PROPOSE A SECURE FRAMEWORK FOR ISOLATING VARIOUS TYPES OF ATTACKS IN MOBILE AD HOC NETWORKS USING INTRUSION DETECTION SYSTEM

A Thesis

Submitted in partial fulfillment of the

Requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

IN

(Computer Science and Engineering)

By

Pooja Rani

(41300132)

Supervised By:

Dr.Kavita

Transforming Education Transforming India

LOVELY PROFESSIONAL UNIVERSITY

PUNJAB

2020

CERTIFICATE

I hereby certify that the work which is being presented in the thesis, entitled "**Propose a secure framework for isolating various types of attacks in mobile ad hoc networks using intrusion detection system**" in fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science & Engineering and submitted in **Lovely Professional University,** Jalandhar is an authentic record of my work carried out during a period from August 2013 to May 2020 under the supervision of Dr.Kavita.

The matter embodied in this thesis has not been submitted by me for the award of any other degree of this or any other University/Institute.

(Pooja Rani)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

(Dr. Kavita)
(Supervisor)

DECLARATION BY THE CANDIDATE

I the undersigned solemnly declare that the thesis report "**Propose A Secure Framework for Isolating Various Types Of Attacks In Mobile Ad Hoc Networks Using Intrusion Detection System**" is based on my work carried out during our study under the supervision of **Dr. Kavita.** I assert the statements made and conclusions are drawn are an outcome of my research work. I further certify that

I. The work contained in the report is original and has been done by me under the supervision of my supervisor.

II. The work has not been submitted to any other Institution for any other degree/diploma/certificate in this university or the any other University of India or abroad.

III. We have followed the guidelines provided by the university in writing the report.

Pooja Rani

Name: Pooja Rani

Reg. No.:41300132

ABSTRACT

MANET stands for "Mobile Ad Hoc Network". It is an itself-governing scheme of portable nodes that are linked by radio links. The behavior of the node is likely to route and both source along with the destination node to pass data inside the system. The movement of nodes are freely and maintain their position itself in the network.

The nodes are considered as a kind of ad-hoc network and changed their position frequently and interconnected with each other through wireless links. Therefore, to transfer data in such a dynamic scenario of MANET, routing algorithms are required. There are many routing protocols developed each used as per the network conditions. The selection of routing protocol has to be performed based on the network properties like density, size, nodes mobility, and, many more. The researcher is continuing on MANET and the scholars aim to designed better protocols by following different strategies and approaches. Presently, this research aims is to design a secure MANET against three different network attacks such as (i) Black Hole Attack (BHA), (ii) gray Hole Attack (GHA), and (iii) Selective packet Drop attack. The entire work is mainly categorized among four specified sub-sections named (i) Deployment of nodes, (ii) Route Creation using AODV, (iii) Optimization of the route through ABC, and (iv) Threat detection using classifiers such as SVM and ANN. Using AODV, a route is formed from source to target node. Based on the optimized features classifiers SVM using different kernel functions and ANN is trained. So, that if any node appears having the threat like properties is detected and the direction of the route is diverted through the other normal node. At last, the work performance of a designed secure network is analyzed for energy consumption, packet delivery ratio (PDR), Delay, and throughput. It has to be cleared from the examined outcome of the presented protocol performs better in contrast to the existing work under an above-defined- attack condition.

ACKNOWLEDGMENT

First and foremost, I would like to express my appreciation and thanks to my supervisor Dr. Kavita, Assistant Professor, LPU, Punjab. She has been a tremendous mentor for me. I am honoured to pursue my Ph.D. under her guidance. I would like to thank her for his encouragement and for allowing me to grow as a research scientist. I appreciate all her contributions of time and ideas to make my Ph.D. experience productive and stimulating.

I would like to express my special appreciation to Dr. Sahil, Assistant Professor, LPU, Punjab. His advice on both the research as well as on my career has been priceless.

I would like to mention a special thanks to my family. I am grateful to my mother, father, my mother-in-law for all their sacrifices. Their prayer for me was what sustained me thus far. I would also like to thank my brother and my friends who continuously supported me and incanted me to achieve my goal. In the end, I would like to express my hearty appreciation to my beloved husband Mr. Pankaj Sharma who has spent numerous sleepless nights and has always been my support even when there was nobody to answer my doubts.

I am also thankful to my colleagues at Rayat-Bahra University, Mohali Campus for their untiring devotion and dedication to mould me into a better human and achieve something which I would not be able to do without their enthusiasm and teachings.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ABC	Artificial Bee Colony
ACO	Ant Colony Optimization
AI	Artificial Intelligence
AJ	Adaptive Judgment
ANN	Artificial Neural Network
BA	Bat Algorithm
BBO	Biogeography Based Optimization
CBR	Cased Based Reasoning
CS	Cuckoo Search
DE	Differential Evolution
AODV	Ad Hoc On-Demand Distance Vector Routing
ML	Machine Learning
FA	Firefly Algorithm
GA	Genetic Algorithm
SVM	Support Vector Machine
PDR	Packet Delievery Ratio
PSO	Particle Swarm Intelligence
SI	Swarm Intelligence
MANET	Mobile Adhoc Network

CHAPTER 1: INTRODUCTION

1.1MANET

MANET (Mobile Ad-hoc Network) is an ad-hoc network, a combination of mobile wireless nodes. The interchange of information is carried out without the requirement of centralized control. Other routing protocols may not have actual-time communications, and they depend upon the requirement and condition. MANET is considered a combination of mobile devices, truly wireless nodes that coordinated and instinctive for the creation of an IP-Based network. This network is not dependent on any type of fixed infrastructure or centralized system.MANET is considered as an uninterrupted, self-directed network of wired and connected through mobile devices. MANETs posses an infrastructure of the network which is flat. It has a method of radio communication that is demanding from one another. Each mobility system or node in the MANET architecture means any device that functions as a router, as well as an end host. Usually, MANET concept nodes or modules are decentralized. MANET has an environment of dynamic topology that significantly promotes mobility.

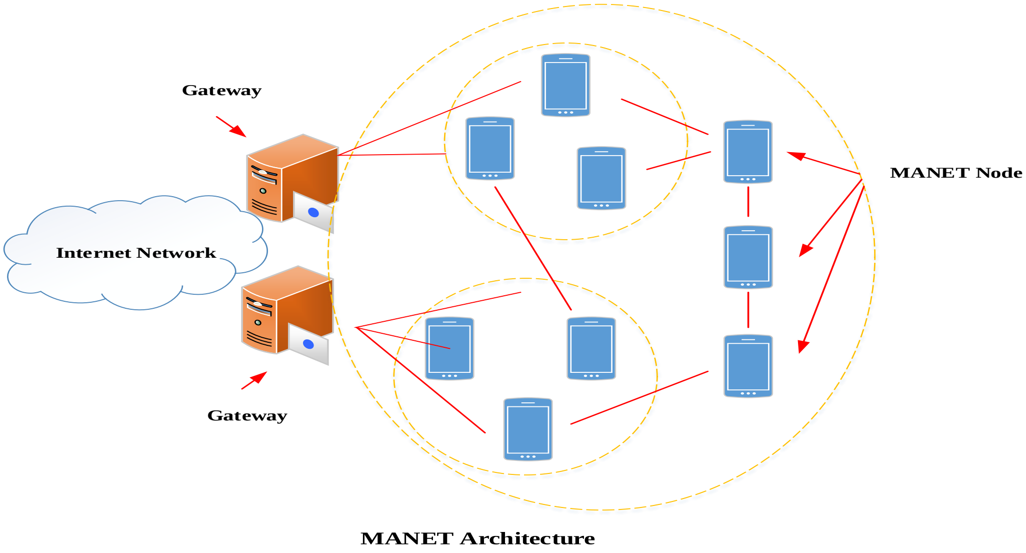


Figure 1.1 Architecture of MANET

1.1.1 Feature of MANET

Essential features of MANETS given below:

1. **Infrastructure less nature -** For a specific purpose, MANET facilitates to communicate among individual peer-to-peer endpoints interactions with different nodes. There is no previous base system or organization; the same function performs on all devices in the network. There are no predetermined roles, like routers or gateways, because the anodes of the network are offered; the system can behave as a router as well as nodes simultaneously.
2. **Dynamic Topology -** There's free to move nodes everywhere, gradually moving in as well as out of the network, adjusting the connections and topology continuously. Conversely, bidirectional or one-way interactions among knots can exist. However, this interest induces a high degree of application volume and versatility of the devices.
3. **Bandwidth Constraints and Variable Link Capacity -** Wireless connection, which connects the bandwidth to MANET nodes much lower than cables. Depending on the effects of numerous access privileges, loss of multipath, vibration, distortion, fluctuation, and signal disruption, the effectiveness of a wireless network may be reduced considerably, including effective communication could be lower than the peak transmission power of the radio.
4. **Multi-Hop Communication -** MANETs require multi-hop connectivity assistance owing to wireless transceiver signal amplification functionality. For a message's both the nodes i.e., origin along with target is not lie in radio range, MANETs can multi-hop routing to cellular nodes that can not reach the target node. Because of the restricted transmission range, a message moves through node from origin to target over various processors. The node behaves like a router to transfers packets to different nodes by which enable multi-hop communication.
5. **Constrained Resources (Light-Weight Terminals)** -The majority of MANET products are small handheld devices, from smartphones to notebooks. Such

devices have limited energy, i.e., battery activity, processing, and storage capacities.

6. **Restricted physical Security -** Just because of the wireless links rendered MANET highly vulnerable to attacks on physical layer hackers, including eavesdroppers, jamming, spoofing as well as Denial of Service (DoS). MANET's distributed nature helps them to be adequately protected against performance degradation. However, wireless networks are, in other aspects, quite vulnerable to attacks, unlike infrastructure networks.
7. **Short Range Connectivity -** MANET is centered on a communication infrastructure with radio frequency (RF) or may be infrared (IR); both of them are mostly used short-range communication networks. The nodes that would like to communicate directly, therefore, requires to be adjacent to one another.

1.1.2 Structure of MANET

MANET comprises of portable hosts furnished with cordless phones. Because of the communication idea of remote correspondence and the Omni-directional receiving wires, all hosts get the transmission of a convenient host inside its transmission run. Sometimes, the two remote has in the systems that are outside their scope of transmission, distinctive system gadgets in the middle of can send their messages, adequately assembling associated arranges between the versatile has in the conveyed zone. The phone host will generally move and can be turned on or off without notifying another host. Mobility, as well as autonomy, explore a transmission power of the networks not only due to the existence of the end-hosts is transient but because of the intermediate host of the route on a connection is short-term.

The structure of MANET is represented in figure 1.2. Specifically, it can be categorized into three sub-parts as pointed

1. Enabling Technologies

2. Networking

3. Middleware & Application

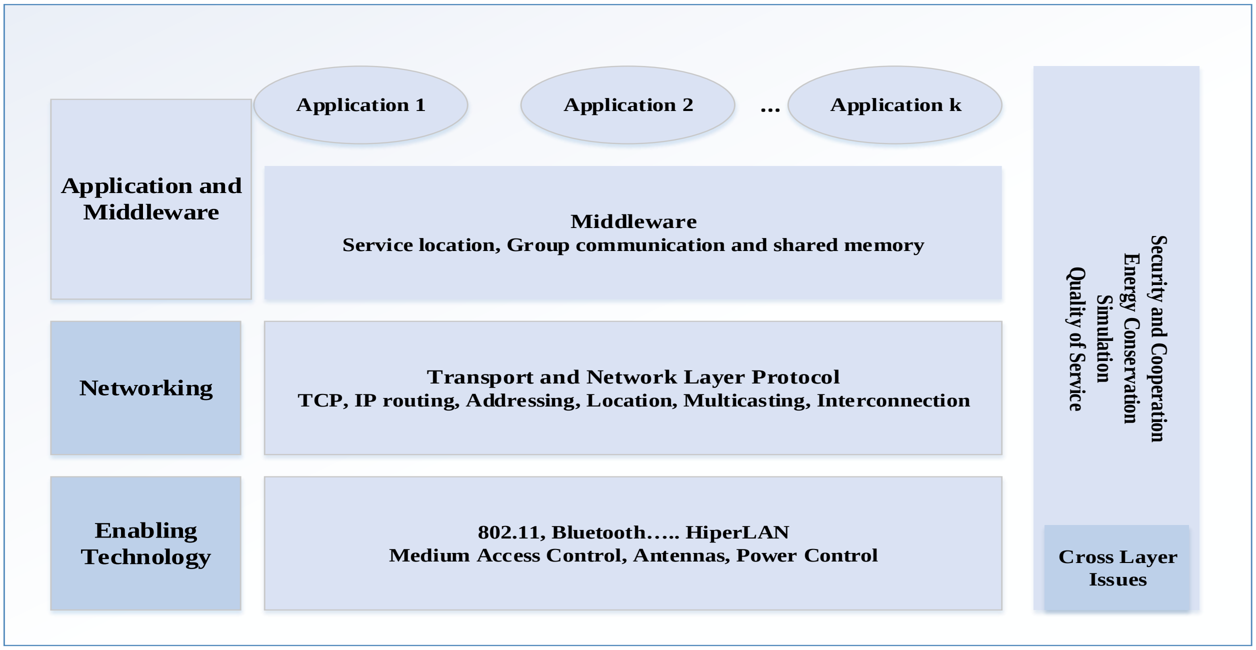

Application 1
Application 2
...
Application k
Application and Middleware
Middleware
Service location, Group communication and shared memory
Networking
Transport and Network Layer Protocol
TCP, IP routing, Addressing, Location, Multicasting, Interconnection
Enabling Technology
802.11, Bluetooth….. HiperLAN
Medium Access Control, Antennas, Power Control
Security and Cooperation
Energy Conservation
Simulation
Quality of Service
Cross Layer Issues

Figure 1.2 Structure of MANET

1. Enabling Technologies: Enabling technologies are also characterized by various classes dependent on the scope of system region.

(a) BAN (Body Area Network): In BAN, the network area is too small and about 1 to 2 meters connectivity area. The general purpose of the BAN to connect the wearable computer topology such keyboard, mouse, and other wired devices having short in range.

(b) PAN (Personal Area Network): PAN is like the BAN; however, the fundamental distinction is about the network territory. The network area of the PAN is about 10 to 12 meter and provide the intercommunication among the mobile devices and other stationary devices.

(c) WLAN (Wireless Local Area Network): The significant difference between the WLAN and different is the communication range, and it is about 100 - 500 in meters. The single or multiple buildings are connected by WLAN.

2. Networking: Most of the networking protocol's core functionalities require to be revamped to make it a self-configured, complex, insecure, peer-to-peer(P2P) communications system in MANET architecture. To utilize the one-hop communication is the initial goal of networking protocols that facilities from a recipient to the receiver, enabled by allowing technology to establish efficient end-to-end networks. A positioning service's main task is to automatically link the receiver device's address to its current network position.

3. Middleware & Application: Remote frameworks, for example, Ethernet, Bluetooth, IEEE 802.11, WiMAX, and Hyper LAN, are supporting the presentation of specially appointed procedures and novel impromptu systems administration arrangements explicitly for specific territories, crisis administrations, catastrophe recuperation, and ecological checking. MANET's effortlessness permits this innovation perfect for certain pragmatic circumstances, for example, PAN, home systems administration, law implementation, business and scholastic gadgets, and sensor organize. As of late made portable specially appointed frameworks follow the methodology of not giving a middleware however, rely upon each solicitation to deal with all the assets it needs.

1.1.3 Types of MANET’s

MANET is categorized among three basic categories, such as VANET iMANET, and In VANET elaborated below.

1.1.3.1 Vehicular Ad Hoc Networks (VANET)

Specially appointed Ad-hoc Vehicle Network (VANET), is comes under the kind of MANET. VANET is a specific, especially ad-hoc remote system class with solid hub adaptability abilities and quick topology changes. It is used for rounded communication with remote vehicles. Therefore, contact is carried out even if the car is traveling in different directions in a particular region.

1.1.3.2 Internet-Based Mobile Ad- Hoc network (iMANET)

Customary ad hoc algorithms don't make a difference straightforwardly in such kind of system. Mobile ad-hoc networks concentrated on the Internet, which associates portable hubs with fixed web entryway hubs. Such types of systems are most appropriate for conditions where there is no settled framework or where one system can't be actualized.

1.1.3.3 Intelligent Vehicular Ad- Hoc Network (In VANET)

VANET used in a situation where vehicle collisions or other mobility issues arise. This ad-hoc network is part of artificial intelligence (AI) that lets cars act smartly when vehicle-to-vehicle crashes, injuries, drunken driving, and other technical problems occur. This describes a smart approach to the use of vehicle networking. VANET incorporates various techniques of ad-hoc network named as Wi-Fi IEEE 802.11, WAVE IEEE 1609, WiMAX, and Bluetooth to promote, reliable, secure, and convenient connectivity between capable mobility vehicles.

1.1.4 Challenges and issues in MANET

As of late MANET turns into over the previous scarcely any years, MANETs have been a famous field of investigation. About each component of the system has been learned at particular issue levels in some way. The MANET's most noteworthy difficulties and most recent analysis patterns are discussed beneath

1. **Limited Bandwidth** – As the increase in the connecting tropology, the use of bandwidth increases rapidly, which affects the availability of bandwidth. Wireless connectivity continues to be substantially smaller than the infrastructure system. As per the restricted bandwidth, rapid communication, and error-free communication can be intruded on by the network.

2. **Routing** – For network topology, routing is an essential viewpoint point because routing protocols is a key issue in this field since shifts to network topology frequently arise.
3. **Time-varying nature of wireless links -** Multiple variables hinder the efficiency of wireless transmission. Communication impediments, such as fading, path interruption, blockage, and noise, lead to the reactive actions of wireless networks.
4. **Route challenge due to Mobility –** Due to rapid movement of the node in the network, path break is regularly occurring. MANET is due to its dynamical behavior becomes challenging to handle to discover the route and transmission of the packet.
5. **Dynamic topology** - Complex topology membership will interrupt the interconnection of confidence between nodes. Confidence may also be disrupted if it is discovered that certain nodes are affected.
6. **Packet losses because of transmission errors –** Ad hoc wireless systems lose packets significantly more due to the elements, for example, expanded clashes because of the nearness of mystery terminals, blockage, single direction connects, and visit nodes to nodes.
7. **Hidden Terminal problem -** The concealed terminal difficulty involves a packet breakdown at the receiving node because of the synchronous transmission of the hubs, which are not inside the recipient 's prompt transmission go; however, the receiver range to transmit.
8. **Security threats –** MANETs ' ad hoc wireless phone structure raises new safety issues in the network design. Since the wireless media is vulnerable to auditing, and the ad hoc network infrastructure is built by node coordination, remote ad hoc networks are essentially exposed to endless safety assaults.
9. **Fault tolerance -** MANET's this issue involves the identification and repair of faults once networks have collapsed. Fault sensitivity strategies are incorporated

for survival when node shift, mixture, or network divergence arises when a failure occurs.

1.1.5 Routing in MANET

A routing protocol is characterized as the arrangement of decides that causes the parcels to transmit from source to goal inside the system

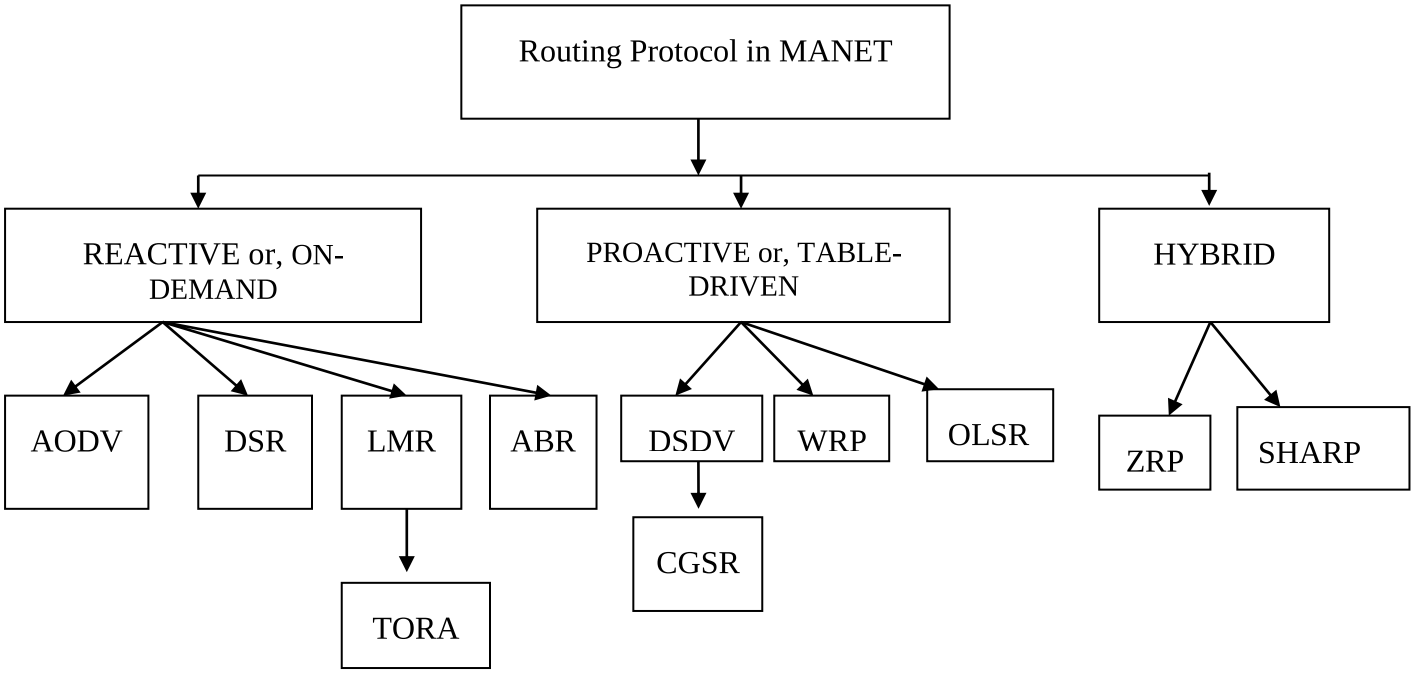


Figure 1.3 Routing protocols

Several routing protocols are used in MANET that is applicable as per the different circumstances. The most commonly used protocols are listed in figure 1.3 above.

