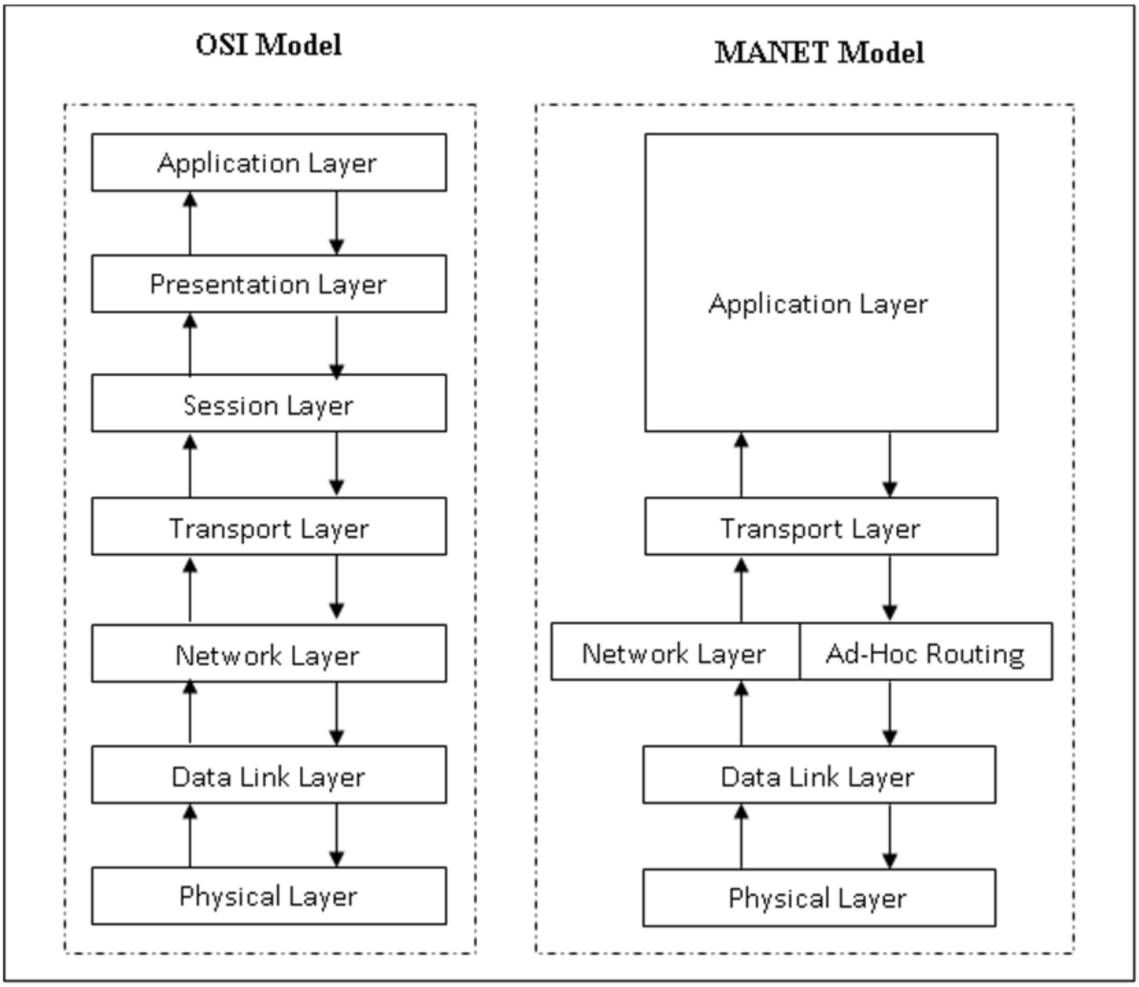


Figure 2.2: Comparing Layer Architecture for OSI and MANET

OSI and MANET are different. Comparision of layer architecture is presented in figure 2.2 [7].

As shown in figure 2.2, the application layer of MANET protocol stack combines application, presentation and session layers. The network layer of MANET is divided into two layers: network layer and ad-hoc routing layer. As like OSI model, MANET model uses Internet Protocol (IP). But the major difference between two models lies in ad-hoc routing layer. In this layer, various ad-hoc routing protocols are used for communication. These routing protocols are presented in next section.

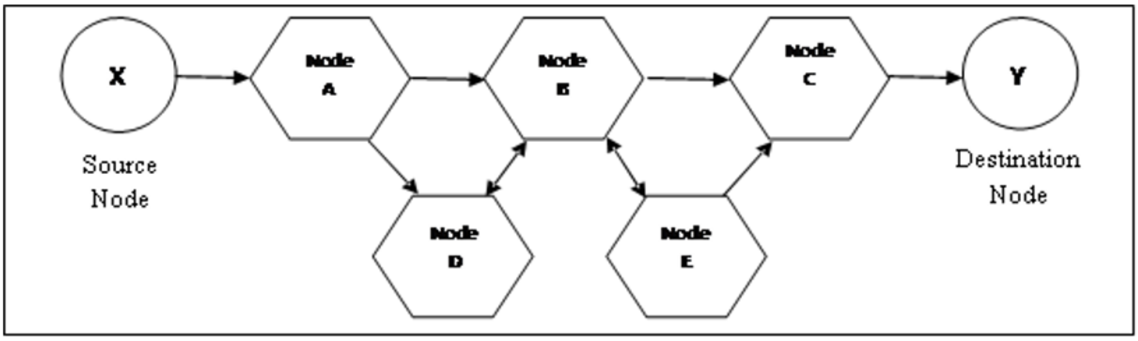


Figure 2.3: Typical Routing Network

2.3 Ad-Hoc Routing Protocols

An ad-hoc network is an interconnected set of nodes. If the communicating nodes are in radio range of each other (one hop distance), then there is no need of routing protocol. Direct links for communication is handled through device drivers in such case. However, when node size is bigger and direct communication is not possible between communicating nodes, routing protocol needs to be designed. The routing protocol must be able to manage node diversity in quality of service (QoS) parameters. A typical routing network is shown in the figure 2.3. Node Xand Y represents source and destination nodes respectively. Node A,B,C,D and E are intermediate nodes.

A routing protocol is a convention or standard to decide packet route between communicating nodes. Many researchers have evaluated routing protocols performance based on parameters such as hop count, packet loss ratio, the overhead incurred, bandwidth availability, energy and other measures. Each node listens to broadcast communication by neighboring nodes and also announces its presence in the network to nearby nodes. MANET routing protocol plays a vital role in topology formation and routing performance. Various routing protocols are available in MANET each with their own advantages and limitations. Routing protocols are categorized on the basis of when and how the routes are discovered [8]. Mainly routing protocols are divided into three categories: proactive, reactive and hybrid.

Proactive routing protocols use link state routing and frequently exchanges control packets among network nodes. It stores routing information at each node and uses the same for communication. These types of protocols are also called as table-driven protocols. Commonly used

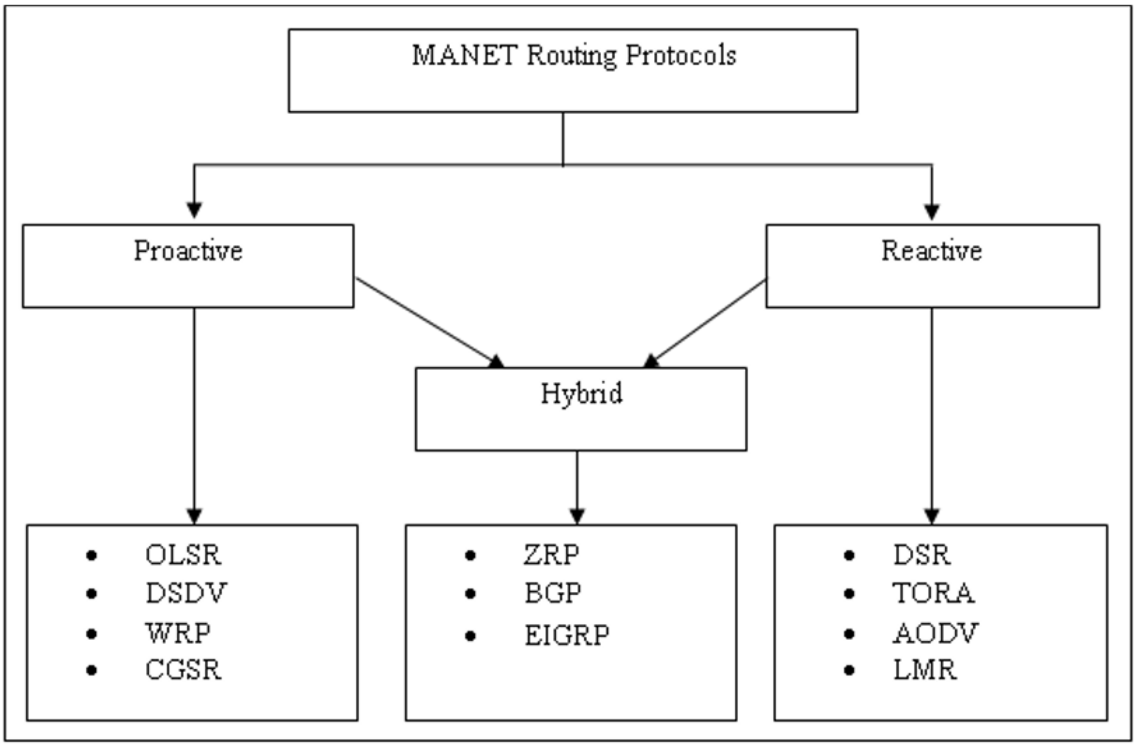


Figure 2.4: Types of Routing Protocols

proactive routing protocols are Optimized Link State Routing (OLSR), Destination-Sequenced Distance-Vector Routing (DSDV), Wireless Routing Protocol (WRP) and Clusterhead Gateway Switch Routing (CGSR).

Reactive types of protocols establish the communication only when any network node demands the same. These protocols are also called on-demand protocols. These protocols use distance vector routing algorithms and reduce the overhead of the proactive type of protocols. Examples of reactive routing protocols are Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA), and Ad-hoc On-Demand Distance Vector (AODV), Lightweight Mobile Routing (LMR) etc.

Hybrid types of protocols are mixture of the proactive and reactive type of routing protocols. Examples of these protocols are Zone Routing Protocol (ZRP), Border Gateway Protocol (BGP), and Enhanced Interior Gateway Routing Protocol (EIGRP) etc. The figure 2.4 shows a diagrammatic representation of types of routing protocols.

2.4 MANET Routing Attacks

Based on attack behavior, MANET attacks are classified into three categories: passive attacks, active attacks, and advanced attacks [9]. Passive attacks are less harmful if compared with active and advanced attacks. In passive attacks, an attacker monitors information about topology, routing protocol, duration of the communication, source and destination nodes etc. Passive attacks do not hamper the communication. Examples of passive attacks are eavesdropping, traffic analysis and monitoring.

In case of active attacks, attacker disrupts the communication and is more harmful when compared with passive attacks. Advanced attacks are even more harmful than active attacks and involve a combination of various active attacks. Major active and advanced attacks are briefed below:

2.4.1 Active Attacks

Most of the routing protocols do not provide an authentication mechanism for packets received at the source and destination nodes. An intruder is able to inject active attacks because of the same. Common active attacks are listed below:

- **Spoofing Attacks**

  Spoofing attacks are also called as impersonation attacks. In this attack type, the attacker tries to get the identity of the genuine node. An attacker node is able to receive legitimate packets and misuse them. Further, these packets might get modified and sent to other nodes. The intruder might alter source address and other information in the packet to fake the communication [10]. Types of spoofing attack are IP spoofing and Mac Spoofing.

- **Malicious Flooding**

  Malicious Flooding attack clogs the target node and network with fake packets. When this attack is performed by multiple attackers becomes hazardous for network and difficult to prevent. Usually, attacker node uses RREQ packets to flood the network. All nodes receiving RREQ packets start forwarding these fake packets to all neighboring nodes resulting in network congestion [11].

- **Fabricated Route Messages**

  Using fabricated route attack, attacker node sends false route messages, such as route requests and replies with malicious information. Such attacks are difficult to identify as the false routing packets bear valid constructs for routing [12]. In some cases, the genuine node available for routing is declared as not available and makes difficult to prevent.

- **Wormhole**

  Wormhole attack is challenging to defend and can cause a serious threat to security. An attacker captures the packets and tunnels them to some other location. In general, a path is created between two colluding nodes that can be used to transmit packets secretly [13].

- **Denial of Service (DOS)**

  This is another serious type of attack which reduces network performance significantly. These types of attacks not only consume system resources but also isolate legitimate nodes from the network. Targeted performance parameter may be different in such attacks. In [14], the author presented various DOS attacks targeting performance parameters viz. bandwidth and energy.

- **Sinkhole**

  In this attack type, an attacker tries to attract routing packets by sending fake routing information claiming that it has an optimum route to the target. Generally, the attacker compromises one network node to launch an attack. Sinkhole attack may further used by an attacker to launch other attacks such as spoofing, selective forwarding and altering route information [15].

- **Sybil Attack**

  In Sybil attacks, an attacker uses multiple identities or identity of another node present in the network. There are two forms of Sybil attack namely, join and leave sybil attack and simultaneous sybil attack [16]. If attacker begins this attack using beacon message then it is called as Join and Leave Sybil attack. If attacker node is altering its identity for every communicating node then it is called as Simultaneous Sybil attack.

2.4.2 Advanced Attacks

Most of the advance attackers are proactive and are harmful to authentication of data in multiple ways.

- **Black hole**

  In this attack type, all packets are routed to a specific node which will not forward them at all [17–19]. It results in data loss and deteriorates network performance. Attacker node floods false route information to source node resulting source node to route all packets through the malicious node. Table-driven protocols such as Optimized Link State Routing (OLSR), Ad-hoc On-Demand Distance Vector routing (AODV), Wireless Routing Protocol (WRP), and Destination Sequenced Distance vector routing (DSDV) mostly suffers from black hole attack.

- **Replay**

  In this attack, intruder records valid control messages of other nodes and resends to destination later resulting in disturbing routing tables of network nodes [20]. Based on message destination, repay attacks are divided into deflections, reflections and straight replays, interleaving, and classic replays.

- **Network Partition**

  One of the unavoidable routing attacks is network partitioning. Intruder divides the network into sub-networks where nodes cannot communicate each other even though path exists between them [21].

- **Selfishness**

  Selfishness is another serious attack. In this attack, a victim node will not serve as a router for other nodes [22]. A node may not be selfish from the beginning. Due to energy depletion, a MANET node may become selfish. In presence of selfish node, the efficacy of communication is significantly reduced.

- **Sleep deprivation**

  This type of attack is similar to DOS attack. An attacker node interacts with the legitimate node as like a genuine neighboring node. The intention behind this communication is to keep victim node to use up its battery power [23]. This results in putting victim node into sleep node.

- **Cache Poisoning**

  Cache is the internal memory with each MANET node. Intruder convinces all neighboring nodes to update their cache Address Resolution Protocol (ARP) tables [24]. Information in routing tables is modified, deleted or contains false information.

- **Rushing**

  Because of rushing attack, the attacker node blocks legitimate messages that arrive later by distributing a false control message. In [25], authors discussed the impact of rushing attacker node present near sender, receiver and within the network.

- **Byzantine**

  The Byzantine attack is very dangerous and difficult to predict. A compromised intermediate node or a set of compromised nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal routes and dropping packets resulting in disruption or degradation of routing services [26].

2.5 Intrusion Detection System

Any network is based on three pillars namely integrity, confidentiality and availability. The same pillars are applicable to the wireless distributed environment of MANET. To ensure secure communication, routing protocol, network topology and legitimate nodes plays a vital role. Intrusion is an attempt to break the security and disrupt the communication. An Intrusion detection system is any software or hardware which collects information, detects intrusions and report to the administrator. It is a countermeasure to prevent an attacker from injecting attacks on the network.

Literature available in form of publications shows that authentication and encryption techniques used for securing MANET are insufficient [27]. Security attacks such as intrusions are serious issue needs to be addressed in greater depth. Intrusion is any unauthentic attempt to get into the system with a malicious purpose. An intrusion detection system is a software or hard-

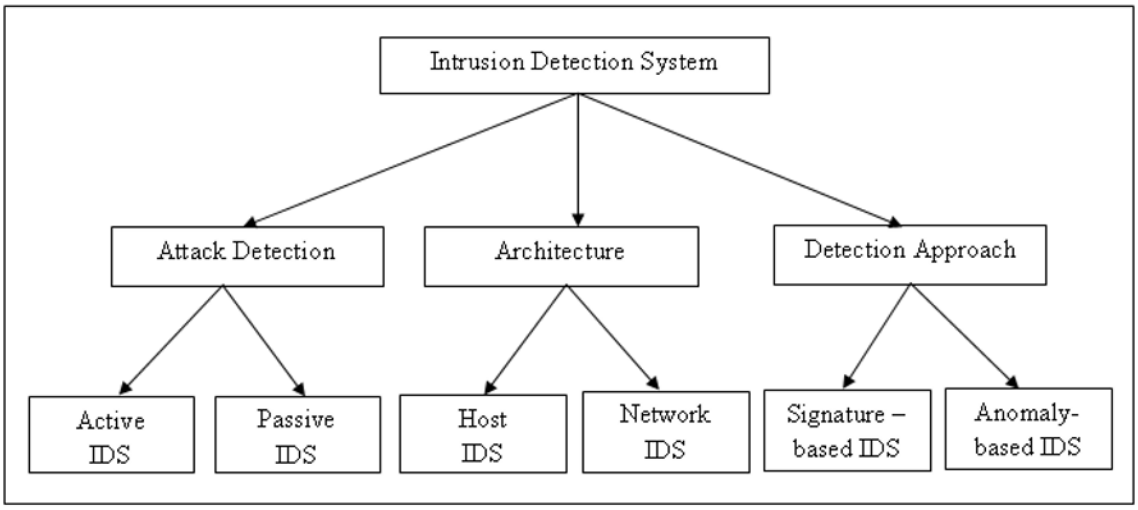


Figure 2.5: Classification of Intrusion Detection Systems

ware which prevents intrusions and report to the administrator. Cooperative and attack prone environment such as MANET requires a robust intrusion detection system (IDS) to protect the network against ever increasing advanced and multi-objective attacks.

IDS are mainly divided into three categories as shown in the figure 2.5 [28]. Based on attack detection behavior, IDS are categorized as active or passive IDS [29]. Active IDS does attack detection without the intervention of an operator. Whereas, passive IDS monitors the network and identifies the threats present if any based on operator commands. It does not initiate actions without explicit commands given by the operator.

IDS are further divided based on architecture into host-IDS and network-IDS. Host IDS are responsible for monitoring traffic associated with the individual node and does not bother about communication happening in the network. In HIDS, each node works individually for attack detection. HIDS generate less traffic. In network IDS all nodes have an equal responsibility to monitor network and detect any malicious events. Along with keeping track of individual audit traces, nodes keep track of traces with any other node in the network.

Based on detection approach, IDS are divided into signature based and anomaly based types. Signature-based IDS detects attacks with the help of packet signatures present in the database. Signature-based IDS try to detect only abnormal signatures. Generally, attack signatures are based on pre-specified performance parameters such as number of packets sent, number of packets received etc.

Anomaly-based intrusion detection involves comparing packet signatures with pre-existing database available either centrally or at the individual node. Any new signature pattern than already existing one is claimed as suspicious and can further be investigated. The major challenge before anomaly-based IDS is high false alarm rate. Because of ever increasing and the combination of active attacks, more efforts are needed in the development of robust, low-cost intrusion detection technique to eradicate security threats.

2.6 Existing Significant Intrusion Detection Models

Achieving secure mobile ad hoc network involves mainly two aspects namely:

1. Development or improvement of secure routing protocol for MANET to improve quality service parameters and
2. Implementation of the robust intrusion detection system.

Many researchers have taken efforts in the betterment of one or the other aspects mentioned above. Various distributed and cooperative intrusion detection systems based on conventional attack types are discussed in literature so far. Our approach focuses on the active, anomaly-based intrusion detection system which can serve as host as well as network IDS. The models found significant in literature and which are evaluated and compared with the PSO-based model presented in this thesis are briefed below.

2.6.1 Watchdog/Pathrator

This model was suggested for intrusion detection containing two modules namely, Watchdog and Pathrator [30]. These two modules work in collaboration with each other for intrusion detection. The first module is called Watchdog which identifies misbehaving nodes. Whereas, Pathrator computes a secure route by avoiding misbehaving nodes. Both the modules are run by every node in MANET. The Watchdog listens to the packets transmitted by next node and determines whether the packet is correctly forwarded or not. Based on the rating given by Pathrator to every node, the path metric is calculated. The path containing highest metric will be followed for communication. If any of the node do not forward packets then it is declared as a malicious node. The limitation of this system is that the Watchdog running at a particular node may not be able to detect compromised node behavior in some situations such as:

- Packet collisions may not be differentiated with the misbehaving node or not forwarding packets.
- Possible collisions on transmission path can't be sensed by the source node.
- Lower packet drop rate than threshold can 't be identified.

2.6.2 Enhanced Adaptive ACKnowledgement (EAACK)

Considering limitations of watchdog such as false misbehavior, limited transmission power and receiver collision, an acknowledgment based scheme for intrusion detection is proposed called EAACK [31]. It contains three components namely ACK, Secure-ACK and Misbehaviour Authentication Report (MRA). ACK is end-to-end acknowledgment module to reduce network overload. If the packet delivery is unsuccessful, the source node S switches to S-ACK by sending S-ACK packet to detect misbehaving nodes. Out of three consecutive nodes, every third node sends S-ACK packet to the first node. Whenever there is misbehavior report generated, MRA component will verify for alternate routes between source and destination. If the MRA packet is correctly received by the destination, then MRA declares that it is false misbehavior report. This way, EAACK also overcomes false alarm rate of watchdog scheme. A major limitation of EAACK as per author is poor resistance towards the multi-objective type of attacks.

2.7 Related Work

A significant development in intrusion detection in MANETs is seen in last two decades and many journal, transaction papers, patents, reviews, and surveys are available in the form of literature. Researchers have promoted different models and claimed to overcome limitations of existing models over time. Apart from two noteworthy models discussed in section 2.6, research approaches published so far by researchers are categorized and presented in subsequent sections.

2.7.1 Research Approaches to Securing MANET Communication

To secure volatile network such as MANET is a fascinating research area. Many researchers have put forth their efforts in securing MANET. The existing research on MANET attacks, topologies, MANET applications, simulation tools and performance parameters is presented in this subsection.

IDS are useful in wide variety of application areas. Few authors tried to excavate the practical usefulness and challenges of using IDS in different sectors [32]. They also revealed practical approach of deployment and configuration of user-specific IDS in organization categories like academic, financial, scientific etc. Authors also commented on challenges, advantages, and disadvantages of IDS.

Contributions by researchers are also observed in the betterment of protocols specific attacks such as location disclosure attack [33]. Authors surveyed topology variations and identified chances of fake position declaration by malicious nodes. They also commented on modification required in Echo protocol which was developed for node region identification problem. The need for robust scheme to avoid location disclosure is outlined by authors.

In [34], authors surveyed various IDS models and claimed that out of publications they reviewed, 75.5% authors used simulation tools for experimentation. They also found that 43.8% researchers used network simulator version 2 (NS2) for networking related research. However, simulators such as GloMoSim (10%), QualNet (6.3%), OPNET (6.4%), MATLAB (3.8%) and CSIM (2.5%) are also used for research. Authors commented that 27.3% researchers used self-developed simulation tools. Guidelines provided in the testing of IDS through tools and precautions for testing proved helpful for conducting this research.

Depending on attack detection type, protocol behavior and method used, IDS can be categorized in various ways. In [35,36], authors explored various types of IDS such as credit-based, reputation based and end-to-end acknowledgment schemes. Authors focused on limitations of existing IDS models and need of efficient IDS system. Authors claimed that digitally signed end-to-end acknowledgment is more efficient for secure packet data communication among IDS nodes.

In [37–40], authors presented state of the art survey of current IDS models in MANETs. Authors evaluated Intrusion Detection Systems in the literature based on parameters used for implementation. Authors highlighted the need for energy efficient, intelligent routing and distributed IDS.

Swarm Intelligence (SI) has proved itself as an emerging trend in a wide variety of sectors. In [41], authors surveyed network security applications of swarm intelligence techniques namely, Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) and Ant Colony Clustering (ACC). Authors claimed that IDS based on swarm intelligence algorithms serve better than existing intrusion detection algorithms. They also pointed to the necessity of distributed algorithms based on swarm intelligent techniques to enhance security in wireless networks.

Each routing attack has a different impact on MANET communication. To overcome such attacks, target area and route nodes need to be identified. In [42], authors presented state of the art survey of routing attacks and their countermeasures. Authors also provided a summary of security threats applicable to different commonly used MANET protocols. As per research done by authors, security threats are of two types namely, selfish behaviors and malicious attacks. Authors also presented measures to prevent these attacks.

Watchdog is the most popular IDS for intrusion detection. Researchers have repeatedly attempted to improve it or to compare it with their own model. In [43], author focused on limitations of existing IDS models specifically Watchdog. The author commented on MANET limitations in terms of communication, power consumption and limited computing capability. The limitation of model presented is inability to detect advanced attacks. The paper concluded with the need for robust, distributed IDS model which is safe from attackers.

2.7.2 Parameter Specific IDS Models

Depending on the application of MANET, performance parameter to which priority to be given may vary. Attempts to improve various QoS parameters are presented in this subsection.

Rule-based approaches are very popular in identifying malicious nodes. In [44], authors proposed rule based intrusion detection algorithm for most common intrusive attacks in MANET and presented a novel IDS model resistant to these attacks. In this anomaly approach based on cross-feature analysis, authors conducted an experiment in NS2 and claimed to achieve better false alarm rate in presence of different types of attacks separately. In this model, single node clustering protocol is used for cluster formation. One of the nodes with maximum score is elected as leader. Security of cluster head node is a major limitation of this approach.

In [45], authors proposed an approach based on distributed agent framework for intrusion detection in MANET. A layered architecture for each MANET node is used in the proposed case-based model. Node density against packet drop rate is analyzed in this experiment. Authors claimed that case based agents minimize network load by sharing it among neighboring nodes. Overhead of processing IDS agent databse is major limitation of this model.

On the contrary to existing agent-based approaches, data mining techniques are also proposed for intrusion detection models. In [46]. authors discussed an IDS agent based approach using data mining. In this anomaly approach, MANET is divided into two types of agent namely mobile agent and the home agent. The home agent is responsible for data collection from application to routing layer. The mobile agent continuously monitors its own system. Cross feature analysis is used for attack detection. The author claimed to achieve minimum false alarm rate.

MANET nodes use battery power for computation purpose. So, node energy is one of the important parameter to optimize. To disrupt the communication, attacker node may use energy draining attacks. In [47], authors presented an energy efficient IDS model for MANET. Authors evaluated energy levels of MANET under attacks such as grey hole and draining attack. Survivability performance of the proposed model is compared against these two attacks. The adaptation module trade-offs between energy consumption and parameters affected by the attack. Authors claimed that inclusion of adaptation module saves CPU energy up to 14%. Authors conducted this experiment using NS3 simulation tool.

Another intrusion detection approach for energy conservation of MANET nodes is presented in [48]. Authors suggested an AODV based IDS model for MANET to minimize energy consumption for packet transmission. Malicious nodes are identified based on trust level and data rate. Node behavior is categorized into three types namely, regular, malicious and suspicious nodes. Energy consumption parameters are adjusted based according to node to deal with. The confidence value of each node is maintained in trust table at each node. Route maintenance and sequence number handling of this model are same as AODV protocol. Performance of proposed model is compared with AODV based MANET using simulation. Performance metrics used for experimentation are packet throughput, energy consumption, and end-to-end delay. Authors claimed to achieve better results than plain AODV based IDS model.

2.7.3 Attack-Specific IDS Models

Researchers have put their significant efforts on a survey of the impact of these attacks on MANET and solutions to deal with these attack cost effectively. All such contributions are presented in this subsection.

In attacks such as black hole, attacker disrupts communication by not forwarding a packet received. In [49], author surveyed the efficiency of various intrusion detection schemes in MANET against the black hole attack. Authors claimed that AODV and DSR based schemes proved to be effective against routing based attacks. Authors claimed that proactive type of IDS systems suffers from routing overhead which can be eliminated by the use of reactive routing methods.

Another name for black hole attack is packet dropping attack. In [50], authors surveyed various techniques proposed over the period against packet dropping attack. Authors summarized root causes of this attack and provided state of the art review on research approaches to tackle the same. Authors commented on the usefulness of many such approaches proposed in literature to defend this attack.

Packet replication attack injures network in many ways such as falsifying data, extra resource allocation etc. In [51], authors commented on packet replication attack in MANET. They also proposed a defense mechanism for this attack. The model uses swarm intelligence technique for attack detection. This model is based on watchdog IDS module. In this model, each node maintains recently sent packets in the buffer. The model proposed is evaluated using parameters such as throughput, end to end delay, energy consumption etc. Authors claimed that use of swarm intelligence techniques significantly reduces energy consumption by MANET nodes.

In [52], authors presented a Logless Fast IP Traceback (LFIT) scheme against distributed denial of service attacks. As per authors investigation, frequent overwriting of packet markers in the dynamic ad-hoc network makes packet tracing susceptible to this attack. Each node maintains hash information. Accordingly, nodes keep track of partial path information probabilistically. This model is suitable to limited number of nodes.

In [53], authors discussed state of art methods to prevent black hole attack. They also presented trust-based routing method for black hole attack detection. This model contains two modules namely, watchdog and reputation system. Besides monitoring misbehaving nodes, Watchdog reports to reputation system which maintains reputation value at each node. The mechanism is repeated after a fixed interval. Authors claimed that this method can handle colluding attackers problem in MANET.

AODV is the most commonly used protocol in MANETs. Many researchers have put their efforts into improving security in AODV based routing. In [54], authors presented a novel IDS model to detect packet dropping, fabrication, and resource consumption attacks. In this AODV based approach, four modules work collectively for intrusion detection namely, traffic interception module, event generation module, attack analysis module and countermeasure module. Attack behavior against time is evaluated. Experimentation is carried in the NS2 simulation tool. Authors claimed to achieve less overhead for attack detection than existing models. This model is limited to three attacks mentioned only.

Measures over packet replication attack are observed in [55, 56]. Authors presented an IDS model based on swarm intelligence approach to prevent packet replication attack. Authors addressed the issue of packet replication in multipath MANET environment. In this model, Ant Colony Optimization (ACO) is used for route establishment in collaboration with Watchdog-Pathrator algorithm. The route with a highest collective value of node energy, bandwidth, and trust value is selected for data transmission. The experiment is conducted in the NS2 simulation tool. Performance of proposed IDS is evaluated using end-to-end delay, bandwidth, packet throughput etc.

Yet another AODV based approach for intrusion detection is presented in [57]. Authors proposed a scheme based on AODV protocol. This model uses dynamic learning process and is effective over common attacks namely, address spoofing, eavesdropping, packet forging, denial of service etc. Authors identified multi-dimensional features of attacks mentioned. Node positions are determined using principal component analysis using statistical theory. This model was claimed to achieve high attack detection rate and low false alarm rate.

Neural networks have many application areas such as sales, data validation, risk management etc. They are most suitable for data pattern validation. In [58], authors proposed an IDS model based on neural networks. This model focused on the black hole and grey hole attacks. AODV is used as a MANET protocol for implementation in this model. Audit source is prepared from a simulation of attacks. Audit source is further classified based on features selected. Performance parameters such as an end to end delay, packets sent and received packet throughput are used for model evaluation. Simulation tool called TANGARA is used by authors for experimentation. The limitation of this model lies in the detection of normal or malicious packet signatures only. It is not capable of identifying the type of attack.

In [59], authors presented yet another IDS model specifically for detecting black hole and grey hole attacks. Trust-based routing is a major characteristic of this model. Trust values are estimated by observing the behavior of neighboring nodes. Each node is monitored for a number of packets forwarded and to be forwarded. For each violation of threshold value, trust value of the node is decremented. The route with highest trust value is selected for communication. Authors claimed to save transmission energy due to traffic observance on limited routes only. This experiment was conducted using network simulator 2.32. Performance parameters used are packet delivery ratio, an end to end delay, route frequency, route load and average throughput.

2.7.4 Routing Protocol-Specific IDS Models

In a multi-hop environment such as MANET, routing of packets is the biggest challenge. To ensure secure routing, routing protocol plays an important role. There are two approaches significantly noted in the literature. The first approach is improving existing routing protocols. Whereas, the second approach found in the literature is developing a new protocol for MANET. All notable efforts by researchers are presented below.

In 2002, authors [60] proposed a new IDS model named CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks). They developed a new protocol for MANET communication and proposed a novel scheme for intrusion detection based on it. Authors claimed that, this model is effective on limitations of Watchdog and Pathrator. In this protocol, each node learns from all its neighboring nodes in its radio range. Misbehaving nodes are prohibited from further communication. Proposed scheme consists of four components namely: Monitor, Reputation System, Trust Manager, and Path Manager. The monitor is responsible for inspecting node to node message communication and noting observations. Trust Manager warns other nodes by sending ALARM messages. Reputation system keeps track of node rating and path manager deletes the path containing malicious node(s). The major limitation of this protocol is that, as nodes are using ALARM messages to warn about malicious nodes, an attacker may also send false ALARM messages to disrupt communication and misguide the system about trustful nodes.

In [61], authors presented a modified version of DSR protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks). Every node in MANET has four components: a monitor for observations, reputation manager for first-hand reports (based on self-observation) and trusted second-hand reports (based on neighbor node ratings), trust manager to update trust values of nodes in its radio range, and a path manager to decide on a trusted path. Authors claimed that routing performance of protocol proposed is cost effective and efficient on QoS parameters than DSR protocol.

In [62], authors presented IDS which forces nodes to cooperate in communication. This system is updated version of CONFIDANT and also contains reputation and monitoring system. CONFIDANT updates trust values in the case of positive as well as a negative rating but CORE updates in case of positive trust reports only. Authors claimed that the CORE is best suited to prevent denial of service attack. The CORE can be differentiated with basic Watchdog and Pathrator in two aspects. First, CORE is designed to improve overall communication performance whereas, Pathrator helps genuine node to prevent communication with misbehaving nodes. Second, it is useful in wide variety of application functions at network and application layer operations whereas the Watchdog-Pathrater is designed for routing purpose only.

The popularity of AODV protocol made intruders seek for limitations of it. To defend against intrusive attacks based on AODV limitations, solid countermeasures are needed. In [63], authors proposed a specification based IDS. Authors discussed various vulnerabilities and attacks against AODV protocol in MANET. To predict correct runtime behavior of AODV, Finite State Machine (FSM) is used. Authors extensively criticized and identified loopholes associated with AODV leading to falsified route opportunity for intruders. This approach is useful only with MANETs based on AODV protocol for communication. The model presented by authors is less useful for routing protocols other than AODV.

Several approaches to eradicate attacks such as packet fabrication and replication are found in the literature. In [64], authors discussed a technique to improve the performance of Watchdog and Pathrator using specific time frame allotted for evaluation to individual nodes. As per this technique, if, the node is not replying in a specific time frame, then it is declared as a misbehaving node. Authors also highlighted the need of securing routing in MANET.

In [65], authors presented an intrusion detection model based on the artificial immune system to detect misbehaving nodes. This model was proposed to overcome security issues in the DSR protocol. Authors implemented this model using simulation tool called Glomosim and claimed to achieve better results than conventional models.

2.7.5 Algorithm-Specific IDS Models

To overcome limitations of existing IDS models, it has become essential either to improve existing models further or to develop new methods and algorithms. Overview of such notable efforts by researchers is presented in this subsection.

In 2005, authors proposed Markov Chain based anomaly algorithm for intrusion detection [66]. The entire network is divided into non-overlapping zones. Each zone contains two types of nodes, namely intrazone nodes and gateway nodes. The gateway node is the node connecting to more than one zone and the intrazone node is responsible for generating alarms. The authenticity of alarms based on traces by intrazone nodes is a major limitation of this model since security of intrazone nodes is not taken care in this model.

Agent-based IDS research approaches are also significantly noted in the literature. In [28], authors presented a new distributed and cooperative model for intrusion detection in MANET. Each node in this model acts as IDS agent and is equally responsible for intrusion detection. Each node communicates its intrusion state information to neighboring nodes. Other IDS agents collaboratively contribute to intrusion detection based on local and global responses. Authors claimed to achieve detection of multiple layer intrusions. Security of IDS agent is not focused in this anomaly IDS architecture.

In [67], authors presented an IDS model based on timed automata theory. The DSR protocol is used for route establishment in this model. Randomly, fair few nodes are selected as monitoring nodes. Periodically, re-election for monitor nodes is conducted. This model works in two phases namely selection phase and maintenance phase. Node selection for packet transmission is done using timed automata until it reaches the destination node. Authors claimed to achieve minimum false alarm rate using this model. However, security of monitoring node is not focused by authors.

On the contrary to central IDS agent-based approaches, distributed models are noted in the literature [68]. Authors identified limitations of the scheme for intrusion detection called Real-time Intrusion Detection for Ad hoc Networks (RIDAN). In RIDAN, there is no central coordinator and cooperating function for monitoring network. To overcome the same, authors proposed new scheme containing central coordinating node. Authors also claimed to optimize energy with the use of this model.

To keep track of genuine nodes, reputation-based schemes are observed in the literature. In [69], authors proposed a reputation based IDS system for MANET. In this model based on the DSR protocol, each node keeps track of reputation value of itself along with its neighboring nodes in one hop. Each node categorizes other nodes into three trust levels namely trustworthy, untrustworthy and trustworthy undecided. Reputation value is dependent on packet drop rate. Each node updates its reputation table based on directly observed values.

In 2010, authors [70] presented an IDS model based on Hidden Markov Model . As per this model, MANET is divided into clusters. Each cluster contains monitoring agent and forms monitoring sequences. Each node in cluster detects attack behaviors by declaring two states namely, normal state or abnormal state. Authors claimed that this model is an effective way for attack detection. For misbehave detection by any neighboring nodes, average sequence value of last packet transferred is used. Authors committed that, this is simulation-based experimentation and practical demonstration results may vary.

In [71], authors discussed a model to improve existing IDS model called Web of Trust (WoT). In WoT, MANET nodes do exchange trust certificates of other nodes in its radio range. For maintenance of the same, each node must have sufficient memory to store certificates. Also, it is not cost effective to exchange data frequently. To overcome these limitations of WoT model, authors presented a new method in their research. In this Certificate Management Node (CMN) method, one node from each cluster is assigned the responsibility of issuing trust certificate to other nodes in its radio range. Certificate of the newly admitted node is also verified by this proxy node. Authors claimed to achieve better results using this method than WoT and other security models in MANET.

Intrusion detection approach using Dempster-Shafer rule for collecting attack traces is presented in [72]. Trustworthiness of a node is decided based on feedback from neighboring nodes in this model. Dempster-Shafer is used as a set of possibilities and probabilities. Authors differentiated between Bayesian theory and Dumpster-Shafer and demonstrated the usefulness of it in intrusion detection.

In [73], authors proposed continuous authentication scheme for intrusion detection to achieve security in MANETs. Authors discussed distributed approach for intrusion detection based on Dempster-Shafer fusion theory. Authors also highlighted limitations of the biometric authentication system. Nodes were used as sensors for anomaly detection. Trustworthiness of sensors was key aspect of this model. Authors compared proposed scheme with existing two models namely data fusion and without data fusion.

Apart from regular routing protocols, some approaches are noted where use of Way Point Routing (WPR) is noted [74]. Authors presented a lightweight intrusion detection model based on WPR protocol. In this model, the hierarchy of routes is maintained initially. In case of a broken link, way out point to repair the route is identified instead of the discovery of new routes. The same is done using intersegment on each route. A new routing protocol is proposed by authors called DOA. It contains a blend of two existing on-demand protocols namely DSR and AODV. Performance parameters used for evaluation of this model are packet delivery ratio, an end to end delay, control overhead, and average route length.

In [75], authors presented a generalized cooperative intrusion detection architecture for MANETs. This model was specifically designed for military applications. MANET nodes are divided into different levels. At each level node representatives are responsible for providing data and securing communications for its child nodes. This approach tries to accommodate host based as well as network-based IDS. The limitation of this model lies in analysis of data at different layers which may flood the network and lead to poor routing performance. This model is not evaluated against advanced attacks.

Giving utmost importance to the bandwidth available at route nodes, few authors presented a method for intrusion detection for MANET using bandwidth shared acknowledgment scheme [76]. Authors claimed to overcome limitations of two conventional methods namely, 2-hop acknowledgment and source directed acknowledgment. The summative bandwidth available at each route from source and destination is calculated well before sending data packets. Route with optimum available bandwidth is selected for acknowledgment exchange. Authors claimed to achieve seamless delivery of acknowledgment and efficient intrusion detection using this method.

In 2014, authors [77] presented a novel model for intrusion detection. In this model, a combination of two popular IDS approaches namely EAACK and LTB-AODV are used. EAACK uses three-layer security for communication whereas, LTB-AODV focused on specific attacks such as grey hole and black hole attacks. Performance metrics used for model evaluation are routing overhead, packet delivery ratio, and average packet throughput. Experimentation is done in NS 2.34 on Linux platform. This model is implemented considering only 15 MANET nodes which seems insufficient.

An attempt to secure MANET communication using fuzzy logic theory [78] is also observed in trust-based IDS model. This model used fuzzy theory for making a distinction between trustworthiness decisions. Fuzzy logic rules are used to update nodes trust. Each node maintains a trust table and blacklist. Blacklist consist all neighboring nodes with lower trust value. Performance parameters used for this experimentation are satisfaction rate, number of good recommendations and detection ratio of malicious nodes.

In [79], authors presented a model to balance resource utilization by MANET nodes. In this model, the whole MANET is divided into multiple clusters. Each cluster with highest remaining resources is nominated as a cluster head. To elect cluster head, incentives based scheme is introduced by authors. Security threats in identifying cluster heads are also discussed in this paper. Authors claimed to optimize resource consumption in presence of selfish nodes and achieve long-lasting MANET performance.

An encryption-based intrusion detection model based on timestamps is presented in [80]. For every encrypted packet, timestamps are allotted. This scheme uses RSA algorithm for encryption purpose. Experimentation is done using OMNET++ simulation tool. Authors claimed that, due to Packet Key Exchange mechanism, energy consumption by each communicating node gets reduced. Performance parameters used for evaluating proposed model are packet delivery ratio, latency, and energy consumption fraction.

In [81], authors proposed a distributed stochastic model based on a combination of continuous authentication and intrusion detection. Biosensors are used for authentication purpose.

IDS nodes are modeled as sensors. Authors claimed that energy state at each node and their securities are achieved using Markov decision process. To find optimal policy, Gittins indices are used. An Objective function is formulated using multi-armed bandit algorithm. Authors also claimed to achieve lower complexity than existing models.

Yet another model to overcome limitations of Watchdog-Pathrator model is presented in [82]. Authors focused on limitations of Watchdog in detecting selfish nodes. The proposed model is named as Collaborative Contact-based Watchdog (CoCoWa). This scheme works well for local intrusion detection and network intrusion detection as well. Authors claimed to reduce detection time, false positives and false negatives simultaneously.

2.8 Challenges and Unaddressed Issues in Existing IDS Models

The performance of most of the intrusion detection systems is highly dependent on routing protocol used for MANET communication. Limitations of existing routing protocol and existing intrusion detection systems are presented below.

1. **Non-availability of the balanced dataset for MANET attacks**

   Looking at the diversity of attributes affected by attacks over MANET, it is very difficult to develop a comprehensive dataset containing all attack signatures. Because of the same, no standard dataset is found in literature which can be used to evaluate any IDS system effectively [46]. Although attempts to build a dataset for specific attacks are observed in the literature, it has its own limitations [83–85].

2. **Poor resistance towards multi-objective advanced attacks**

   Advanced attacks generally involve a combination of multiple attacks. Such types of attacks contain combination of active and passive attacks. To deal with multi-objective attacks is very much complicated and needs designing of robust intrusion detection mechanism [86]. These attacks usually affect multiple network layers. Performance parameters affected by multi-objective types of attacks are different at each execution. That is why, very few attempts prevent multi-objective attacks are observed in the literature.

3. **Most IDS are independent programs**

   Many researchers working in MANET security proposed IDS models which contains intrusion detection as a separate program [87]. However, it is impossible to separate routing and communication security from each other. Secure routing is base of any MANET environment and helps in the construction of better IDS. Such independent IDS programs can easily be attacked by attackers resulting in poor performance.

4. **Limitations of routing protocols**

   Most common routing protocols in MANET used so far in literature are Ad-hoc On-Demand Distance Vector Routing (AODV), Optimized Link State Routing (OLSR), and Dynamic Source Routing (DSR). Internet Engineering Task Force (IETF) has recommended these widely used protocols for implementation [88]. However, these protocols have their own limitations. Some security attacks found are specifically designed on the basis of limitations of these protocols [89, 90]. A reliable routing technique less susceptible to such attacks is required.

5. **Most of the existing intrusion detection systems are parameter specific**

   Most of the intrusion detection systems discussed so far in literature are aimed at improving predefined performance parameters. These parameter specific IDS focused on optimizing some of the performance parameters which resulted in poor MANET security models. Very few attempts are observed in literature at categorizing and improving comprehensive performance parameters. An IDS addressing issues mentioned is needed to ensure secure communication.

2.9 Chapter Summary

To study any network security system, thorough understanding of communication protocols, its characteristics and node behavior is essential. Dynamism of nodes in MANET should also be critically evaluated. Intrusion detection systems also vary greatly in nature. This chapter introduced MANET organization, topologies and security challenges. It also provided security attacks and their influence on MANET communication.

This chapter presents a detailed overview of existing intrusion detection models and research approaches. Based on the nature of these models, they are categorized among separate subsections. Contributions by researchers so far in this domain vary significantly in terms of the routing protocol used, architecture proposed, attacks targeted and algorithms used. Researchers have significantly put their efforts in improving accuracy and minimizing false alarm rate of existing IDS proposed over the period. Limitations of routing protocols in securing communication is another key research area. Overall, there is need of IDS which considers dynamic nature of MANET and results in high accuracy. It must be reliable, robust and invulnerable to selfish and misbehaving nodes. At the same time, it should be able to handle trade-offs between high performance and resource consumption.

Chapter 3

PSO Based Existing Research Approaches and Selection of Performance Parameters

3.1 Overview

Swarm Intelligence (SI) is a technique in artificial intelligence which studies nature-inspired algorithms [91]. SI has evolved tremendously since last two decades. SI techniques such as Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Fish Schooling (FS), Ant Clustering Algorithm (ACA), and Flower Pollination Algorithm (FPA) have been used successfully in a wide variety of applications ranging from electronics to medical science. This chapter presents an overview of publications on intrusion detection using PSO algorithm found so far in the literature. Based on extensive literature review, attributes selected to evaluate the performance of routing protocol are presented in section 3.3. Section 3.4 presents performance parameters used to evaluate IDS.

3.2 Particle Swarm Optimization

Swarm Intelligence is a discipline that deals with computation methods to solve complex problems by using methods inspired by the collective social behavior of relatively homogeneous swarms [92].

Particle Swarm Optimization (PSO) is a swarm based stochastic optimization technique invented by James Kennedy and Russel Eberhart [93]. This algorithm is based on social behavior and movement dynamics of birds, insects, and fish. This technique is best suitable to continuous variable problems. PSO is successfully been applied to structural optimization, neural technology, shape technology etc. Major advantages of this heuristic technique are a simple implementation, scalability for designing variables, concurrent processing and efficient global search.

Birds adjust their flying as per their own experience and experience from the swarm. Each of the members tries to reach optimum position using this experience. Each particle keeps track of best fitness value achieved so far called pbest and the best value by neighboring coordinates called gbest. Particles keep on changing their velocity based on pbest and gbest locations leading to the optimum location. Particles try to modify its position using the following information:

- the current positions,
- the current directions,
- the distance between the current position and pbest, and
- the distance between the current position and the gbest.

The modification of the particles position can be mathematically modelled according the equations 3.1 and 3.2:

$$V_i^{k+1} = \omega V_i^k + c1 * rand() * (pbesti - s_i^k) + c2 * rand() * (gbest - s_i^k).... \tag{3.1}$$

where,

v_i^k : direction of agent i at iteration k

ω : weighting function

c_j : weighting factor

rand : uniformly distributed random number between 0 and 1

s_i^k: current position of agent i at iteration k,

$pbest_i$: pbest of agent i

gbest: gbest of the group.

$$s_i^k + 1 = s_i^k + V_i^k + 1 \tag{3.2}$$

The beauty of this algorithm is that required performance attributes can easily be accommodated. In [3–6], authors suggested that swarm intelligence algorithms such as PSO serves better for route finding in dynamic networks like MANET. Following are the major variants of PSO [94]:

1. **Binary PSO**

   In random value parameter (rand) in PSO route guidance equations, only real numbers are allowed. To deal with discrete optimization problems, Binary PSO (BPSO) was evolved. BPSO constrains velocity values in [0,1] where 1 means 'included'and 0 means 'not included'.

2. **MINLP PSO**

   This version of PSO was developed to solve nonlinear kind of problems. MINLP stands for 'Mixed Integer Non-Linear Problem'. Equality constraint is estimated through this variant.

3. **Hybrid PSO**

   PSO can be further modified to fit the problem space. The same can be done by using a combination of versions discussed above. Multi-objective functions are used to achieve a desirable solution.

A modified version of PSO algorithm to optimize it for MANET environment is presented in this chapter.

3.3 Publications on PSO based Intrusion Detection

In [94], authors comprehensively surveyed and compared PSO-based methods published in 2315 research papers. Authors claimed that 536 papers related to improved PSO methods are surveyed. Authors discussed various applications of PSO and also commented on modifications suggested in PSO by researchers so far. Various types of particles and their use in specific application domain are discussed by authors in this research article. Authors also presented the comparative table containing model-specific PSO parameter values used so far by researchers in this paper.

In [95], authors presented a survey on PSO based applications and categorized the same into 26 broad areas. The author claimed to review 700 research papers stored in IEEE explore discussing PSO applications. The author pointed enormous growth in the use of PSO for various applications ranging from medical, electrical, electronics, image processing, signal processing, robotics etc.

In [96], a rule generation model for misuse intrusion detection using statistical methods and PSO algorithm applied in MANET is presented. This model focused on records which are mistakenly classified as attacks by providing comprehensive fitness function. Authors claimed that proposed model finds records with high speed than conventional models.

In [97–99], authors presented state of the art survey on applications of particle swarm optimization and its variants. They commented on research in swarm intelligence techniques in various computational domains. Authors also summarized approaches based on modified PSO and claimed that PSO serves better in intrusion detection than conventional algorithms.

In [100], the author presented an algorithm for network-centric target localization based on dedicated nodes called mobile robots. The author demonstrated the use of modified PSO algorithm in quicker convergence and collaborative navigation using MATLAB simulation.

Approaches, where PSO is used for clustering, are also noted in the literature [101]. The model presented used three objective functions based on QoS parameters viz. trust value, lifetime and available bandwidth. Authors claimed to achieve multiple objectives using PSO objective function. This is the first attempt in literature to achieve three performance parameters satisfactorily using PSO algorithm. Modification of pBest and gBest PSO parameters supports analogy used for research work presented in this thesis.

To reach at never improving state is called convergence state. In [102], authors presented thorough convergence analysis of PSO algorithm. The author claimed that some of the original PSO parameters add no flexibility to the algorithm and such parameters must be discarded to use this algorithm more effectively in the specific application domain. This research motivated notably to develop a new PSO based IDS presented in this thesis.

In [103], authors discussed a novel model based on a blend of two algorithms namely support vector machine (SVM) and particle swarm optimization. Size of fitness is calculated using SVM and route finding is handled using PSO. A concept called punishment factor is introduced by authors in this model. Punishment factor and kernel factors are evaluated using PSO and SVM simultaneously. Performance parameters used for measuring the effectiveness of this model are recognition rate, recognition time, normal data on support vector, support vector count etc. Authors claimed that this model is better for reducing false alarm rate and improving the accuracy of intrusion detection.

In [104], authors presented a PSO based approach for attack detection. In this scheme, PSO based fitness function is used for attack detection and to identify the type of attack. This model mainly targets wormhole and web exploits attacks. Gateway for organizing node dynamism and route maintenance is used in this model. Authors claimed that this model achieves optimum false alarm rate.

In [105], authors examined existing monitoring based intrusion detection models. Authors claimed that simulation tools such as NS2, glomosim, and OPNET are unable to obtain accurate results on false alarm rate due to varying noise and different propagation directions. They also proposed a noise generator model using simulation in glomosim to mitigate this issue. Authors used two performance parameters to evaluate proposed model such as a number of nodes suspected and total false positives. Authors also claimed to improve monitoring based intrusion detection techniques using model presented.

In [106, 107], authors explained the significance of various swarm intelligence techniques in intrusion detection under three main categories like Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) and Ant Colony Clustering (ACC). Authors claimed that hybrid PSO approaches are superior to hybrid ACO under various performance criteria.

Anomaly-based PSO intrusion detection attempts are also noted in the literature [108]. Authors commented on advantages and disadvantages of anomaly techniques namely, PSO based clustering, PSO with neural networks, PSO and Support Vector Machine, feature subset based PSO etc. Authors claimed that use of PSO improves intrusion detection performance. Authors also expressed need of setting PSO parameters effectively to achieve better performance and amendment of position and velocity formula appropriately.

In [109], authors proposed a MANET link performance model using ACO and PSO. ACO is used for route establishment using mobile agents. Whereas, hybrid PSO is used to find next node with optimum objective cost and a minimum end to end delay. This model is scalable and applicable to large networks also. Authors claimed that this PSO-ACO model generates better link performance than conventional models over the period of time.

Sybil attack is yet another serious advanced attack over MANET where attacker nodes take the identity of other legitimate nodes. In [110], authors presented a novel model specifically to fight against Sybil attack. Sybil attacker generally tries to replicate the node identity and confuses the network. For calculating node fitness, PSO algorithm is used in this model. For information exchange, DREAM and AODV protocols are used. This model focuses on higher MANET layers namely, Secure Shell (SSH) and Secure Socket Layer (SSL). Authors used GPS for node position identification. Experimentation is carried using NS2 simulation tool. Authors also presented a survey of MANET routing protocols and relevant attacks.

Although research on the use of particle swarm optimization algorithm is proved to be effective over security attacks over MANET, very few attempts were identified in the literature for effective utilization of cooperative nature of PSO algorithm for secure routing. Specifically, route guidance using PSO is yet to be achieved up to a satisfactory level. To find best fit node while identifying route nodes is a key point of the proposed model.

3.4 MANET Performance Parameters

This research is conducted in two parts, firstly finalizing routing parameters in MANET and secondly, implementation of intrusion detection algorithm with predefined performance parameters. To achieve effective routing in MANET, attribute selection is a most important part. Researchers [111] have focused on attribute selection guidelines in depth. However, identifying features contributing to intrusion detection and achieving the quality of service simultaneously is still an elementary field.

3.4.1 Average End-to-End (ETE) Delay

End-to-end delay (ETE) is the delay incurred in the transmission of a data packet from source to destination (received time minus sent time) [112]. As far as communication in MANET is concerned, delay factor varies from node to node. Varying receiving and transmission capabilities of nodes have high impact on ETE delay.

To calculate average ETE delay, it is essential to evaluate ETE delay at all nodes on the transmission line. To identify the best route for data transmission, an average of ETE delay at intermediate nodes need to be calculated. While calculating ETE delay, three factors should be considered namely transmission delay, processing delay, and propagation delay. Assuming there is no congestion in the network (queuing delay can be neglected) and there are N nodes on the selected route, ETE delay is modeled as,

$$d_{end-end} = N[d_{trans} + d_prop + d_{proc}] \tag{3.3}$$

where,

$d_{end-end}$ = end-to-end delay

d_{trans}= transmission delay

d_{prop}= propagation delay

d_{proc}= processing delay

Also,

$$d_{trans} = L/R \tag{3.4}$$

where,

L= packet size,

R= transmission rate is R bits/sec

3.4.2 Packet Loss Ratio

Packet loss occurs when packets transmitted from source node are not received at the destination node. Factors such as errors in data transmission, network congestion, buffer overflow and intrusive attacks result in packet loss. Maintaining transmission window may reduce packet loss in communication. When the threshold of packets accumulated in the buffer at sender node is reached, the flow of transmission should be slowed down. Threshold value depends on link capacity. Link capacity is measured in terms of maximum transmission count of data packets.

Packet Loss Ratio (PLR) is the ratio of the total number of data packets dropped to the total number of data packets sent [113]. Poor connection between two communicating nodes results in high packet loss. Higher PLR usually results in poor quality of service in wireless communication and lowering packet throughput.

3.4.3 Average Packet Throughput

In general, the rate of successful packet transmission is called as throughput of communication channel. Throughput is measured in bits per second or number of data packets per second. The rate of successful packet delivery varies from node to node. Responsible factors affecting transmission channel throughput are node energy limitations, poorly configured system, the unreliable medium of communication etc.

In an asynchronous environment such as MANET, the throughput of the nodes present on route opted for data packet delivery is evaluated to calculate throughput of the link. The average number of packets successfully received by all nodes on the optimal route per second is termed as average packet throughput [114, 115].

3.4.4 Hop count

If two communicating MANET nodes are in radio range of each other, peer to peer communication is possible. However, due to dynamic and ever-changing MANET environment, it's hardly possible for nodes to be always in radio range of each other. In such scenario, hopping becomes unavoidable for communication. Every intermediate node contributed for packet forwarding is counted as one hop [116]. The number of hops required to deliver packets from source to destination is called hop count. If there are n nodes on a route chosen for communication, then n-1 is the hop count.

3.4.5 Signal to Noise Ratio

Noise is any type of disruption with communicating links. MANET communication usually suffers from signal noise due to unpredictable wireless media. Reasons behind noise in communication links are broken links, link outage, the poor transmission capacity of MANET node etc. Signal to Noise ratio (SNR) is the level of signal strength relative to the noise level [116–118].

SNR is generally measured in decibels.

$$SNR = P_{Signal}/P_{Noise} \tag{3.5}$$

Where,

P_{Signal} is average signal power and,

P_{Noise} is average noise power

Higher SNR is positive and results in efficient delivery of data packets. High noise power leads to poor communication quality.

3.4.6 Data Rate available on the route

Node dynamism often incorporates varying bandwidth at MANET nodes. Higher available bandwidth at different nodes collectively results in improvement in the quality of transmission [119]. Bandwidth estimation of an individual node is based on bandwidth availability of neighboring node, channel bandwidth etc.

Multipath routing produces different routes for communication between the source and destination nodes. In general, routes are obtained by flooding ‘hello’packet in the network. Routing protocol should follow the route with maximum available bandwidth for communication.

3.5 IDS Performance Parameters

There are four parameters to measure the accuracy of an IDS. Most of the packet signatures observed at MANET nodes are varying in nature. IDS classify these signatures into abnormal and normal signatures. The accuracy of this classification is termed as the efficiency of any IDS. The four IDS states in packet signature evaluation are True Positive (TP), False Negative (FN), True Negative (TN), False Positive (FP) [120]. These performance parameters are discussed below.

3.5.1 True Positive Rate (TPR)

A major requirement of IDS is the high positive rate. It is also called as recall or sensitivity in terms of information retrieval. Based on training set available at MANET node, packet signatures are compared and declared as normal and abnormal traces. The fraction of attack signatures correctly diagnosed out of total signatures received is termed as true positive rate.