1.1.6 Proactive Routing Protocol

This type of protocol is also sound, as a table-driven routing protocol is constructive routing protocols. This protocol retains a routing table where the network topology data is found in all nodes inside the system. Thus, the table for routing will be updated correctly whenever the system topology shifts. With full nodes, constructive protocols are not appropriate because they update the complete entry of nodes in the network. A number of constructive protocols, named as DSDV, OLSR, and WRP, is used in the MANET.

1.1.6.1 Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)

The destination-sequenced distance vector (DSDV) protocol is a table-driven routing protocol on the basis of the original Bellman-Ford routing algorithm's modified version. DSDV relies on routing information protocol that is abbreviated as RIP. Using RIP, individual nodes in the network hold the required routing table information, including the number of hopes to every target node. DSDV has a bi-directional link and based on distance vector routing. There is a various disadvantage of the DSDV routing mechanism is that it provides a single route for the packets for transferred from initial to target node.

i. Routing Tables

For the DSDV protocol, the routing table is feasible. Each table section created a succession number, which builds each time a hub moves a refreshed message. Routing tables are consistently refreshed, dependent on changes in MANET topology, and move over the system to hold uniform data over the structure.DSDV node maintains two routing tables: one is utilized to forward packets, and the other to increase routing packets. The routing information was consistently transmitted by means of a hub. It conveyed an inventive arrangement number, the location of the goal, the number of hops to the goal hub, and the succession number of destinations. An identification hub moves an update packet to the closest hubs while changing the system topology. Endless supply of an update packet from a neighboring hub, the hub gets the parcel data and updates its routing table as follows:

a) As the recent location involves a top sequential number like the old sequential number in the hub, at that point, the hub chooses the course with a higher sequential number.
b) On the off chance that, if the approaching succession number of route id is like the past course, the course with least expense is trailed by the hub

c) The routing table is increased by 1 after transferring the information.

This procedure is rehashed until all the hubs in the system are refreshed.

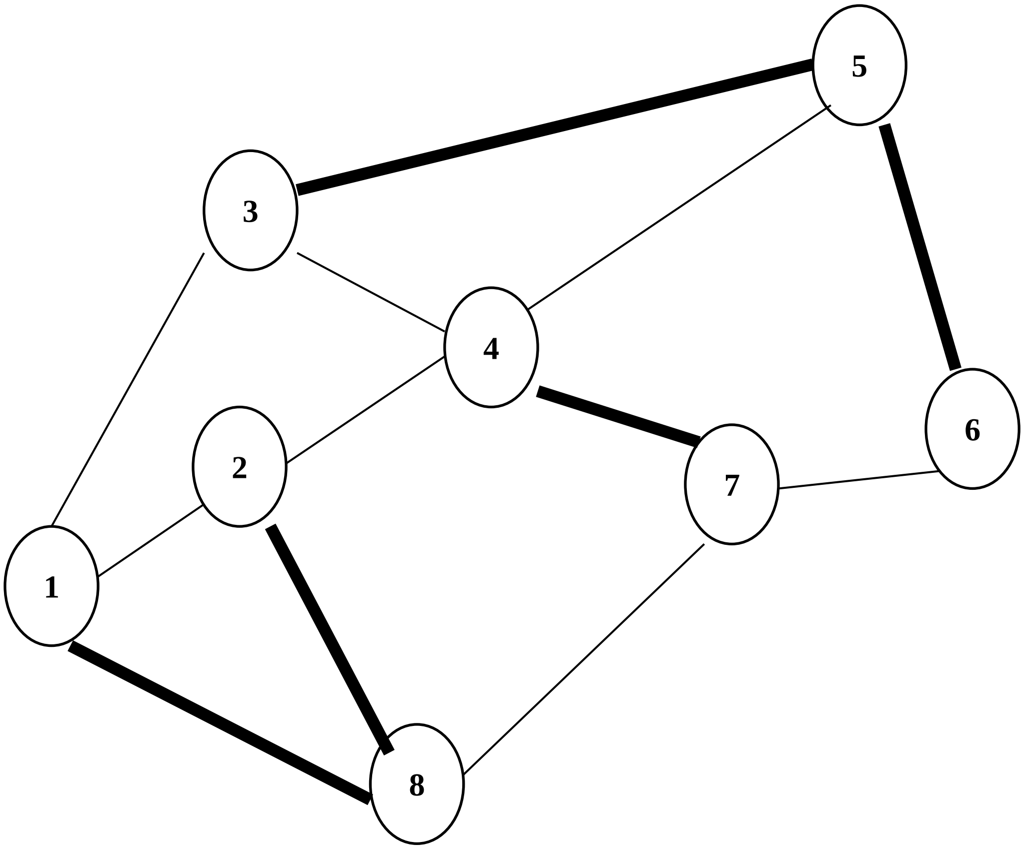


Figure 1.4 DSDV routing protocol

As depicted in figure 1.4, relates to hub 2 the contiguous nodes are 1, 8, 4, and 3. There is no connection to impart among pairs of hubs is demonstrated by the dark black line. So it tends to say that node 2 doesn't include any data about node 8

1.1.6.2 Wireless Routing Protocol (WRP)

This routing protocol is a table-based that keeps up to convey messages on all the hubs in the system. This convention is additionally founded on a Bellman-Ford disseminated calculation, like the DSDV routing protocol. The advantage of the WRP convention is that the quantity of steering circles decays just as the directing convention needs to hold four tables referenced beneath.

i. A distance table: Address of destination, separation, next bounce, and ancestors of every goal and each neighbor is held by this table
ii. Routing table: It keeps the location of the destination, subsequent hop, distance, predecessor, alongside a name relates to each target hub, characterizing whether that section looks like a straightforward way
iii. Link-cost table: It produces the cost of the connection to every area, just as the measure of occasional updates in light of the fact that the hub acknowledged any error-free message
iv. Message transmission list table: It is taking care of the updated message that has to be retransmitted and which needs acknowledgment. The sequence number, along with the counter of the updated message, is stored in the table. Whenever the link changes in the network, nodes inform each other by using the updated message.

In the event that a hub doesn't transmit any message, it must need to send a "HELLO" message inside a constrained time-interval to guarantee their availability inside the system when the neighboring hub gets a HELLO message, that hub is added to the routing table. This procedure overcomes the issue of count to Infinity that has happened in the DSDV routing protocol. The drawback of the WRP routing protocol is that it needs four tables that involve a lot of memory space, and continuously sending HELLO messages consumes bandwidth and power.

1.1.6.3 Cluster Head Gateway Switch Routing Protocol (CGSR)

The CGSR is a table-driven routing protocol. The CGSR routing protocol uses the routing scheme of DSDV. CGSR uses the concept of Clusters and cluster heads, and routing is done through cluster head and gateways. Vehicular Ad Hoc Networks is a unique wireless ad-hoc network class with elevated node mobility features and rapid topology adjustments. It is used for mobile vehicle-rounded communications.

Communication is therefore carried out even if the car passes in a particular region in distinct directions.

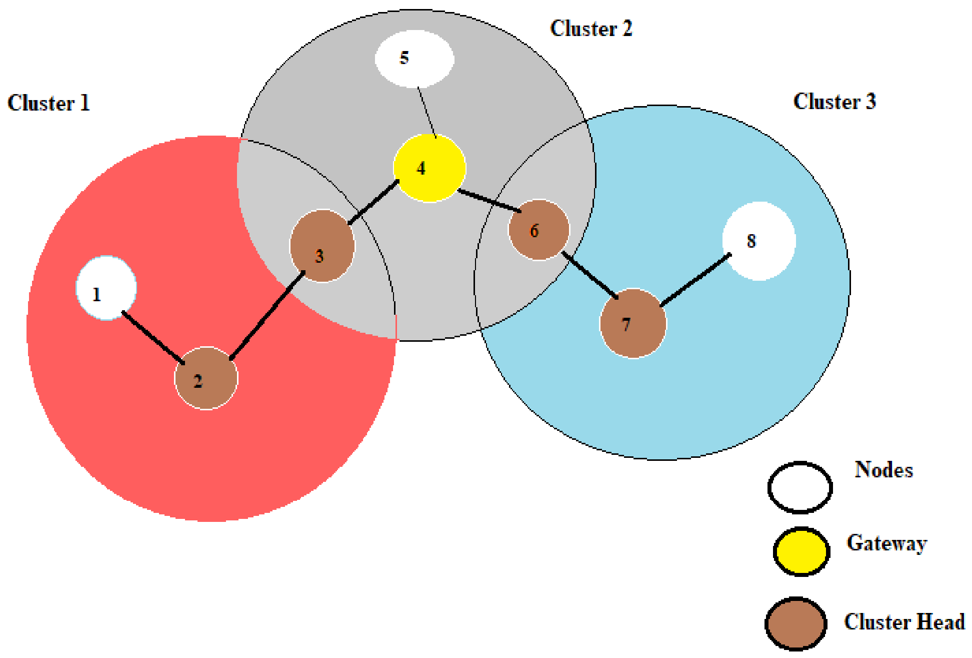


Figure 1.5 An example of CGSR

The packet that has been transmitted from the source is routed first to its cluster head and afterward through the entryway to another cluster head, etc. This procedure is rehashed until the packets are reached as the target node. A case of CGSR routing protocol is demonstrated as follows:

i. Cluster Head: It is a node within the cluster that helps to transmit the packet to gateways, and it is elected dynamically.

ii. Gateway: The node that is situated inside the range of at least two cluster heads is known as Gateway.

CGSR utilized bandwidth in better ways and also decreases the distance vector table size because the routing is done over the cluster heads. Due to the node of one cluster head are started to travel then onto the next cluster head so it may be talked regarding numerous way breaks. For the choice of the cluster head, it requires additional time.

1.1.6.4 Optimized Link State Routing (OLSR)

It is a proactive routing protocol worked by a table. It permits the connection state technique pertinent to the scattering of topology data. OLSR is the directing convention that conveys HELLO messages to recover the associations. It knows all the network nodes, along with the routing, is focused on the flooding algorithm. This requires no discovery of packets. As it is an OLSR protocol, larger bandwidth along with CPU power, is needed by it.

Here the three essential types of control messages such as HELLO, TC, including MID used by OLSR.

i. HELLO –"HELLO" messages are sent among all neighbors. This information is used to track the neighbor button and MPR computation.

ii. TC - Topology Control messages are the switch status signals done by OLSR. These messages are optimized in various ways using MPRs.

iii. MID -Several interface statement messages are forwarded by nodes carrying OLSR on more than one interface. These messages contain a list of each IP address used by a node.

1.1.7 Reactive Routing Protocol

A dynamic routing protocol is additionally called an on-demand routing protocol. At the point when hubs need the way to send information just, at that point, the course will be found in the responsive routing protocol. A bearing is found through the root hub that starts a pattern of route investigation. The routing protocol is made up basically of two segments called route discovery and route maintenance.

i. Route discovery

The Discovery of the route is the way toward finding the most limited and most secure route dependent on the requirement for the topology of the system. Connection hubs search their routes in the memory of the store on the off chance that it is accessible, at that point, follow the route, and in the event that there is no route discovered, at that point, they find the path utilizing the procedure of route discovery. Packets of knowledge messages sent from origin to goal providing detailed information about the destination node with intermediary nodes from which to fly.

ii. Route maintenance

In the routing protocol scheme, if the association breaks, the security of the route is a significant feature. Connection parts because of the topology utilized in the system's dynamic nature. Keeps up the breakdown way with the guide of the recognition framework responsive methodology. In MANET, some notable receptive directing conventions, for example, DSR, AODV, TORA, and LMR, are restricted.

1.1.7.1 Ad Hoc On-Demand Distance Vector Routing (AODV)

The communication protocols in remote frameworks are creating. The protocol named AODV as on-demand routing protocol/reactive protocol as an association of DSDV just as DSR. A similar method of DSR computes the path in AODV with the procedure of route discovery. AODV maintains the table for routing information in which one entry per destination, but DSR has several entries of route cache for every goal. Pure AODV has traditional routing tables and a succession number of destinations for the identification of a new route from the destination, including the generation of routing loops. To maintain the route, three kinds of control messages are composed by AODV as listed below:

- RREQ(Route Request)
- RREP(Route Reply)
- RRER(Route Error Message)

While passing the RREQ, the intermediate nodes register their routing tables at the location of neighbors from which the initial copy of the communicating packets was gotten, in this way, making an opposite way. It also possible that extra duplicates of the equivalent RREQ are gotten later; these packets will be kept away from. When RREQ arrives at the goal or a moderate node with a new enough course, the goal/middle hub reacts by sending an RREP to the neighbors from where it previously got the RREQ figure.

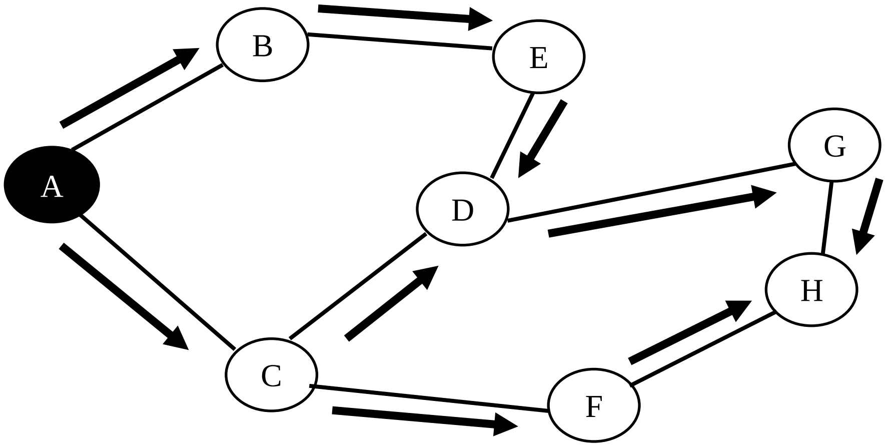


Figure 1.6 RREQ broadcast

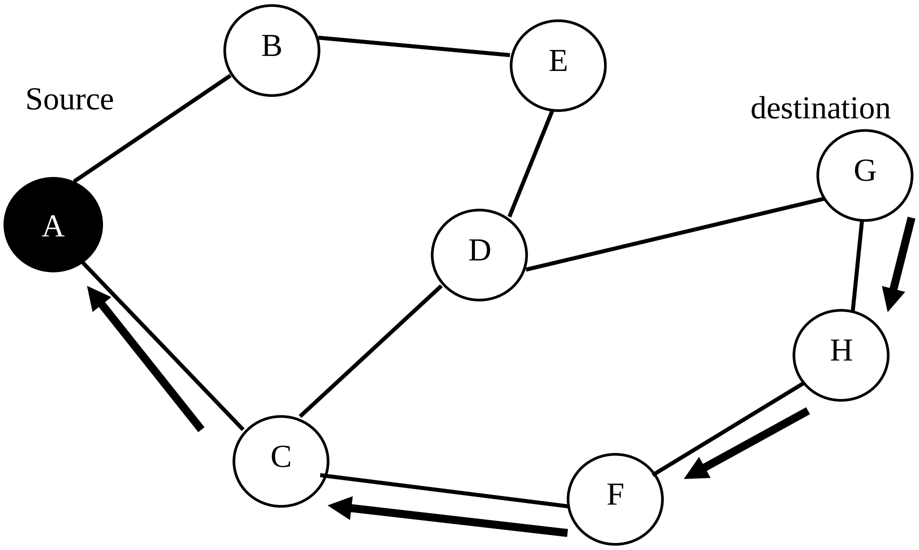


Figure 1.7 RREP propagation route

1.1.7.2 Dynamic Source Routing (DSR)

This works in two phases, named investigation of the way and safeguarding of the street. Transmitter sends away demand parcel to the closest hub during the discovery of route. The goal hub admires the way reserve for discovering from source to goal about the previously existing route. If the route cache includes the destination address, then delete another path reaction. Route answer is produced while in the case of the middle hub or the goal node enters the source packet. The source node picks the briefest way between all the ways it gets. The shortest path between all the paths it gets it has chosen by the source node. When a connection breaks between two nodes, route maintenance is established in DSR. Nearby nodes sensed the breakable connection node, an original node i.e., a route to the error message. The source node can delete the route path held in the cache and will use a different route or request a new route.

1.1.7.3 Light-weight mobile routing (LMR)

The LMR protocol is another on-demand routing mechanism that utilizes a flood methodology to assess the paths. The LMR hubs hold different routes to each desired destination. This improves the proficiency of protocol by expecting nodes to pick the following open way for a specific goal without beginning a route revelation process. The main benefit of LMR is; every hub just holds its neighbors with routing information. This ensures the unnecessary disruptions and cost of overhead to keeping full routes are eliminated. LMR will generate temporary invalid paths, though, which causes unnecessary delays in deciding the right path.

1.1.7.4 Associativity-based routing (ABR)

ABR is another routing mechanism actualized by the source, which uses a question-answer strategy to characterize the path to the required destination. By the by, the plan of the ABR paths depends fundamentally on stability. To pick a safe way, every node has a cooperative tick with its neighbors. The ties with a higher acquainted click are chosen in contrast with the one with a lower cooperative tick. While this may not mean the briefest way to the objective, the ways seem to last more. So, less rebuilding of the route is required, and more capacity for data transmission will be usable. The downside of ABR is that to assess the degree of the associativity of the connections, it requires regular beaconing. The essential for beaconing permits all hubs to stay dynamic at extremely inconvenient times, which can prompt extra power utilization. Another drawback is that it doesn't hold different path or a way archive, that guarantees about elective routes won't be accessible right away. The use of connection loss would entail route exploration. Nonetheless, a targeted path exploration protocol (i.e., LBQ) has been implemented by ABR to some extent, compensated for not having multiple paths.

1.1.8 Hybrid Routing Protocol

This kind of protocol is an exchange off among positive, including reactive protocols. Reactive protocols are not so much exorbitant but rather more idleness, while conservative protocols are progressively costly and less inertness. To address the inadequacies of both proactive along with reactive routing mechanism, the hybrid protocol is required. Its framework is a mixture of both proactive, including reactive routing strategy. This consolidates the reactive protocols on-demand mechanism and the adaptive protocol's table-driven component to diminish network congestion and overhead problems. The hybrid design is fitting for enormous systems with huge quantities of hubs. A broad system is partitioned into an assortment of zones wherein routing is accomplished inside the region utilizing a proactive methodology, and directing is done outside the zone utilizing a reactive approach. There are various hybrid routing mechanism for MANET, as ZRP, SHRP, and so on

1.1.8.1 Zone Routing Protocol (ZRP)

The network is split into areas called intra-zone and inter-zone in state routing protocols. For path seeking and Interzone, a constructive routing protocol is utilized in the Interzone framework. In response to the route appeal, the target node transfers a path answer code. If the road splits, the route will be repaired.

1.1.8.2 Sharp Hybrid Adaptive Routing Protocol (SHARP)

By using this protocol, each node is identified as an active area. A constructive zone is built up through nodes that rely on the region's size. Because of the invisibility of the target in the active region, the reactive protocol is used to locate the path.

As the RREP is redirected back along the back lane, nodes in this direction place their forward path in their route table, referring to the node from which the RREP arrives. The inclusion of the route often deletes routes that do not operate for the lifespan of the specified path. Because RREP is transferred on the RREQ route, AODV allows only the use of symmetric connections.

1.1.9 Types of Attack in MANET

The categorization of assaults could be made based on acts of assault, such as Passive and Active attacks. This categorization is necessary because the intruder will infect the network and interfere with regular contact between the nodes and thus that the overhead in the network. Such attacks that result in congestion or jamming in the network, such as DoS promoting false routing details, etc. The attacks present in the routing protocols are listed, and the consequences are shown in Figure 1.8.

Only because of the handheld existence of wireless communication apps, they are restricted to their use. Often, due to the lack of organized control, the intruder joins the network. This poses security threats such as those posed by wired networks. These include spoofing, passive eavesdropping, DoS, and much more.

i. Active and Passive attack

MANET is more vulnerable to Active Attack, where the network becomes very challenging to stop flow-node messages. Attacks may be both internal and external. The active cyber threats have an impact on network efficiency through foreign sources. It was not possible to transfer data variability in passive attacks in the network. But the passive assault is triggered by the introduction of unauthorized users of network traffic or data collection. The passive intruder once in a while takes steps to disrupt the routing protocol, yet consistently looks to locate the fundamental information from the active information packet. The location of this kind of assault is extremely convoluted on the grounds that it doesn't affect the movement of the system itself.