Formula for TPR is:

$$TPR = TP/(TP + FN) \tag{3.6}$$

Where,

TP- True Positive

FN- False Negative

3.5.2 False Negative Rate (FNR)

It is the most serious type of state in attack detection. The fraction of attack signatures incorrectly diagnosed as legitimate packets (including not detected) is called as FNR. It highly affects accuracy percentage of IDS. FNR is defined as,

$$FNR = FN/(TP + FN) \tag{3.7}$$

Alternatively,

$$FNR = 1 - TPR \tag{3.8}$$

Where,

TP- True Positive

FP- False Positive

FN- False Negative

TPR- True Positive Rate

3.5.3 True Negative Rate (TNR)

The true negative rate is also termed as specificity. TNR is a fraction of non-intrusive signatures correctly diagnosed as normal signatures.

$$TNR = TN/(TN + FP) \tag{3.9}$$

Where,

TN- True Negative

FP- False Positive

3.5.4 False Positive Rate (FPR)

Fraction of normal signatures incorrectly diagnosed as intrusions is termed as FPR.

$$FPR = FP/(TN + FP) \tag{3.10}$$

Alternately,

$$FPR = 1 - TNR \tag{3.11}$$

Where,

FP- False Positive

TN- True Negative

TNR- True Negative Rate

3.5.5 Accuracy and False Alarm Rate

Based on TPR, TNR, FPR and FNR, accuracy and False Alarm Rate (FAR) are calculated. Accuracy defines a total number of correctly identified abnormal signatures out of total packet signatures encountered. Whereas, total incorrectly and not detected signatures are termed as false alarm rate. Based on four performance parameters discussed above, Formulae for accuracy and false alarm rate are as follows [121]:

$$Accuracy = [TP/(TP + FN + FP + TN)] * 100 \tag{3.12}$$

Where,

TP- True Positive

FN- False Negative

FP- False Positive

TN- True Negative

and,

$$FalseAlarmRate = [FP/(FP + TN)] * 100 \tag{3.13}$$

Where,

FP- False Positive

TN- True Negative

3.6 Chapter Summary

Researchers have repeatedly indicated that, PSO is best suitable swarm intelligence technique to dynamic and distributed environment of MANET. As like MANET, PSO has the cooperative and collective responsibility of each particle. Decision making is the most resembling part of PSO and MANET. However, its stochastic nature must be handled appropriately to fit the requirements of MANET. Mapping of PSO parameters with MANET performance attributes is another challenge. PSO is used in different roles in intrusion detection approaches such as classification, clustering, route guidance, node fitness evaluation etc. Most of the models presented in literature tried to use PSO varidly. PSO for route guidance and agents based anomaly approach for intrusion detection is used in this thesis. Key aspect of this research is that, PSO is used to find a route with best-fit intermediate nodes. Considering most of the limitations of research approaches found in the literature, this thesis proposes an evolving IDS algorithm for MANET using PSO.

MANET attacks vary in nature and affect the different quality of service parameters. Multi-objective intrusive attacks are even more difficult to tackle. Threshold values for these QoS parameters is cumbersome task. It is easier to generate set of normal signatures and to compare identified signatures with the same. Packet signatures with unsatisfiable parameter values are classified as abnormal signatures. Most of the research approaches in the literature are based on parameter specific intrusion detection models and presented in chapter 2. To achieve efficient routing in MANET, it is essential to accommodate common QoS parameters. In this approach, PSO is used to achieve most of the essential QoS parameters. On the other hand, IDS performance parameters such as accuracy and false alarm rate are evaluated in this research.

Chapter 4

PSO-based Intrusion Detection Algorithm

4.1 Overview

Despite endless efforts by researchers in the improvisation of security measures in an ad-hoc environment such as MANET, secure routing is still like daydreaming. Insecure channels, dynamic topology, node dynamism, ever-increasing advanced attacks are key challenges yet to be addressed. Limitations of existing popular MANET routing protocols have provided a gateway for attackers to breach the security. To balance communication overhead and secure routing is major issue to overcome. To address such issues, an evolving intrusion detection algorithm for MANET is presented in this thesis.

This research is divided into two parts. In the first part, PSO algorithm is proposed as efficient packet routing method. The second part focuses on the development of evolving IDS. The detailed implementation plan is presented in this chapter. This experiment is conducted using popular simulation tool called Network Simulator (NS2). Other network simulation tools popular among researchers are OPNET, Glomosim etc.

4.2 Network Simulator 2 (NS2)

NS2 stands for Network Simulation Tool version 2. Most of the researchers working in the field of networks have used NS2 for their experimentation [122]. NS2 is open source tool and the best discrete event simulator for networking research. The experiments which need packet level monitoring can easily be implemented using NS2. It provides ready support for routing protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Dynamic Source Routing (DSR), File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) [123]. NS2 has become a time-saving tool for researchers working in networking domain. NS2 is suitable to simulate wired as well as wireless networks. It was developed initially for UNIX operating system. The scripting language used for NS2 is Tool Command Language (TCL). It is possible to run NS2 in Unix platform and also in Windows operating systems using Cygwin tool.

4.2.1 Features of TCL

The reason behind overwhelming response by researchers to TCL scripts in NS2 is its lightweight nature. Following are the key features of TCL [124].

- TCL is platform independent scripting language. It runs across all platforms such as Windows, Mac and all UNIX platforms. It's write once, run anywhere nature made it popular among researchers working in the networking domain.
- TCL existing applications can easily extend to other programming languages such as C, C++, Java etc.
- TCL has a rich set of networking constructs and functions.
- It is open source and capable of executing commercial applications without any issues.

4.2.2 Network Animator (NAM)

NAM is graphical animation tool designed to animate packet tracing and works in conjunction with NS2. Trace files are generated as an output of executing real-time network environment using network simulator. These trace files are used as input to NAM to generate graphical representation.

Table 4.1: Simulation Parameters

Sr. No.	**Simulation Parameter**	**Value**
1	Simulator	Network Simulator 2
2	Node Size	200
3	Channel	Wireless Channel
4	Mac Type	Mac 802.11
5	Queue Type	Queue/Drop Tail/ PriQueue
6	Queue Length	200 Packets
7	Antenna Type	Omni Antenna

4.3 Experiment Design and Simulation Environment

Initialization of proper simulation parameter values plays a vital role in the performance of any simulation experiment. Table 4.1 presents values used for initialization in our experiment.

Fitness function used for node evaluation is:

Fitness Function, F_i= Min (Distance between node i and Destination Nodes)

To obtain statistical analysis, 10 trial runs are performed. At each PSO search iteration, the route gets established towards destination node progressively. Performance parameters in fitness function can possibly be added as per model requirement. While route establishment, the best fit node with optimum QoS parameter is chosen as a next route node.

4.4 Simulating Dynamic Source Routing (DSR) Protocol

Dynamic Source routing is another reactive routing protocol. This protocol is based on link state routing protocol. DSR routing contains mainly two phases: route identification phase and route maintenance phase. Each node maintains route information in the cache. The packet header contains information of all intermediate nodes visited by the packet which helps in route guidance. Step-wise execution of communication using DSR are as follows:

Step 1: Source node floods network using route request (RREQ) packet.

Step 2: Each intermediate node forwards RREQ packet to its neighboring nodes after append-

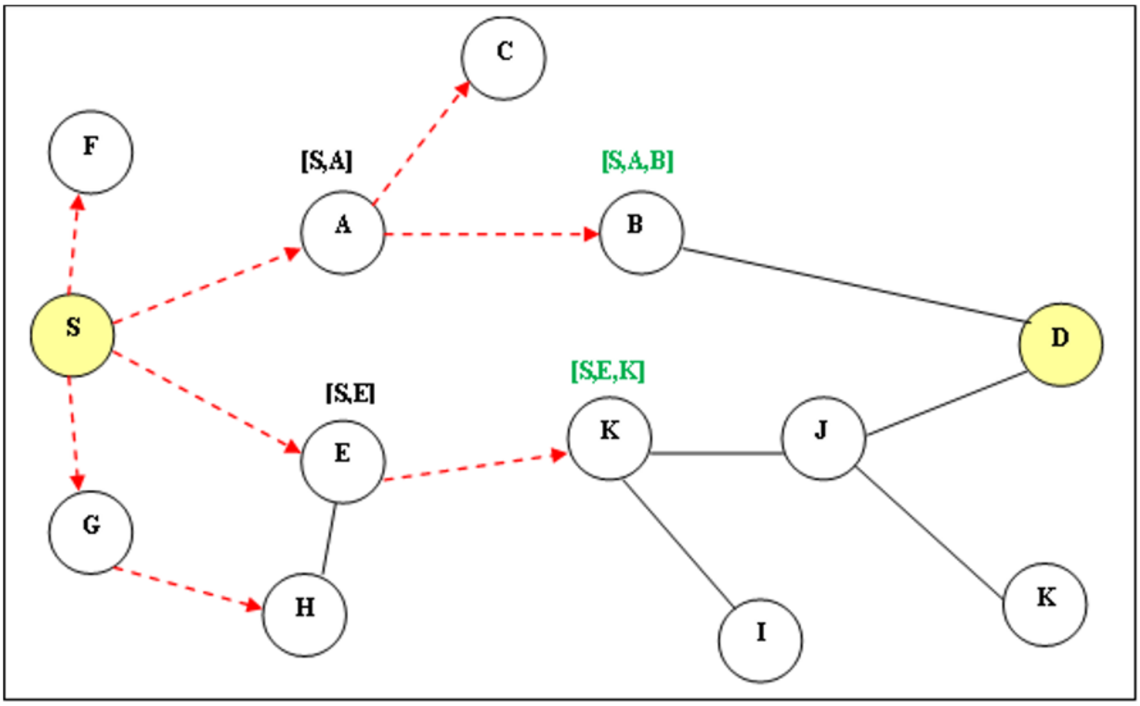


Figure 4.1: Route identification using DSR Protocol

ing its node name to the packet header.

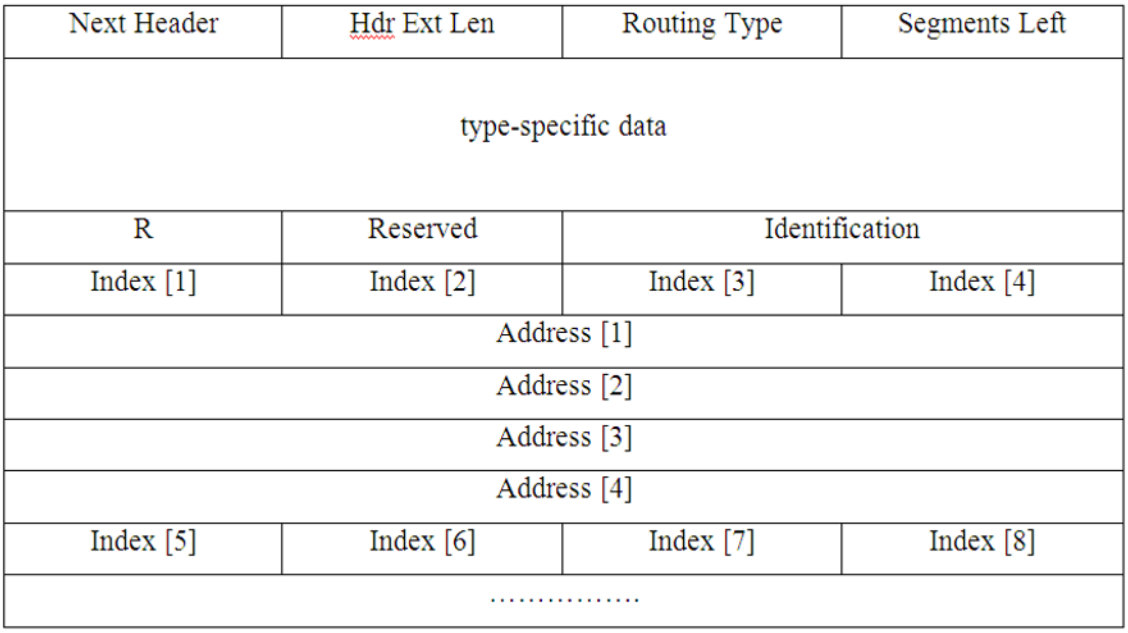
Step 3: Destination node on receiving RREQ packet unicast RREP to source node by simply reversing the hops received through packet header.

Step 4: If a route in the record received through packet header in RREQ is broken, the destination node may perform its own route discovery to the source node.

Figure 4.1 shows route discovery process in DSR routing. Red arrows represent RREQ broadcast. S and D represent source and destination nodes respectively. Since route traversed by RREQ packet is through node A, route information in packet header at node B contains route [S, A, B]. Destination node D will have two routes. The first route is through nodes A and B. Second route is through nodes E, K, and J. Route with minimum traverse time is backtracked by destination node.

4.4.1 DSR Header Format

Routing header is used by source node as a way to packets destination. The figure 4.2 shows routing header used by DSR protocol.



Next Header	Hdr Ext Len	Routing Type	Segments Left
type-specific data			
R	Reserved	Identification	
Index [1]	Index [2]	Index [3]	Index [4]
Address [1]			
Address [2]			
Address [3]			
Address [4]			
Index [5]	Index [6]	Index [7]	Index [8]
……………			

Figure 4.2: DSR Routing Header

The fields associated with DSR routing header are:

- Next Header: It is used as identification of packet header
- Hdr Ext Len: It represents the length of the header
- Routing Type: It represents the type of routing used.
- Segments Left: It represents a number of intermediate nodes left before reaching the destination node.
- Acknowledgment Request (R): It is a field to receive an the acknowledgement from next node.
- Reserved: This field is set to 0, set to 1 on reception of the acknowledgement
- Identification: This feild is set to a unique number by the source of the packet. On receiving an acknowledgement, acknowledgment packet number is matched with this field to ensure delivery of the packet.
- Index [1n]: It is interface index represented as Index[i] used to show an index of the ith hop in the index header

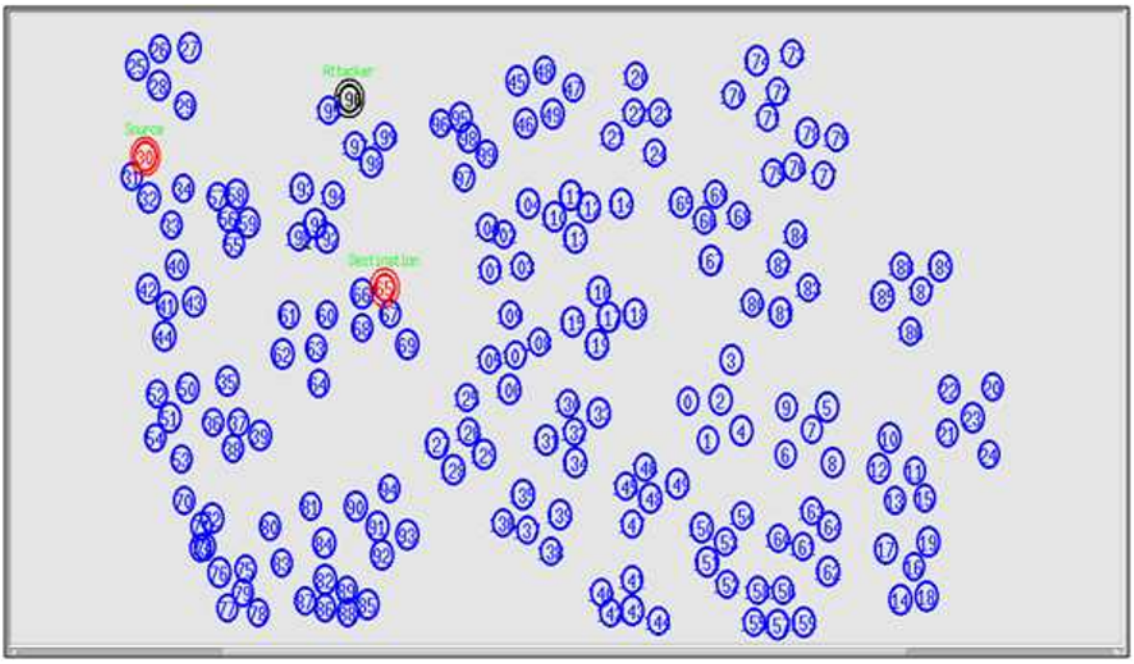


Figure 4.3: NS2 Simulation of DSR routing

- Address [i]: It is used to represent the address of the ith hop in routing packet header.

4.4.2 Simulating DSR using NS2

NS2 simulation of MANET containing 200 nodes is presented in the figure 4.3. Node 36 and 165 represents the source and destination nodes respectively. Node 196 represents attacker node. Since it is the dynamic scenario, all nodes keep on changing their positions. Routing and rerouting happen as explained in section 4.4.

4.5 Simulating Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol

Ad-hoc On-Demand Distance Vector Routing (AODV) is a reactive type of on-demand distance vector routing protocol. It is improved version of Destination Sequenced Distance Vector (DSDV) routing protocol. It establishes the communication routes as and when needed. The reason behind the popularity of this protocol is that it is capable of providing unicast as well as multicast routing. Every node in AODV routing maintains only information of next-hop routing. Fields in the routing table at each node are:

- IP Address of next hop
- The destination address
- The list of intermediate nodes to reach destination nodes
- The destination sequence number
- Timestamp for each route (time for which route information is valid)

Stepwise execution of AODV routing is as follows:

Step 1: The source node initiates route discovery procedure by sending RREQ packet. RREQ packet contains four fields such as source node IP address, destination node IP address, sequence number and broadcast id.

Step 2: Timer is set to wait for a reply.

Step 3: Intermediate nodes receives RREQ packet.

Step 4: an Intermediate node checks unique identifier (broadcast id and source IP address) of RREQ.

- If broadcast id is already seen, discards the packet.
- If not seen, setup reverse route for the destination node, increase RREQ hop count and broadcast the RREQ to its neighbors.

Step 5: An intermediate node (Not destination node) may also respond to source node generate RREP packet containing hop count to the destination node and record of the destination sequence.

Step 6: On receiving RREP from any node (either from an intermediate node or destination node), the source node will use route information received in RREP and sets up forward path entry in its routing table.

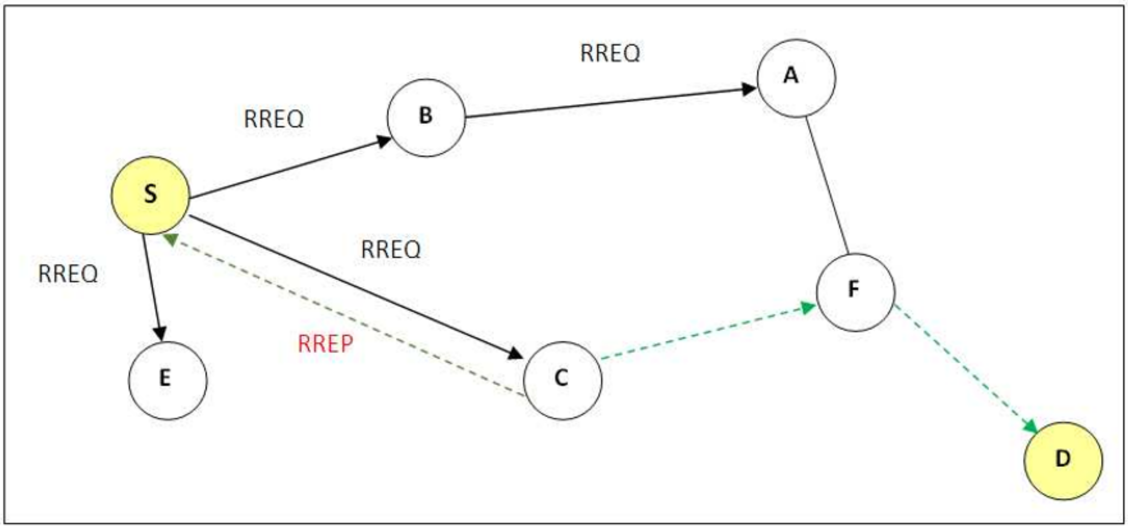


Figure 4.4: Route Establishment in AODV Routing

The figure 4.4 shows route establishment mechanism using AODV protocol. Node S is source node and node D is destination node. Node S broadcast RREQ packet to all its neighboring nodes (node B, C, and E). Since node C has routing information available for node D, it responds to source node S by sending RREP packet resulting in route establishment. The route is maintained as long as needed. To avoid network flooding, the timestamp is set to minimum. If source node is moved during an active session, route discovery is reinitiated. If the destination node is moved in active session then Route Error (RERR) message is generated by intermediate nodes.

4.5.1 AODV Header Format

As mentioned earlier, AODV uses sequence number to discard timed-out packets. Each node maintains a sequence number. On receiving packet, node increments sequence number and forward the same to next node. Header format used for RREQ is presented in figure 4.5. Top row represents bit size of the field.

The fields associated with DSR routing header are presented below.
Type indicates the type of routing used in MANET and J, R, G, D, U flags.

- J and R: used to show multicast messages

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td></tr>
<tr><td colspan="8">Type</td><td>J</td><td>R</td><td>G</td><td>D</td><td>U</td><td colspan="11">Reserved</td><td colspan="8">Hop Count</td></tr>
<tr><td colspan="32">RREQ ID</td></tr>
<tr><td colspan="32">Destination IP Address</td></tr>
<tr><td colspan="32">Destination Sequence Number</td></tr>
<tr><td colspan="32">Originator IP Address</td></tr>
<tr><td colspan="32">Originator Sequence Number</td></tr>
</table>

Figure 4.5: AODV Routing Header

- G: represents a flag to show whether an RREP packet should be sent to the destination or not.
- D: flag used by the source to check if RREP by destination is received or not. It is also used by the source node to distinguish between RREP by intermediate node and RREP by the destination node.
- U: It is used when the sequence number of the packet is unknown at receiving node.
- Reserved: It is used to keep track of hop count. Set to zero at the source node and incremented at each hop.
- Hop count: represents a number of hops between source and destination nodes.
- RREQ ID: It is a unique number which indicates route request id. Source node uses it to match with RREP id.
- Sequence number: Each packet has a sequence number which is incremented at each hop. Packets with old sequence number are ignored at receiving node.

4.5.2 Simulating AODV using NS2

The figure 4.6 shows NS2 simulation for AODV routing mechanism of MANET containing 200 nodes. Node 100 and node 170 represents source and destination nodes respectively. Node 167 represents attacker node.

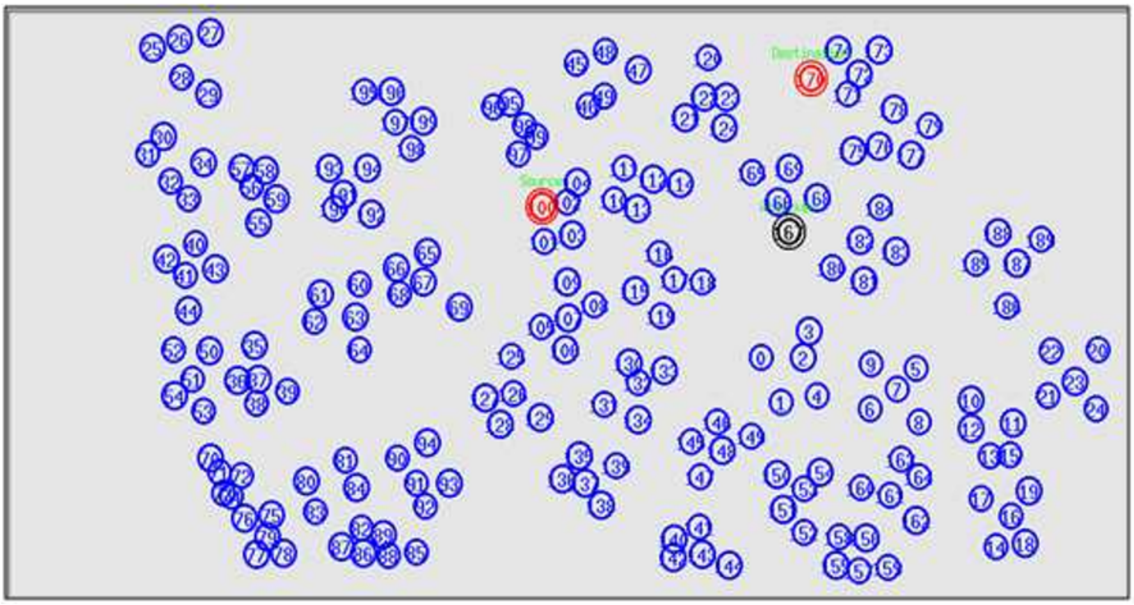


Figure 4.6: NS2 simulation showing AODV routing

4.6 Simulating Particle Swarm Optimization (PSO) Algorithm as a Routing Protocol

A stochastic algorithm such as Particle Swarm Optimization needs parameter tuning before applying for MANET.

Route discovery using PSO is explained in figure 4.7. Node S and D represents source and destination nodes respectively. Dotted circles represent radio range of respective nodes. Nodes C, G, and H are intermediate nodes on route S-C-G-H-D. These nodes are selected since they possess greater fitness levels in terms of energy and bandwidth.

4.6.1 PSO Packet Header

PSO-based routing uses fitness criteria for selecting next node. The fitness of the node depends on bandwidth and battery energy of the node. The fields associated with PSO routing header are indicated in the figure 4.8.

The fields associated with DSR routing header are as follows:

- Packet ID: It indicates unique packet id to avoid duplication of packet

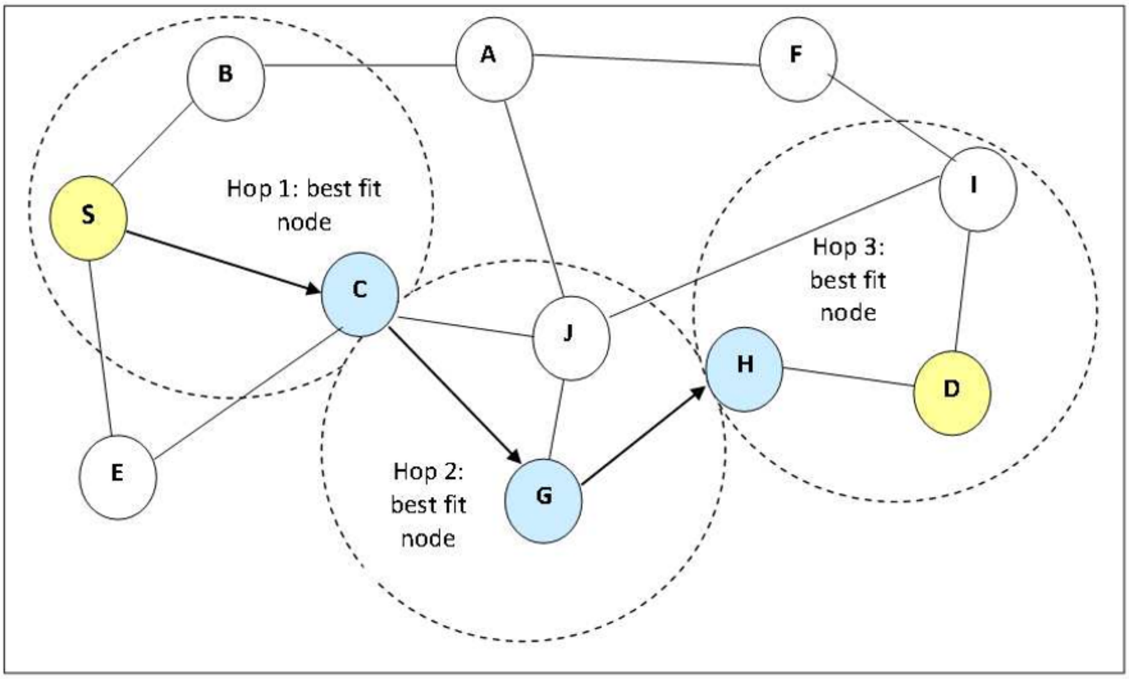


Figure 4.7: Route discovery using PSO

<table>
<tr><td>Packet ID</td><td>Header Len</td><td>Rand</td><td>Timestamp</td></tr>
<tr><td colspan="4">Source node IP address</td></tr>
<tr><td colspan="4">Source node Current position</td></tr>
<tr><td colspan="4">Destination node IP address</td></tr>
<tr><td colspan="4">Position Vector [……]</td></tr>
<tr><td colspan="4">Bandwidth Vector [……]</td></tr>
<tr><td colspan="4">Energy Vector [……]</td></tr>
<tr><td colspan="4">Current node IP address</td></tr>
<tr><td>Hop count</td><td>Routing type</td><td>Sequence number</td><td>Reserved</td></tr>
</table>

Figure 4.8: PSO routing header

- Header len: It represents header length. Depending on field values in header packet may vary depending on transmission capacity of the individual node
- Rand: It is uniformly distributed random number between 0 and 1. Random function generator generates different random number at each iteration.
- Timestamp: It is predefined timestamp value assigned to each packet. When it reaches to zero, the packet is discarded by the recipient.
- Source node current position: It indicates the current position of the node. The position of node keeps on changing at each iteration.
- Position Vector: To keep track of best fit node, this vector maintains positions of intermediate nodes.
- Bandwidth Vector: It maintains bandwidth available at each intermediate nodes.
- Energy Vector: It maintains battery energy available at each intermediate nodes.
- Current node IP address: When the packet is received by an individual node, the IP address of node is copied in this field
- Hop count: It indicates a number of intermediate nodes traversed by the packet.
- Routing Type: Indicates type of routing used. In case of non-overlapping radio range of source and destination nodes, it is multi-hop routing.
- Sequence Number: To avoid processing of packets received earlier, sequence number field is used by communicating nodes.
- Reserved: It is reserved for the flag to match request packet with a response packet.

4.6.2 Simulating PSO routing using NS2

NS2 simulation of 100 nodes is presented in figure 4.9. Node 134 and node 5 represents source and destination nodes respectively. Node 3 is representing attacker. The ultimate aim of this simulation is that a route between the source and destination nodes should be established by avoiding attacker node.