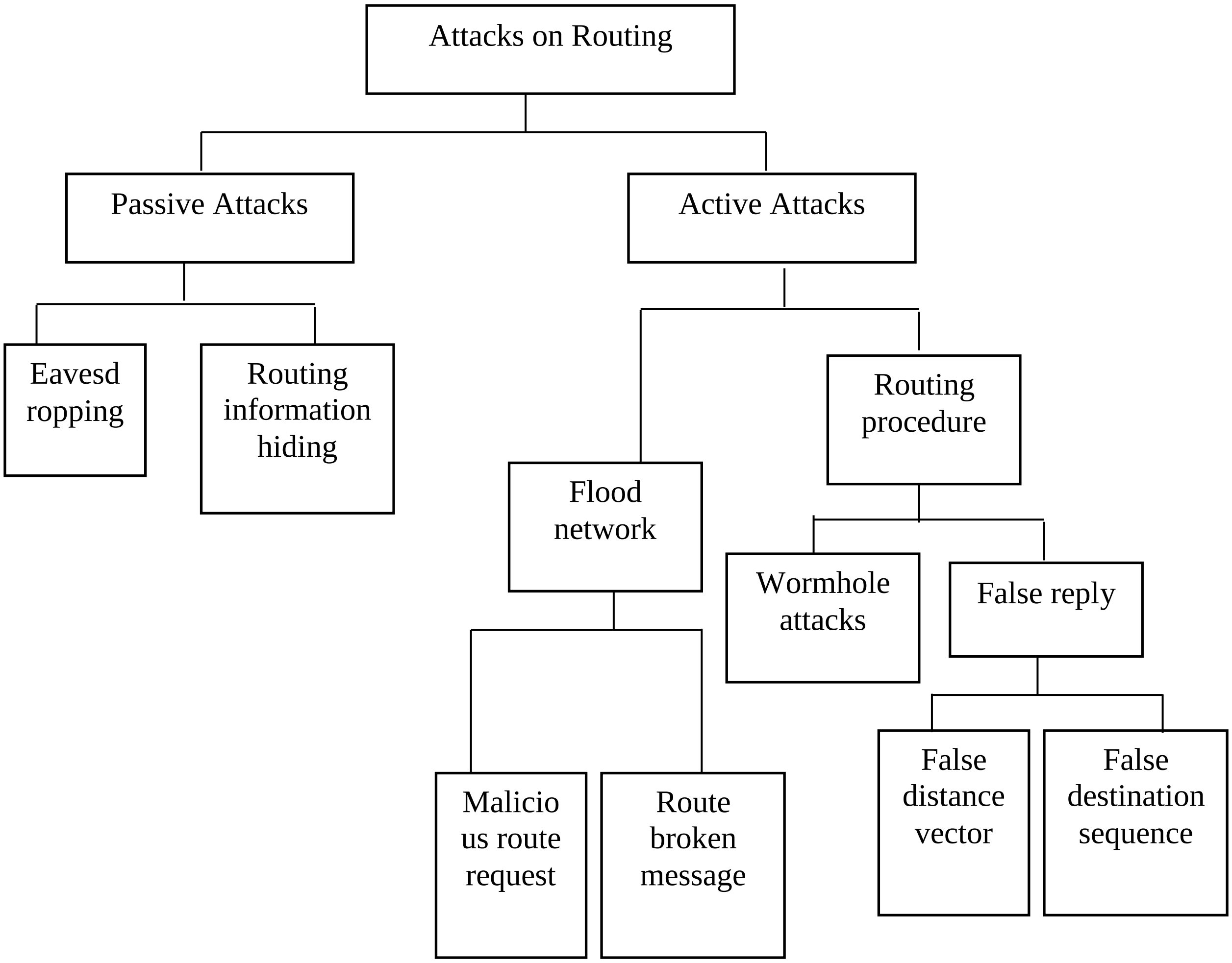


Figure 1.8 Attacks on Routing

ii. Distributed Denial of Service (DDoS) attack

Accordingly, an assault is aimed at preventing legitimate and accepted consumers from the network-based services offered. The DDoS attack can have multiple effects on the network. The typical way is to pass the packets to all network nodes in some consolidated location that resides on the system because the consequence where the network is not working in the manner it is intended to work. It can result in a service interruption for end users that the wired communication network cannot connect. When submitting authentication permission, the server or network host cannot locate the attacker's return address, forcing the server to wait before disconnecting it. When the server disconnects the link, the sender can send further authentic packets with invalid return addresses, as shown in the figure. 1.9.

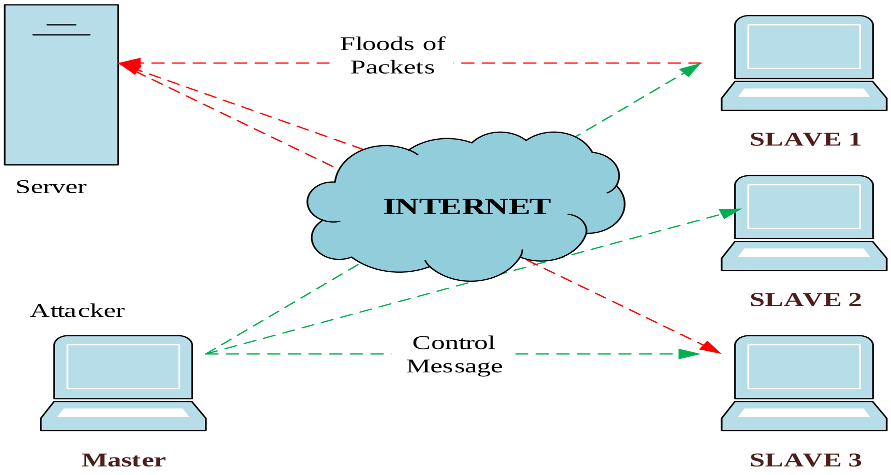


Figure 1.9 DoS Attacks

iii. Blackhole attack

In this sort of attack, one of the routing protocols is esteemed by the malicious node to show that it has the shortest route to the destination or the information that malicious node requirements for the interrupt. This node broadcasts the existence of the latest path in the routing table without checking the direction. According to the black hole attack, the malicious node would always be ready for replying to the routing request, hence catch the packet, and keep it. Some agreements are relied on forwarding the messages; the requested node would acquire the malicious node reply before receiving a response from the genuine node; therefore, the malicious/ fake route is developed. While the direction of the communication path is recognized, it currently depends upon the node whether to discards all packets or forwards them to an unfamiliar address.

Figure 1.10 depicts an instance of a black hole attack in which node 1, as well as node 4, is the source and target node, respectively. Node 3 is the malicious node identified by the red color that responds to the RREQ message sent from the first node. Node 1 discovers the path via node 3 and sends data to node 3 using the route discovery process.

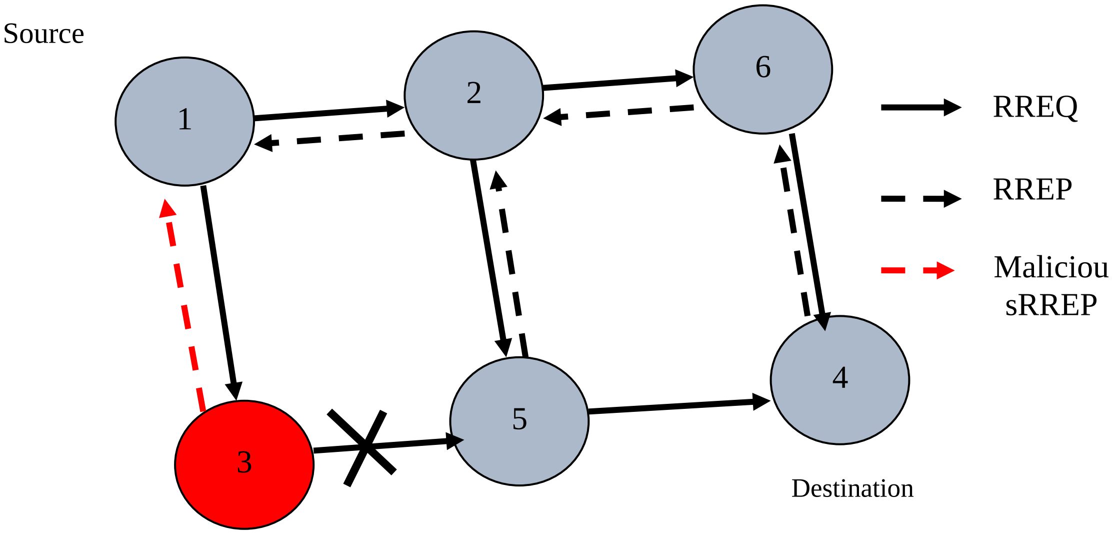


Figure 1.10 Black-Hole Attack

iv. Wormhole attack

They are often classified as wormhole assaults are tunnel threats. During the tunnel attack, the intruder obtains a packet at a single node inside the network and tunnels these packets to another node inside the system and then replays them as the created node inside the system. It is regarded as a tunnel attack when colludes intruder nodes that are attached to a wider variety through a private network.

In Figure 1.11. Node S2, an example of a wormhole assault, is shown, and the target and source node is node S9, respectively. The data is transmitted through a tube. Packets represent the path request sent from the initial node.

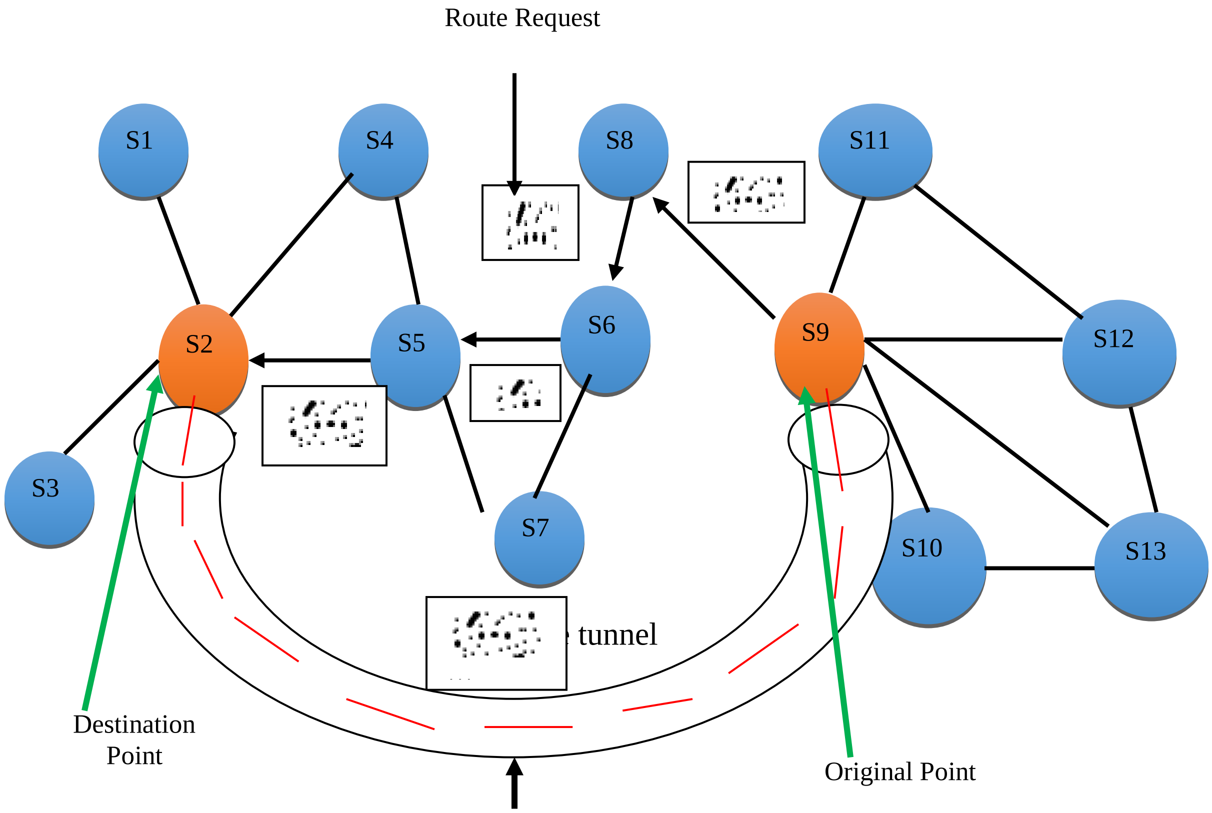


Figure 1.11 Worm Hole attack

1.1.10 Grey hole Attack

Grey hole assault is essentially a Packet Drop Assault, where the node of the Compromised or Grey Hole transmits and monitors the routing packets, but the packets of knowledge are fully lost. This assault is done by ads the wrong way, thus luring the lawful nodes for the establishment of the route through the node of malice.

The gray hole assault may apply through two different ways which are provided underneath;

i. I am dropping all incoming UDP packets.

ii. The incomplete dropping of UDP packets with the arbitrary choice procedure.

Grey-hole is an attack that can turn from a real action to a sinkhole. Because it can act as a regular node update to a malicious node, deciding whether the node is benign or malicious becomes too common.

There are twp phases of gray hole attack is provided below;

Phase 1: Hostile node exploits bugs inside the AODV routing strategy at this point and changes the source routing table as the shortest path in the next-hop board. The primary objective of this update is to redirect all packets instead of actual routes to hostile nodes.

Phase 2: It is the execution stage of the grey-hole assault where the malicious node dropped the disturbed packets with a certain likelihood. A probabilistic approach is used for the distribution of packages. The attacker's node switches actions quickly in ordinary circumstances. So the file will sometimes be passed, and the packets will sometimes be lost, also, in this state, where the malicious node is also pushing any packet forward to build only an honest node imagination. Because of this activity, finding out about this type of attack in the network is very challenging. There are two types of assaults of a grey hole in the MANET, as appeared in Fig.1.12. The first in the grey hole assault chain of importance is a grey hole attack dependent on the arrangement level. Contrasted with the source node, the grey hole node is a data packet, including a greater succession number and a low count of the hop.

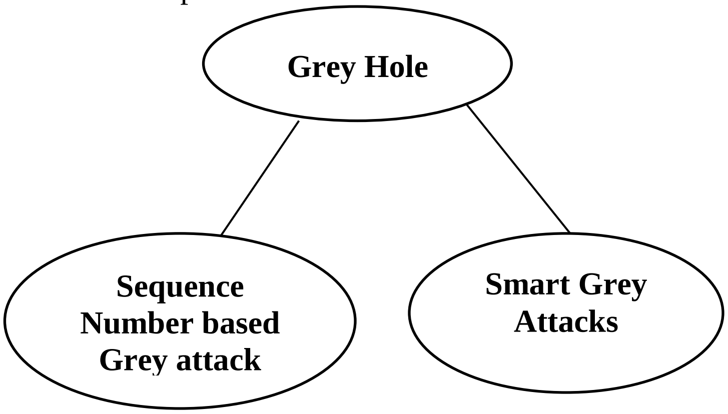


Figure 1.12 Types of Grey Hole attack

It is to be assumed by the source node; it is a legitimate node after receiving the data packet with a large sequence number and transmitting the actual data to the grey hole node and thus dropping the package.

This type of attacker node extracts the features of the genuine node and behaves like a normal node. Inside the system, grey-hole nodes work uncertain, so it's elusive this kind of assault as opposed to a black hole node where the undermined node disposes of the considerable number of required packets. Grey-hole nodes act in an unreliable manner in a system, so this kind of assault is hard to track down rather than a dark gap hub where the undermined node disposes of all the suitable packets.

1.1.11 Detection of Grey hole attack

Except for a scheme with a large detection algorithm, which is responsible for all the output of the network node, so it's challenging to identify this phenomenon attack. Occasionally nodes that refer to each other and are advised to ensure the existence of malicious nodes to pleasant nodes that precede them. The technique is the same as an attack on Black-Hole, where the reaction to the sequence number may detect an attack on Grey Hole. When different routes live between source and target, a vivid Grey Hole assault can be detected through sufficient detection. However, this technique makes it difficult to identify a latent or activated attack.

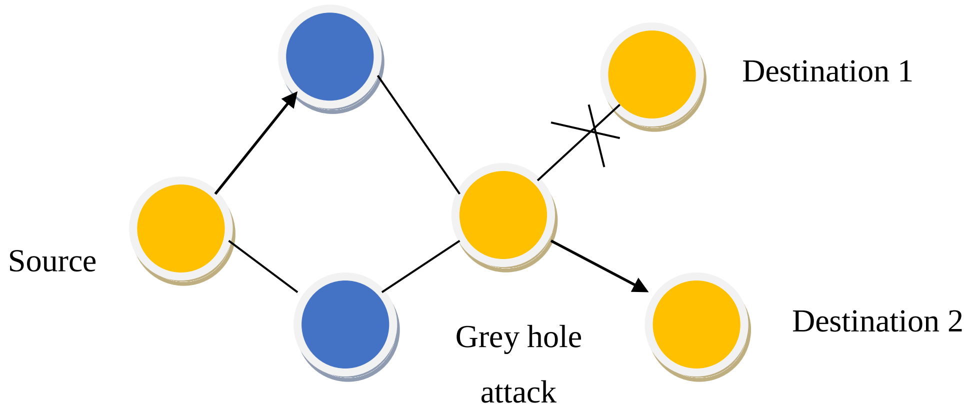


Figure 1.13 Grey Hole Attack Detection

That node holds a routing table in the AODV routing phase that includes definite destination and next-hop information. Its knowledge has utilized for route classification through source up to the destination.

1.1.12 Prevention Mechanism for MANET

As in the above section, we discussed enormous kinds of attacks in the MANET network tropology. Among them, the Blackhole attack, wormhole attack, and DoS attack are considered as an important one. Here we discuss the prevention mechanism regarding these attacks.

1.1.12.1 Prevention mechanism through Swarm Intelligence

Before starting discussing the prevention mechanism using swarm intelligence, we shortly consult the swarm intelligence, characteristics and how it helps to prevent the attacks in MANET

1.1.13 Swarm Intelligence

G. Beni and J. Wang have been incorporated the phrase first "Swarm Intelligence" in 1989. Swarm is a significant amount of homogeneous, basic drugs interrelated in the environment and their condition, with no focal control to advance abnormal worldwide conduct. Swarm intelligence, now and again called collective intelligence, is characterized as the critical thinking conduct emerging from singular operators that connect with different specialists by following up on their nearby surroundings. Anyway, these specialists are moderately modern with constrained capacities all alone; they associate with explicit standards of conduct to achieve undertakings essential for their endurance. The social collaboration between swarm individuals can be either immediate or backhanded. The immediate correspondence happens through visual or sound contact, for example, the honeycomb of honey bees; then again, backhanded correspondence happens while separate modifications come in the environment. The others react particularly for different circumstances; For instance, ants dump the pathways of unstable synthetic substances known as 'pheromones' to scan for the food sources.

Ant algorithm must be effectively applied to an assortment of issues with combinatorial improvement across discrete pursuit spaces. This thought is applied by the particle swarm optimization (PSO) that applies to the issue of finding an ideal answer for a given issue via looking through a multidimensional arrangement space. The underlying arrangement is a swarm particle, every one of which speaks to a potential answer for the issue. Every molecule has its speed, which relies upon its past speed (inertial part), the propensity to the best situation before, and the inclination toward an ideal neighborhood ideal or nearby neighborhood ideal (the social segment). In this manner, particles are travel through multidimensional space and, in the end, go to a point between the worldwide best and their own best. The typical swarm intelligence system composes of below-given properties:

i. It comprises a large count of individuals;

ii. Either all the individuals are related, or they belong to a few typologies, i.e., relatively homogeneous.

iii. The communications between the people are established on basic behavioral instructions which utilize just neighborhood data that is traded legitimately or by means of the earth, i.e., stigmergy.

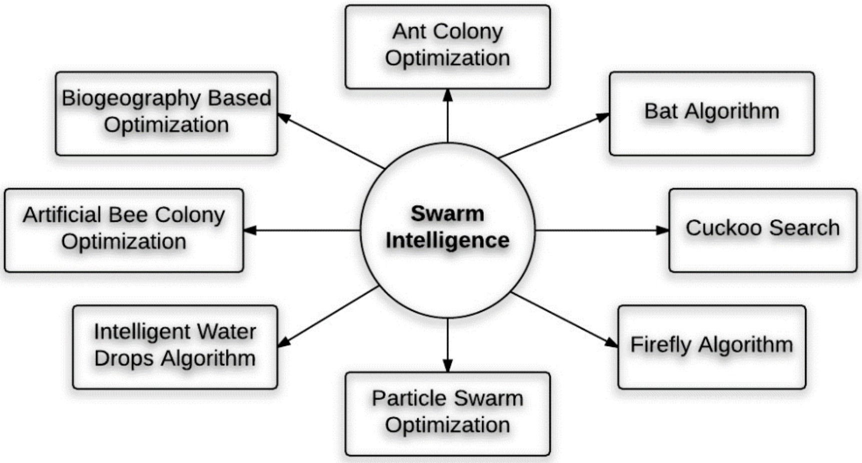

Ant Colony Optimization
Biogeography Based Optimization
Bat Algorithm
Artificial Bee Colony Optimization
Swarm Intelligence
Cuckoo Search
Intelligent Water Drops Algorithm
Firefly Algorithm
Particle Swarm Optimization

Figure 1.14 Various Techniques of Swarm Intelligence

The communications among individuals, including all the other individuals and the communications with their environment, predict the overall behavior of the system, i.e., the group behavior self-organizes. There are a lot of technics, such as Ant colony optimization (ACO), Artificial Bee Colony (ABC), Firefly, Glow warm, and many more, come under the swarm intelligence technique. Still, here we mainly focus on the Artificial Bee Colony (ABC) algorithm.

1.1.13.1 Firefly algorithm

The optimization problem is a calculation type problem in which the item is the best among all possible solutions. Can say that the issue of optimization is to find an answer in the executable area that contains the minimum or maximum obtained value corresponding to objective functionality. In an optimization problem, the kind of mathematical relationship goal and constraints and the decision variables how difficult to solve it determine the solution methods or algorithms that could be utilized to determine the optimal result. The light has no infrared or ultraviolet (UV) frequency, chemically produced from the lower abdomen, called bioluminescence. By using the flashlight, especially to attract friends or prey, the flashlight also acts as a protective warning mechanism to remind the fireflies of the possible predators.

Firefly algorithm discovered by Wang et al. is a metaheuristic algorithm motivated by the flashing behavior of fireflies including some mechanism for bioluminescent communication that the Firefly algorithm formulated through given such specific assumptions;

i. Fireflies will attract each other, not considering the sex because they are asexual.

ii. Attractiveness is equivalent to their glow whilst attracting the less bright firefly to the brighter firefly. Attractiveness is nevertheless decreased if the distance between the two fireflies rises.

iii. If both fireflies are equal in brightness, the fireflies can move randomly. The new solutions are generated randomly, and the fireflies attract. The brightness of fireflies has to be closely linked to the optimal solution of the potential issue. The attractiveness of swarm allows for the division across smaller segments, so each subgroup integrates by local models.