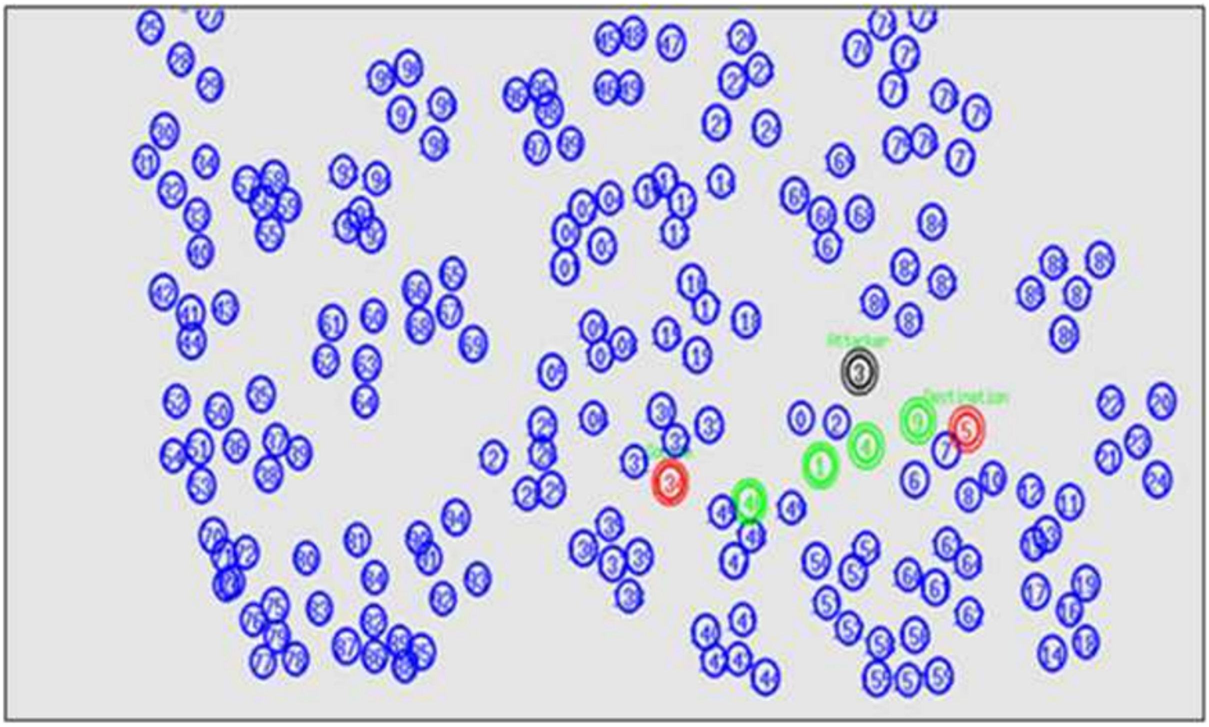


Figure 4.9: NS2 simulation showing PSO routing

4.6.3 PSO-based IDS Agent Architecture

An architecture of PSO-based intrusion detection model is presented in figure 4.10. The model developed contains five units as follows:

1. Data Collection Unit

2. Secure communication engine Unit

3. Local detection and Evaluation Engine

4. Cooperative detection and Evaluation Engine

5. Audit Source Unit

The local data collection unit records audit data of user and system activities. Local detection and evaluation engine compare the obtained packet signature patterns with the attack signatures available in the audit source unit. Whereas, cooperative detection and evaluation

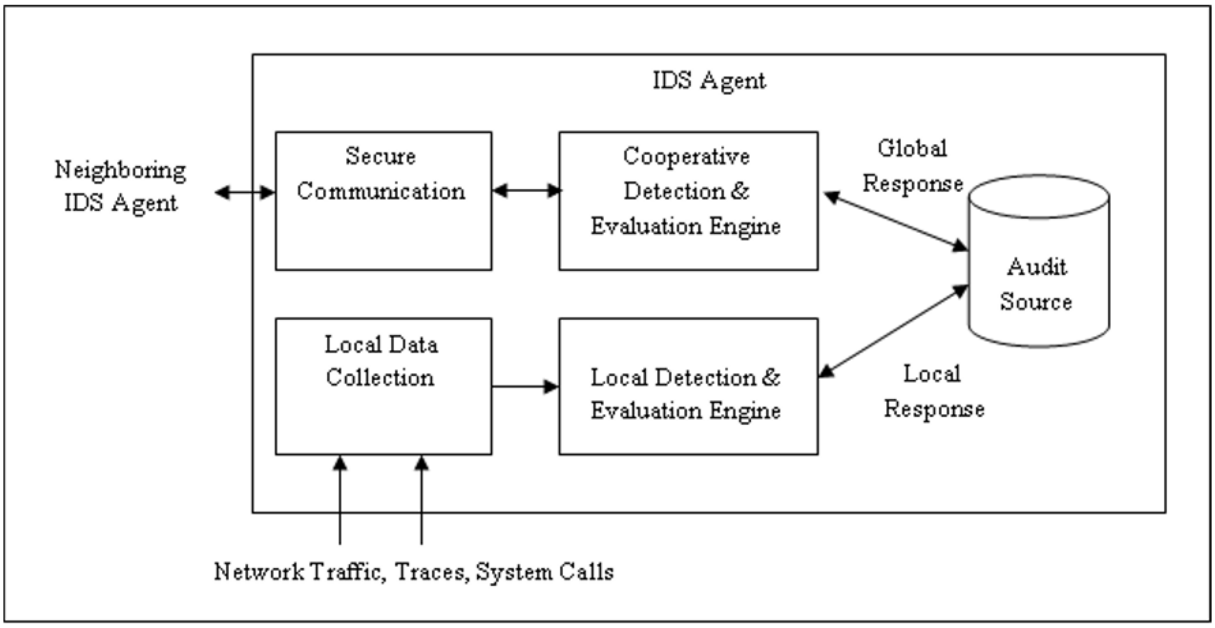

IDS Agent
Neighboring IDS Agent
Secure Communication
Cooperative Detection & Evaluation Engine
Global Response
Audit Source
Local Data Collection
Local Detection & Evaluation Engine
Local Response
Network Traffic, Traces, System Calls

Figure 4.10: Architecture of PSO-based IDS Agent

engine checks the records and evaluate traces of network traffic network for any anomalies if present. The secure communication unit is responsible to allow or block the communication and also to inform all IDS agents in its radio range about the newly detected attack signatures.

Step 1: MANET environment consisting of n nodes is created. Initialized parameters viz. distance, bandwidth, energy randomly. The user-defined fitness function is used for evaluation of next node in PSO.

Step 2: The source node initiates communication by sending hello packet. Available routes using PSO algorithm are identified.

Step 3: Protocol performance parameters are saved in a training audit source at each node.

Step 4: Attacker program at a specific node starts execution.

Step 5: Packet signatures in presence of attacker node are obtained and the training audit source at each node is updated.

Step 6: Repeat Step 4 and 5 for major types of attacks namely DOS, Blackhole, Sybil, Fabrication, and Replay

Step 7: In presence of updated training audit source at each node, performance parameter values are observed and attack signatures are recorded.

Step 8: Attacker node is identified and route without attacker is selected for communication.

Comparing with the existing IDS systems discussed in the literature, it is observed that frequently used protocols for node communication in MANET are Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector Routing (AODV). So, IDS based on these two routing protocols are chosen to compare with the proposed model.

Watchdog-Pathrator is the technique attributed to Sergio Marti, T.J. Giuli et.al. [30]. Authors have used DSR as a routing protocol for the implementation in MANET. Once routing behavior of DSR is compared with PSO, it would be easier to compare Watchdog-Pathrator and PSO-based IDS. Comparing only one existing IDS merely will not suffice the purpose. So, another recent technique proposed by Shakshuki et. al. called EAACK [31] is compared with PSO-based IDS. The algorithm used in this scheme is bidirectional search. Watchdog and EAACK algorithms are implemented as per actual guidelines provided by authors. Performance parameter values (presented in section 4.4), are compared with the proposed PSO-based IDS algorithm. In the model proposed in this thesis, every node containing updated audit training set works as an IDS agent and is capable of detecting attacks.

4.7 Mapping PSO-based routing with MANET

In [102], authors claimed that some of the PSO parameters in the original algorithm (equation 3.1 and 3.2) such as weighing factor and random numbers r1 and r2 add no flexibility to the algorithm and can be completely removed or mapped without loss of generality. To find the best next node for optimum route establishment, these parameters are modeled as per the need of MANET as follows:

1. As per PSO algorithm, c1 is cognitive acceleration constant and c2 is social acceleration constant. In our approach, c1 (individuality) and c2 (sociality) factors are inferred as the energy efficiency of individual node and average energy efficiency of neighborhood network respectively.

2. rand is any random number with range varying between 0 and 1 with uniform distribution.

3. In PSO route finding equations, ω is used to show inertia coefficient where

$$\theta\omega 1$$

   As per PSO algorithm, the weight of particle constrains modification of searching point and delays the discovery of ultimate destination. So, in this approach, is modeled as average bandwidth efficiency of neighborhood nodes.

4. In the PSO algorithm, pBest is the best fitness value of the individual node. Node finds the nearest node to a destination with higher efficiency (in terms of fitness function). So, In this research, pBest is the position of the individual node when fitness function value is optimum.

5. As per the PSO algorithm, gBest represents the best fitness function value of entire swarm. But in the case of MANET, It is required to find any nearest node within the network to a destination with higher efficiency (in terms of fitness function). So, in our approach, gBest is the position of any MANET node within its radio range, with optimum fitness function value.

6. Node positions (on X-Y plane), bandwidth and energy values of nodes are initialized randomly.

7. PSO algorithm on execution provides a trajectory, unlike conventional routing algorithms. These trajectories are in a random direction and not an exact position of next node. To overcome this limitation, the nearest node to the position directed by trajectory is assumed as next node, which occasionally result in increased hop count.

4.8 Route Discovery using PSO-based Routing Algorithm

PSO parameter values used for this experimentation are presented in the table 5.2. Values used are best fit for training and testing phase for PSO-based routing. Since bandwidth efficiency and energy efficiency of nodes varies from 0.0 to 1.0, the generality of the algorithm is maintained.

Steps involved in route discovery process in PSO routing are as follows:

Step 1: MANET containing predefined node size is implemented. Node positions, bandwidth and node energy of nodes are randomly initialized. Node position keeps on updating periodically.

Step 2: While finding next node itself, the fitness of node is well-taken care. Equations for finding next node are as follows:

$$V_i^{k+1} = [s_i^k * \sum_{n=1}^{n} (b_1 + b_2 + ... + b_n)] + e1 * rand * (pbest_i - s_i^k) + \sum (e1 + e2 + ... + en) * rand * (gbest - s_i^k) \tag{4.1}$$

where,

- v_i^k :the direction of agent i at iteration k
- b_i :bandwidth available at node i
- e_i :energy available at node i at iteration k
- rand :a uniformly distributed random number between 0 and 1
- s_i^k :the current position of agent i at iteration k,
- $pbest_i$:the position of the individual node when its objective function value obtained so far is optimum.
- gbest : the position of any node when its objective function value obtained so far is optimum when compared with other nodes.

pbest and gbest values are calculated using following fitness function F.

$$F_i = Min(Distance\ \ between\ \ node\ \ i\ \ and\ \ Destination\ \ Node) \tag{4.2}$$

Step 3: The node nearest to next node position calculated through equations 4.1 and 4.2, is considered as next node.

Step 4: Out of neighboring nodes available for next hop, a node with highest energy and bandwidth is chosen as intermediate node.

Step 5: Repeat steps 2 to 4 till destination node is reached.

Step 6: All intermediate nodes visited are tracked in RREQ packet header. The reverse route is followed by sending RREP packet.

Table 4.2: The PSO Parameter Values used for Experiment

Sr. No.	Simulation Parameter	Value
1	Max number of PSO iterations	198
2	Number of execution trials	10
3	Inertia coefficient (ω)	0-1
4	Learning factor (rand)	2
5	Individuality (c1)	0-1
6	Sociality (c2)	0-1

4.9 PSO-based Intrusion Detection Algorithm

A general framework of proposed intrusion detection model in this research is presented in figure 4.11. Execution steps involved in our proposed architecture are listed below:

Step 1: Create MANET consisting of n nodes. Randomly initialize parameters viz. distance, bandwidth, energy etc. The user-defined fitness function is used for evaluation of next node in PSO based routing.

Step 2: The source and destination nodes are allowed to communicate under a controlled environment. The MANET parameter values are noted. The performance of the system is evaluated using performance metrics presented in section 3.4 (Chapter 3).

Step 3: The observed values for parameters mentioned in step 2 are saved in a training dataset at every node.

Step 4: Dedicated node for each attack behavior is assigned and implemented.

Step 5: Packet signatures (pre-decided parameter values) in presence of attacker node are obtained and the training dataset is updated.

Step 6: In presence of updated training dataset at each node, performance parameter values are observed.

Step 7: Attacker node is identified and route without attacker node is chosen for packet transmission.

Step 8: Repeat step 4 to 7 for implementing this model against other types of attacks.

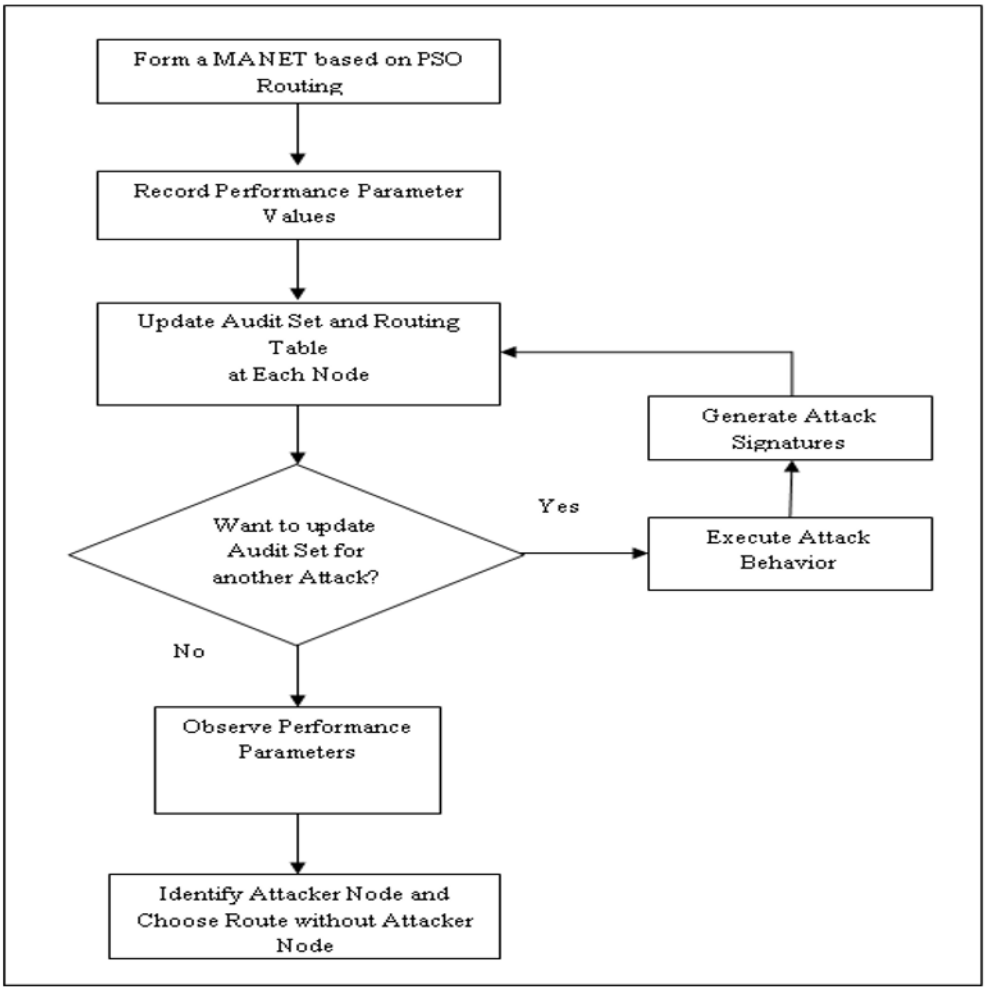

Form a MANET based on PSO Routing
Record Performance Parameter Values
Update Audit Set and Routing Table at Each Node
Generate Attack Signatures
Yes
Want to update Audit Set for another Attack?
Execute Attack Behavior
No
Observe Performance Parameters
Identify Attacker Node and Choose Route without Attacker Node

Figure 4.11: Intrusion Detection Approach using PSO

Watchdog and EAACK algorithms are implemented as per actual guidelines provided by inventors of these algorithms and performance parameter values are compared with PSO-based IDS algorithm presented in this thesis. Every node containing final training dataset works as IDS agent and is capable of detecting attacks. Though there is only single fitness function [94] used in this model, it is possible to use multiple fitness functions for optimum route evaluation.

4.10 System Model for PSO-based Intrusion Detection Algorithm

The system is presented using set theory as follows:

Let S be an IDS, such that,

$$S = U, N, D, A, C, R, P, M, I, L$$

where, U represents users.

$$U = \{u1, u2\}$$

N represents set of nodes

$$N = \{n1, n2, n3, n4....nn\}$$

D represents dataset

$$D = \{d1\}$$

A represents Attacks

$$A = \{a1, a2, a3, a4, a5....an\}$$

C represents Comparison

$$C = \{c1, c2, c3\}$$

R represents results

$$R = \{r1, r2, r3, r4....rn\}$$

P represents performance

$$P = \{p1, p2, p3....pn\}$$

M represents MANET

$$M = \{m1\}$$

I represents intruder

$$I = \{i1, i2, i3....in\}$$

L represents logs (packet signatures against specific parameters)

$$L = \{l1, l2, l3....ln\}$$

Let F be a Rule of A into N, such that Attackers will perform attacks on Node.

$$F(A)\| \rightarrow N$$

For example,

$$F(A)\| \rightarrow \{no, n1, n2....nn\} \in N$$

Let F be a Rule of N into P, such that Nodes will follow the Protocols.

$$F(N)\| \rightarrow P$$

For example,

$$F(N)\| \rightarrow \{po, p1, p2....pn\} \in P$$

4.11 Chapter Summary

This chapter focused on actual implementation methods and tools used for this research. For ensuring securing routing, PSO algorithm is used. This research claims that, route identification and maintenance is better achieved using PSO algorithm. In this experiment, it is found that routes discovered by PSO routing contain best-fit nodes compared to other two methods namely Watchdog and EAACK. To ensure actual Watchdog and EAACK intrusion detection mechanisms, respective routing protocols namely, Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector Routing (AODV) are simulated as per actual IETF guidelines. Routing results in DSR and AODV are compared with proposed PSO routing. Experiment values for attributes presented in section 3.4 are obtained and a training dataset containing normal signatures is generated.

In the second part of this research, intrusion detection algorithm capable of detecting host as well as network generated abnormal signatures is developed. The architecture of proposed IDS agent is also presented in this chapter. Performance parameters of intrusion detection and significance of these parameters is also explained in this chapter. Since this model is inspired by PSOs cooperative nature, the key strength components of PSO such as individuality and sociality are effectively used in this model. Results obtained out of the model proposed are presented in chapter 5.

Chapter 5

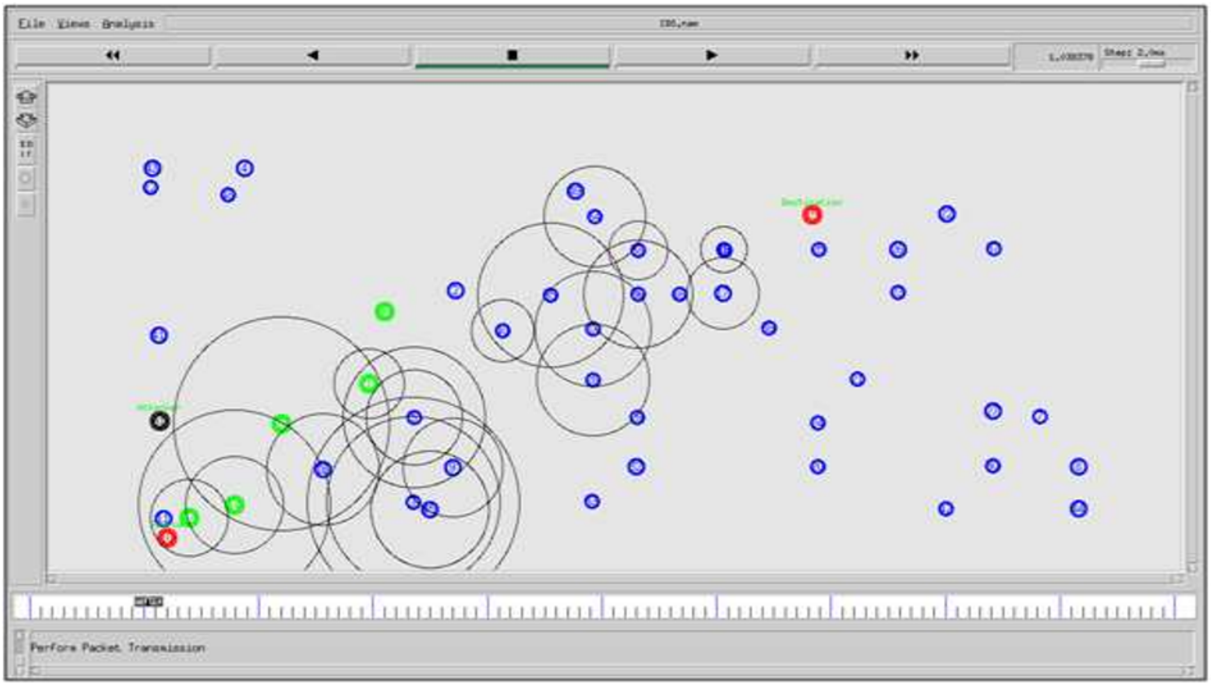
Results and Evaluations

Efficient routing is undoubtedly the most important part of MANET. Secure and efficient routing comes from the efficient routing protocol. The route guidance technique used in this research is based on modified PSO. Starting section of this chapter comprises results of PSO-based routing approach. The capability of PSO to find best-fit next helps in identifying route possessing high data transmission rate. The route identified also ensures nodes with high bandwidth and optimum energy.

In the second part of this experimentation, each node is well equipped with IDS agent architecture discussed in the section 5.6. Each node updates itself using two ways. The first way is its own communication with neighboring nodes and the second way is observing communication between two neighboring nodes. We call it as local response and global response respectively. As discussed in the previous chapter, this experiment is conducted using NS2 simulation tool. The results obtained are discussed in detail in subsequent sections of this chapter.

5.1 PSO-based Routing

Node scalability plays a very important role in MANETs. It is very difficult to predict the efficiency of MANET performance containing fixed number of nodes. In the literature, researchers attempted using varying MANET size. To ensure accuracy, MANET performance parameters are evaluated using node size 50, 100, 150 and 200 respectively.



Perform Packet Transmission

Figure 5.1: Node clustering using PSO routing at node size 50

5.1.1 Node Clustering

Before communication starts between sender and receiver nodes, each node tries to find its neighborhood network. The area in which a node can communicate with neighboring nodes without interface is called as its radio range. The phenomena using which each node tries to track its neighboring nodes is called as clustering. Figures 5.1 to 5.4 presents snaps of MANET node clustering observed at different node size obtained through NS2.

Since the MANET environment is dynamic, node position keeps on changing. Depending on the geographical position of nodes, position of cluster node changes frequently. To reformulate cluster becomes necessary to make communication happen. The same is well taken care in this experiment.

5.1.2 Route Identification using PSO

The crux of our PSO based routing lies in the identification of best suitable route between the source and destination nodes. The best suitable node is capable to identify the route which con-

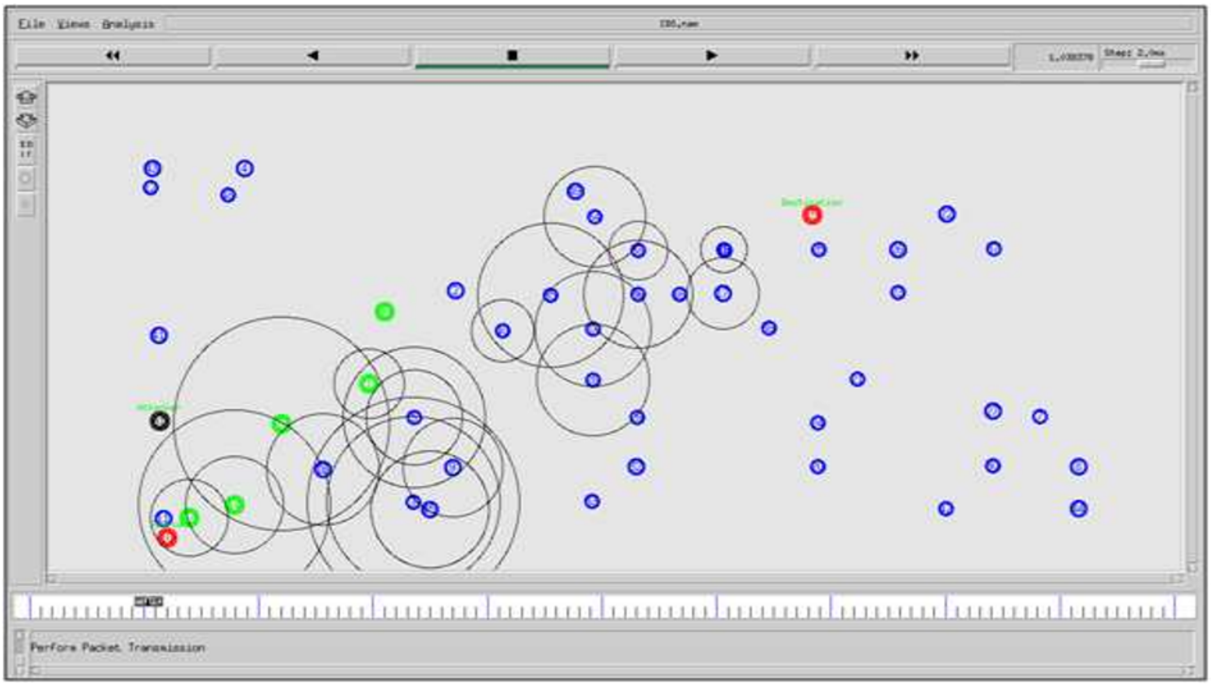


Figure 5.2: Node clustering using PSO routing at node size 100

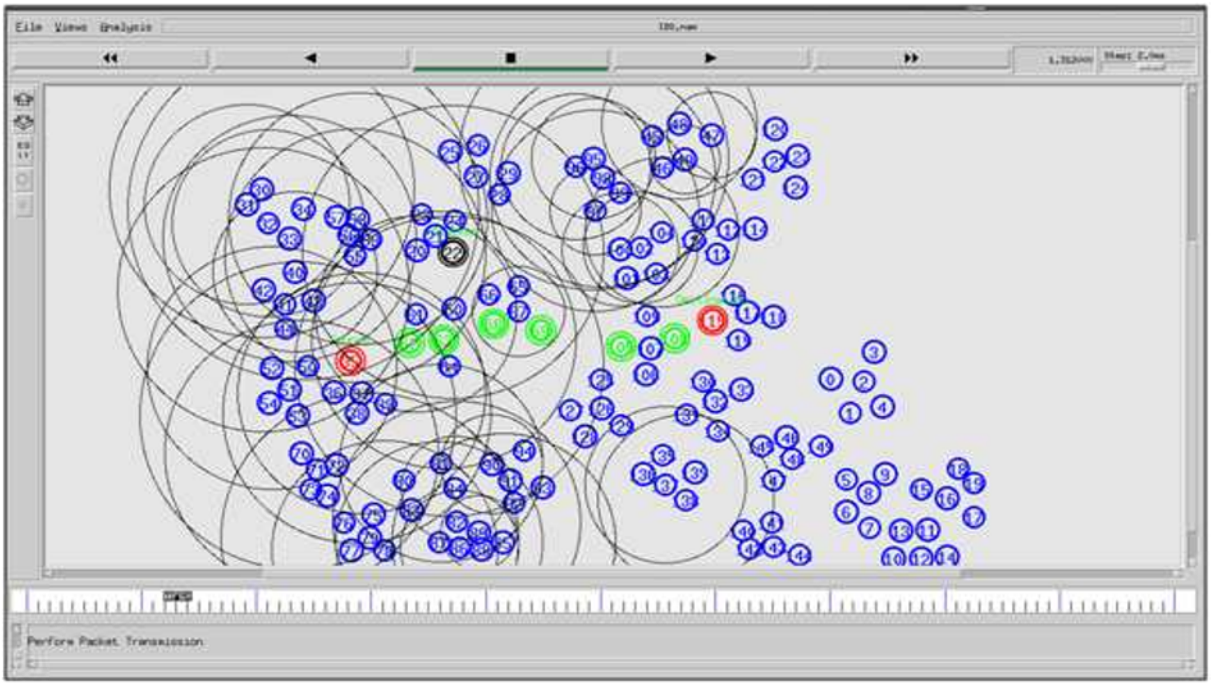
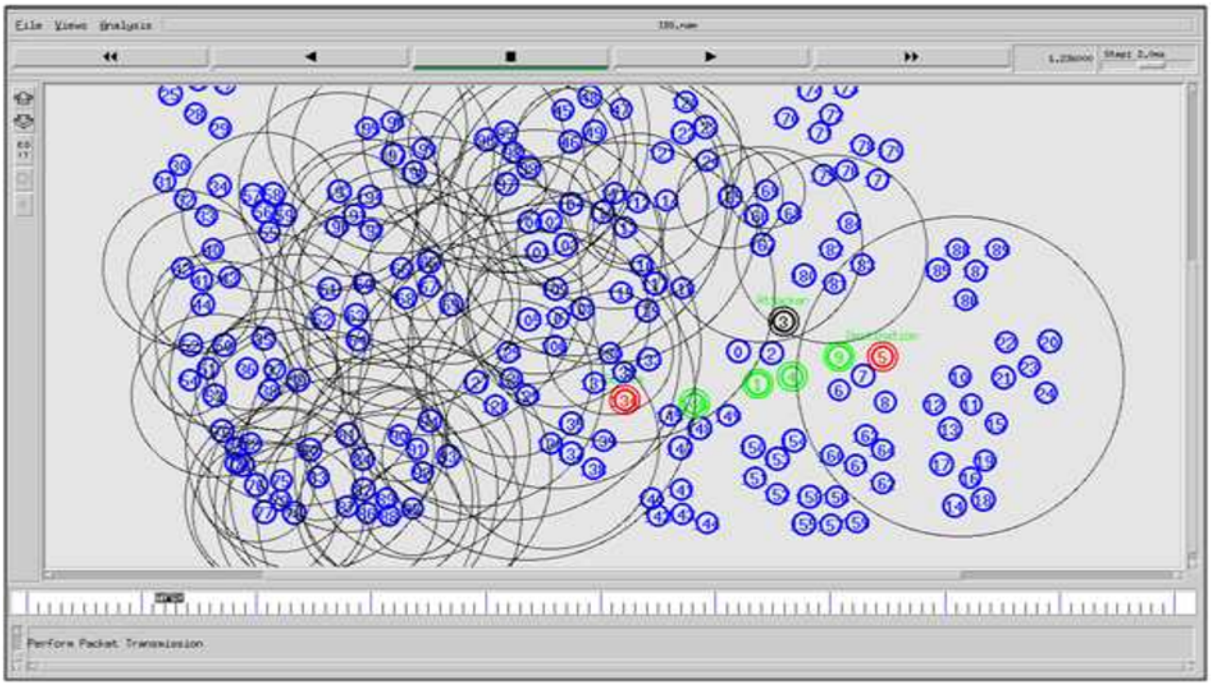


Figure 5.3: Node clustering using PSO routing at node size 150



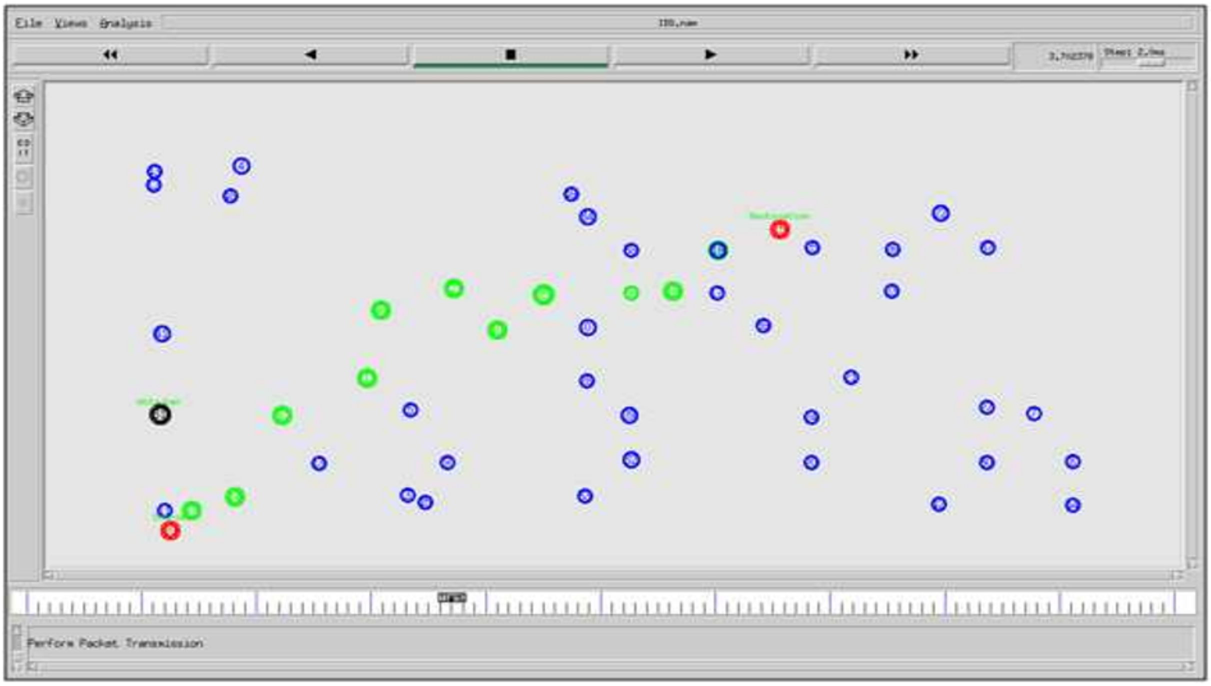
Perform Packet Transmission

Figure 5.4: Node clustering using PSO routing at node size 200

tains fittest nodes in terms of energy and bandwidth. Initially, the source node sends hello packet to its all neighboring nodes. Each neighboring node forwards it in turn to all its neighboring nodes. The mechanism of forwarding hello packet continues till it reaches to the destination node. The fitness value of all nodes who forwarded the packet is calculated and the same is shared with all nodes involved in communication.

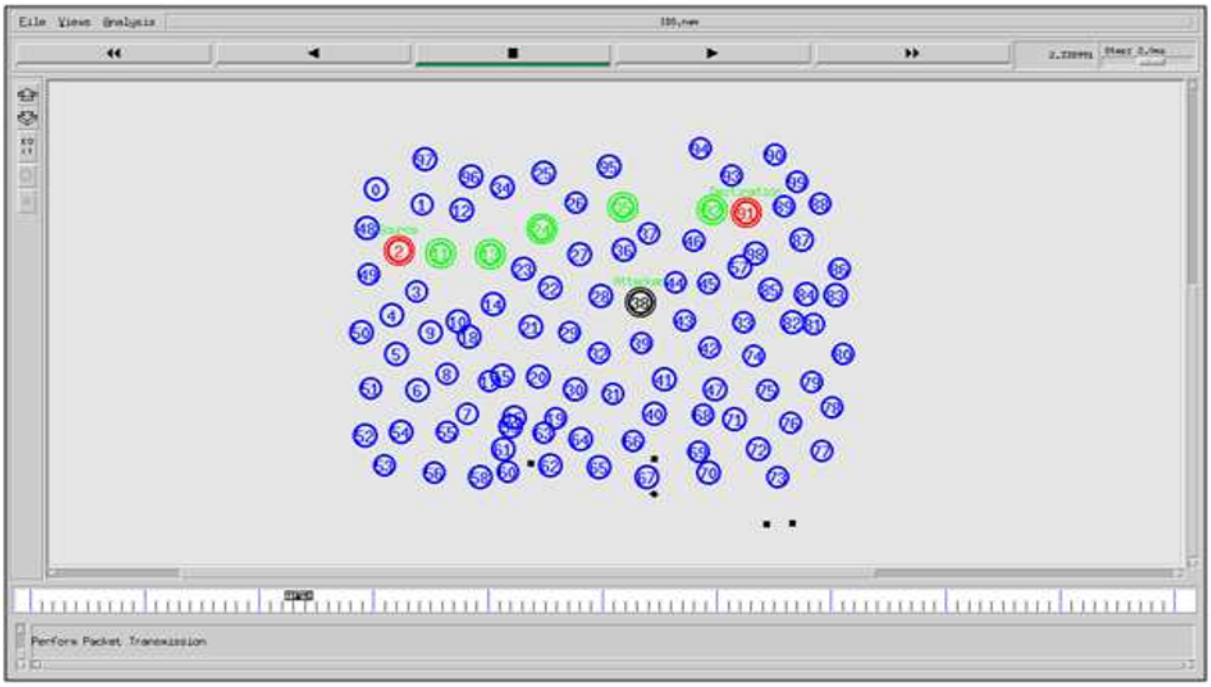
The node with best fitness value and near to destination node is selected for packet transfer. Route identification at different node size is observed through network animator (NAM) module of NS2 and is presented in figures 5.5 to 5.8.

Dynamic nature of MANET leads to ever-changing node position. Fitness value of nodes also changes accordingly. In case of 200 nodes scenario, node density also increases resulting in the identification of route containing high fitness value.



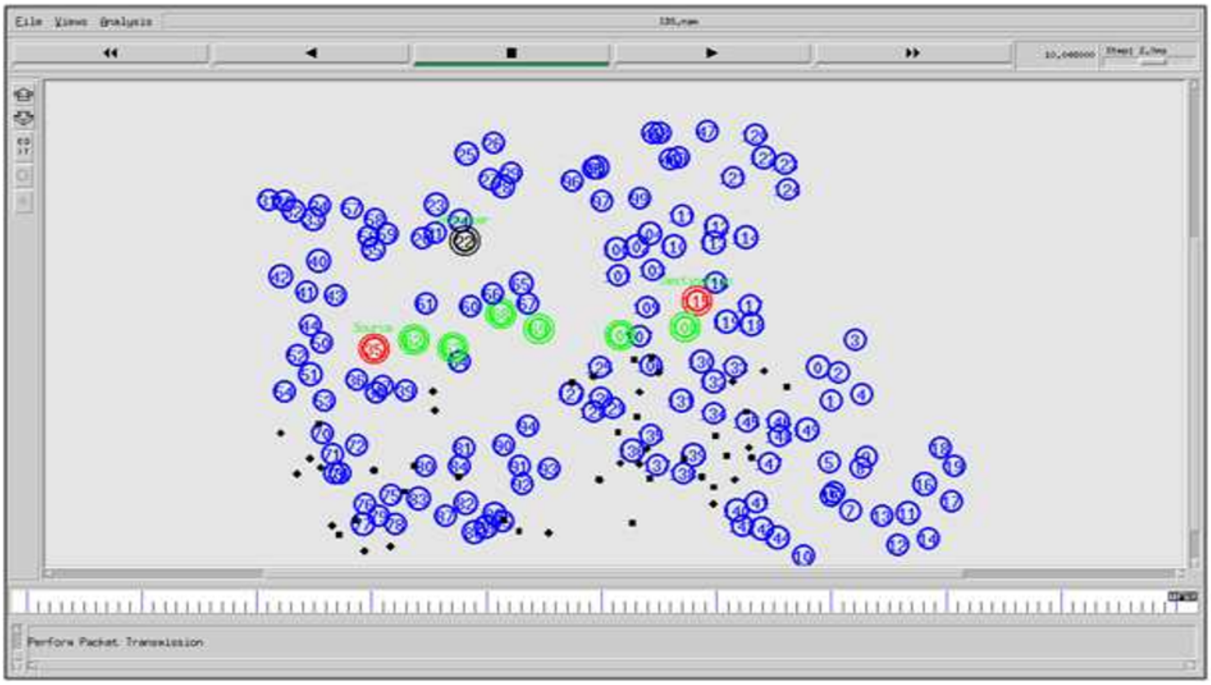
Perform Packet Transmission

Figure 5.5: Route identification using PSO routing at node size 50



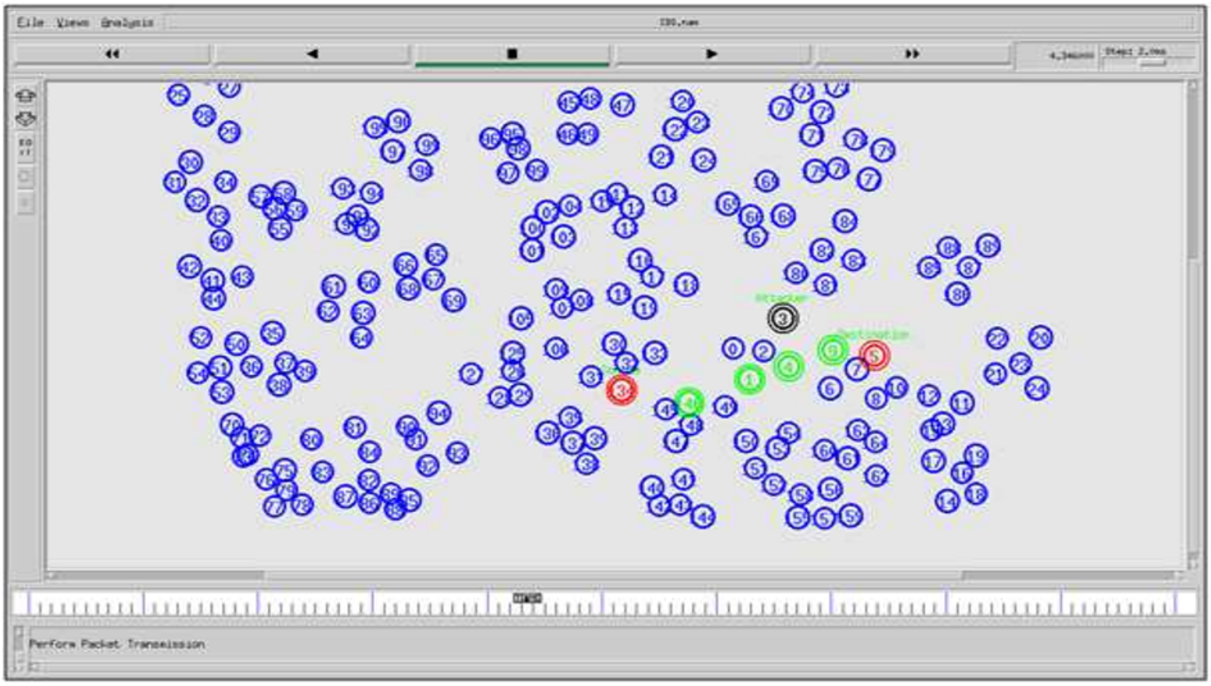
Perform Packet Transmission

Figure 5.6: Route identification using PSO routing at node size 100



Perform Packet Transmission

Figure 5.7: Route identification using PSO routing at node size 150



Perform Packet Transmission

Figure 5.8: Route identification using PSO routing at node size 200

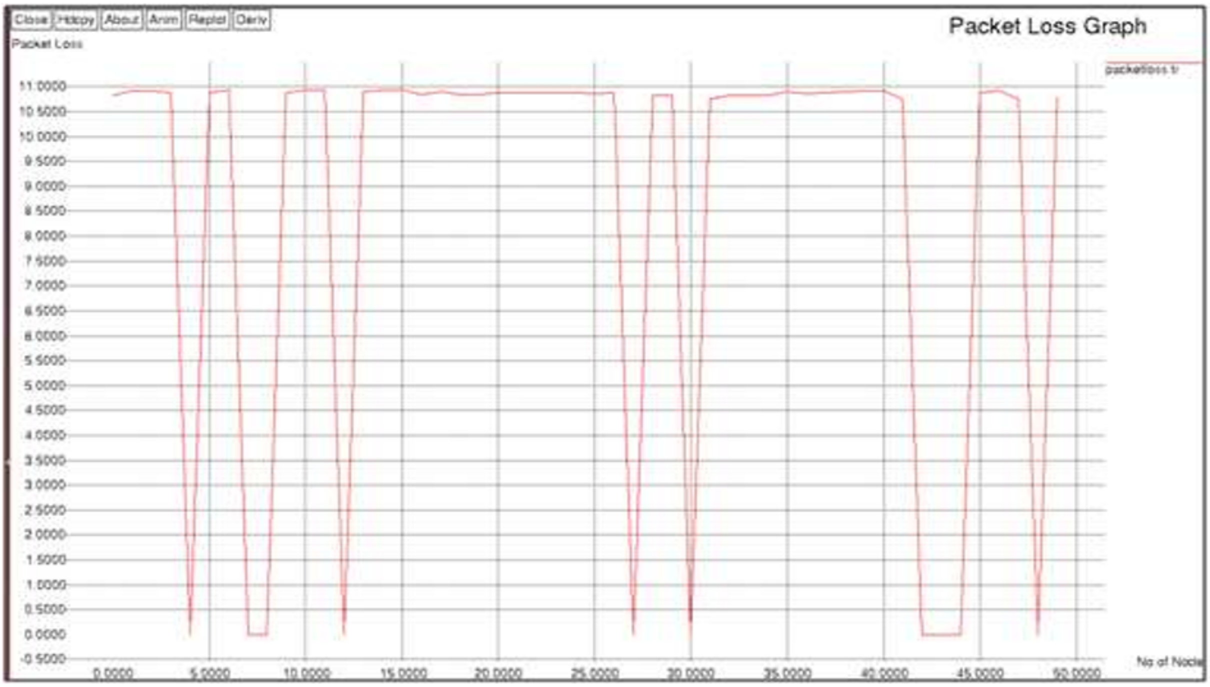


Figure 5.9: Packet loss ratio in PSO routing at node size 50

5.1.3 Packet Loss in PSO-based routing

Packet Loss Ratio is the ratio of the total number of data packets dropped to the total number of data packets sent. Figure 5.9 to 5.12 presents average packet loss at node size 50,100,150 and 200. The x-axis is representing the number of nodes whereas; the Y-axis is representing average packet loss (%) scale. Packet loss observed is high at nodes contributing to packet forwarding. There may be few nodes which do not directly contribute to communication. In such cases, packet loss at those nodes is less. The communication overhead of any network is directly proportional to packet loss.

When observed packet loss at different node size, it is noted that packet loss is high where node density is high. If more nodes are involved in packet transmission, packet loss increases. Table 5.1 provides statistics of packet loss at different node size. Packet loss at node size 50,100 and 150 is less in comparison to node size 200.

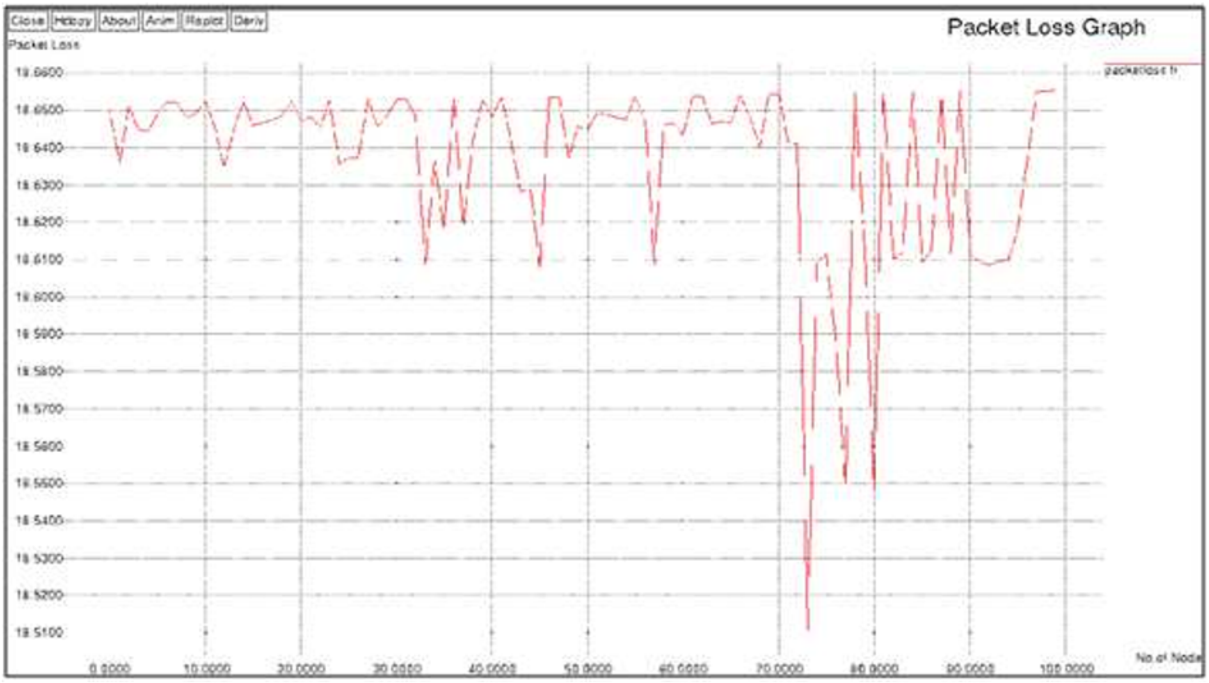


Figure 5.10: Packet loss ratio in PSO routing at node size 100

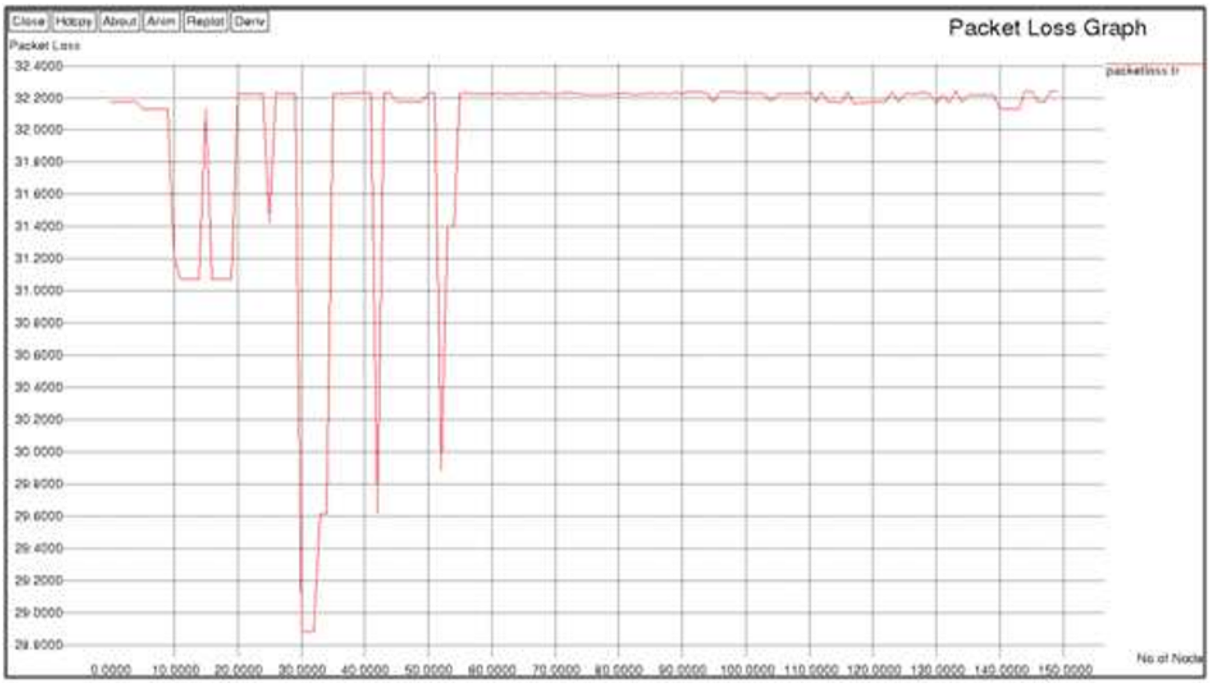


Figure 5.11: Packet loss ratio in PSO routing at node size 150

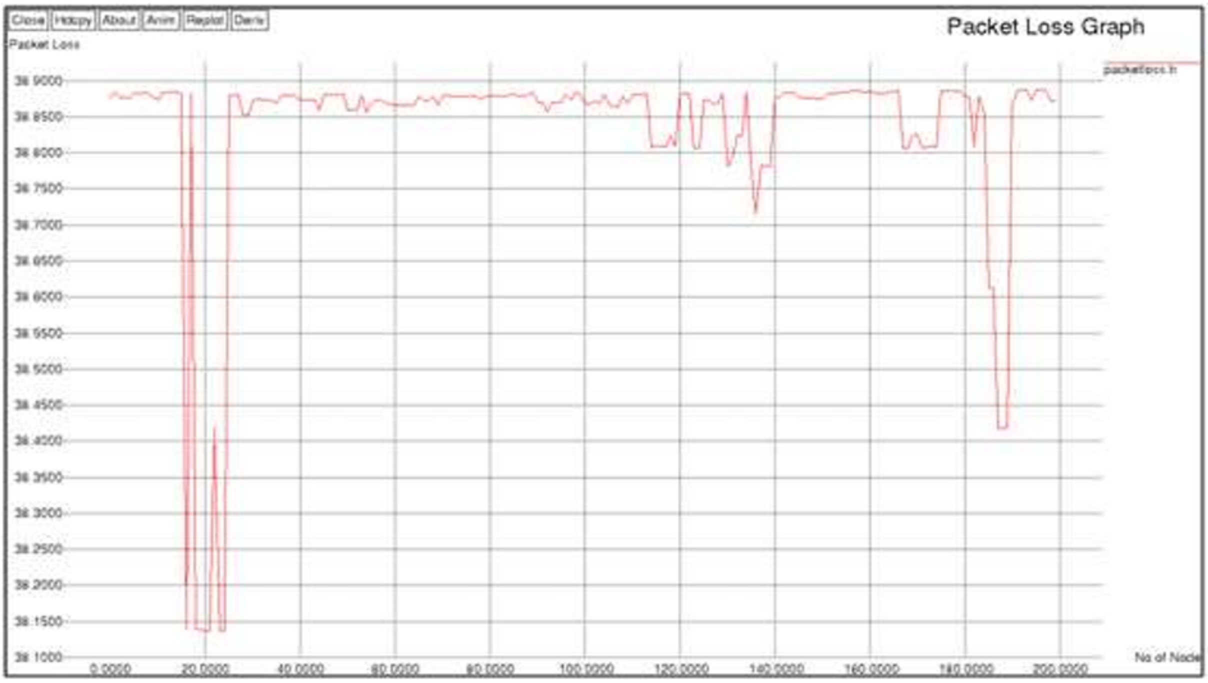


Figure 5.12: Packet loss ratio in PSO routing at node size 200

Table 5.1: Average packet loss at varying node size

Sr. No.	No. of Nodes	Average Min PLR (%)	Average Max PLR (%)
1	50	0.3	10.9
2	100	16.67	18.5
3	150	28.85	32.23
4	200	38.13	38.88

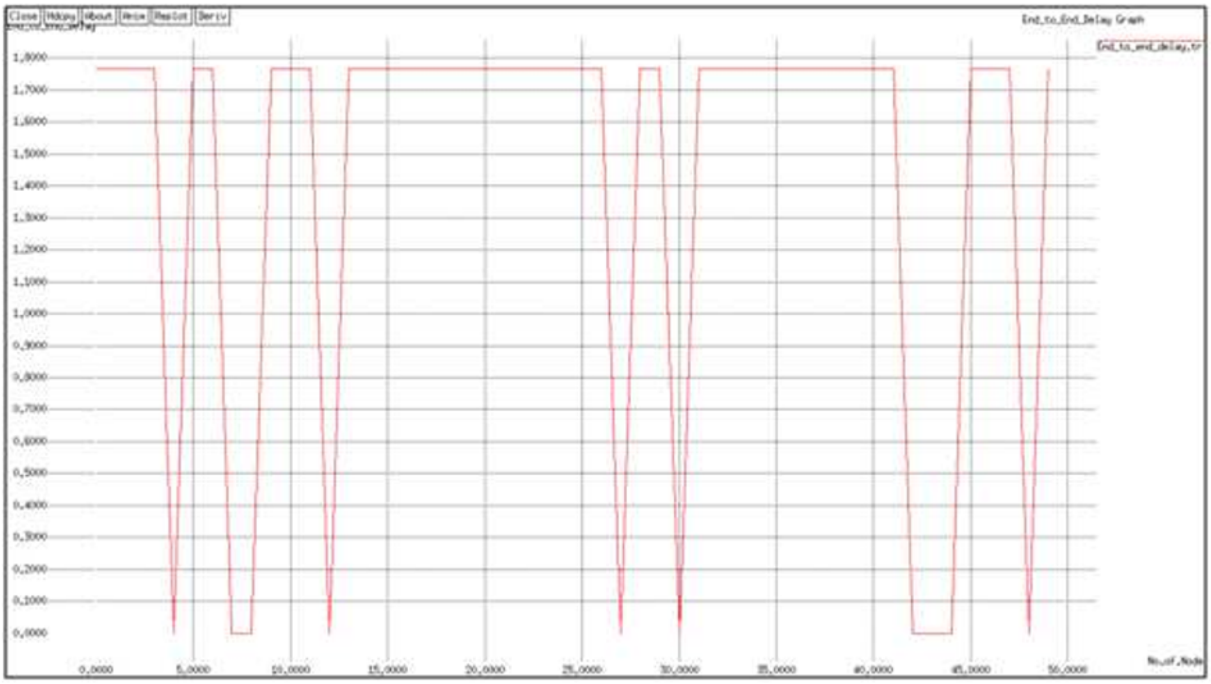


Figure 5.13: End to End Delay in PSO routing at node size 50

5.1.4 End to End Delay in PSO-based routing

Transmission of packets from source to destination node is one of the measures to check the quality of routing. As bandwidth at individual MANET node varies, the delay in transmission varies at different routes. To ensure secure and timely delivery of packets, the routing protocol should always choose the route containing nodes capable of transmitting data packets efficiently. End to End Delay is the delay incurred in the transmission of a data packet from source and destination (received time minus sent time). Figure 5.13 to 5.16 shows ETE at different node sizes.