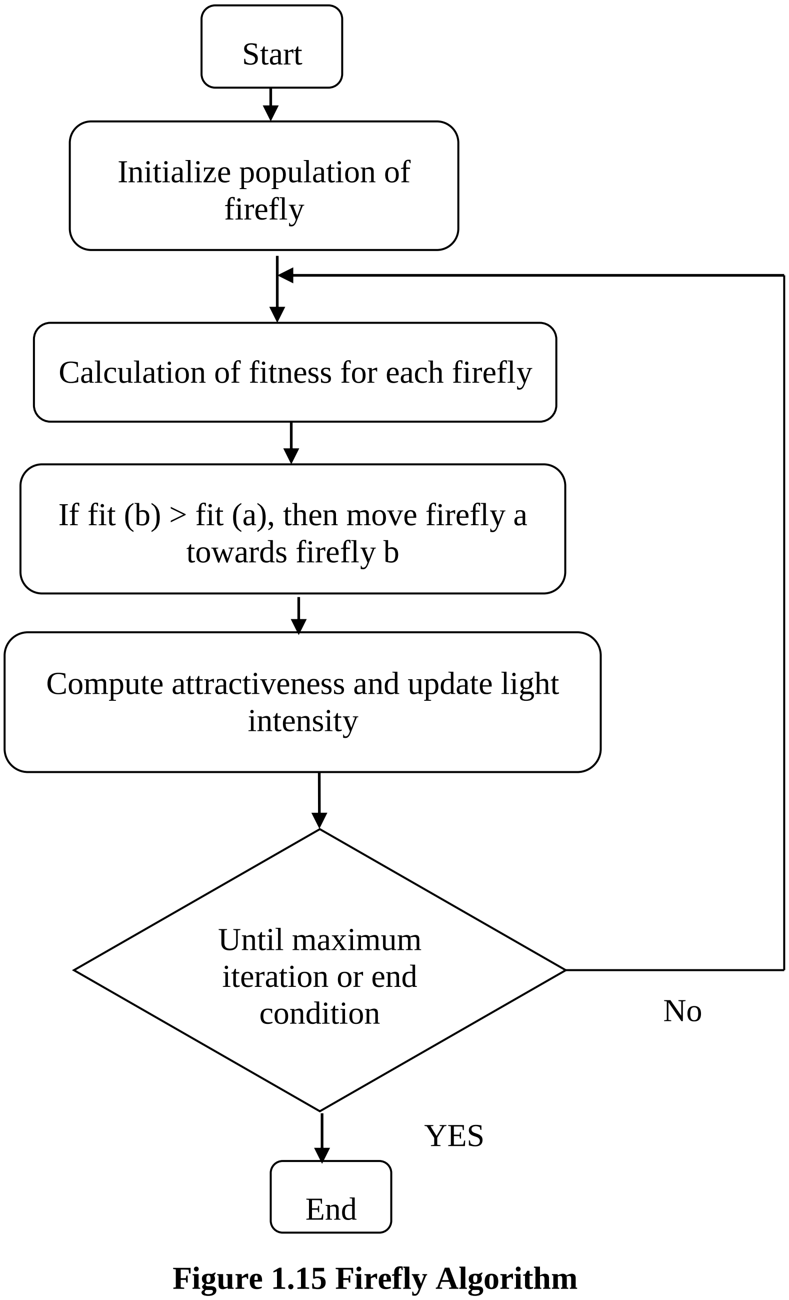

Start
Initialize population of firefly
Calculation of fitness for each firefly
If fit (b) > fit (a), then move firefly a towards firefly b
Compute attractiveness and update light intensity
Until maximum iteration or end condition
No
YES
End

Figure 1.15 Firefly Algorithm

As shown in the given above, the flow chart of a firefly in figure 1.15 in which firstly starts the algorithm means to initialize the population of firefly. After that, compute the fitness of every firefly to compare obtained fitness of one firefly with the next one. If the fitness of the next firefly is higher than the previous one, then move towards the next firefly. After that, the computation of attractiveness and modify the intensity of light, until higher iteration obtained.

1.1.13.2 Artificial Bee Colony (ABC)

In particular, three sorts of honey bees are remembered for ABC: Employed honey bees that identify with explicit food sources, onlooker honey bees that take a gander at the honey bees' moving in the hive to choose a food source, and scout honey bees that haphazardly scan for food sources. The two watchers and scouts are likewise called jobless honey bees. At first, all food source positions are recognized by analyst honey bees. At that point, the nectar of food sources is abused by working honey bees and honey bees, and this progressing misuse will inevitably make them become depleted. At that point, the utilized honey bee utilizes the exhausted food source, turns into a scout honey bee looking for extra food sources. As such, the assigned individual whose food source is exhausted turns into a scout honey bee. In ABC, the situation of a food source is a potential answer for the issue, and the measure of nectar from a food source compares to the quality (reasonableness) of the related arrangement. In the essential structure, the number of honey bees utilized equivalents the quantity of food sources (arrangements) since every honey bee at work is related to one and only one food source.

Pseudocode→ ABC Algorithm

The basic framework of the ABC algorithm is provided below as:

```
Phase for Initialization
Repeat
        → Employed bees
        → Onlooker bees
        → Scout bees
        → The best solution needs to be memorized
Until (Cycle = highest cycle number as well as maximum CPU utilization)
```

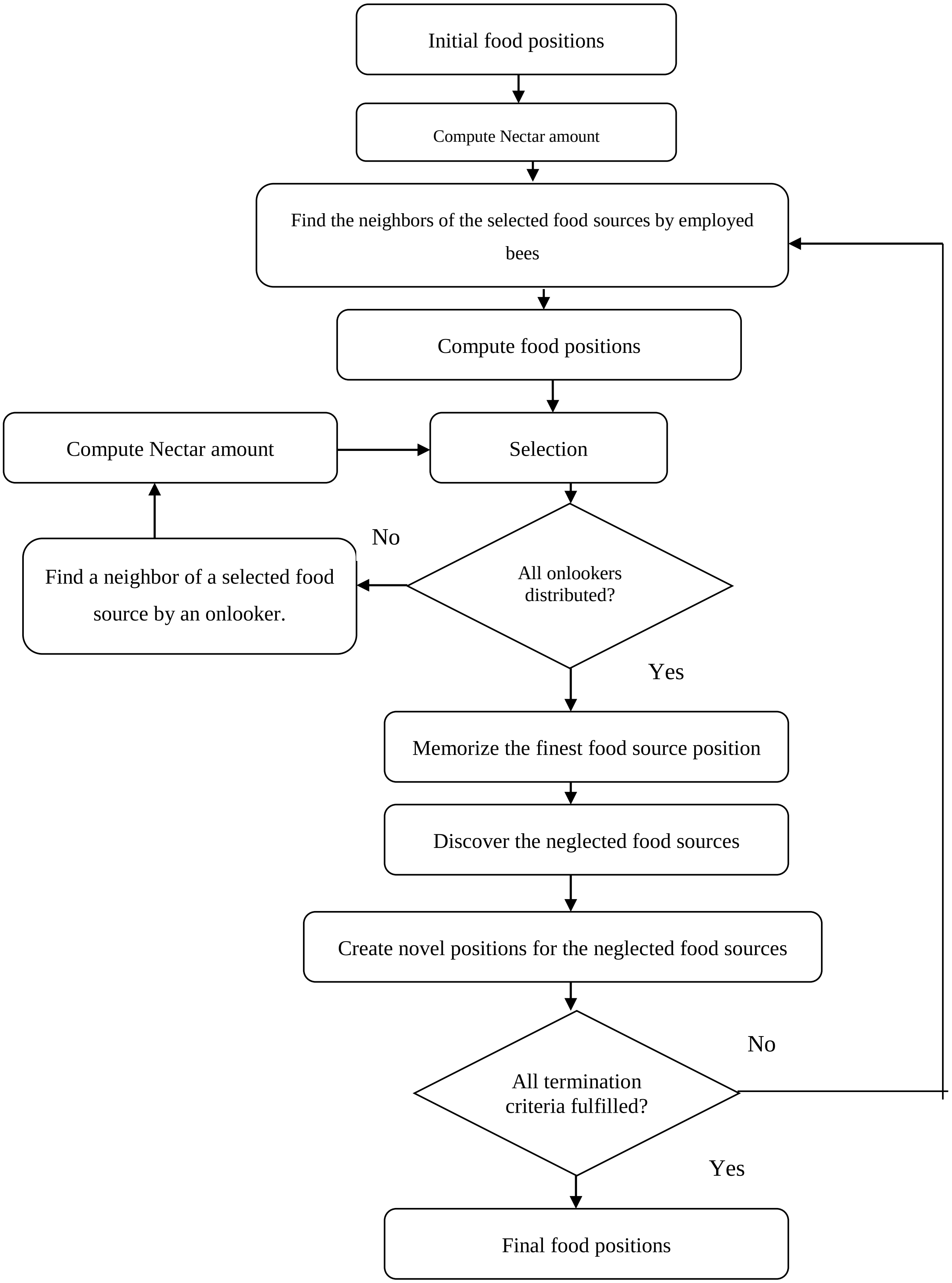

Initial food positions
Compute Nectar amount
Find the neighbors of the selected food sources by employed bees
Compute food positions
Compute Nectar amount
Selection
No
Find a neighbor of a selected food source by an onlooker.
All onlookers distributed?
Yes
Memorize the finest food source position
Discover the neglected food sources
Create novel positions for the neglected food sources
No
All termination criteria fulfilled?
Yes
Final food positions

Figure 1.16 Artificial Bee Colony Flowchart

- **Different Phases ABC optimization approach:**

i. Initialization phase

Artificial scout bees initialize the population of food sources (solutions), and the control parameters are set.

ii. Employed bees phase,

Artificial honey bees are searching for new food sources with more nectar in the region of the food source in their memory. They discover a food source for a neighbor and afterward assess their fitness. When the new food source has been created, its fitness needs to be determined, and a covetous decision is made between the parent and the child. A while later, honey bees share their food source data with onlooker honey bees holding up in the hive by moving on the dance zone.

iii. Onlooker bees phase

Artificial honey bees likely pick their food sources, contingent upon the data utilized by the honey bees. For this reason, a fitness-based choice strategy can be utilized, for example, the roulette wheel choice technique. Subsequent to choosing a food hotspot for a trailer honey bee, a wellspring of nature is resolved, and its wellness esteem is determined. As in the honey bee stage utilized, a covetous determination is applied among more than one source.

iv. Scout bees phase

The solutions of utilized honey bees can't be enhanced by a foreordained number of preliminaries, "limit," are scouts, and their answers are deserted. Scout bees eventually exploit the available food sources at random and determine the quality of food sources.

Scout bees verify the amount of sugar in flower spots to notify some other bees inside hives, searching for details on the quality of food source. Such contact technique of scout bees is conducted through 'wangle dance' with several other accessible bees. This bee creates a loud humming noise from wiggle dances and exchange information regarding the quality of food sources, direction along with the distance of food sources from the hive.

At first, ABC was proposed to find a solution to the optimization of combinatorial problems. ABC works in two stages as mentioned: forward stage and backward stage. In the forward stage, the solution for the combinatorial problems has been generated in individual manner, and collective experience has been shared. This partial generated solution has been further utilized in a backward stage, and quality has been assured with probability distribution function. Overall concept work in the local and global search solution process.

1.1.14 Prevention mechanism through Machine learning

In the earlier, we discuss the prevention technique using the swarm intelligence (Artificial Bee Colony) in an AODV routing topology. In this part, we discuss how the machine learning mechanism helps to detect the attacks in the routing protocol in the MANET. Before directly going to the Support Vector Mechanism (SVM), we shortly discuss machine learning, characteristics of machine learning, and how it helps to detect the attack in the MANET.

Machine learning

Machine learning is a subfield of Artificial intelligence introduced by Arthur Samuel in 1959. Machine learning (ML) is one of the most powerful, influential, and frequently used technology in the daily world. It is a tool for changing the raw information into knowledge. ML techniques are used to solve complex problems automatically, such as valuable underlying patterns inside the complex data that we would struggle to discover. There is a various feature which gives a perfect option to the user for selecting machine learning techniques for solving their complex problem. For example, the ability to perform automated data visualization, the ability to take efficiency to the next level while integrated with the IoT, the ability to minimize the error, and increases the efficiency of the work and much more. The major advantage of machine learning is that it requires minimum human interaction and produce high-quality output without interruption. **Machine learning Types:**

i. Supervised Learning

In this scheme, we suppose that the required system reaction is acquired at every moment the input is applied. For known examples, it attempts to predict results. Such a system compares its predictions to the known outcomes and learns from errors.

It based on the experience that we have learned in the past, according to this predicted event of the future. Initiate from the analysis of known training data sets; the learning algorithm used to make predictions about the output values by using the produced inferred function. After the complete training, the systems can have the capability to give targets for any new inputs. This algorithm also compares its outputs with the correct output if an error occurs, then modify the model to remove these errors.

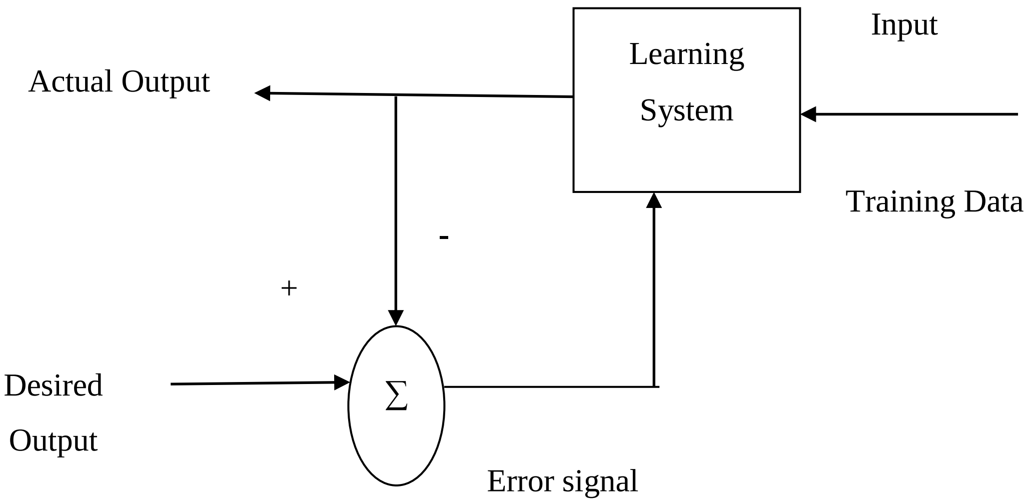


Figure 1.17 Supervised learning

ii. Unsupervised learning

The required reaction is not known in this mode, so it is not possible to explicitly use error data to enhance network behavior. Since there is no data available as to the correctness or incorrectness of the answers, learning can somehow be achieved based on input answer observations that we have a marginal understanding or no understanding.

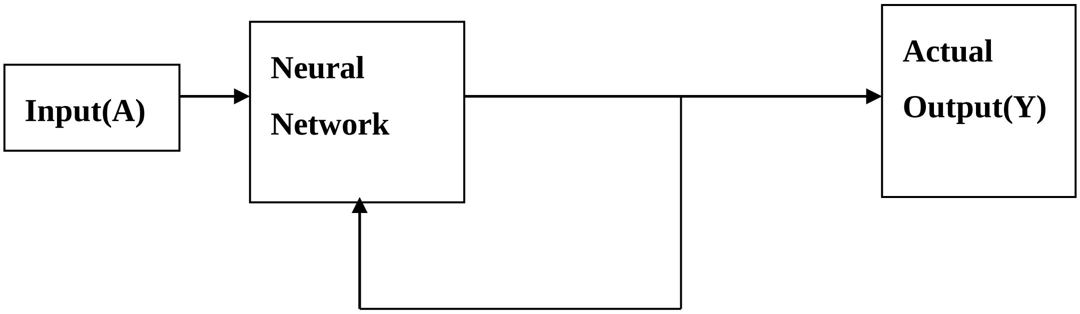


Figure 1.18 Unsupervised learning

This algorithm is useful when data we used to train in not classified nor labeled. It learns how systems can derive a function from explaining about the hidden structure of unlabelled data. In this technique, the system doesn't obtain the correct output, but it can the ability to expose the information and draw layers from datasets to describe in detail about hidden structure of unlabelled data.

iii. Semi-supervised machine learning algorithms

This occurs somewhere between supervised and unsupervised methods because they have trained both kinds of data (labeled and unlabeled data), essentially the unlabeled data in a higher amount and labeled data in a small amount. This approach can be used to improve the learning accuracy. Semi-supervised learning is typically preferred when the marked knowledge obtained requires qualified and sufficient funds to learn or practice from it. Reinforcement machine learning algorithms

In this learning, the method interacts with the surroundings through acquiring activities and got errors or rewards. Important features of these methods are Trial and discover an error and delayed reward. Particularly this approach helps one to automatically obtain the optimal actions for performance benefit within a given context. The agent requires clear incentive feedback to determine the behavior is best; this is called the motivational signal.

Regression, Classification, Clustering, Dimensionality Reduction, and neural network and other techniques are the difference in the machine learning techniques frequently used in daily life. For solving the preservation problem here, we use the Support Vector mechanism (SVM).

1.1.15 Support Vector Mechanism (SVM)

Mobile ad-hoc network is becoming more difficult day by day as opposed to its brother wired network and facing new kinds of weaknesses. MANET's pervasive popularization often makes it more attractive to the advanced attacks.

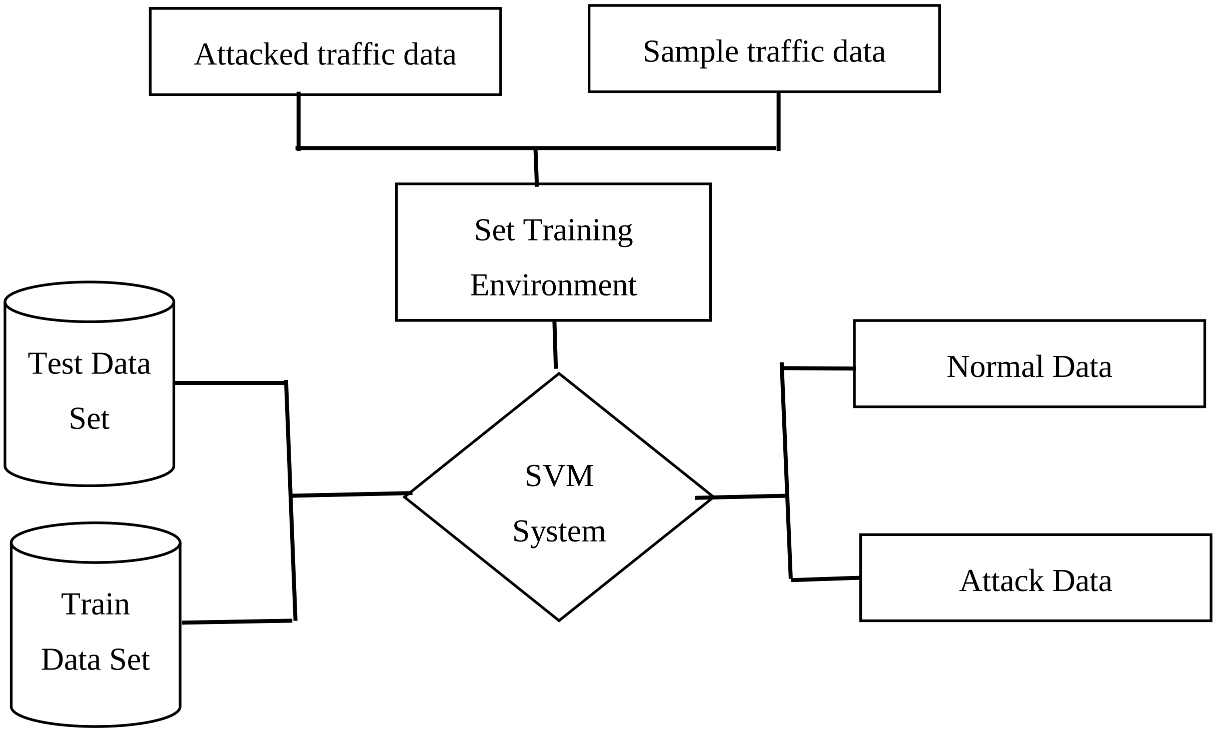


Figure 1.19 SVM Structure

Figure 1.19 demonstrates the flow architecture of the SVM system. In this, it classified the Normal data and Attacked data from the test data and the training data in the set training environment. Training environment both the sample traffic and attacked traffic are used for the training purpose of the dataset.

SVM is applied to distinguish the attacked traffic from the normal traffic with the basis of the classification approach as we know that for the classification problems, SVM can easily handle the problem successfully in the simple set and is easy to implement. The classification process includes both the training data and the testing data sets, which are formed by several data sets. The main motive of the SVM is to produce a system that predicts the targeted traffic of the network tropology instances in the testing set that is given the attributes only.

1.1.16 Artificial Neural Network (ANN)

ANN is the technique of machine learning that is designed to work like a human brain. The working of ANN is similar to a human brain is works and memorize from the past experience. ANN is a non-linear statistical model, which processed input to discover a new pattern. The ANN consists of three layers, as discussed below.

Input layer: The input regarding the node's properties like packet delay, energy consumed by nodes, and nodes position is provided as input information.

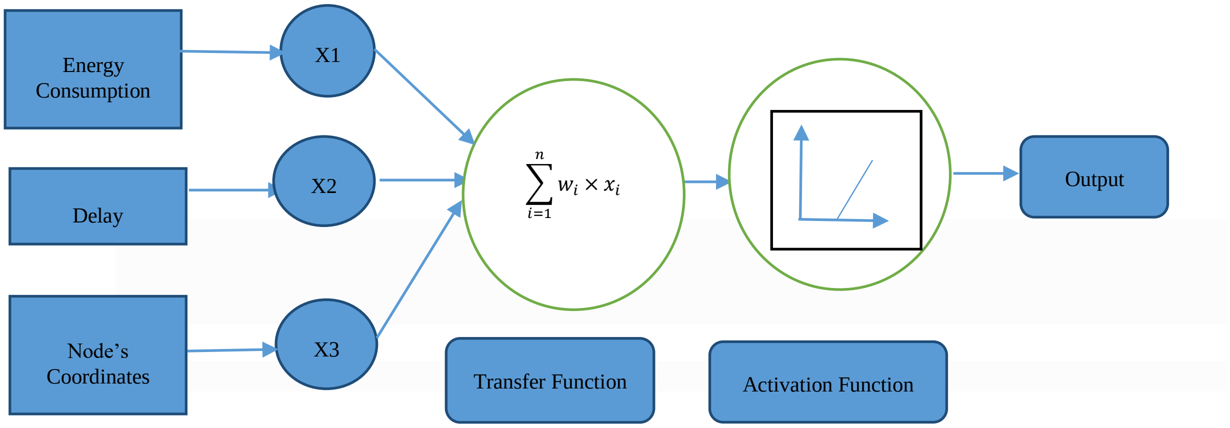


Figure 1.20 ANN Structure

Hidden Layer: This is positioned between the input and output. It can be single or multiple layers can be used. The main function of this layer is to process the input data to know the relationship between the attributes fed to the input layer.