As indicated in graphs obtained through NS2, the nodes which are not involved in packet transmission do not show any ETE delay at all. Whereas, nodes contributing to communication incurs ETE delay. A minimum number of clusters lead to high node density. If node density is less in the unit area, it results in a high end to end delay. The ETE delay observed at node size 200 is high if compared with less node size scenarios. To compare ETE delay at different routes, the experiment is conducted at node size 50,100,150 and 200 nodes. The result statistics

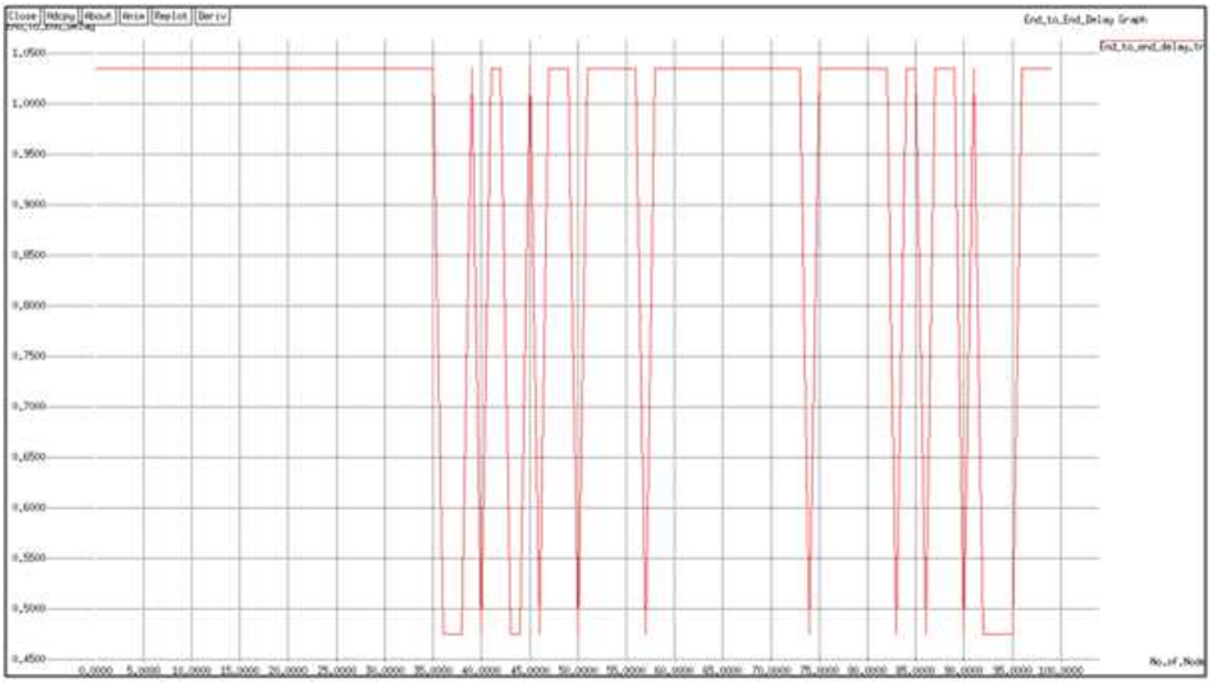


Figure 5.14: End to End Delay in PSO routing at node size 100

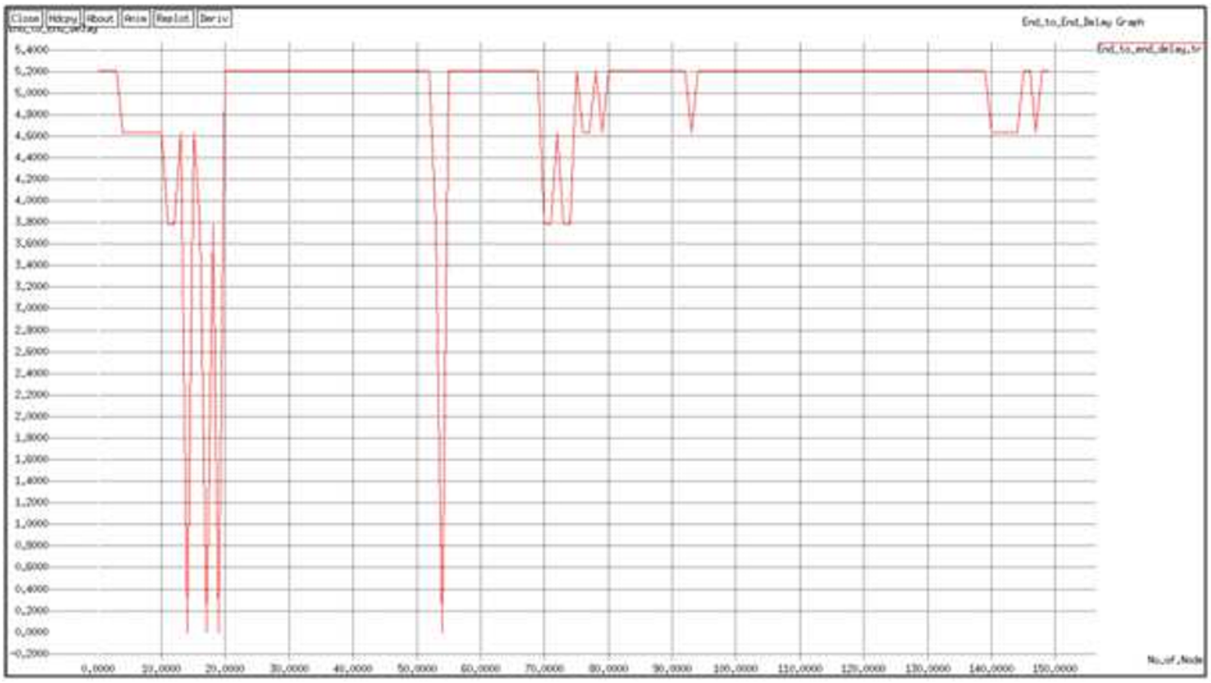


Figure 5.15: End to End Delay in PSO routing at node size 150

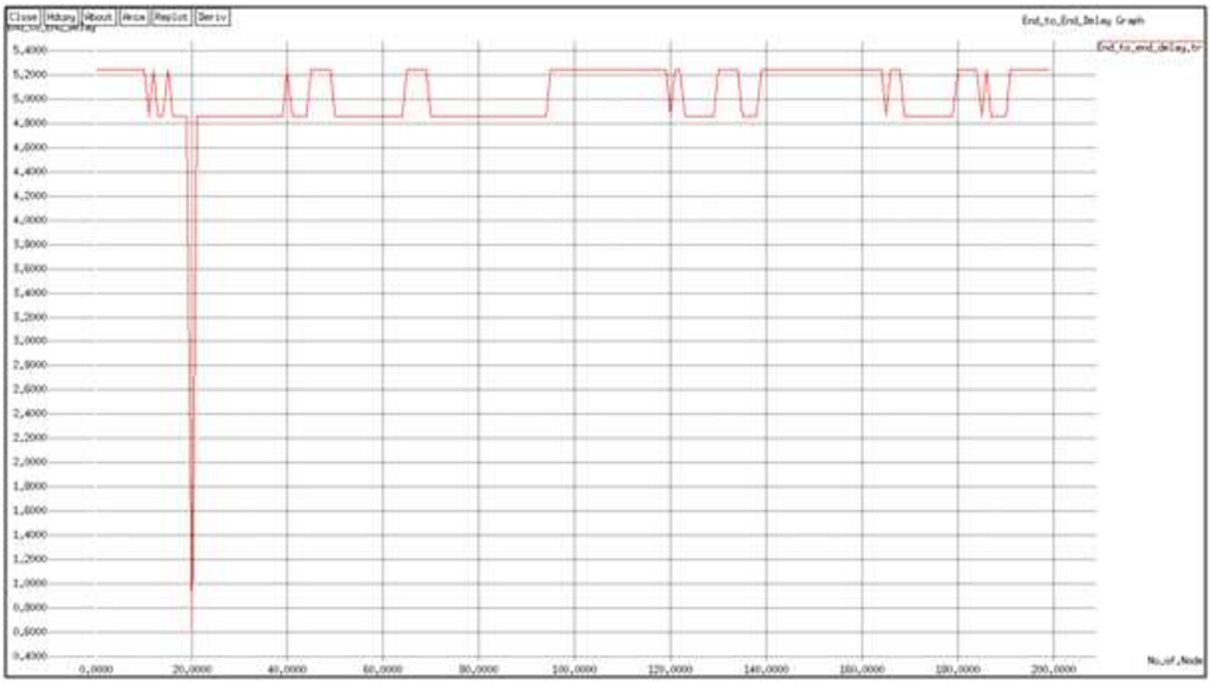


Figure 5.16: End to End Delay in PSO routing at node size 200

on ETE delay is shown in the table 5.2.

5.1.5 Throughput in PSO-based Routing

Successful packet delivery depends on node fitness. The high fitness of nodes results in higher node throughput. The rate of successful packet transmission is called as throughput for that particular communication route. It is usually measured in bits per second (bits/sec) or number of data packets successfully transmitted per second. While estimating throughput in this exper-

Table 5.2: Average End to End Delay at varying node size

Sr. No.	No. of Nodes	Average Min ETE Delay (ms)	Average Max ETE Delay (ms)
1	50	0.2	1.79
2	100	0.47	1.03
3	150	0.5	5.20
4	200	0.6	5.22

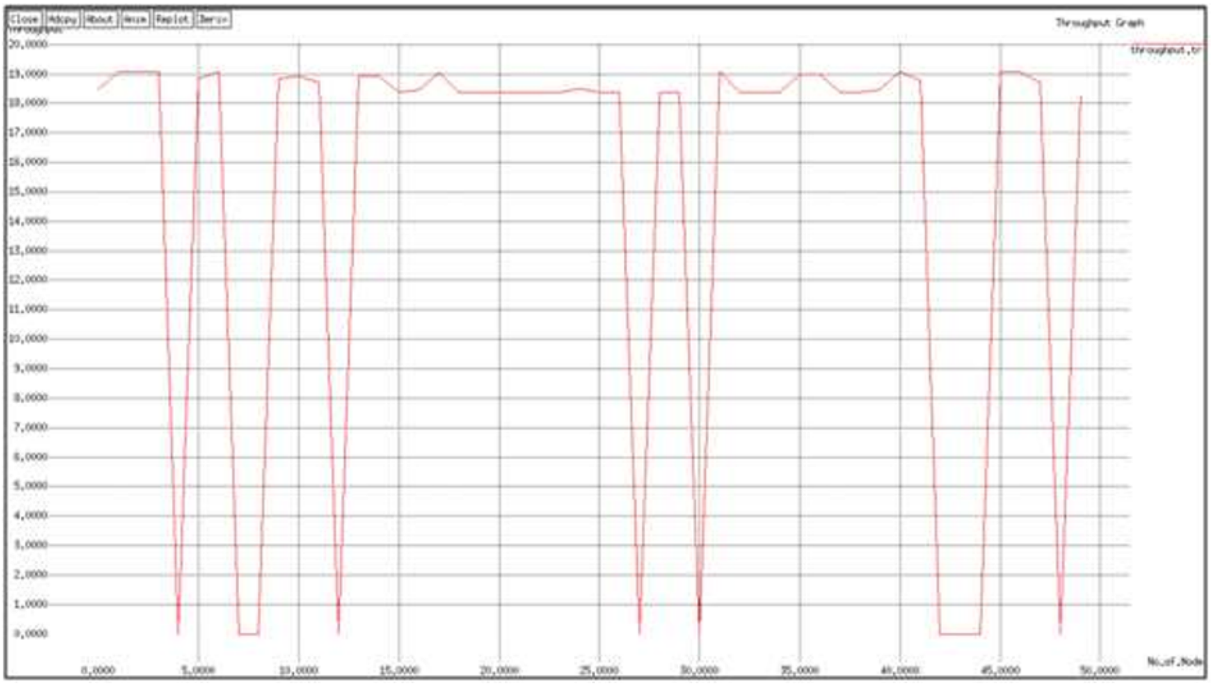


Figure 5.17: Throughput in PSO routing at node size 50

iment, average throughput observed at route nodes are graphically represented against varying node sizes. Average node throughput observed at varying node density is presented in figures 5.17 to 5.20.

As indicated in figures 5.17 to 5.20, all nodes that are in direct or indirect communication with the source and destination nodes shows high throughput value. Average packet throughput at nodes which are directly involved in the communication is higher than those which are indirectly involved or not involved at all. After route identification at such nodes, traffic gets significantly reduced. It is also noted that, when node density is low, some of the nodes do not fall in radio range of any neighboring nodes. Such phenomenon is called as a hidden terminal in MANETS. Throughput count at such nodes is negligible (sometimes zero) since these nodes are not available for communication. The table 5.3 presents statistics of average packet throughput at varying node sizes. It is stated that node density is directly proportional to average packet throughput. In presence of a minimum number of nodes, few nodes may not contribute at all to packet transmission as like in the case of 50 node size. Such nodes are called as hidden terminals.

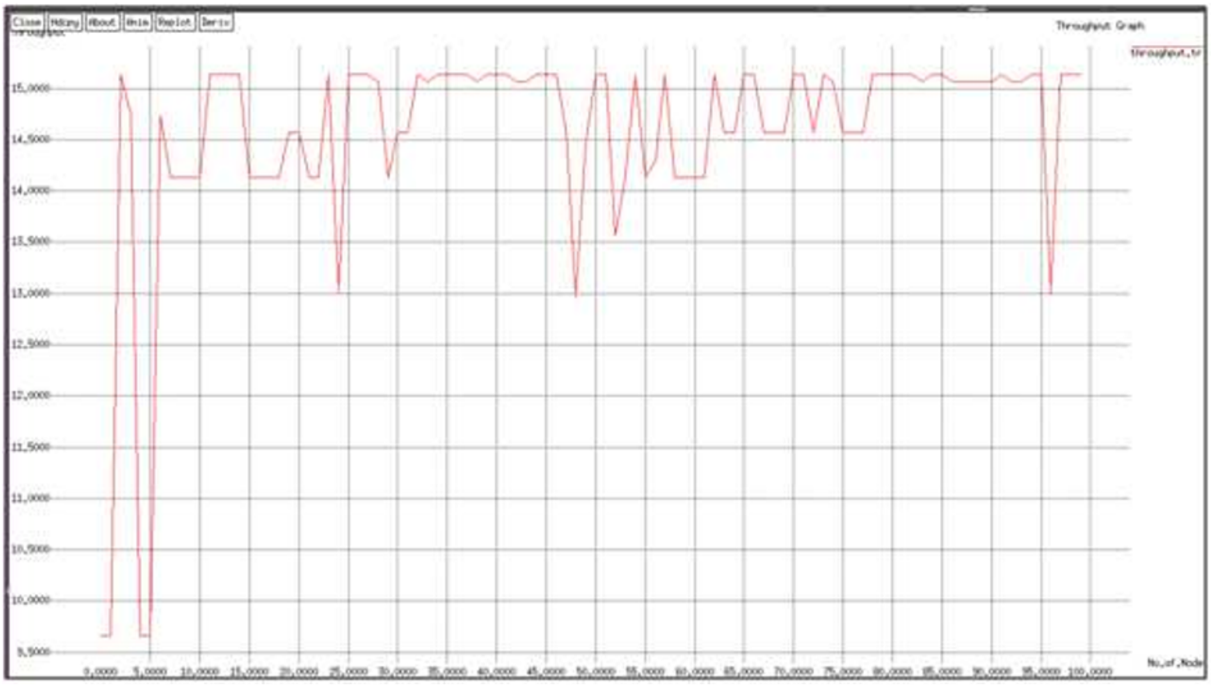


Figure 5.18: Throughput in PSO routing at node size 100

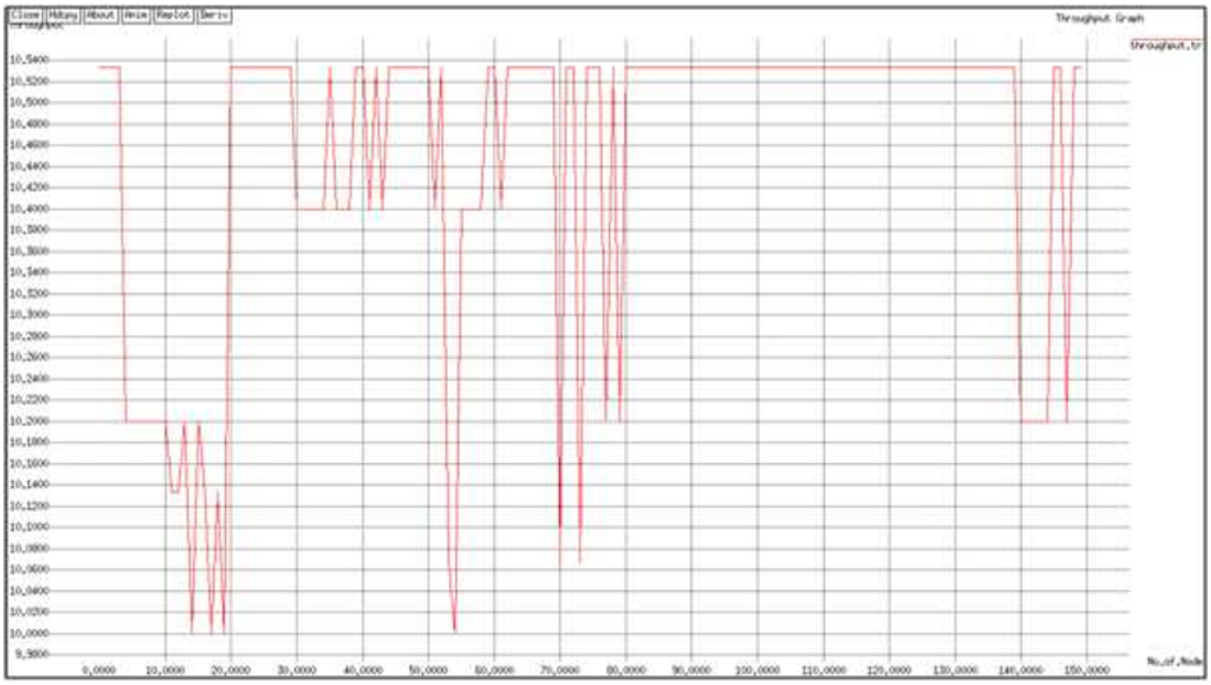


Figure 5.19: Throughput in PSO routing at node size 150

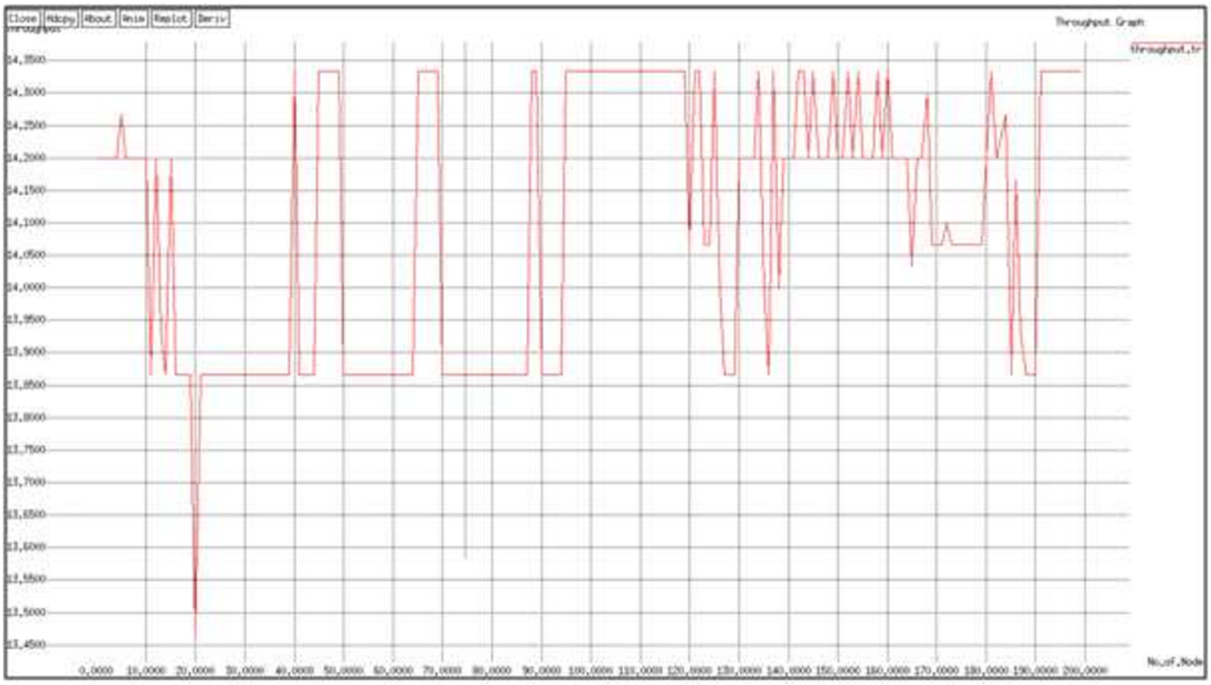


Figure 5.20: Throughput in PSO routing at node size 200

Table 5.3: Average Packet Throughput at varying node size

Sr. No	Node Size	Avg. Min. Throughput (packets/sec)	Avg. Max. Throughput (packets/sec)
1	50	0.0	19.1
2	100	9.65	15.2
3	150	10.0	10.53
4	200	13.46	14.34

5.2 Performance Analysis of PSO-based Intrusion Detection Algorithm

5.2.1 False Alarm Rate

In a cooperative environment such as MANET, intrusion detection is the responsibility of all nodes collectively. To evaluate the trustworthiness of individual node in MANET is another important aspect. In this approach, each node acts as IDS agent and continuously monitors neighboring nodes for malicious events. So while establishing route itself, intrusive nodes are identified and a route without suspicious node is identified for communication.

As per this research, each node is equipped with an audit set containing packet signatures. This audit source is updated as and when abnormal signatures are identified. Sometimes, due to unavailability of matching packet signatures, IDS may falsely declare a genuine neighboring node as an intruder. The rate of such false claims is called as false alarm rate. In this experiment, false alarm rate of proposed system against various node size is tested. Figure 5.21 to Figure 5.24 shows the results of false alarm rate against a number of nodes.

Observations on false alarm rate against varying node size are presented below:

1. False alarm rate of the PSO-based intrusion detection algorithm is high in presence of fewer nodes. Whereas, it decreases gradually in presence of high node density. So, it is implied that false alarm rate of IDS is inversely proportional to a number of nodes. It may be the possible implication of availability of stable routes in high node density scenarios.

2. Intermittent highs and lows in false alarm rate are observed. There are following two possibilities for the same.

   - Neighboring nodes always bears random fitness.
   - The inability of route nodes (at particular instance) in secure delivery of packets.

Table 5.4 presents average false alarm rate observed over 10 execution trials. It clearly indicates that minimum false alarm rate observed using proposed intrusion detection algorithm is 17.3%. The reason behind high FAR is that the number of packets lost also contributes to

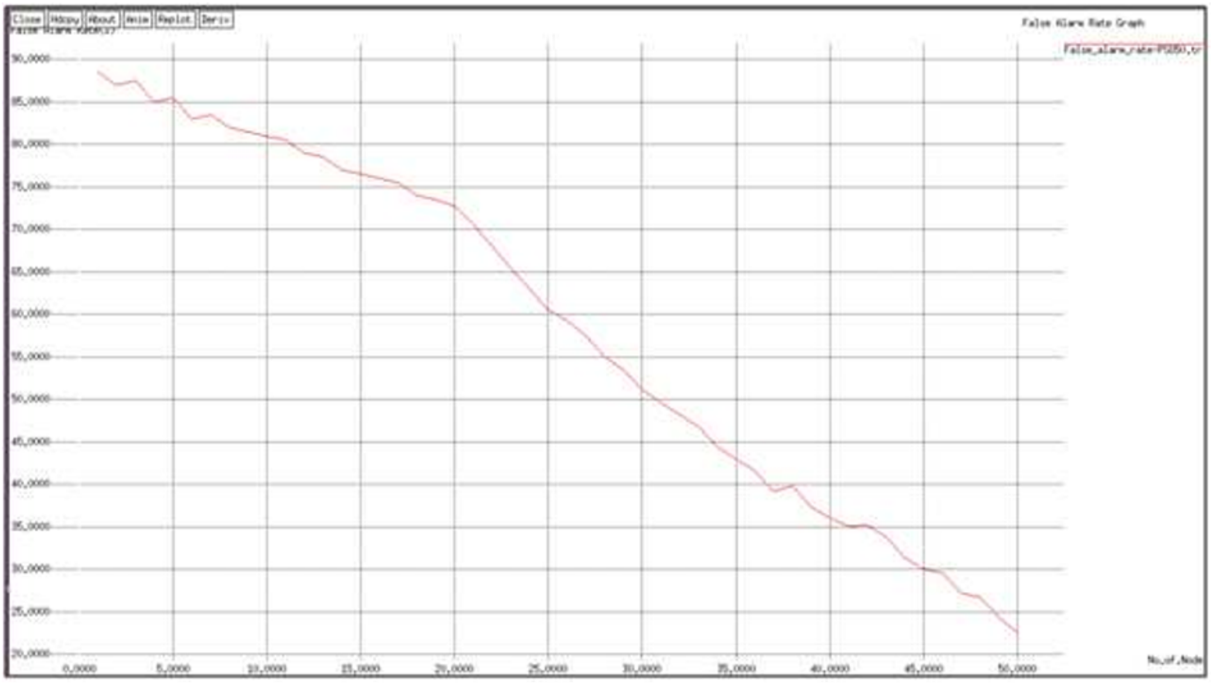


Figure 5.21: False Alarm Rate at 50 nodes using PSO based routing

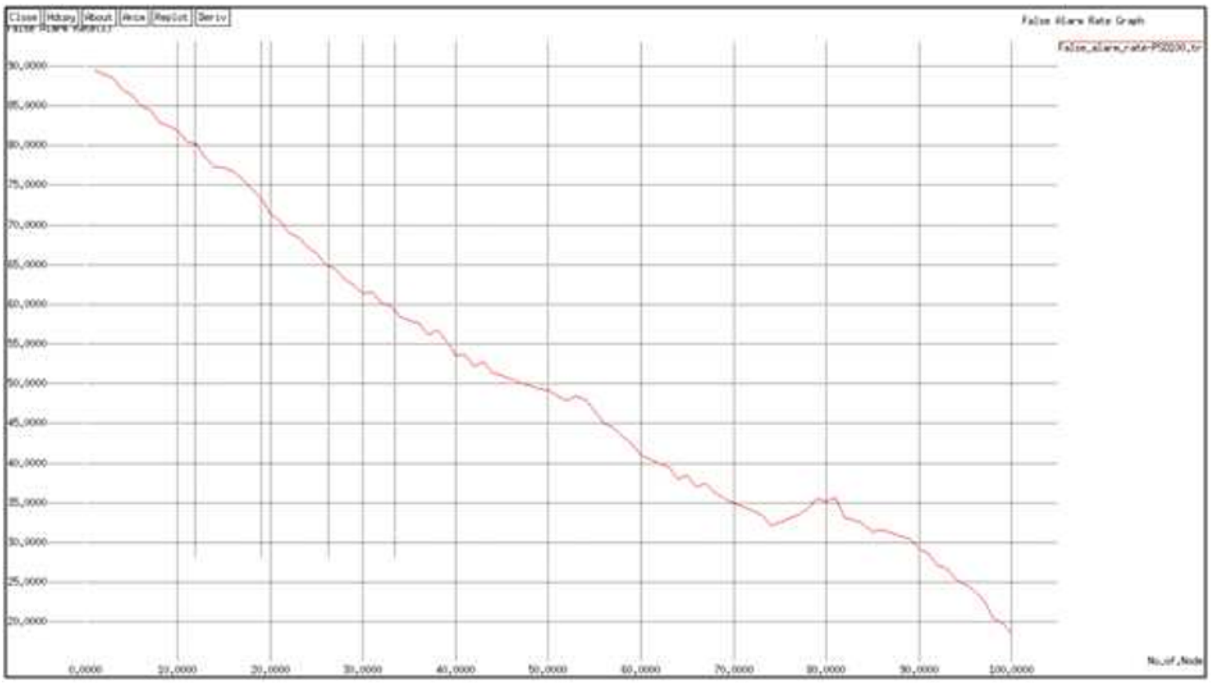


Figure 5.22: False Alarm Rate at 100 nodes using PSO based routing

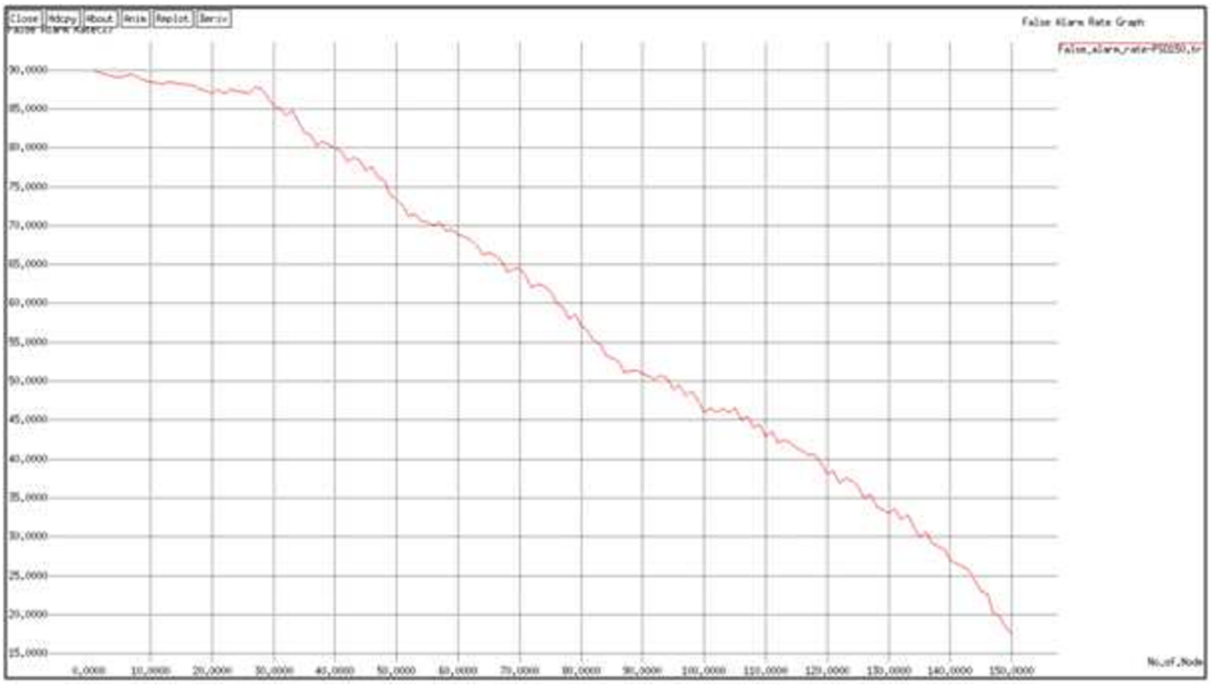


Figure 5.23: False Alarm Rate at 150 nodes using PSO based routing

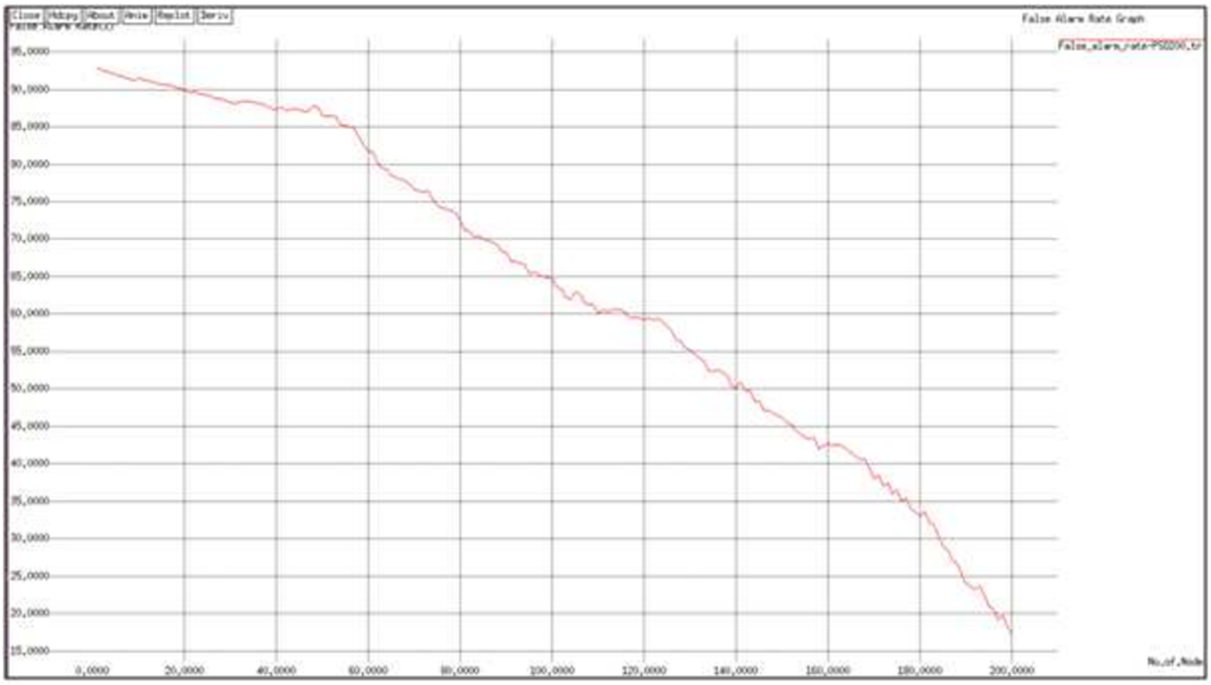


Figure 5.24: False Alarm Rate at 200 nodes using PSO based routing

Table 5.4: Average False Alarm Rate at varying node size

Sr. No.	Node Size	Avg. FAR (%) at minimum Node size	Avg FAR(%) highest node size
1	50	89.5	22.6
2	100	89.3	18.6
3	150	89.8	17.5
4	200	89.7	17.3

false alarm rate. Maximum FAR shown in the table is 89.8% at node size 3. FAR found to be decreasing gradually with increasing node size.