Output layer: The resultant value after computation is obtained at this layer. The complete structure of ANN is shown in Figure 1.20.

SUMMARY

This chapter provided a brief review of the MANET framework to isolating various kinds of attacks using an IDS technique. In the introduction about MANET, the features i.e., its infrastructure less nature, Dynamic Topology, Bandwidth Constraints and Variable Link Capacity, Multi-Hop Communication, Constrained Resources, Limited physical Security and Short Range Connectivity and so on are discussed briefly. After that, the structure of MANET is explained in which mainly three parts are involved named enabling technology, networking, and middleware, including application. The enabling technology part of a structure is divided into distinct categories as per the range of network areas such as BAN, PAN, and WAN, etc. MANETs can be mainly categorized into three specific parts named as Vehicular Ad Hoc Networks (VANET), Internet-Based Mobile Ad- Hoc network (iMANET), Intelligent Vehicular Ad- Hoc Network (In VANET). Apart from several features in MANET, there is various challenges and issues are present in MANET like limited bandwidth, Routing, Characteristics of the wireless link are time-varying in nature, Route challenge due to Mobility, Dynamic topology, Packet losses due to transmission errors, Hidden Terminal problem, Security threats, and Fault tolerance. The packets can be transmitted from source to destination within the network with the help of a routing protocol that can be categorized into reactive, proactive, and hybrid routing mechanisms these are applicable according to the circumstances. The various types of attacks in MANET that need to be identified and resolved, which is mainly categorized into passive and active attacks, which are further partitioned among various attacks. MANET is more vulnerable to Active Attack, where the network becomes very challenging to stop flow-node messages; the attacks can be both external as well as internal. To detect both active and passive attacks are very complicated since it does not impact the activity of the network itself. The passive intruder rarely threatens to disrupt the routing protocol, but always seeks to find the essential data from the outgoing data packet. Other attacks are DDoS, Blackhole attack, Wormhole attack, Grey Hole Attack, etc. The attack in MANET is prevented in various ways, like through such an optimizer named swarm intelligence, firefly algorithm, artificial bee colony (ABC). The optimization problem is a computational type of problem in which the item is to find the best among all possible solutions. We can also say that the challenges of optimizations are to find an answer in the feasible areas that composed of minimum or, the maximum value of the objective function. Here, the utilization of machine learning is also discussed, like supervised learning and unsupervised learning. Regression, Classification, Clustering, Dimensionality Reduction, and neural network and other techniques are the difference in the machine learning techniques frequently used in daily life. For solving the preservation problem here, we use the Support Vector mechanism (SVM) as it can easily handle the problem successfully in the simple set and is easy to implement and artificial neural network (ANN).

CHAPTER 2: LITERATURE SURVEY

Security is the most important issue in the MANET that ensures the message authentication and integrity packet. A packet (information message) transmitted from the source to the destination node must be secured against different attacks, such as a black hole, gray hole, and other. In this section, we discuss different routing mechanism issues, prevention, and other security issues in MANET proposed by many other authors.

This chapter divided into four sections (i) Routing in MANET, (ii) Attacks in MANET, (iii) Research Gap, and (iv) Problem Formulation. The summary is given after discussing the review of the literature along with the research gap. Initially, a brief introduction about the routing in MANET is given. After that, the work performed by several researchers using proactive and reactive protocols is also discussed how the routing protocols helps to create a valid route for data transfer. In section 2.2, various types of attacks appear in the network are discussed, and then work performed by several researchers to secure the network against these network attacks is presented. Several researchers used different approaches such as thresholding-based approach, optimization, and machine learning approach to secure MANET against the attacks.

2.1 ROUTING IN MANET

In the MANET, there is no fixed infrastructure that causes different forms of difficulties. One of them being the key concern is routing. Routing is the process of selecting paths in a network from which data packets will be sent to the destination. An ad hoc routing protocol is an event or norm that controls how nodes determine whether to pass packets between computing devices inside a mobile ad hoc network.

Routing protocol provides a path for the data transfer between nodes without any defined infrastructure. Routing is the method to establish a path between the source node and the destination node utilizing intermediate nodes. The selection of route performed in the first two phases is to select a route between the source and intermediate nodes, while the second is to deliver data to the destination node from the intermediate nodes. The routing knowledge is exchanged between the nodes through the routing protocols, and an appropriate path can be chosen. Routing protocols describe a series of rules to determine the best path, and the data is distributed in a managed manner between original and goal node. Every node inside the network serves as a path that correctly gathers data collected and transmitted to the next node. The node that holds knowledge regarding the nodes that join the network as well as exiting the network maintains a routing list.

Brindha et al. (2019) proposed a Fuzzy-based secure multicast routing protocol to tackle the attacks and provide more security in the mobile nodes. The proposed Fuzzy decision technique was used to detect the authentication of nodes, i.e., normal or abnormal nodes. Another method has been implemented in the multicast environment, such as encryption and key generation techniques, to enhance the security of a node in the topology of a network. Using a network simulation tool, many parameters would show the FSMR performance, such as packet authenticity and average delay. Based on the simulation results, the presented mechanism accomplished enhanced performance based on certain parameters as compared to the previous schemes [1].

Yang et al. (2019) proposed a novel combined technique based onDSR for the better link among the different nodes as a matrix of routing, and the CHNN has been used to get the better stability of the link as a path. The proposed work helps to detect the issues in the routing mechanism by providing the enhanced routing table. After performing the Network simulation, a different parameter such as packet transmission rate, average end-to-end lag, etc., shows better performance results. Still, there are possibilities of issues presented in the routing area of MANET and must be short out in future work [2].

Jamaesha et al. (2019) proposed a secure location-aware routing protocol for the detection of the attacker node in the routing mechanism of MANET. The proposed work node was arranged with the help of a clustering mechanism form the network topology using elliptic curve cryptography. The author demonstrated that the proposed mechanism would provide a future location through PSO. For optimization of the node, different parameters such as connection lifetime, pace, size, and position of the node are determined earlier. The trust value of a large node was calculated using the potential position of the closest node, and a fake node was located in the network to minimize packet loss [3].

Deepa et al. (2019) suggested an ad hoc Dynamic Energy Delivery Distance Demand Protocol (DE-AODV) to eliminate packet delays, optimize network life as well as reduce energy usage. Not only does the proposed strategy raise energy levels, but it also increases the network 's life significantly. The packets were effectively moved to the preferred access route by energy reliability criteria. The metrics used for determining the efficiency of this research are energy usage, latency, packet transmission ratio and packet failure, end-to-delay, and network life. The suggested protocol indicates that our simulation tests provide improved energy performance compared with other current protocols. The DE-AODV protocol decreases total packet loss, increases network life, decreases node change errors, and reduces packet delay [5].

Bhattacharyya et al. (2018) proposed a modification based AODV protocol to minimize the energy consumption while transmitting data through reduction of packet size along with managing the 'Energy/Distance' ratio like the metric to tracking the best route. The author demonstrated that the proposed method reduces the required power transmission and battery life by taking the help of these combinations. In the future, they also think about implementing techniques of Artificial Intelligence to determine the route in the protocol [8].

Balamurugan et al. (2018) proposed a routing protocol of hierarchical nature, including the framework of data propagation with varying amounts of transceivers, have provided smooth routing protocols in FSO MANET. The process of clustering is done in this work according to the neighbor discovery algorithm after that cluster head is chosen by the network source connector. Here, the benefits of the presented mechanism through varying the number of transceivers is that it produces enhanced delivery ratio, drop, delay, higher throughput, and a visible line of sight. In our future work, the comparison with existing hierarchical cluster-based routing protocol through varying the node amounts [9].

Sethuraman et al. (2017) suggested a refined energy-efficient Trust-based routing strategy i.e., ReTE-AODV, to minimize consumption of energy in MANET. From this work, it must be demonstrated that the proposed algorithm creates MANET with an efficient route, even after its dynamic topology and openness. The packets are transferred through the source to the destination rather than transmitted via the shortest path but after getting a reliable path that consumes minimum energy as well as trustful to transfer the packets. On the basis of result simulation of this work, it outperforms as compared to the previous mechanism in terms of Trust-based routing and energy efficiency [12].

Pathak et al. (2016) presented an approach named Improved cluster Maintenance Scheme of cluster formation. For cluster construction and cluster head selection in mobile network topology, the two key factors — node degrees and bandwidth requirements — are regarded. The presented approach to the algorithm minimizes the likelihood of unnecessary fusion if the groups pass. WBC 's algorithm was designed to simulate in ns-2 as well as compared with protocol LCC and CBRP. It is to be cleared from the outcome; that the WBC proposed does better than the other two protocols [11].

Venkanna et al. (2015) introduced a robust trust-based model distinguishing node suspicious as well as affected actions through continuously measuring the node trust along with energy values in the topology. It must be obvious from the presented research, confidence, as well as energy-based ad hoc on-demand space, to improve traditional AODV algorithms by dynamically combining confidence and energy values for each node in topology to establish cooperative routing. Following virtual network simulation, the experiments demonstrated that the proposed AODV trust and energy-based routing protocol differentiates suspicious and selfish nodes as well as significantly improves the performance of routing, like PDR and end-to-end delay [6].

Sherin et al. (2015) proposed a novel crypt-biometric perception technique for the improvement of security in ad-hoc mobile networks. The author found that by adding exclusive identity features, the biometric-based authentication system became the most adaptable and safer in diverse networks. After the simulation, result shows that various factors such as True Positive Rate(TPR=1), True Negative Rate (TNR=0.987), False Positive Rate (FPR=0.012), False Negative Rate (FNR=0) ,Accuracy=0.988 , Precision=0.944, Recall= 1and F-measure (0.9629) shows good result [7].

Mukherjee et al. (2015) proposed a trust basis routing strategy, namely, AER-AODV protocol, that can examine direct trust, including average encounter rate (AER), containing the frequency of successful cooperation. By utilizing the revised D-S evidence theory, indirect trust is examined. As per the outcome of this work, the AER-AODV can eliminate compromised nodes while establishing the route. In terms of PDR, the presented approach accomplished enhancement. However, throughput is compromised; the approach can isolate the affected node by enhancing the lifespan of nodes inside the network [19].

Ullah et al. (2015) recommend a computation of trust metric on the basis of node's impulsive behavior for becoming malevolent in the distributed environment, as well as the proposed methodologies to assess each node 's confidence. The proposed confidence-based protection model (TSRM) verifies both the new nodes and the nodes that were involved in the current communication network. After the computation of the final result, it has to be cleared that having enhanced packet delivery rate as well as efficiency as compare to DSR [20].

2.2 ATTACKS IN MANET

A mobile ad hoc network (MANET) is a virtual node network that develops itself. No fixed infrastructure exists, such as an entry point or base station. It does not have unified control and is linked via wireless links/cables. A wireless ad hoc network can be set up where wireless communication is not possible or where wired connectivity is not feasible.

All resources ad hoc on the network are planned and developed. So it's obvious that protection is becoming an intrinsic flaw in ad hoc networks with a shortage of technology support and vulnerable wireless communication assaults. Nodes with links to traditional radio networks inside nomadic regions will effectively contribute to the creation of ad hoc infrastructure. But the encrypted communication connection is required to communicate between nodes in a secure manner. Connecting the node has to be sufficient to recognize another node before secure communication is established. As a consequence, other nodes, as well as related connections, must be granted their name. However, the identification of both distributed and credentials must be checked and protected in such a manner that the receiver node does not question the authenticity and integrity of the identification and credentials distributed not compromised. To ensure ad hoc networking, it is, therefore, essential to provide security architecture. We have found that many of the current attacks have different similar features, and have been classified into different attacks based on their slight differences. So we try to classify among two major categories, such as attacks of DATA traffic and CONTROL traffic. It will help to design security measures in the future that can mitigate these broad categories at once.

Zulfiqar et al. (2019)proposed a well-known strategy, named as "dual attack detection" for black along with gray hole attacks (DDBG) in MANETs. Using the connected dominant set (CDS) technique, the provided DDBG approach will pick the IDS node using an intrusion detection system (IDS) with two additional features; the energy along with its inclusion on the blacklist is also checked even before nodes are put in the package. The identified IDS nodes transmitted a sort of condition packet to retrieve the entire descriptive data inside the underlying set size through respective nodes. The experimental outcome of this approach has suggested that it service quality criteria than that of the current routing schemes [103].

Abdel-Azim et al. (2018) proposed a model to mitigate the effect of a black hole attack using an optimization algorithm (GA) as well as an integrated neural network Fuzzy. The proposed model consists mainly of four components: (i) Elimination of fuzzy-based parameters (ii) Fizzy interface component used to calculate the membership functions corresponds to each fuzzy set as well as to minimize the error (iii) Modules to decide, (iv) Answer component. The researchers used optimization procedures known in three stages as pre-preparation, ANFS, and GA to optimize as well as the fuzzy interface component. The conclusion here is that in the scenario of a black hole, the PDR parameter of the program was lower than the PDR obtained when a black hole attack was used with IDS[64].

Usman et al. (2018)proposed a made sure about information correspondence calculation, called QASEC, for error-free transmission o packets in MANET. The creators showed that including secure data trade, the created framework could arrive at more noteworthy transfer speed. The introduced approach utilizes solid verification to secure a packet of data through one node to another. They gave work used the encryption-based made sure about the key in the way that recognizes the malignant node and continued interfering with the transmission of information through another particular path [21].

Shams et al. (2018) developed a program for detection of intrusion i.e., IDS, to recognize just as impair DOS assaults in MANET. The introduced approach utilizes the SVM as an order calculation to distinguishing and evacuating the DOS assault in the topology of MANET. Following the reproduction on a virtual system, the outcome demonstrates that the proposed IDS instrument can without much of a stretch distinguish and evacuate the DoS assault with a high identification rate and less processing time. It was likewise seen that the development of the hub and the size of the system didn't influence the identification rate [22].

Anbarasan et al. (2018) developed the LEACH protocol on the basis of a bunching calculation, which would give MANET support as extra whole system assets. The instrument depicted joins the hubs comprised of group head alongside bunch director used to move the bundles among hubs. The essential point of the introduced structure needs to give error-free packet transmission between the various nodes through encryption guidelines applied to create the necessary vitality prerequisite for improved security in MANET from DoS assault. The creator demonstrated that the vitality had been spared by utilizing the LEACH convention and consequently, the improvement in battery life [29].

Bhuvaneswari et al. (2018) implemented an OLSR routing algorithm to avoid a DoS attack by the system. The malicious nodes have been detected through their "HELO" response and also the TC notifications sent at a daily timespan from the node. It has to be examined that with the increase in network size, the overhead would become insignificant. The performance of the OLSR protocol is enhanced in such a case and thus tends to increase security measures. The findings of the experiment show that the performance parameters, such as throughput, PDR, are lower than the attack concentration, while no fictitious node is included [36].

U. Ghugar et al. (2018)described a PL-IDS scheme to compute wireless sensor networks (WSNs) faith in the physical layer, which is based on the physical layer recognition of attacks. This implemented method is intended to be successful in detecting anomalous nodes within WSN. Abnormal nodes attack primarily via the assault on the physical layer, called as DoS. They also used the periodic question attack to perceive the view of PL-IDS, and the skill of this implemented conspire has to be tested as far as both false alarm rate (Early) and malicious node detection accuracy are concerned. Considerably, the exactness of location at thickness 20, 40, and 60 is 84, 88.6 and 94.2% and the bogus caution rate obtained relates to a gave thickness is 15.8%, 11.4 and 5.8% It should subsequently be expected that the thickness has improved as an outcome of the ascent in FAR precision identification and decline[80].

Alsumayt et al. (2018) Presented a novel approach called "Detection and Recovery Tracking" to avoid a DoS attack by a network. This method is determined by analyzing the number of real values inside the sensor network that may or may not trust. The proposed approach has contrast through past"trust enhanced anonymous-on-demand routing protocol," along with has to be cleared perhaps the strategy did much enhanced using packet delivery ratio[24].

Duan et al. (2018) presented new metrics for evaluation of the susceptibility of certain arbitrary targeted system or directory to accelerate DDoS attacks and its approximate impact on network vulnerability. Second, the author's proactive path union strategies to decrease weakness to the assaults by overwhelmingly moving intermittent streams to discredit organize data and forestall focused on, immaterial connections. The most recent arrangement has viably changed the bearings of the system, as it offers insurance and effectiveness score needs [40].

M. M. Ozcelik et al. (2017) developed a hybrid Intrusion Detection System (IDS) technique used to bunched WSNs identified with the utilitarian believability and misuse distinguishing proof standard. The core idea here is that every node in the network helps determine functional reputation values for its neighbors by monitoring their behaviors. Base Station (BS) identifies malicious activity by combining possible credibility values with abuse rules. The system offered increased the system's lifetime as well as the increased perceived quality of the data while consolidating the detection of suspect nodes via increased energy consumption [68].

V. R. Prabha& P. Latha (2017)executed a trust-based following of interruption trust the executives by multi-credit to improve the expected execution. It utilized an upgraded technique to figure decentralized trust that incorporates observing neighboring hubs and estimating trust utilizing trust measurements, node time, accuracy, and fairness achievement rate. Moreover, the standard cooperation based trust asset MSR, dynamic measurements, for example, ETN have been utilized to fundamentally modify data and record assaults, and two social association rules accuracy and fairness have been utilized to appropriately distinguish trust-related assaults [69].

S. Otoum et al. (2017) introduced a hybrid architecture for destructive activity identification between networked investment instruments' key components, for example, atmosphere, clinical, and brilliant frameworks. This planned determination is frequently utilized in these cases to distinguish the problematic action of sensors, i.e., known and obscure obligation cycling attack of Enhanced Density-Based Spatial Clustering of Noise Applications (E-DBSCAN) and Random Forest (RF) plans. Eventually, this present structure has demonstrated that if there should be an occurrence of known and obscure conduct of nosy sensor hubs of location rate (99.73%) and complete exactness (98.95%), it has a higher ability to distinguish [70].

Z. Zhang et al. (2017)implemented a system for intrusion detection centered on an adaptive state context as well as in a hierarchical structure of trust in WSNs that is extensible as well as appropriate in constantly evolving WSNs identified through cognitive environment variations, transformations of node state and trust-value variations. The certainty of sensor systems is inspected through bunch heads and here additionally assessed the certainty of group heads utilizing neighboring CHs, which also decreased the complexity of the evaluation without even any evaluation through the network's completely different cluster heads [72].

M. Wazid, & A. K. Das (2017) introduced a new, successful group-based technique for the primary detection purpose, as well as prevention of a huge black hole attack in WSNs, which appears necessary. Thus the entire WSN has been divided into separate clusters in which each cluster has a strong high-end sensor node recognized as the CH, capable of detecting nodes assaulted by a black hole. This method has reached an average detection rate of 90%, and the FPR (false positive rate) is 3.75% higher than the previous analysis [73].

A. Basan (2017) established a confidence evaluation framework to determine the node'soutstanding burden esteems just as residual energy. The supposition of such factors with limit assessment permits us to recognize pernicious properties of specific hubs while assessing the likelihood of qualities that fit the certainty stretch, surmised the first just as second request mistakes. The level of errors with the number of dangerous nodes below 70% enables malicious nodes to be detected and blocked with rather a high efficiency. As per the number of defected nodes exceeding 70%, the accuracy decreases, but in the case of thousands of nodes in larger areas, it is incredibly difficult for a possible attacker to exceed even the 50% level of malicious nodes [72].

R. Singh et al. (2017) proposed a sophisticated Hybrid Intrusion Detection Device (AHIDS) solution is for the automated identification of WSN attacks. AHIDS makes use of cluster-based architecture with an improved LEACH protocol to minimize power consumption for sensor nodes. Together with included with Multilayer Perceptron Neural Network, AHIDS utilizes anomaly identification and abuse identification according to the fuzzy rule sets. The Feed-Forward Neural Network and the Backpropagation Neural Network could be utilized in the way to combine the effects of detection and show the various kinds of attacks, namely, wormhole attack, hello flood attack and Sybil attack with different rate of accuracy and false-positive rate [74].

Schweitzer et al. (2016) suggested an explanation to defend the OLSR protocol from an isolation attack that utilized a similar policy as utilized by the attack itself. By experimenting extensively, it has been observed that the protection is more common as compared to 95% of the attacks with the overhead requires drastic reduction when the network size enhances until it is undetectable. Finally, it has been observed that this clarification could be enhanced by utilizing the OLSR protocol [35].

Zakariaa et al. (2015) Suggested a swarm intelligence dependent framework inspired by a firefly optimization scheme to look for the smallest root between the source node and the queuing model for the destination node. The authors integrated the firefly algorithm with a queuing scheme to discover the best route to the destination node between nodes of origin for the best optimal result. The experimental outcome indicates that the suggested hybrid solution research network was used to evaluate the minimum answer time with the destination node among the source nodes [23].

J. Zhou et al. (2015)presented a practical situation of cloud-assisted WBANs in mobile health care social network. Here, it presented a stable and privacy-conserving authentication scheme that is robust to both time-based as well as location-based mobile attacks. In the end, the results of the security modeling and optimization demonstrate that the proposed method far surpasses the previous ones in the aspects of resisting mobile attacks as well as the overhead of storage, computation, and communication [78].

Shone et al. (2018) presented a new deep learning technique for the identification of intrusion. An unsupervised feature learning scheme with a non-symmetric deep autoencoder (NDAE) has been used. The design has been implemented using the Graphical Processing Unit (GPU) that utilized KDD Cup 99 & NSL KDD dataset. The results have been find improvement compared to the existing work [79].

M. A. To et al. (2016) have analyzed the interoperability of ad-hoc routing protocol that is not wireless; Interoperability operates in the same way in which more than two independent systems, even though they operate separate routing protocols, can relay messages to a neighboring network. This work focused on the Strip Interoperability method of proactive, which has proved to cross diverse networks through layer 3 protocols exclusively. The testbed of this work executed on wireless ad hoc routing protocols, Ubuntu Linux and, the implementations of OSLR and BMX6 have done by using IPv6 and some other relevant protocols [84].

Gurung&Chauhan (2019) introduces the smart grey hole attack along with a novel approach for validating the effect of smart grey hole assault. Mitigating the Gray Hole Attack Mechanism (MGAM) has introduced numerous specific nodes, called the Gray Hole-Intrusion Detection System (G-IDS), which are used in MANETs to identify and prevent smart grey hole attacks. MANET is mentioned as the kind of wireless network that can operate without any permanent infrastructure at all. The principal prediction considerable in this network is that all nodes have sensitive information. Nevertheless, in real situations, some nodes may be a hostile node and will thus drop data packets selectively instead of transmitting data packets to the target node [104].

Singh et al. (2019) discussed some significant methods used to identify black hole attacks in MANETs using the AODV routing protocol, including their pros and cons that play a significant part in future studies. The mobile ad hoc network (MANET) is dynamic and consists of less topology infrastructure and node centralized behavior. Since every node is elastic, it is free to switch everywhere to render the network more vulnerable to attacks like the black hole, the gray hole, and several other forms of attacks. Fewer infrastructures mean that for some moment, every node acts as a host and sometimes as a router. During communication between nodes black hole attacks, AODV is a data routing protocol, and control packet wording between nodes is a significant problem in MANETs[105].

SUMMARY

The previous chapter begins with the basic concepts of MANET, Types of MANET, features of MANET, Routing in MANET, and its further types, Swarm Intelligence Technique. Types of Swarm Intelligence and Also, the concepts of Artificial Honey Bee Optimization and ANN have been discussed in detail. These concepts have been used for the detection of various types of attacks in MANET. Briefly, a review of existing works is discussed here and includes the existing works performed by the number of investigators as well as related experts. A comparative overview of different feature extraction techniques on the basis of different specifications is seen based on the review of the literature. Furthermore, the extensive research gaps in the substantial studies are greatly lightened. The review of literature in this chapter is specifically divided into Routing in MANET, including attacks in MANET. In which summarises the literature survey of various types of routing techniques such as thresholding-based approach, Fuzzy based secure multicast to detect the authentication of nodes, location-aware routing protocols, dynamic energy ad-hoc on-demand distance vector routing protocol i.e., DE-AODV) along with the refined trust-based energy effective routing algorithm termed as ReTE-AODV with the aim to reduce the packet delay and energy consumption along with maximizing network lifetime. For forming a clustering method named improved cluster Maintenance Scheme is presented, and the biometric-based security mechanism is also given named as crypt-biometric perception algorithm. After discussing the routing in MANET part of literature here, go through the attacks included in MANET that needs to detect and overcome. The utilized techniques are detection for dual attack (black and gray hole attacks) that taken the node of IDS through connected dominating set strategy. An unsupervised feature learning scheme with a non-symmetric deep autoencoder (NDAE) has also been used as well as the design has been implemented using the Graphical Processing Unit (GPU) that utilized KDD Cup 99 & NSL KDD dataset. To enhance the performance of work, the optimizer i.e., genetic algorithm (GA), is combined with fuzzy logic, including neural network, the support vector machine (SVM) is also utilized as a classifier. For clustering purposes, LEACH protocol is presented to groups the nodes that consist of CH (cluster head) and CM (cluster manager) that used to send the packet between the nodes. To prevent the network from the DoS attack, OLSR routing protocol, and physical layer-based intrusion detection scheme (PL- IDS) and the "monitoring detection and rehabilitation" technique is presented. To automatically detect WSN attacks, Advanced Hybrid Intrusion Detection System (AHIDS), and to for justifying the effect of a smart gray hole attack, Mitigating the Gray hole Attack Mechanism (MGAM) implemented various special nodes called gray hole-intrusion detection system (G-IDS) nodes are presented. These security techniques using existing approaches and it's different applications and also various types of attacks that are possible on Mobile Adhoc Network.

2.3 RESEARCH GAP

After studying the past work performed by many researchers, a few points are drawn:

i. If the attacker node is far from the original node, the delay will increase.

ii. Binary classifiers such as SVM have been used to classify attacker nodes, but any binary classifier is more complex because they have merged attributes.

iii. Fuzzy logic is utilized as a classification technique, and using fuzzy logic to classify attacker nodes is a time-consuming process. Because, when fuzzy logic checks node attributes, calling the ruleset and calling process is very time-consuming.

iv. The existing work has used the DSR routing protocol but does not include the concept of trusted routing tables, and the search mechanism of the DSR routing protocol is very energy-intensive.

v. It can be seen from the investigation that the AODV routing protocol performs well in other routing technologies because the concept of trusted routing tables is adopted in the AODV routing protocol. Therefore, the search time of the next node in the path can be easily determined.

vi. In the existing work, due to the lack of a suitable classifier to classify better nodes for data transmission, the energy consumption rate is very high.

2.4 PROBLEM FORMULATION

MANET is a structured network that changes the position of a node while transmitting data. Any network in the world is designed to transmit data from one end to the other. The data transfer process requires the process of finding a route, so you need a position monitor on the network. Since all nodes are portable, it is difficult to save any folder if there is any network loss. When it comes to security risks, there are two possibilities in the network: one is that the attacker does not change its relative position. In this case, the entry is easy to track.

Mobile Ad hoc Network is a built-in network, where nodes change their location L as the time value changes. Any network in the world aims to transfer data from one end to the other. The process of finding a route is required because the data transfer process requires a location controller on the network. Because all nodes are portable, it is difficult to signal at any node if there is any network loss. From the security network, there are two types of technical networks, one of which is that the attacker does not change its relative position. It is easy to find traces of such intruders. The second type is when the attacker and the nodes that go into it are mobile and distributed. The network monitor finds itself very fussy when it comes to identifying intruders in such a situation.

The utilized routing mechanism in previous work is based on the searching strategy along with energy consumption is higher in data transmission, so it requires to be an improvement in routing protocols. There are various smart attackers among them DDoS is one that doesn't let the system feel that it is under danger or anything like that. The bundles are dropping ceaselessly by an interloper, and the system continues attempting to dissect what is happening. In this circumstance, an adjustment in the AI calculation would be favorable.

CHAPTER 3: OBJECTIVES

3.1 OBJECTIVES

1. To Trigger Multiple Blackhole attack, Grey Hole Attack and Selective packet Drop attack on MANET.

2. To analyze the performance of the network before and after triggering the attack of security.

3. To present a novel framework for intrusion detection in ad-hoc network to identify multiple Blackhole, Grey Hole, and Selective packet drop attacks.

4. To implement the proposed structure for interruption recognition in MANET and contrast the outcomes and existing systems as far as system boundaries like Throughput, Delay, Energy Consumption, and PDR.

3.2 HYPOTHESIS

There are two hypotheses of this research work, namely the null hypothesis and the alternative hypothesis as follows.

H0 (Null-Hypothesis): All the nodes are trustworthy and are not consuming any resources other than required

H1 (Alternative): All the nodes are not trusted worthy and maybe consuming resources more than required.

H1: The evaluation parameters evaluate the normal and intruded parameter evaluation, which must satisfy the designed fitness function.

SUMMARY

In the previous chapter, literature work & various gaps in the literature were discussed. Based on the research gaps, different objectives along with the aims of this research work are finalized here, in this particular chapter. This chapter covers the hypothesis and research objectives and the work performed to complete the objectives. Various issues and challenges are derived after the review of the literature in the previous chapter. These challenges helped in setting the objectives of the research work in this chapter. The next chapter covers the methodology used for achieving the objectives.

CHAPTER 4: METHODOLOGY

As studied in prior chapters, MANET suffers from different security attacks due to its mobile nature. Therefore, to analyze the performance of the MANET against different attacks, we first design a network with some dimensions. The designing process of network, with normal and affected nodes specifically, Blackhole attack, Grey Hole Attack (smart gray hole attack), and Selective packet Drop attacks, are discussed along with their pictorial representation. This chapter presented a mechanism to identify and remove the above three types of attacker nodes. The proposed scheme works as follows.

The foremost step of this research is to design a mobile ad hoc network with N number of nodes. The deployment process of malicious and genuine nodes is shown in the following section.

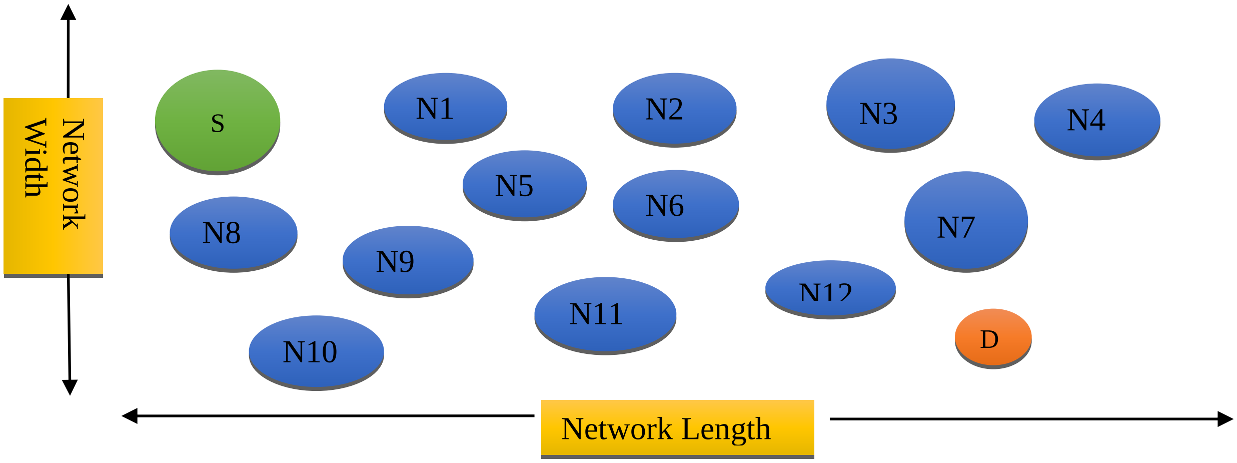


Figure 4.1 Create Network

Initially, the network area of particular length and width (1000×1000) is created, and then the nodes are deployed randomly by using the concept of coordinate geometry. An example of nodes deployed for 12 number of nodes is designed in MATLAB simulator.

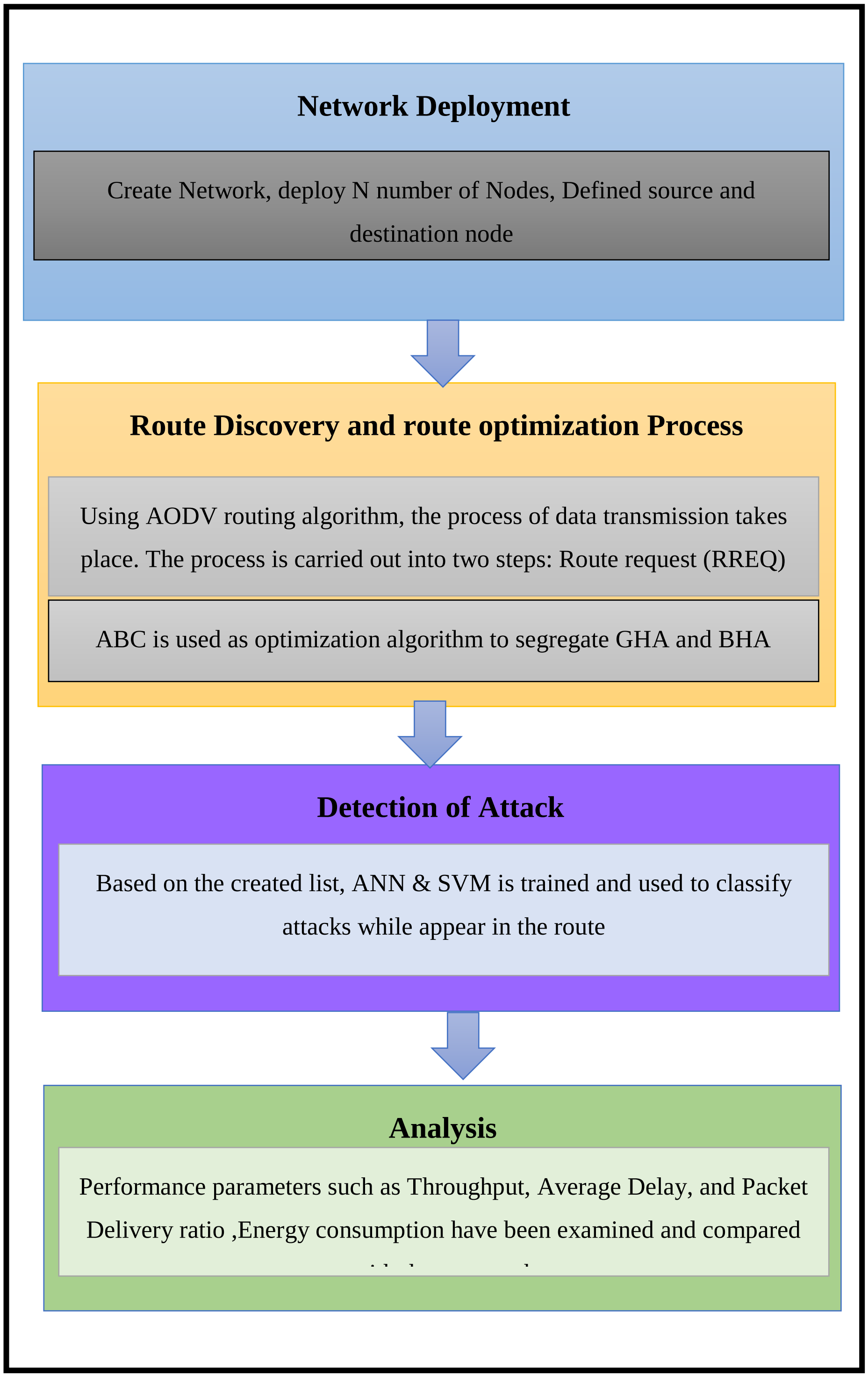

Network Deployment
Create Network, deploy N number of Nodes, Defined source and destination node
Route Discovery and route optimization Process
Using AODV routing algorithm, the process of data transmission takes place. The process is carried out into two steps: Route request (RREQ)
ABC is used as optimization algorithm to segregate GHA and BHA
Detection of Attack
Based on the created list, ANN & SVM is trained and used to classify attacks while appear in the route
Analysis
Performance parameters such as Throughput, Average Delay, and Packet Delivery ratio ,Energy consumption have been examined and compared

Figure 4.2 Flow Chart of Entire process

Following considerations are taken into account as listed in Table 4.1

Table 4.1 Ordinal Measures

Matrix	**Range**
Ranges of node	50 to 100
Region to communicate	1000 sq meter
Number of Packets	1000
Range of Coverage	Approx 25% of the previous location according to IEEE 802.11
Model Type	Heterogeneous

Algorithm 1: Set up as well as the deployment of the model

```
$Model_{Height} = 1000$
$Model_{Length} = 1000$
$For\ each\ mobile$ node $in\ the\ model$
$Initialize\ x\ and\ y\ locations\ of\ mobile\ nodes$
$Initial_{Bandwidth} = Associated_{Bandwidth}$
$Delay(In_{transmission}) = New(Delay_{Transmission})$
$Packet_{Dump} = Initialize$
```

```
$Deploy\ (\ Mobile\ node)$
$EndFor$
```

The structured system has thought about a heterogeneous domain with particular properties of nodes, as well as nodes are conveyed with various estimations of comparative qualities. Concerning a model, every node expends unmistakable vitality, or each system drops information error during correspondence, even the information is passed from the real nodes. In this chapter, the work has been examined under three different attacks, such as (i) Blackhole attack, (ii) Smart Grey Hole Attack, and (iii) Selective packet Drop attack. A node will dump more bundles under contortion, however, what might be the drop tally is obscure, and henceforth the engineering has set arbitrary conduct for the packet dumps and drops. The calculation "Ascertain Coverage" figures the correspondence scope of the nodes.

```
$\boldsymbol{Algorithm\ 2 : Calculate\ Coverage}\ (\,)$
$Input :\ NodeList$
$Coverage = [\,]$
$For_{every} node in Nodes$
$For_{every} node1\ inNodes$
$If node\ != node1$
$dist =\ ⟦sqrt\left(\left(X_{loc}(node) - X_{loc}(node1)\right)⟧^2 + \left(Y_{loc}(node) - Y_{loc}(node1)\right)^2\right)$
$Coverage\ (node, node1) = Node(id_{list}\ )\ (node1)$
$End\ for$
$End\ for$
$End\ Algorithm$
```

Using the above-mentioned algorithm, the distance through one node to another node, such as N1 to N2 is calculated through the formula of distance. If the communicating node lies in the coverage range defined by 802.11, then it can take place in the communication process. The coverage is described through empty parenthesis. The communication process is depicted in figure 4.3. Here, the source node is represented by letter S, and letter D corresponds to the destination node. Now, let the node S wants to establish a communication with node D. To make communication successful, the data has to be transmitted from different intermediate nodes, and this process is possible by using the routing algorithm. In MANET, the transmission of data is done using specifically three kinds of routing processes, namely, proactive, reactive, and hybrid. In this research, we have used AODV as a reactive routing to form a route between the source (S) and the destination node (D). The main advantage of this type of routing protocol is that the route is created only when the node needs to communicate, which saves time as well as increase the speed of data transmission as the route information is carried out in the routing table instead of the header as in the proactive routing. Also, this protocol is more secure compares to the pro-active routing protocol. The process of AODV is given in figure 4.3.

4.1 ROUTE DISCOVERY PROCESS

The AODV routing protocol is utilized to establish a route. AODV is a reactive routing protocol where the path is constructed while it requires to transmit the data through the node. This routing strategy is working specifically in two stages: (a) request for route and (b) discovery of route. Initially, the request for the route is sent through transmitting node across its range of coverage in MANET. After receiving the packet of route request by adjacent node, it stores the address for identification in its route list table. The route list table consists of the following information:

- Address of Destination Node.
- Next, hop of the source node (S) or intermediate nodes (N1, N2, N3……N12).
- A number of hop count.

- The sequence number of the destination node (D).
- Active neighbors of the route.
- Termination time for this route table entry.

4.1.1 Control Packets

Mainly four messages are being used by the AODV routing protocol and are employed to control the process of route discovery along with route maintenance.

i. Route Request Message (RREQ): At the initial stage, when the source node (S) wants to communicate with the destination node (D) and finds no prior entry in the routing table from the (S to D) a control packet is known by the name Route Request message (RREQ); is broadcasted by the node S. the RREQ consists the fields as listed in Table 4.2.

Table 4.2 Format of RREQ message

Source Address
Request ID
Source Sequence No
Destination Address
Destination Sequence No
Hop Count

Each time the source node broadcast a new RREQ message, the request ID is incremented by one. The RREQ, in conjunction with a request ID, form a unique number and moves from node to node. Every node has to record the address of each node from which it received the data. This procedure is known by the Reverse Path Setup (RPS).

ii. Route Reply Message (RREP): If the node is found as an accurate destination node, it sends back a route reply message to indicate its appearance towards the source node. The format used by RREP is listed in Table 4.3.

Table 4.3 RREQ Format

Source Address
Destination Address
Destination Sequence No
Hop Count
Life Time

During the RREQ message broadcasting, each node in between the source node and the destination node record this message. Therefore, when the destination node is identified, the RREP message sends back to the source node through these nodes, and hence no more broadcast is needed. The process of route discovery is discussed in the following section.

4.1.2 Route Discovery

The AODV routing protocol is utilized to establish a route. AODV is a reactive routing protocol in which route is established only when it requires to transmit the data through a node.

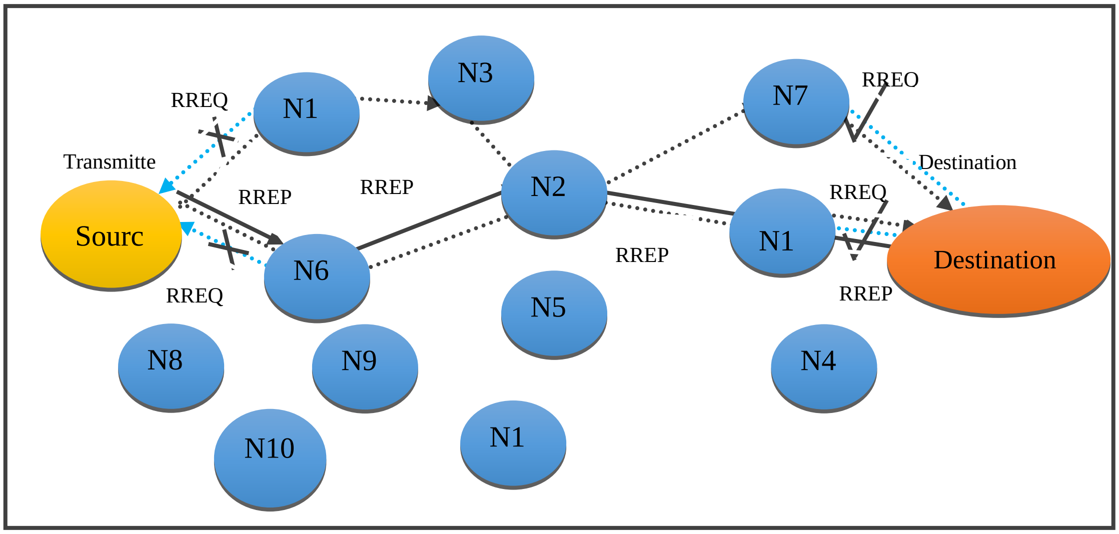


Figure 4.3 Route Discovery Process using (AODV)

This routing strategy is working specifically in two stages: (a) Request for route and (b) Discovery of the route. Initially, the request for the route is sent through transmitting node across its range of coverage in MANET. After receiving the packet of route request by adjacent node, it stores the address for identification in its route list table. If the address is not matched with the adjacent node, then it forwards the request packet to the adjacent node along with an acknowledgment in terms of reply packet send to the transmitter node that means the present node is not considered as a destination. In this way, the packets reached its target node using a number of possible paths. In the AODV protocol, one of the best suitable routes is considered for data transmission among multiple possible routes based on distance measurement. After receiving the data packet, the destination node sends back a route response packet towards the transmitting node through the shortest path. The process to discover route is given in figure 4.3, represents the methodology of route creation using AODV. The blue dotted line represents the Route Request send by the nearby node. The dotted black color line represents the possible route, whereas the solid clack color line represents the appropriate route formed between the source and the destination node. The cross clicks represent that the nods that receive the RREQ packet are not the destination node. The right-click represents that the desired destination is obtained, and it responds with the RREP packet.