5.2.2 Accuracy

Accuracy refers to the total number of correctly identified abnormal signatures out of total packet signatures encountered. Figure 5.25 to 5.28 shows the accuracy of proposed algorithm against varying node size. It is observed that the accuracy of IDS increases with increasing number of nodes.

The intermittent ups and downs in accuracy values are observed in graphs above. Since the node bears random fitness, the average accuracy of detecting abnormal signatures also varies from node to node. It is observed that the accuracy of proposed intrusion detection algorithm is directly proportional to a number of nodes.

Table 5.5 presents comparison of accuracy statistics of PSO-based IDS algorithm at varying node size. Minimum node size considered is 3 to justify the role of source, destination, and an attacker node. Maximum average accuracy observed in presence of 200 nodes is 91.2%. Whereas, minimum accuracy is 19.8% at node size 150.

5.3 Comparative Analysis

In general, to evaluate the performance of PSO-based model presented in this thesis, it is essential to compare its performance against existing proven models. While conducting this experi-

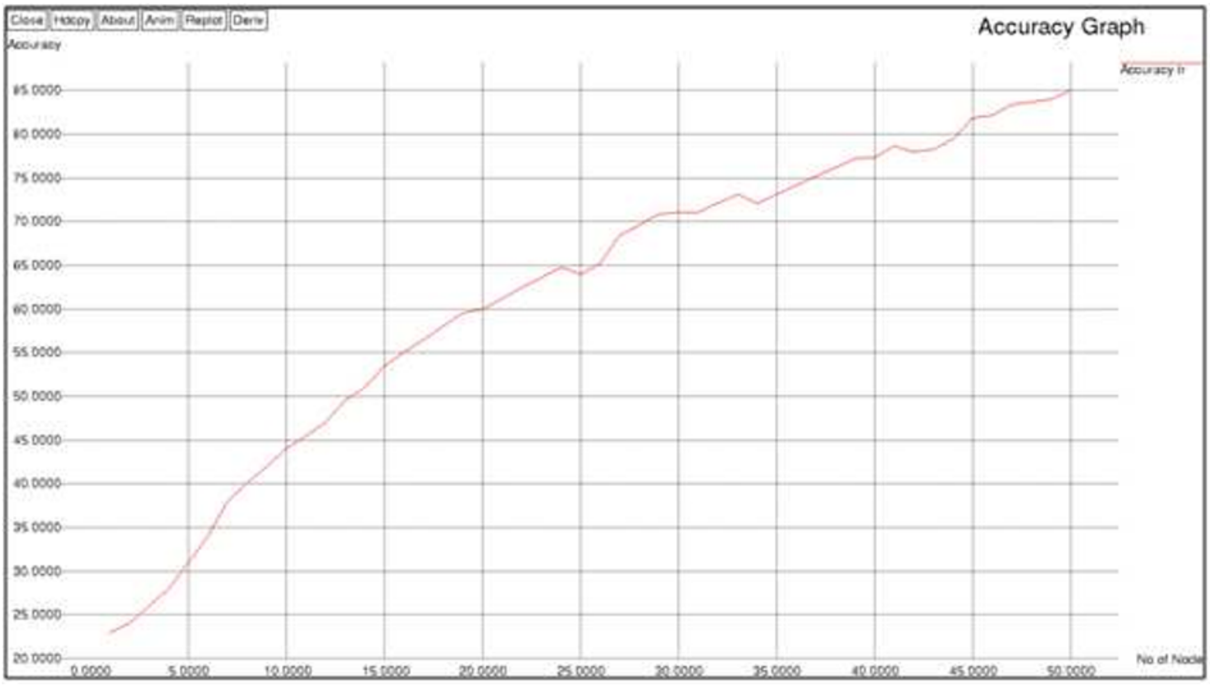


Figure 5.25: Accuracy of PSO-based IDS algorithm at 50 nodes

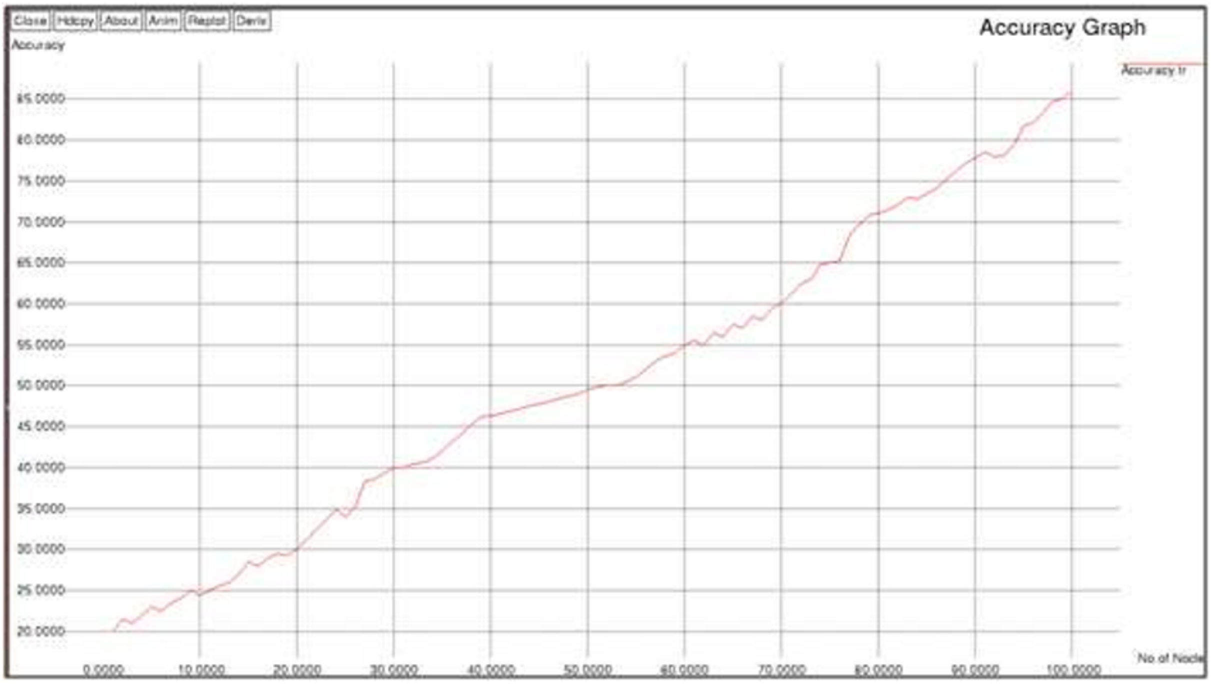


Figure 5.26: Accuracy of PSO-based IDS algorithm at 100 nodes

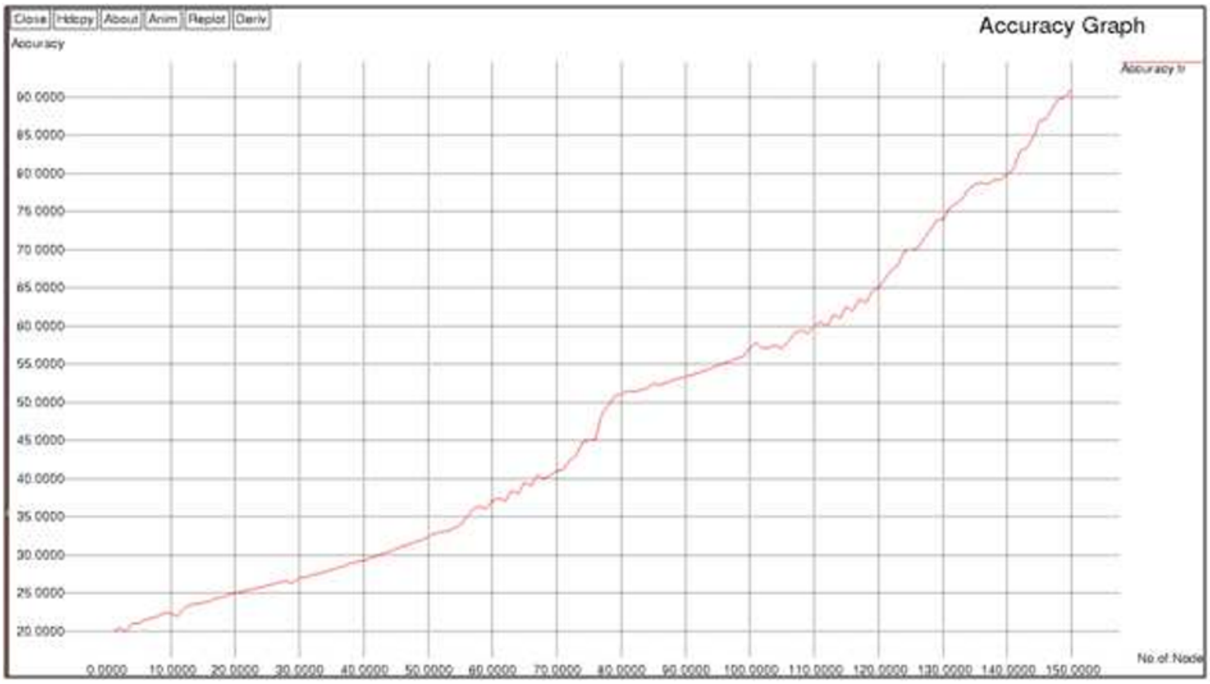


Figure 5.27: Accuracy of PSO-based IDS algorithm at 150 nodes

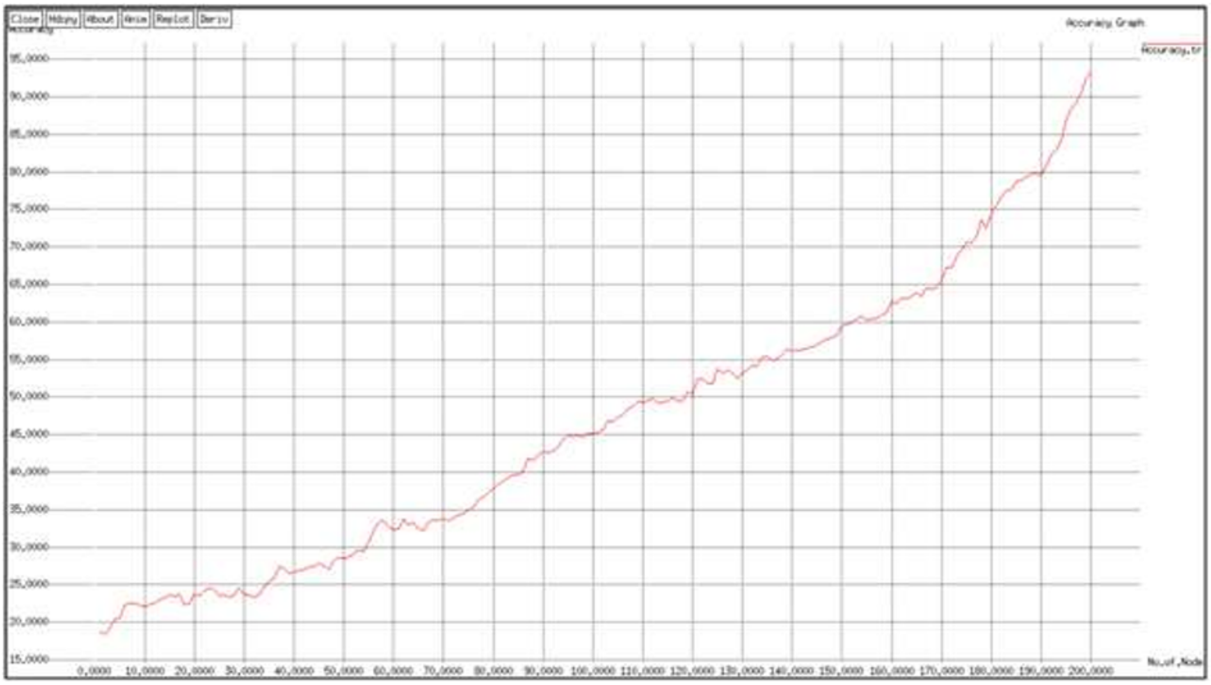


Figure 5.28: Accuracy of PSO-based IDS algorithm at 200 nodes

Table 5.5: Average Accuracy at varying node size

Sr. No.	No. of Nodes	Avg Accuracy(%) at minimum node size	Avg Accuracy(%) at highest node size
1	50	24.3	85.1
2	100	20.4	86.2
3	150	19.8	91.2
4	200	19.9	91.2

ment, it was essential to test other existing models under similar circumstances as like proposed model. With the same purpose, other widely known IDS models namely Watchdog and EAACK are also implemented using NS2. The results of these two models are evaluated using similar performance parameters. Watchdog is the very first successful intrusion detection technique invented by Marti et.al. in 2000. The performance of Watchdog-Pathrator technique is still comparable with recently published models by researchers. Another model implemented and used for comparison with proposed model is Enhanced Adaptive ACKnowledgement (EAACK). The working of Watchdog and EAACK is presented in chapter 2. EAACK is the recent acknowledgment based scheme found successful over advanced attack types. Watchdog-Pathrator uses DSR protocol whereas, EAACK uses AODV routing protocol. So, another advantage of this experimentation is that we can also compare the performance of AODV and DSR protocols with PSO based routing.

5.3.1 Comparing the accuracy of PSO based IDS algorithm with Watchdog and EAACK

The capability to correctly identify intrusive patterns is called as accuracy of an IDS. The accuracy of the proposed algorithm is compared with Watchdog and EAACK and the same is presented in figure 5.29. Accuracy curves of EAACK and Watchdog are close to each other with increasing number of nodes. Since EAACK was developed to overcome limitations of Watchdog and is modified version of it [29], accuracy results of both algorithms are comparable. Also, features such as Secure-ACKnowledgement (S-ACK) and Misbehavior Report Ac-

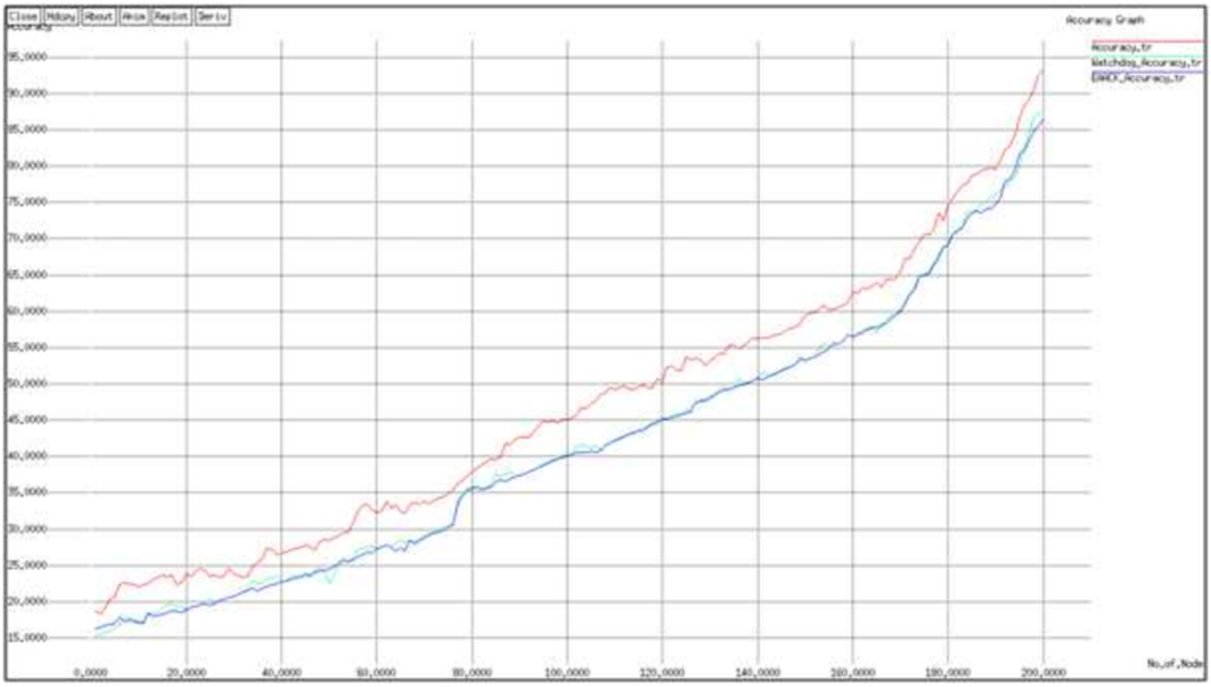


Figure 5.29: Accuracy versus number of nodes in PSO based IDS, EAACK and Watchdog

Table 5.6: Comparing the accuracy of PSO based IDS, EAACK and Watchdog

Sr. No.	Method / No. of Nodes	3	200
1	Watchdog Average Accuracy	15.1 %	86.9 %
2	EAACK Average Accuracy	16.3 %	86.8 %
3	Proposed Algorithm Average Accuracy	19.9 %	91.2 %

knowledgement (MRA) in EAACK doesn't benefit intrusion detection mechanism of EAACK significantly. On the contrary, the accuracy of the PSO-based IDS is consistently high with increasing number of nodes in comparison to Watchdog and EAACK. In common, accuracy of all three algorithms gradually increases with increasing node size.

Accuracy statistics of Watchdog, EAACK, and PSO-based IDS are presented in Table 5.6. In case of all algorithms, average accuracy increases with increasing number of nodes. Average accuracy of PSO-based IDS is high than the other two algorithms. In comparison graph too, the accuracy of PSO based IDS algorithm is consistently high than Watchdog and EAACK against varying node size.

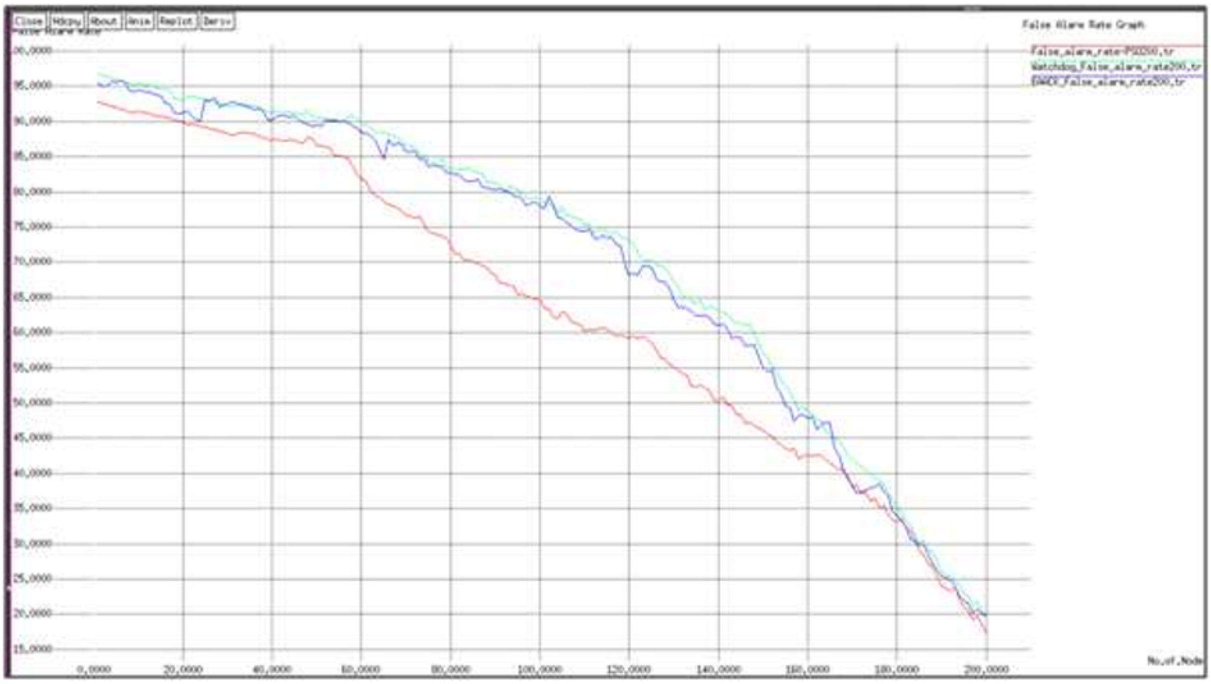


Figure 5.30: False Alarm Rate versus the node size in PSO based IDS, EAACK and Watchdog

5.3.2 Comparing false alarm rate of PSO based IDS algorithm with Watchdog and EAACK

Routing protocol plays a crucial role in secure QoS routing in MANET. Watchdog and EAACK are based on DSR and AODV routing protocols respectively. Limitations of these protocols affect the performance of these two models. Whereas, the routing based on PSO algorithm benefit intrusion detection model presented in this research. False alarm rate of PSO based IDS model is compared with FAR of Watchdog and EAACK and results are presented in the figure 5.30. It is observed that false alarm rate of PSO based IDS algorithm is consistently less than Watchdog and EAACK. The detailed statistics for comparing these three algorithms are shown in table 5.7.

Table 5.7: Comparing false alarm rate of PSO based IDS, EAACK and Watchdog

Sr. No.	**Method / No. of Nodes**	**3**	**200**
1	Watchdog Average FAR	96.1%	21.4%
2	EAACK Average FAR	95.7%	19.9%
3	Proposed Algorithm Average FAR	89.8%	17.3%

5.4 Chapter Summary

This chapter presents results of four experiments. The first experiment conducted is the implementation of PSO as routing protocol in MANET. An audit set is obtained using selected MANET routing performance attributes namely end-to-end delay, packet loss, average packet throughput etc. Other QoS performance attributes such as bandwidth and energy available at each node are well taken care by fitness function designed for PSO routing.

In the second experiment, five active attacks namely, denial of service, blackhole, sybil, fabrication, and replay are implemented and routing performance attribute values are again recorded. Collectively, packet signatures obtained through experiment one and two generates an audit set which is used as a training set for further experimentation.

In the third experiment, an evolving IDS algorithm is designed and implemented using MANET environment obtained in first two experiments. It is notable that this architecture well ensures host as well as network intrusion detection. Each node acts as IDS agent and keeps on updating it's audit dataset containing normal and abnormal packet signatures. Performance of PSO based IDS is tested using parameters such as accuracy and false alarm rate values. To ensure scalability, the same experiment is conducted at different node sizes, particularly 50,100,150 and 200.

Despite proved efficiency of PSO in wide variety of application areas, very few researchers have attempted to apply PSO based routing successfully in their research. Mapping of existing PSO parameters with MANET requires generality of the parameters to be preserved. The same is achieved successfully in this research resulting in efficient routing. The same is observed through comparison of proposed model with frequently used routing protocols namely AODV and DSR.

In the literature, it is found that many researchers have evaluated their models using various performance parameters. Moreover, researchers attempted their experiments at different node sizes while conducting their experiments. So, to finalize the ideal node count for routing experiment was challenging task for us. To ensure the same, the performance of PSO-based routing is evaluated against node size 50,100,150 and 200 respectively. The results presented in this chapter shows vividly that node density affects the performance of IDS system.

Contrary to wired environments, there is no standard dataset containing packet signatures of all known attacks available for MANET. To deal with this issue, an audit set containing packet signatures for five attack types is obtained. This anomaly type of approach may further extend to any number of attacks. The overhead of updating this audit set at each MANET node can be addressed using agent-based approach. Attack behaviors of individual attacks are coded at a specific node. The fitness function is possible to update further based on parameters designed for QoS routing in this model.

The performance of proposed algorithm is tested against well-known IDS algorithms namely, Watchdog and EAACK in the fourth experiment. To ensure originality of results obtained, similar MANET environment is used for experimentation. Also, same performance parameters are applied to evaluate the results.

Chapter 6

Conclusions and Future Scope

6.1 Conclusions

MANET with IoT is proving itself a solution to cater ever increasing need of society in a wide variety of sectors such as healthcare systems, transports, safety zones etc. The focus of this research is on designing an evolving intrusion detection algorithm using PSO-based routing. Thus, the entire research discussed in this thesis is to achieve this aim. Conclusions of this research are presented below:

1. MANET is a wireless network with an autonomous group of nodes. Dynamic nature of MANET node makes it susceptible to security threats. Depending on nature of attack type the appropriate measure to detect and prevent such attacks are required. At the beginning of this research, various MANET security attacks, their effects on MANET communication are studied in depth. Overview of the same is presented in chapter 2.

2. So far, many researchers have presented their intrusion detection approaches in the literature. A rigorous survey of various intrusion detection models is conducted in this research. The same is discussed in chapter 2. Also the existing IDS approaches are categorized based on architecture, attack detection method used and routing specific algorithms used etc. The limitations of each of these models are also well discussed in chapter 2. The same proved helpful in designing an evolving IDS model capable of addressing limitations of existing IDS models.

3. Since this research is based on PSO-based MANET routing, existing PSO based approaches for MANET routing and intrusion detection are also reviewed extensively. The intrusion detection models based on PSO are presented in chapter 3. Discussion on performance parameters for PSO based routing and IDS algorithm is also presented in chapter 3. Since PSO is a stochastic algorithm, applying it in MANET requires proper mapping of PSO parameters with MANET scenario. Based on a comprehensive study presented in earlier chapters, algorithm for intrusion detection is proposed and presented in chapter 4. The same chapter describes the architecture of IDS agent and NS2 simulation settings used in this experimentation.

4. Chapter 5 presents results of experiments conducted throughout this research. In initial section of chapter 5, results of PSO based routing are presented. The parameters used for this evaluation are discussed in chapter 5. The route identification of PSO based routing is presented using graphs obtained from NS2 simulation. Whereas, proposed IDS model is evaluated using two performance parameters, accuracy and false alarm rate. This evaluation proved that PSO based IDS is efficient than other two algorithms.

5. To compare proposed model with existing models, well known IDS techniques namely Watchdog and EAACK are also implemented using same MANET environment. The accuracy and false alarm rate of these three algorithms are described using graphs obtained from the NS2 xgraph module. All evaluations are conducted at varying node size. Statistical analysis of results obtained through graphs is also presented in chapter 5.

In this thesis, an evolving IDS algorithm for MANET based on PSO algorithm is proposed. The model presented in this thesis is low cost and effectively solves routing issues in an ever-changing environment of MANET. It is also claimed to be effective over major advanced attacks such as denial of service, blackhole, sybil, fabrication and replay. The performance of proposed IDS system is evaluated against two existing IDS models namely Watchdog and EAACK.

This research shows that intrusion detection model based on PSO minimizes false alarm rate up to significant level and gives better results on QoS parameters. This model is flexible enough to inculcate most of the desired QoS parameters by reformulating fitness function. Looking at the unavailability of a standard dataset containing packet signatures of all types of routing attacks in the current scenario, this research provides a better training dataset which can be standardized further. This model is tested in presence of a single attacker node at an instance. Also, the proposed model is tested considering maximum size of 200 nodes. The performance parameters may observe a significant difference with higher node density.

6.2 Future Scope

This chapter concludes the thesis and provides a summary of scope for future research. The contributions and limitations of this research are also presented in this chapter. It also provides directions for future research. To address all security issues in MANET is very difficult to achieve but this research mitigates most of the limitations of existing research towards achieving efficient routing and secure communication.