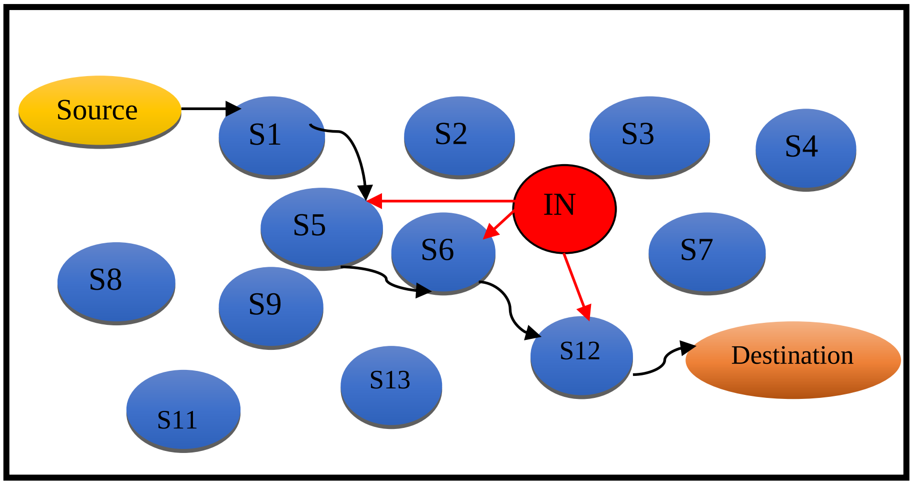


Figure 4.4 Network with Blackhole / Gray hole Attack

After the formation of the route, data transmission is started.

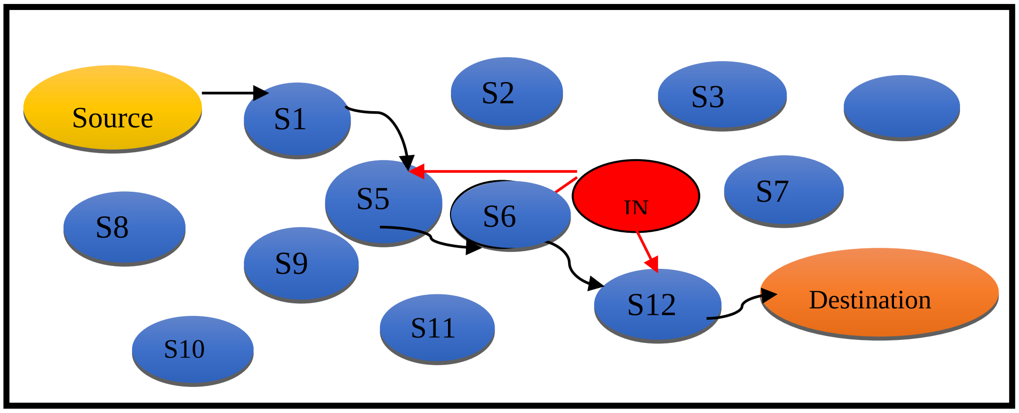


Figure 4.5 Affected Node

The case when an attacker exists in the network is indicated by the red circle. This attacker node affects the nodes that appear in the route that is the server N5, N6, and N12, respectively. The throughput is deceased through the black hole attacker initiates the dumping of the data packets. The nodes that are affected are represented through grey color, as represented in figure 4.5.

4.2 TRIGGERING MECHANISM OF MULTIPLE ATTACKS

This section highlights the triggering mechanism of the smart gray hole, black hole, and selective packet drop attack one by one. Triggering is the most commonly used factor in MANET that is utilized to measure the distance of sending data node to gateways. The distance is measured in terms of the number of hop counts. After receiving the data, the gateway has decided to which node the data has to be forwarded. The triggering process in the presence of different attacks is discussed in the following section.

4.2.1 Triggering Process of Smart Grey hole detection Node

In this section, the process of transmitting data to the genuine node instead of a grey hole attacker node is discussed. The scenario for the smart GHA node is depicted in figure 4.6 as well as in figure 4.7 correspondingly.

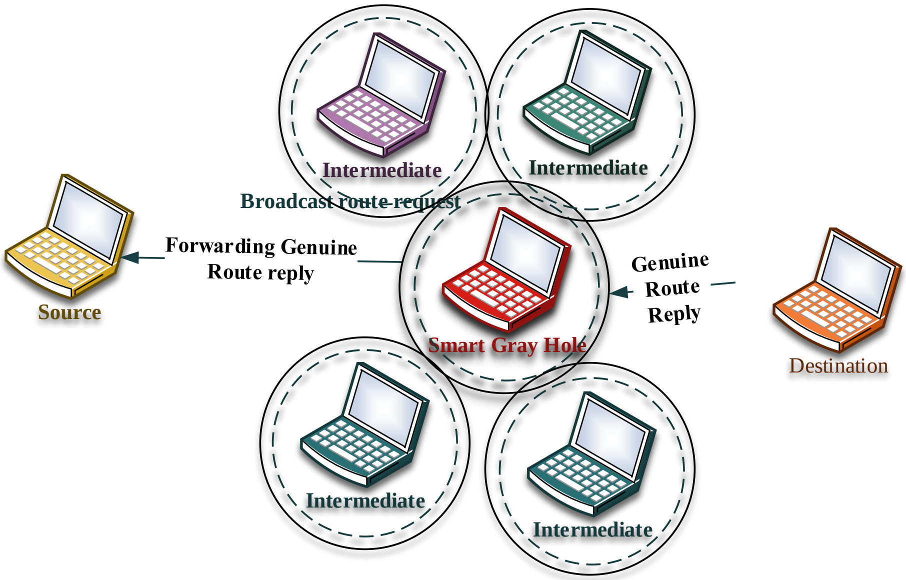


Figure 4.6 Participation of Smart Gray hole Attack as a Normal Node during Route Discovery process

Figure 4.6 represents the involvement of the GHA node during the route discovery process. The GHA node behaves like a normal node and drops the data traffic. Also, the scenario of partial packet drop is shown in Figure 4.7.

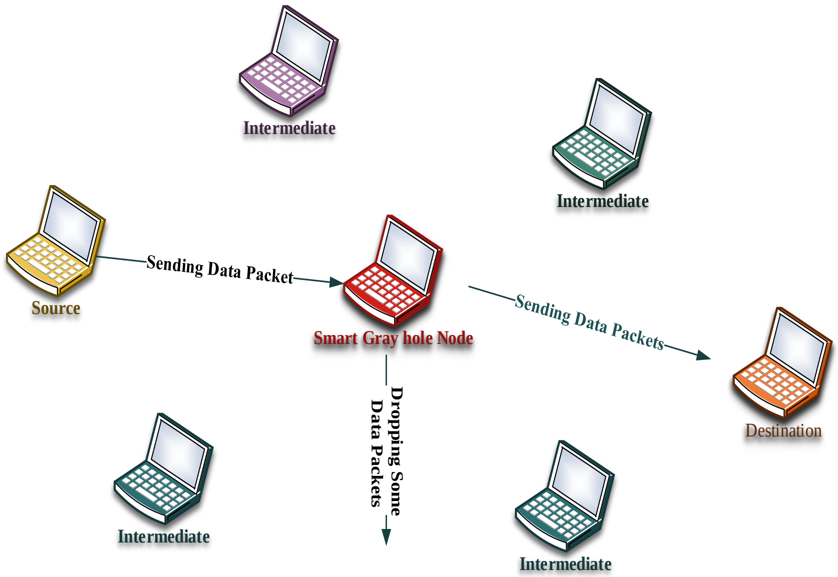


Figure 4.7 Partial packet Drop by Smart Gray Hole Attack

The detection process of the smart gray hole attack is depicted in figure 4.8

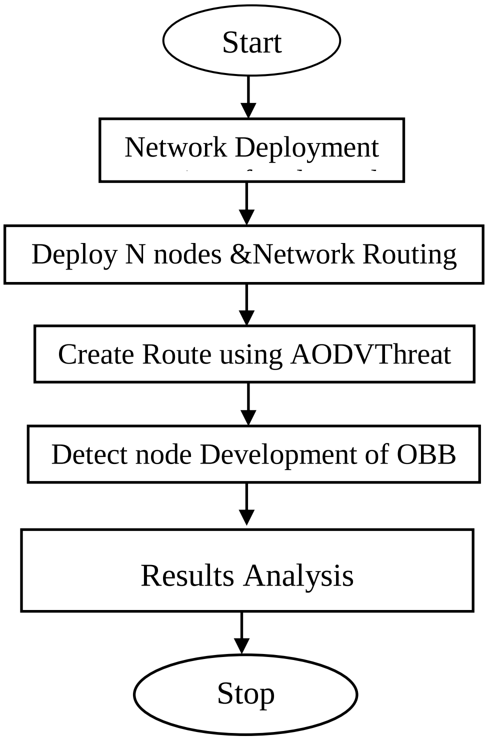

Start
Network Deployment
Deploy N nodes &Network Routing
Create Route using AODVThreat
Detect node Development of OBB
Results Analysis
Stop

Figure 4.8 Detection process of Gray hole Attack

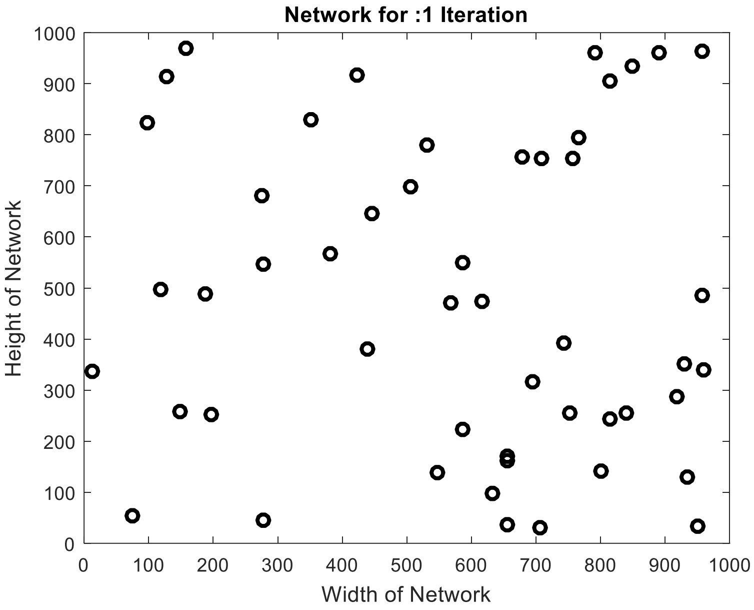


Figure 4.9Nodes Deployment

Initially, an area of particular length and width is designed, and nodes are deployed, as shown in Figure 4.9, on a random basis. After that, nodes are labeled by names like N1, N2, N3,………………N50, as shown in Figure 4.10.

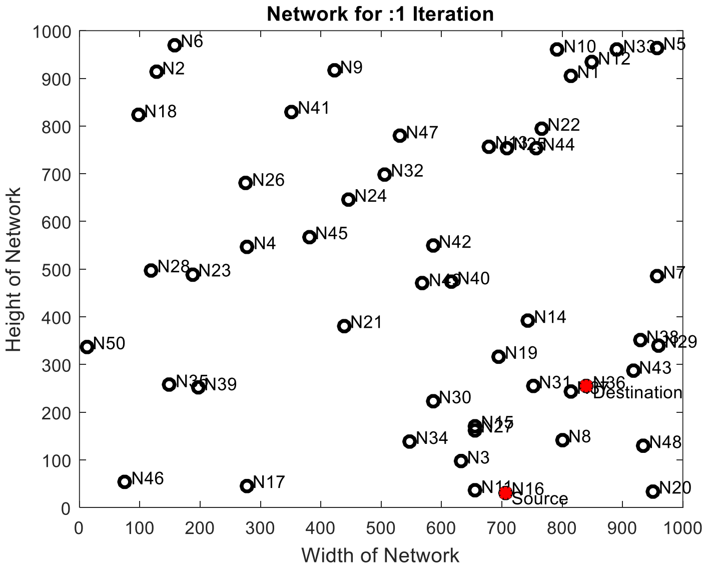


Figure 4.10 Nodes Labelling

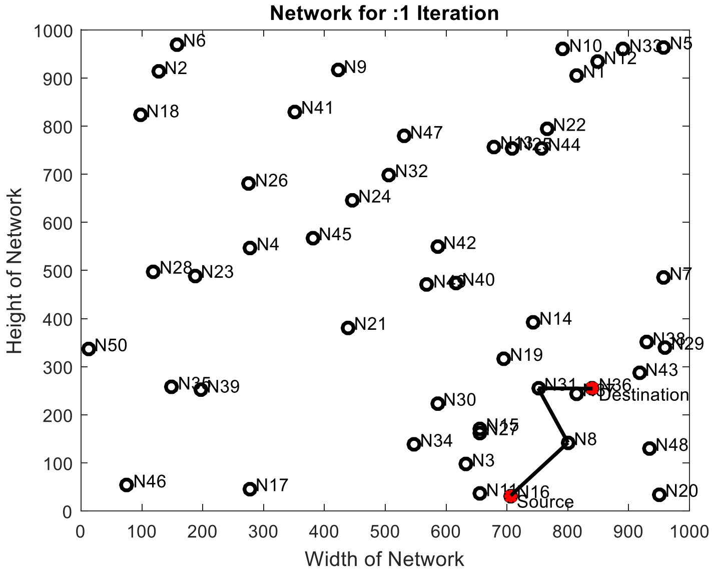


Figure 4.11Route Creation

The route formed using AODV is shown in Figure 4.11. In the given scenario, node N16 is a source node, and N36 is a destination node. Node N16 forward data to its nearby node, which is also near to the destination node N36. The AODV routing protocol follows a strategy like forwarding data that node, which is close to the destination node.

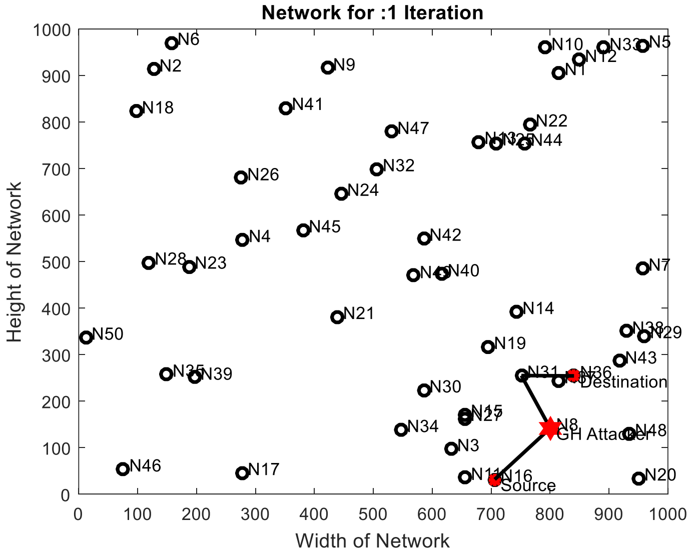


Figure 4.12 GHA

The node (N8), is a GH node, which drops the packet. To detect a node as a Grey hole, a threshold value is defined for the RREP sequence number. In case if the value is higher than the defined threshold, then the node is considered as a GHA node otherwise, considered as a healthy node. The detected GH node is represented by the red star. If the node properties satisfy the fitness function, then the node is considered as a normal node otherwise considered as a GHA node.

4.3 TRIGGERING PROCESS OF BLACKHOLE DETECTION NODE

The attack of the black hole is equivalent to the grey hole i.e. dead star that can consume energy along with matters. In a similar way, an affected node drops that data packets that are passed through it. The drawback of the route discovery process of reactive routing protocols is used in this attack b sending a fast false route response signal. It's difficult to have the shortest and fastest route to reach the destination, however, it does not have a path to the destination. As depicted in figure 4.13, the path request packet is transferred through source node(S) with the aim of path establishment as well as the fastest way to reach the destination node (D). After getting the RREQ packet, the affected node i.e. M quickly transfers the false RREP packet to the source node for pretending that it having the shortest path to reach up to the destination. When the source node gets this forged RREP packet, it discards other RREP packets and starts transmitting data packets that the node M will drop after it gets them.

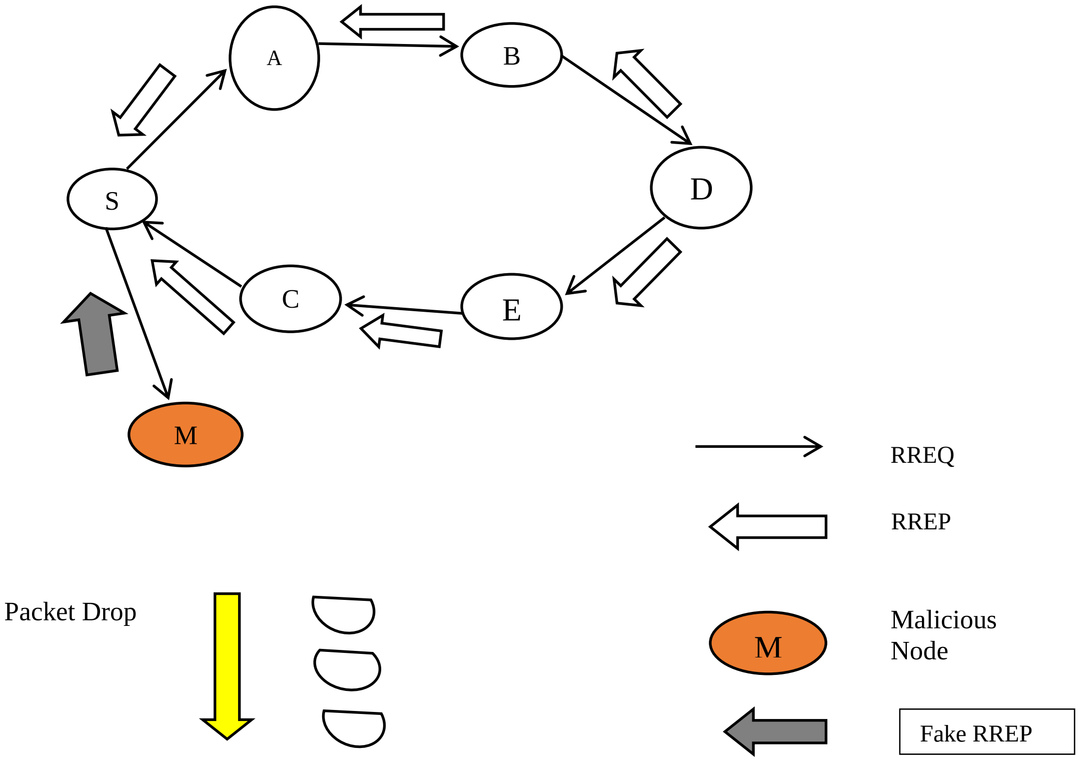


Figure 4.13 Black Hole Attack

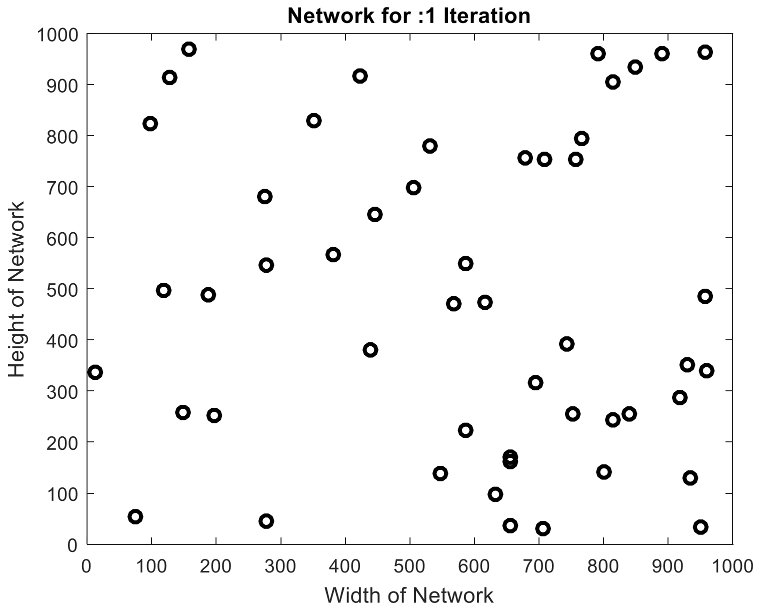


Figure 4.14Nodes Deployment

Initially, an area of particular length and width is designed, and nodes are deployed, as shown in Figure 4.14, on a random basis. After that, nodes are labeled by names like N1, N2, N3,………………N50, as shown in Figure 4.15.