It is further possible to improve and standardize IDS model presented in this thesis for multi-objective and multi-layered types of attacks. A comprehensive dataset containing packet signatures containing advanced attack types can also be generated with this model. Efforts in minimizing the overhead of communication incurring in updating audit set at each node need to be minimized to some extent. Some of the genuine MANET nodes are unable to contribute to communication. Such nodes lower MANET performance. Efforts to eliminate such hidden and exposed terminal phenomena are required.

References

[1] N. Raza, M. Aftab, M. Akbar, O. Ashraf, and M. Irfan, “Mobile Ad-Hoc Networks Applications and Its Challenges,” *Communications and Network*, vol. 8, pp. 131–136, 2016.

[2] R. Mitchell and I. R. Chen, “A Survey of Intrusion Detection in Wireless Network Applications,” *Computer Communications*, pp. 1–23, 2014.

[3] B. Kannhavong, H. Nakayama, and Y. Nemoto, “Mobile Ad Hoc and Sensor Networks: A Survey of Routing a Ttacks in Mobile Ad Hoc Networks,” *IEEE Wirel. Commun.*, vol. 8, pp. 85–91, 2007.

[4] H. Otrok, J. Paquet, M. Debbabi, and P. Bhattacharya, “Testing Intrusion Detection Systems in MANET: A Comprehensive Study,” in *Proc. - CNSR 2007* 5^{th} *Annu. Conf. Commun. Networks Serv. Res.*, pp. 364–371, 2007.

[5] A. Bang and P. Ramteke, “MANET: History, Challenges and Applications,” *Int. J. Appl. or Innov. Eng. Manag.*, vol. 2(9), pp. 249–251, 2013.

[6] M. Conti and S. Giordano, “Mobile Ad-hoc Networking: Milestones, Challenges, and New Research Directions,” *IEEE Communications Magazine*, vol. 22(1), pp. 85–96, 2014.

[7] B. Peacock, “Connecting The Edge: Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare,” *Blue Horizons Paper Center for Strategy and Technology*, pp. 1–47, 2007.

[8] Y. Tseng and W. H. Liao, “Mobile Ad Hoc Networks and Routing Protocols,” *Handbook of Wireless Networks and Mobile Computing*, vol. 8, pp. 371–392, 2002.

[9] A. Dorri and S. R. Kamel, “Security Challenges in Mobile Ad Hoc Networks: A Survey,” *Int. J. Comput. Sci. Eng. Surv*, vol. 6(1), pp. 15–29, 2015.

[10] W. S. Bhaya and S. A. AlAsady, “Prevention of Spoofing Attacks in the Infrastructure Wireless Networks,” *J. Comput. Sci.*, vol. 8(10), pp. 1769–1779, 2012.

[11] H. Kim, R. B. Chitti, and J.-S. Song, “Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks,” *J. Inf. Process. Syst.*, vol. 7(1), pp. 137–150, 2011.

[12] W. Alnumay and U. Ghosh, “Secure Routing and Data Transmission in Mobile Ad Hoc Networks,” *Int. J. Comput. Networks Commun*, vol. 6(1), pp. 111–127, 2014.

[13] L. Qian, N. Song, and X. Li, “Detection of Wormhole Attacks in Multi-path Routed Wireless Ad-hoc Networks: A Statistical Analysis Approach,” *Netw. Comput. Appl.*, vol. 30(1), pp. 308–330, 2007.

[14] M. K. Denko, “Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme,” *J. Syst. Cybern. Informatics*, vol. 3(4), pp. 1–9, 2012.

[15] G. W. Kibirige and C. Sanga, “A Survey on Detection of Sinkhole Attack in Wireless Sensor Networks,” *Int. J. Comput. Sci. Inf. Secur*, vol. 13(5), pp. 1–9, 2015.

[16] D. Shehzad, A. I. Umar, and N. U. Amin, “A Novel Mechanism for Detection of Sybil Attack in MANETs,” in *Proc. International conference on Computer Science and Information Systems (ICSIS2014)*, pp. 119–122, 2014.

[17] M. Elboukhari, M. Azizi, and A. Azizi, “Impact Analysis of Black Hole Attacks on Mobile Ad Hoc Networks Performance,” *Int. J. Grid Comput. Appl.*, vol. 6(1), pp. 1–11, 2015.

[18] Z. Hicham, T. Ahmed, L. Rachid, and I. Noureddin, “Valuating and Comparison of Intrusion in Mobile Ad Hoc Networks,” *International Journal of Distributed and Parallel Systems (IJDPS)*, vol. 3(2), pp. 243–259, 2012.

[19] M. Fihri, M. Otmani, and A. Ezzati, “The Impact of Black-Hole Attack on AODV Protocol,” *International Journal of Advanced Computer Science and Applications, Special Issue on Advances in Vehicular Ad Hoc Networking and Applications*, pp. 20–24, 2014.

[20] S. Malladi, J. Alves-foss, and R. Heckendorn, “On Preventing Replay Attacks on Security Protocols,” *Int. Conf. on Security and Management*, pp. 77–83, 2002.

[21] M. S. Khan, M. I. Khan, S. Malik, O. Khalid, M. Azim, and N. Javaid, “MATF: a Multi-attribute Trust Framework for MANETs,” *Eurasip Journal on Wireless Communication and Networking*, vol. 1, 2016.

[22] D. G. Kampitaki, E. D. Karapistoli, and A. A. Economides, “Evaluating selfishness impact on MANETs,” in *Proc. Int. Conf. Telecommun. Multimedia (TEMU)*, pp. 64–68, 2014.

[23] A. Nadeem and M. P. Howarth, “A Survey of MANET Intrusion Detection and Prevention Approaches for Network Layer Attacks,” *Commun. Surv. Tutorials*, vol. 15(4), pp. 2027–2045, 2013.

[24] B. B. Wernik, “ARP Spoof Attack Mitigation and Threat Analysis in Mobile Ad-Hoc Networks(MANETs),” *Honors Project Report*, pp. 1–57, 2012.

[25] S. Ghoreishi, S. A. Razak, I. F. Isnin, and H. Chizari, “Rushing Attack Against Routing Protocols in Mobile Ad-Hoc Networks,” in *Proc. International Symposium on Biometrics and Security Technologies (ISBAST)*, p. 220224, 2014.

[26] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, “Mitigating Byzantine Attacks in Ad Hoc Wireless Networks,” *Dep. Comput. Sci. Johns Hopkins Univ. Tech. Rep. Version (2004)*, vol. 1, pp. 1–16, 2004.

[27] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security In Mobile Ad Hoc Networks: Challenges And Solutions,” *IEEE Wireless Communications*, vol. 11(1), pp. 38–47, 2004.

[28] Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad-hoc Networks,” in *Proc.* $6^{th} Annu.Int.Conf.Mob.Comput.Netw. - MobiCom2000, p. 275283, 2000.$

[29] H. Kayacik, Zincir-Heywood, and N. Heywood, "Intrusion Detection Systems: Encyclopedia of Multimedia Technology and Networking," *Idea Group Reference*, vol. 1, pp. 494–499, 2005.

[30] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks," in *Proc.* 6^{th} *Annu. Int. Conf. Mob. Comput. Netw. MobiCom 00*, vol. 1(18), pp. 255–265, 2000.

[31] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK A Secure Intrusion-Detection System for MANETs," *IEEE Trans. Ind. Electron*, vol. 60(3), pp. 1089–1098, 2013.

[32] R. Werlinger and K. Hawkey and K. Muldner and P. Jaferian and K. Beznosov, "The challenges of using an intrusion detection system: Is it worth the effort," in *SOUPS 08 Proc.* 4^{th} *Symp. Usable Priv. Secur*, vol. 1, pp. 107–118, 2008.

[33] I. Broustis, M. Faloutsos, and S. Krishnamurthy, "Overcoming The Challenge of Security in a Mobile Environment," in *Conf. Proc. IEEE Int. Performance, Comput. Commun. Conf.*, pp. 617–622, 2006.

[34] Y. Li and J. Wei, "Guidelines on Selecting Intrusion Detection Methods in MANET," in 21^{st} *Annu. Conf. Inf. Syst. Educ. (ISECON)*, vol. 21, pp. 4–7, 2004.

[35] M. R. Chinthireddy and S. Aravind, "A Survey Comparison Of Intrusion Detection Systems In MANETs," *International Journal of Emerging Trends Technology in Computer Science (IJETTCS)*, vol. 3(3), pp. 58–64, 2014.

[36] S.Parameswari and G. Michael, "Intrusion Detection System in MANETS: A Survey," *International Journal of Engineering and Technical Research (IJETR)*, vol. 3(4), pp. 60–63, 2014.

[37] V. L. Pavani and P. B. Sathyanarayana, "A Survey on Present State of the Art of Intrusion Detection Systems in MANETs: Finding Research Gaps," *International Journal of Science and Research*, vol. 3(9), pp. 2010–2014, 2014.

[38] M. K. Rafsanjani, A. Movaghar, and F. Koroupi, "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes," *World Academy of Science, Engineering and Technology*, vol. 2(8), pp. 351–355, 2008.

[39] S. Gangwar, "Mobile Ad Hoc Network: A Comprehensive Study and Survey on Intrusion Detection," *Int. J. Eng. Res. Appl.*, vol. 2(1), pp. 607–612, 2012.

[40] Y. X. B. Sun, L. Osborne and S. Guizani, "Intrusion Detection Techniques in Mobile AD Hoc and W Ireless S Ensor Networks," *Korea Adv. Inst. Sci. Technol*, pp. 56–63, 2007.

[41] M. S. Iftikhar and M. R. Fraz, "A Survey on Application of Swarm Intelligence in Network Security," *Trans. Mach. Learn. Artif. Intell.*, vol. 1(1), pp. 1–15, 2013.

[42] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks," in *Proc. - UKSim 15th Int. Conf. Comput. Model. Simulation, UKSim 2013*, pp. 693–698, 2013.

[43] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," *Wireless/Mobile Network Security*, pp. 170–196, 2006.

[44] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," in *Proc.* 1^{st} *ACM Work. Secur. Ad Hoc Secur. Ad Hoc Sens. Networks (in Assoc. with 10th ACM Conf. Comput. Commun. Secur*, pp. 135–147, 2003.

[45] R. Guha, O. Kachirski, D. G. Schwartz, S. Stoecklin, and E. Yilmaz, "Case-based Agents for Packet-level Intrusion Detection in Ad Hoc Networks," in *Proc.* 17^{th} *Int. Symp. Comput. Inf. Sci.*, pp. 315–320, 2003.

[46] A. Esfandi, "Efficient Anomaly Intrusion Detection System in Adhoc Networks by Mobile Agents," in *Proc.* 3^{rd} *Int. Conf. Comput. Sci. Inf. Technology*, vol. 7, pp. 73–77, 2010.

[47] M. Raciti, J. Cucurull, and S. Nadjm-Tehrani, "Energy-based Adaptation in Simulations of Survivability of Ad Hoc Communication," *IFIP Wirel. Days*, vol. 1(1), pp. 1–7, 2011.

[48] S. Umang, B. V. R. Reddy, and M. N. Hoda, “Enhanced Intrusion Detection System for Malicious Node Detection in Ad hoc Routing Protocols using Minimal Energy Consumption,” *IET Commun.*, vol. 4(17), pp. 20–34, 2010.

[49] F. Tseng, L. Chou, and H.-C. Chao, “A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks,” *Human-centric Comput. Inf. Sci.*, vol. 1(1), pp. 1–16, 2011.

[50] F. Na, “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges,” *IEEE Communications Surveys Tutorials*, vol. 13(4), pp. 658–672, 2011.

[51] S. R. Radhakrishnan and S. Muthukumar, “Avoid Packet Replication Attack Based on Intrusion Detection and Defense Mechanism over MANET,” *International Journal of Engineering Research and Technology*, vol. 3(2), pp. 369–374, 2014.

[52] Y. Jing, X. Wang, X. Xiao, and G. Zhang, “A Logless Fast IP Traceback Scheme Against DDoS Attacks in Wireless Ad-hoc Network,” in *Proceedings of Wireless, Mobile And Multimedia Networks. Iet International Conference (ICWMMN)*, 2006.

[53] U. Venkanna and R. L. Velusamy, “Black Hole Attack and Their Counter Measure Based on Trust Management in MANET: A Survey,” in *Adv. Recent Technol. Commun. Comput. (ARTCom 2011),* 3^{rd} *Int. Conf.*, 2011.

[54] L. P. Rajeswari, R. a. X. Annie, and a. Kannan, “Enhanced intrusion detection techniques for mobile ad hoc networks,” in *IET-UK Int. Conf. Inf. Commun. Technol. Electr. Sci. (ICTES 2007)*, pp. 1008–1013, 2007.

[55] G. Indirani, K. Selvakumar, and V. Sivaaamasundari, “Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET using Swarm Intelligence,” in *Proc. 2013 Int. Conf. Pattern Recognition, Informatics Mob. Eng. PRIME*, pp. 152–156, 2013.

[56] G. Indirani and K. Selvakumar, “A Swarm-based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET),” *Int. J. Parallel, Emergent Distrib. Syst.*, vol. 29(1), pp. 90–103, 2014.

[57] H. Nakayama, S. Kurosawa, A. Jamalipour, and Y. Nemoto, “A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks,” *IEEE Transactions on Vehicular Technology*, vol. 58(5), pp. 2471–2481, 2009.

[58] A. Damodaram and K. Pavani, “Intrusion Detection using MLP for MANETs,” in *Proc. of* 3^{rd} *Int. Conf. Comput. Intell. Inf. Technol. (CIIT 2013)*, pp. 440–444, 2013.

[59] N. Marchang and R. Datta, “Light-weight Trust-based Routing Protocol for Mobile Ad Hoc Networks,” *IET Inf. Security*, vol. 6(2), pp. 77–83, 2012.

[60] S. Buchegger and J. L. Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Adhoc NeTworks),” in *Proc. MobiHoc 02 Proc.* 3^{rd} *ACM Int. Symp. Mob. ad hoc Netw. Comput.*, pp. 226–236, 2002.

[61] S. Bansal and M. Baker, “Observation-based Cooperation Enforcement in Ad Hoc Networks,” in *Proc.Comput. Res. Repos.*, pp. 1–10, 2003.

[62] P. Michiardi and R. Molva, “Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,” in *Adv. Commun. Multimed. Secur. IFIP TC6/TC11* 6^{th} *Jt. Work. Conf. Commun. Multimed. Security*, pp. 107–121, 2002.

[63] C. Tseng, C. Ko, J. Rowe, and K. Levitt, “A Specification-based Intrusion Detection System for AODV,” in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pp. 125–134, 2003.

[64] C. Obimbo and L. M. Arboleda-cobo, “An Intrusion Detection System for MANET,” *Communications in Information Science and Management Engineering*, vol. 2(3), pp. 1–5, 2012.

[65] J. L. Boudec, “An Artificial Immune System Approach With Secondary Response for Misbehavior Detection in Mobile ad hoc Networks,” *IEEE Transactions on Neural Networks*, vol. 16(5), pp. 1076–1087, 2005.

[66] B. Sun, K. Wu, and U. Pooch, “Zone-based Intrusion Detection For Mobile Ad Hoc Networks,” *Int. J. Ad Hoc and Sensor Wireless Networks*, vol. 2(3), pp. 297–324, 2003.

[67] P. Yi, V. Wu, and J. Li, "Malicious Node Detection in Ad Hoc Networks Using Timed Automata," in *Proceedings of IET Conference on Wireless, Mobile and Sensor Networks (CCWMSN07)*, 2007.

[68] H. Ding and X. Xu, "Real-time Cooperation Intrusion Detection System for MaNets," in *IET Int. Conf. Wirel. Mob. Multimed. Networks Proc. (ICWMMN 2006)*, pp. 406–410, 2006.

[69] H. Bathla and K. Lakhani, "A Novel Method For Intrusion Detection System To Enhance Security In Ad Hoc Network," *Journal of Computing*, vol. 2(5), pp. 101–107, 2010.

[70] X. Ye, J. Li, and Y. Li, "An Anomaly Detection System based on Hide Markov Model for MANET," in 6^{th} *Int. Conf. Wirel. Commun. Netw. Mob. Computing*, pp. 1–4, 2010.

[71] N. Yosaka, I. Nishimura, and T. Nagase, "Authentication and Certificate Managements of Unauthorized Intrusion in Ad-Hoc Networks, Problems and Solutions," in 14^{th} *Int. Conf. Network-Based Inf. Syst.*, pp. 646–650, 2011.

[72] T. M. Chen, "Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks," *IEEE Internet Computing*, pp. 35–41, 2005.

[73] S. Bu, F. R. Yu, X. P. Liu, P. Mason, and H. Tang, "Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks," *IEEE Internet Computing*, vol. 60(3), pp. 1025–1036, 2011.

[74] R. Bai and M. Singhal, "DOA: DSR over AODV Routing for Mobile Ad Hoc Networks," *IEEE Transactions On Mobile Computing*, vol. 5(10), pp. 1403–1416, 2006.

[75] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C. Tseng, and T. Bowen, "A General Cooperative Intrusion Detection Architecture for MANETs," 3^{rd} *IEEE Int. Work. Inf. Assur*, pp. 57–70, 2005.

[76] P. Selvigrija and J. Premkumar, "Bandwidth Shared Acknowledgment (BSA)-A Secure Intrusion Detection and Multi Path Routing for MANETs," in *Proceedings of International Conference on Information Communication and Embedded Systems (ICICES2014)*, pp. 1–6, 2014.

[77] R. S. Annarasi and S. Sivanesh, "A Recent Secure Intrusion Detection System for MANETs," in *Proceedings of IEEE International Conference on Advanced Communication Control and Computing Teclmologies (ICACCCT)*, vol. 3(1), pp. 54–62, 2013.

[78] H. Xia, Z. P. Jia, and E. H. M. Sha, "Research of Trust model based on Fuzzy Theory in Mobile Ad Hoc Networks," *IET Inf. Secur*, vol. 8(2), pp. 88–103, 2014.

[79] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in MANET," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2816–2821, 2008.

[80] G. Kulkarni, B. Patel, and P. Laxkar, "Time Stamp based Cross Layer MANET Security Protocol," in *Proceedings of IET Conf. Publ.*, pp. 191–199, 2013.

[81] H. T. S. Bu and F. R. Yu, "A Computationally Efficient Method for Joint Authentication and Intrusion Detection in Mobile Ad-hoc Networks," in *Proceedings of EEE International Conference on Communications*, pp. 1–5, 2011.

[82] E. Hernndez-Orallo and M. D. S. Olmos and J. C. Canoand C. T. Calafate, and P. Manzoni, "Cocowa: A collaborative contact-based watchdog for detecting selfish nodes," *IEEE Trans. Mob. Comput*, vol. 14(6), 2015.

[83] Y. an Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies," in *Proceedings of IEEE International Conference on Distributed Computing Systems*, pp. 1–25, 2003.

[84] C. Panos, C. Xenakis, and I. Stavrakakis, "A Novel Intrusion Detection System for MANETs," in *Proceedings of IEEE International Conference on Security and Cryptography (SECRYPT)*, pp. 25–34, 2010.

[85] S. Sen and J. Clark, "Intrusion Detection in Mobile Ad hoc Networks," *Guide to Wireless Ad Hoc Networks*, pp. 427–454, 2009.

[86] D. Fu and H. Wang, “The Implementation of A Intrusion Detection System Model Based on Particle Swarm Reduction,” in *Proceedings of IEEE International Conference on Information Science and Engineering (ICISE)*, pp. 1–3, 2010.

[87] P. Goyal, V. Parmar, and R. Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application,” *IJCEM Int. J. Comput. Eng. Manag.*, vol. 11, pp. 32–37, 2011.

[88] P. Johansson, T. H. Larsson, N. Mielczarek, and B. Degermark, “Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks,” in *Proceedings of the 5^{th} annual ACM/IEEE international conference on Mobile computing and networking*, pp. 195–206, 1999.

[89] T. Clausen, J. Yi, and A. C. D. Verdiere, “LOADng: Towards AODV version 2,” in *Proceedings of IEEE Veh. Technol. Conf.*, pp. 2–6, 2012.

[90] S. Mohapatra and P. Kanungo, “Performance Analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator,” in *Procedia Eng.*, vol. 30, pp. 69–76, 2012.

[91] S. Xiaonan and W. Wolfgang, “The Use of Computational Intelligence in Intrusion Detection Systems: A Review,” *Elsevier’s Applied Soft Computin*, pp. 1–35, 2008.

[92] M. Fleischer, “Foundations of Swarm Intelligence: From Principles to Practice,” *Swarming: Network Enabled C4ISR*, pp. 1–139, 2005.

[93] J. Kennedy and R. C. Eberhart, “Particle Swarm Optimization,” in *Proc. IEEE Int. Conf. Neural Networks*, pp. 1942–1948, 1995.

[94] D. Sedighizadeh and E. Masehian, “Particle Swarm Optimization Methods , Taxonomy and Applications,” *Int. J. Comput. Theory Eng*, vol. 1(5), pp. 486–502, 2009.

[95] R. Poli, “An Analysis of Publications on Particle Swarm Optimisation Applications,” *J. Artif. Evol. Appl*, pp. 1–57, 2007.

[96] Z. L.-j. Z. Vi and N. Network, “A Rule Generation Model Using S-PSO for Misuse Intrusion Detection,” in *Procedings of International Conference on Computer Application and System Modeling (ICCASM)*, pp. 418–423, 2010.

[97] Y. Zhang, S. Wangand, Y. Zhang, S. Wang, and G. Ji, “A Comprehensive Survey on Particle Swarm Optimization Algorithm and Its Applications,” *Hindawi Publishing Corporation Mathematical Problems in Engineering*, pp. 1–38, 2015.

[98] Y. Kim and K. H. Lee, “Visualizing the Search Process of Particle Swarm Optimization,” in *Procedings of Genetic and Evolutionary Computation Conference*, pp. 49–55, 2009.

[99] Bhushan Chaudhari and Rajesh Prasad, “Particle Swarm Optimization Based Intrusion Detection for Mobile Ad-hoc Network,” *Proceedings of International Conference on Advances in Information Science and Computer Engineering, WSEAS, Dubai*, pp. 477–482, 2015.

[100] R. V. Kulkarni, G. K. Venayagamoorthy, A. Miller, and C. H. Dagli, “Investigating Open Issues in Swarm Intelligence for Mitigating Security Threats in MANET,” *Int. J. Electr. Comput. Eng.*, vol. 5(5), pp. 1194–1201, 2015.

[101] M. Achankunju, R. Pushpalakshmi, and A. V. A. Kumar, “Particle Swarm Optimization based Secure QoS Clustering for Mobile Ad hoc Network,” in *Procedings of Int. Conf. Commun. signal Process*, pp. 315–320, 2013.

[102] I. C. Trelea, “The Particle Swarm Optimization Algorithm: Convergence Analysis and Parameter Selection,” *Elsevier Information Processing Letters*, vol. 85(6), pp. 317–325, 2003.

[103] T. Zhou, Y. Li, and J. Li, “Research on Intrusion Detection of SVM based on PSO,” in *Procedings of Int. Conf. Mach. Learn. Cybern*, vol. 2, pp. 12–15, 2009.

[104] S.Subburaj.V and K. Chitra, “Mobile Node Dynamism using Particle Swarm Optimization to fight against Vulnerability Exploitations,” *Int. J. Comput. Appl.*, vol. 41(13), pp. 1–4, 2012.

[105] R. V. Boppana and X. Su, “On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks,” *IEE TraEnsactions on Mobile Computing*, vol. 10(8), pp. 1162–1174, 2011.

[106] G. K. C. Kolias and M. Maragoudakis, “Swarm Intelligence in Intrusion Detection: A survey,” *Elsevier’s Computers Security*, vol. 30(8), pp. 625–642, 2011.

[107] B. Atoufi and H. Shah-Hosseini, “Advanced Knowledge Based Systems Model; Applications Research,” *TMRF e-Book Advanced Knowledge Based Systems: Model, Applications Research*, vol. 1, pp. 126–159, 2010.

[108] S. J. J. Wang, “Research on the Application of Particle Swarm Optimization Algorithm in Anomaly Detection,” *The* 5^{th} *International Conference on Computer Science Education*, pp. 474–476, 2010.

[109] B. Nancharaiah and B. C. Mohan, “MANET Link Performance using Ant Colony Optimization and Particle Swarm Optimization Algorithms,” in *Procedings of Int. Conf. Commun. Signal Process*, pp. 767–770, 2013.

[110] F. Text, “Secure Localized Node Positioning in Mobile Ad-Hoc Networks Using PSO,” in *Procedings of World Congress on Computing and Communication Technologies*, pp. 1–2, 2014.

[111] X. Wang, T. Lin, J. S. Wong, X. Wang, T. Lin, and J. Wong, “Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network,” *Computer Science Technical Reports IOWA State University*, pp. 1–10, 2005.

[112] M. Xie and M. Haenggi, “Towards An End-to-end Delay Analysis Of Wireless Multihop Networks,” *J. Ad Hoc Networks*, vol. 7(5), pp. 849–861, 2009.

[113] Y. Lu, Y. Zhong, and B. Bhargava, “Packet Loss in Mobile Ad Hoc Networks,” in *Department of Computer Science Technical Reports (Purdue University)*, pp. 1–8, 2003.

[114] Y. Yang and R. Kravets, “Throughput Guarantees for Multi-priority Traffic in Ad Hoc Networks,” *Ad Hoc Networks*, vol. 5(2), pp. 228–253, 2007.

[115] P. C. Ng and S. C. Liew, “Throughput Analysis of IEEE802. 11 Multi-hop Ad Hoc Networks,” *IEEE/ACM Trans. Networks*, vol. 15(2), pp. 309–322, 2007.

[116] X. Zhang, Z. H. Qian, Y. Q. Guo, and X. Wang, "An Efficient Hop Count Routing Protocol for Wireless Ad Hoc Networks," *Int. J. Autom. Comput.*, vol. 11(1), pp. 93–99, 2014.

[117] M. Elshaikh, O. B. Lynn, M. Nazri, P. L. Ehkan, and F. F. Zakaria, "SNR-Based Dynamic Manet On Demand Routing Protocol For Vanet Networks," *ARPN Journal of Engineering and Applied Sciences*, vol. 10(2), pp. 1099–1105, 2015.

[118] F. Alnajjar, "SNR / RP Aware Routing Model for MANETs," *Journal of Selected Areas in Telecommunications (JSAT)*, pp. 40–48, 2011.

[119] R. Ali and F. Zafar, "Bandwidth Estimation in Mobile Ad-hoc Network (MANET)," *JCSI International Journal of Computer Science Issues*, pp. 331–337, 2011.

[120] A. Christy, "Classification of Intrusion Detection Into True Positive , False Positive and False Negative by Probabilistic Approach," *Indian Journal of Research*, pp. 221–224, 2015.

[121] H. W. Ferng and C. L. Liu, "Design of a Joint Defense System for Mobile Ad Hoc Networks," in *Proceedings of IEEE* 63^{rd} *Veh. Technol. Conf.*, vol. 1(6), pp. 742–746, 2006.

[122] A. ur Rehman Khan, S. M. Bilal, and M. Othman, "A Performance Comparison of Open Source Network Simulators for Wireless Networks," in *Proceedings of IEEE Int. Conf. Control Syst. Comput. Eng*, pp. 34–38, 2012.

[123] A. Kaponias, A. Politis, and C. Hilas, "Simulation and Evaluation of MANET Routing Protocols for Educational Purposes," in *Proceedings of Pan-Hellenic Conference on Electronics and Telecommunications (PACET)*, pp. 2–5, 2012.

[124] M. Izharul, H. Ansari, S. P. Singh, and M. N. Doja, "Effect of Transmission Range on Ad Hoc on Demand Distance Vector Routing Protocol," *Journal of Computer and Communications*, vol. 4, pp. 34–46, 2016.

Publications

Patent

1. Bhushan S. Chaudhari, Rajesh S. Prasad, ”Design and Development of Evolving Intrusion Detection System for Mobile Ad-Hoc Networks Using Particle Swarm Optimization”, Patent Reference No: 3716/MUM/2015 Date: 30/09/2015 Published on 31/03/2017, Available online at (Page 597):
   http://www.ipindia.nic.in/writereaddata/Portal/IPOJournal/1 454 1/Part-1.pdf

Copyright

1. Bhushan S. Chaudhari, Rajesh S. Prasad, ”Particle Swarm Optimization: An Evolving Routing Protocol in Mobile Ad-Hoc Networks”, Diary Number: 10637/2016-CO/L, Date: 13/09/2016, Granted on 08/06/2017

Journal Papers

1. Bhushan Chaudhari, Rajesh Prasad, ”A Novel Approach for Intrusion Detection in Mobile Ad-hoc Networks”, International Journal of Networking and Virtual Organizations (IJNVO) (Paper Accepted on 09/10/2017). The paper is listed as forthcoming article at:
   http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=IJNVO

2. Bhushan Chaudhari, Rajesh Prasad, Performance Analysis of Particle Swarm Optimization and Dynamic Source Routing for Packet Route Optimization in Mobile Ad-Hoc Networks, Communicated to Journal of Networking and Virtual Organizations (IJNVO), (communicated on 20/02/2018).

Conference Papers

1. Bhushan S. Chaudhari, Dr. Rajesh S. Prasad, ”Particle Swarm Optimization Based Intrusion Detection for Mobile Ad-hoc Network”, Proceedings of International Conference on Advances in Information Science and Computer Engineering, WSEAS, Dubai, February 2015, ISBN: 978-1-61804-276-7, pp-477-482

2. Bhushan S. Chaudhari, Dr. Rajesh S. Prasad, ”Particle Swarm Optimization Based Evolutionary Computation”, Proceedings of International Conference on Internet of Thing, Next Generation Networks and Cloud Computing 2016 Pune, February 2016,
DOI: http://dx.doi.org/10.18797/caasr/2ndiciet/iccse/2016/05/05/20

Grant Fetched

1. Science and Engineering Research Board (SERB), Department of Science and Technology, Government of India sanctioned 100% International Travel and Registration grant for participating in CAASR International Conference on Innovative Engineering and Technologies (CAASR-ICIET16) held on 05/05/2016 and 06/05/2016 in Kuala Lumpur, Malaysia