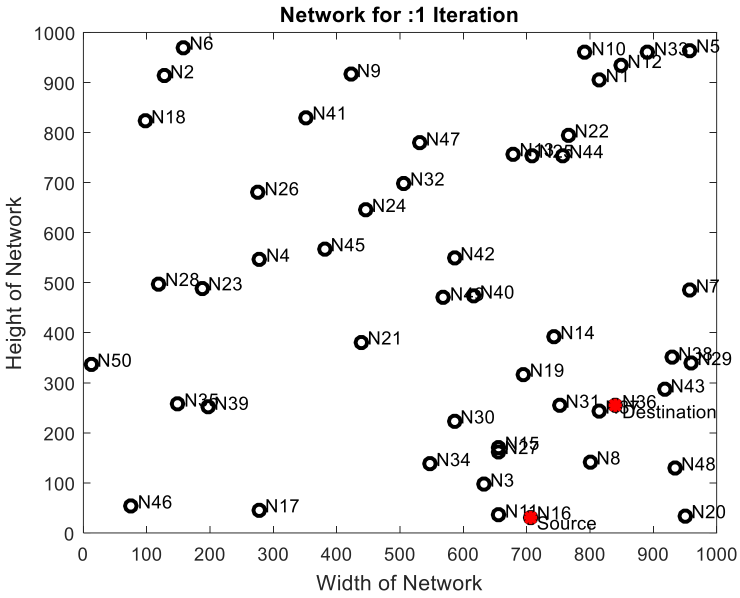


Figure 4.15 Nodes Labelling

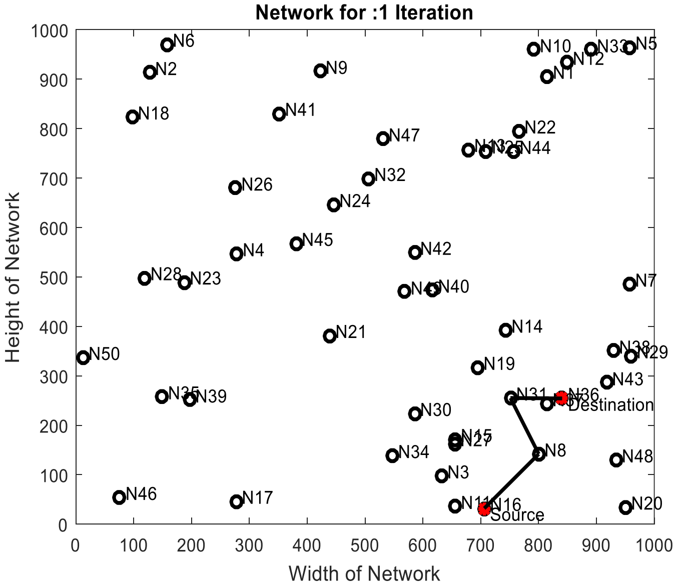


Figure 4.16 Route Creation

The route formed using AODV is shown in Figure 4.16. In the given scenario, node N16 is a source node, and N36 is a destination node. Node N16 forward data to its nearby node, which is also near to the destination node N36. The AODV routing protocol follows a strategy like forwarding data that node, which is close to the destination node.

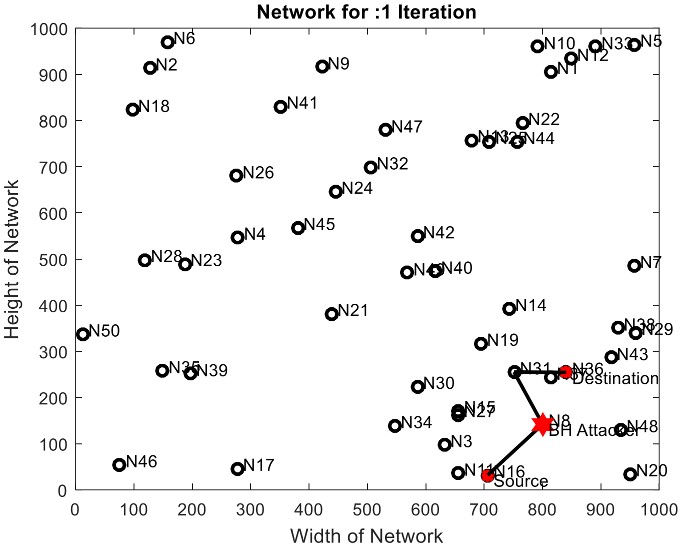


Figure 4.17Occurrence of BHA Node

To detect a node as a black hole, a threshold value is defined for the RREP sequence number. In case if the value is higher than the defined threshold, then the node is considered as BHA node otherwise, considered as a healthy node. The detected BH node is represented by the red star in Figure 4.17. If the node is detected as a BH node, then it is added to the BH list. So that in the future, if any node appears having properties similar to those already stored in the list, then it is detected at the initial stage and also increases the speed of detection.

4.4 TRIGGERING PROCESS OF SELECTIVE PACKET DROP

Selective Packet drop attack (SPDA) is considered as the type of denial of service (DoS) attack. This type of attack is launched on the forward phase, so it's difficult to segregate and considerably it is very complex. To perform this attack is very easy but its detection is challenging. The node drops by selfish node arein different ways. The packet dropping has been done only to save resources not to damage any other nodes. Some missions of applications are damaged by selective forwarding attacks. In such kinds of attacks, the malicious nodes acts as normal nodes most of the time still selectively drop sensitive packets like packet coverage, the movement of the differing forces. This selective dropping is difficult to identify. Countermeasures to selective forwarding attacks cannot recognize malicious nodes or need time synchronization.

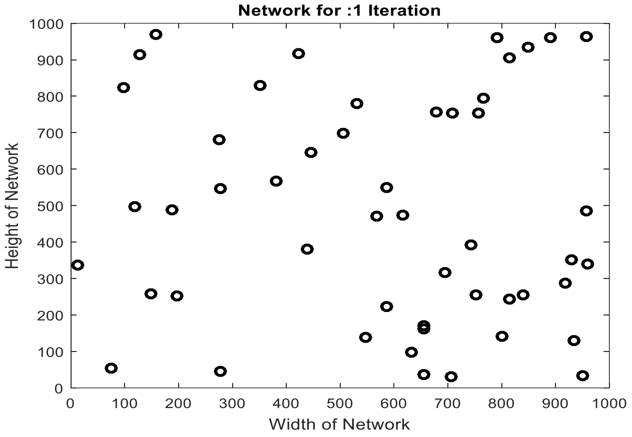


Figure 4.18Nodes Deployment

Initially, an area of particular length and width is designed, and nodes are deployed, as shown in Figure 4.18 on a random basis. After that, nodes are labeled by names like N1, N2, N3,………………N50, as shown in Figure 4.19.

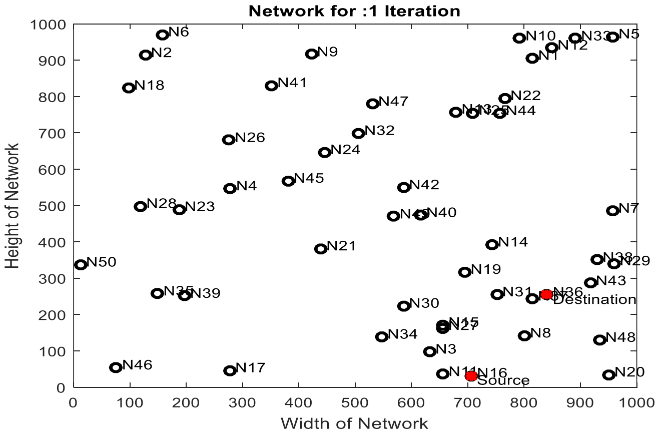


Figure 4.19 Nodes Labelling

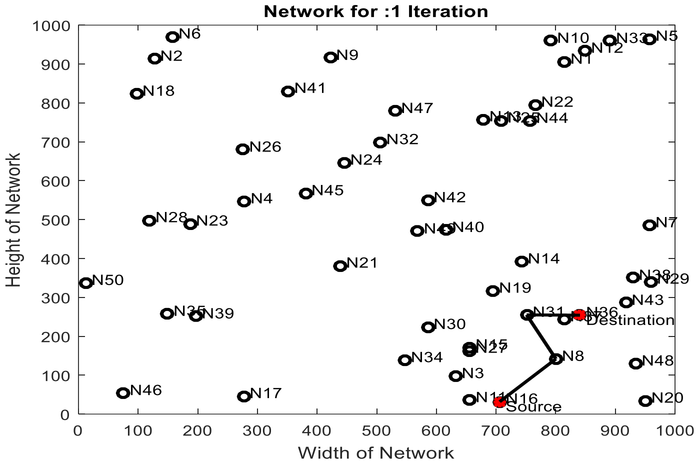


Figure 4.20 Route Creation

The route formed using AODV is shown in Figure 4.20. In the given scenario, node N16 is a source node, and N36 is a destination node. Node N16 forward data to its nearby node, which is also near to the destination node N36. The AODV routing protocol follows strategy like forwarding data that node, which is close to the destination node.

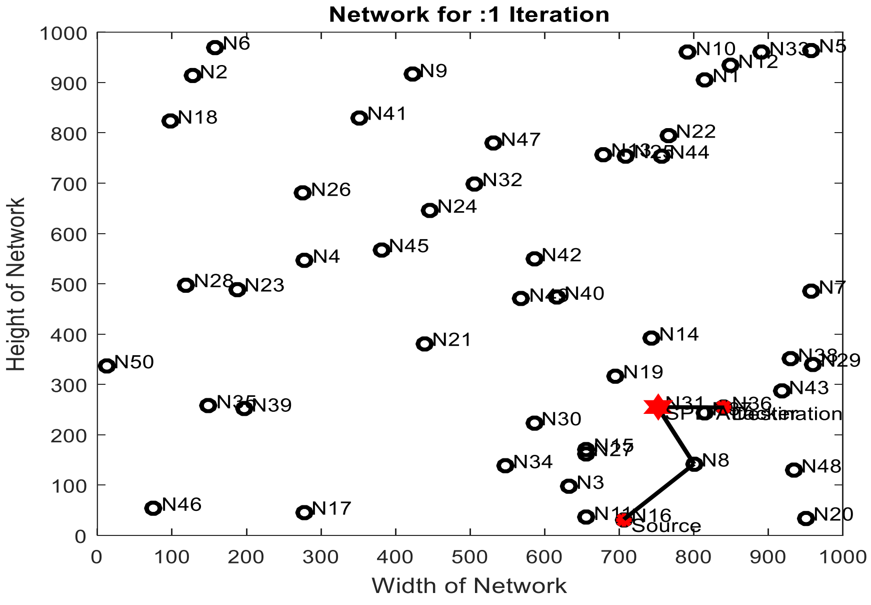


Figure 4.21 Occurrence of Selective Packet drop Attack

In this type of attack, attacker nodes do not drop all packets that they received from the source node. The appearance of selective packet drop is shown in Figure 4.21.

Now next step is to design a new routing protocol that can protect the network from these attacks at the same time. Now the next step is to analyze the network performance before and after triggering the security attacks.

To prevent network against multiple attacks, swarm inspired optimization technique named as Artificial Bee Colony (ABC) with Artificial Neural Network (ANN) is used in combination. The detailed description of both is provided below.

SUMMARY

In the previous chapter, the aim and different objectives of the research work were focussed. This chapter covers the different methodologies used for achieving the proposed research work. This chapter presented a mechanism to trigger multiple attacks on the network and compare the values of parameters after and before the attacks. This chapter deals with the approaches and components used in the research. All the technique relating to the presented scheme is demonstrated through algorithms as well as flowcharts. The next chapter covers the different algorithms for isolating multiple attacks in MANET.

CHAPTER 5: AN OPTIMAL SECURITY MECHANISM TO PREVENT MULTI-THREAT IN MANET USING BEE ALGORITHM

5.1 INTRODUCTION

MANETs exceptional highlights permit clients to get to the advantages gave by the system. Be that as it may, getting to specific offices as high versatility consequently makes an issue of flimsy directing which prompts parcel drops. To fix this issue, this work considers the circumstance of parcel dumping under standard just as twisting mode. In this work have concentrated on the dark gap assault alongside particular bundle drop assault and having danger anticipation system has been introduced. The total part is separated into three casings, for example, utilize the sending model, the hugeness of interruption alongside its counteraction, and enlistment for novel hub through the introduction, for example, Chebyshev strategy. The structure for counteraction has been built by using swarm intelligence (SI). To distinguish the influenced course, the Optimal Bee Behavior (OBB) calculation has been used inspired by Artificial Bee Colony (ABC). The particular boundaries have been processed just as examined to be specific vitality utilization, Delay, PDR and Throughput

5.2 RELATED WORK

MANET is considered as the network of nodes that have no infrastructure linked. Nodes serving like a router along with a transferring of the host; the details from one node to the next. Communication protocols modify as nodes are highly mobile. However, for the MANETS a unicast routing protocol has been developed through a constructive routing scheme. The major disadvantage of the proposed method would be that the determination of the throughput for a massive number of solutions becomes inefficient. In addition, this mechanism has not been able to handle the problem of dumping packets.

By which this methodology dependent on homomorphism has been utilized in the scholarly works for the location of the malevolent assault. The separation vector has additionally been used to get the separation among hubs and to prevent dumping of the packet. Security is another significant perspective which requires a similar concern to improve productivity

S. N. Mohammad et.have utilized micro-techniques to improve the level of security. The system can keep secured from the BHA by utilizing a key-management scheme that gives the MANET i.e.an improved level of security.

Nevertheless, the dissemination of private key utilizes the network's wide energy that hampers network efficiency. In addition, the false idea was implemented to mislead the attackers, which enables the loss of the packets. However, the key challenge of this work is that fraudulent communications enhance energy usage, as well as efficiency decreases as security is also considered due to an attack by intruders. For this reason, a framework based on fuzzy must be adopted for improvement of the security level. The efficiency of the system changes according to the distribution of the packets among nodes. The outcomes are then thought about through the AODV protocol. Nonetheless, the PDR is as yet not feasible alongside an opportunity to reproduce is higher limits the created approach. The possibility of secrecy has been utilized to plan the bundles. In past investigations, in this manner, a scheduling algorithm has been proposed to dissect the traffic.

To increase the rate of detection the fake source localization strategy has been presented. The optimized pathways have been identified through managing the packets through the introduced approach. The false packets are utilized to make confusion in the built-in intruders and false routes. In addition, packets have transferred from main routes. The false routes are intended for the attacker for using this route, and false notifications enhance, that increasing the energy consumption.

The increased consumption leads to a reduction in system performance. Energy consumption is identified by authors in MANET as an essential determinant. The trust-based system guarantees network security and improves network performance. Consequently, the trust-based scheme for the identification of a black hole attack has been presented in previous research. The ABC optimization algorithm is utilized to boost effectiveness, however, such a method also suffering from a deficiency of classifiers. The value of fitness utilized for optimization produces innovative ideas rather than it becomes difficult to classify such solutions.

So using the authentication mechanism, the Fuzzy-based technologies offer secure multicast routing. The knowledge of the existence of misbehaving nodes has mitigated the active and passive attacks.

The previously proposed un-certification routing confirms greater authenticity as well as reduces the utilized energy. The utilized security scheme included here, is now as days need the adjustment so there's more data difficulty that further decreases network performance.

The presented system serves as protection by authenticating the structure using a pseudo-random feature that also builds the process complex. Therefore, it used as a reactive strategy for protection from malicious attacks. The structure founded to identify the intrusion inside the network. Such a presented system doesn't achieve the required throughput and delay. In this work due to the utilization of optimizer, the rate of detection has been improved. The authors are proposing an increase in lifetime strategies that use the LEACH protocol to increase network performance. Highly focused on improving lifespan along with lower usage of energy. Still in this work is not sufficient for energy saving because a higher amount of energies are dispersed whenever the transmission of data is performed from initial to the goal node. Accordingly, researchers tried to increase the durability of the battery utilizing metaheuristic methods including such ant colony optimization to detect the route having shortest distance through starting to target node.

It is helpful into power saver as just an improved framework must be integrated, and digital signatures to minimize the black hole attack.

The outcomes from the recreation showed that the proposed study requires less power and is more successful as compared to AODV routing. Be that as it may, the primary disadvantage is that routing identification enhances the heap as most extreme is the measure of offenders identified toward such path. Along these lines, the consequences of this part have been examined in the outcomes to decide the exhibition of the presented approach.

5.3 PROPOSED WORK

The developed framework of this work is conceived into frames. The very first frame is intended to implement and design the Network. Its next frame reveals what the intrusions mean.

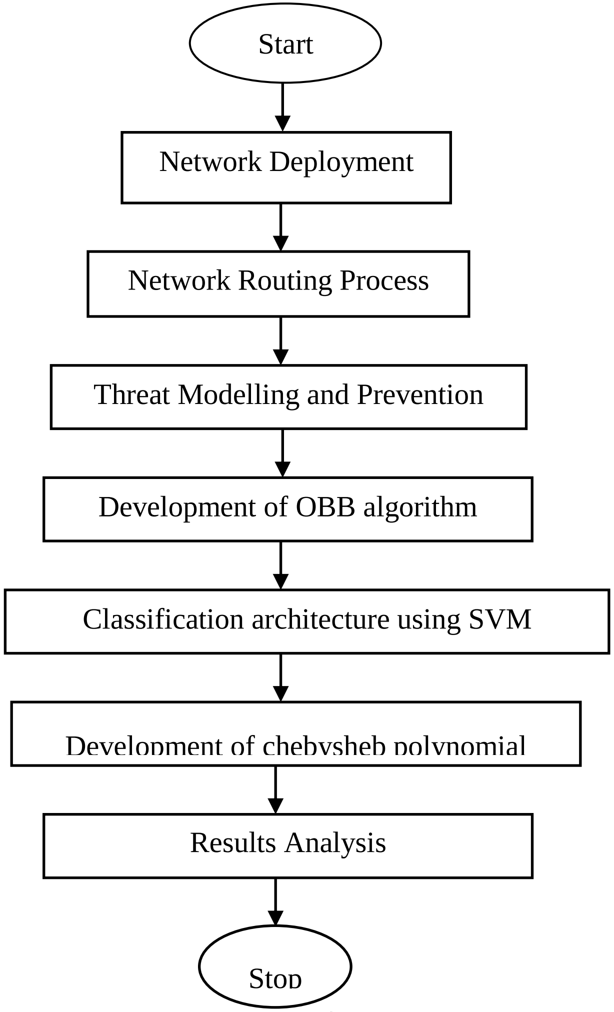

Start
Network Deployment
Network Routing Process
Threat Modelling and Prevention
Development of OBB algorithm
Classification architecture using SVM
Development of chebysheb polynomial
Results Analysis
Stop

Figure 5.1 Flowchart of the proposed approach

The approach also covers the implementation of the platform for avoidance, which includes the combination of the optimizer as well as the classification method.

Deploying a method of interpolation to introduce a new node in the field is involved in the third frame. Figure 5.1 depicts the schematic working flowchart. To achieve objective outcomes the numerous parts have been interconnected.

5.3.1 Network Deployment

In table 5.1 the given the ordinal measures that are the group for network deployment

Table5.1.Ordinal Measures

Ranges of nodes	50 to 100
Area to communicate	1000 × 1000 m
Range of coverage	In the significant amount of 25% according to IEEE 802.11
Number of Packets	1000
Model Type	Heterogeneity

Pseudocode: Setup as well as the deployment of a model

```
$Model_{Height} = 1000$

$Model_{Length} = 1000$

$For\ eachmobil$e node $inthemodel$

$Initializexandylocationsofmobile\ nodes$
```

```
$Initial_{Bandwidth} \; = Associated_{Bandwidth}$
$Delay(In_{transmission}) \; = New(\,Delay_{Transmission}\,)$
$Packet_{Dump} = Initialize$
$Deploy\ (\,Mobile\,node)$
$EndFor$
```

In this presented framework, considered a heterogeneous environment along with properties of distinct nodes and the deployment of that nodes are done with distinct values in similar characteristics.As instance the node (n1), initially composed of 70% combining energy however n2 have 65% of associated energy in the same simulation.

$\boldsymbol{Algorithm\ 1}$: $\boldsymbol{CalculateCoverage}\ (\,)$

```
$Input\ :\ NodeList$
$Coverage = [\,]$
$For_{every} nodeinNodes$
    $For_{every} node1\ inNodes$
        $Ifnode\ != node1$
            $dist = \ \llbracket sqrt\Big(\big(X_{loc}(node) - X_{loc}(node1)\big)\rrbracket^2 + \big(Y_{loc}(node) - Y_{loc}(node1)\big)^2)$
            $Coverage\ (node, node1) = Node(id_{list}\ )\ (node1)$
    $Endfor$
$Endfor$
$EndAlgorithm$
```

The calculated coverage determines the distance from one node to another i.e. $X_1\ to\ X_2$ by utilizing distance formula. If those nodes are present in the remote area described by 802.11 which used to communicate with different nodes. The coverage of the node is initiated through empty parentheses. First of all the nodes are initialized at node -1 as defined in the implemented strategy. As depicted in figure 5.2 the process of communication along with the outcome of given algorithm 1. The route finding process after determining the coverage is provided below;

Algorithm 2: $\boldsymbol{TheRoute\ definition\ (n, Coverage)}$

```
$Input: Source\ , Destination$
$Output\ :\ Route$
$Route(1)\ =\ Source$
$Temp_{Source}\ =\ Source;$
$Source\_Coverage\ =\ Coverage(\ Temp_{Source});$
$Find(Source_{Coverage}\ , Destination\ )$
$If Found\ , AddDestinationtoPath$
$Else$
$Temp_{Source}\ =\ Source\_Coverage\ .Nearest_{Node}$
$AddTemp_{Source}toRoute$
```

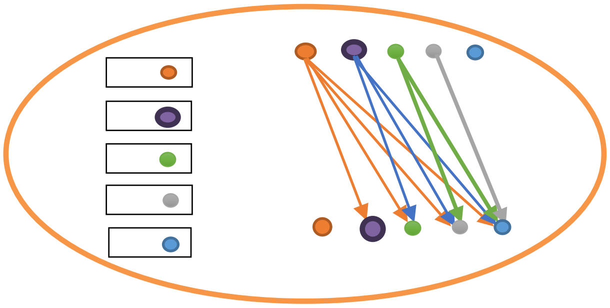


Figure 5.2 Determination of coverage

To filter out the node that lies in the coverage limit of the source node through utilizing source along with destination node in algorithm 2. If a target node is identified directly, no further route is needed as well as data transfer occurs, the destination is identified within the coverage limit. In other cases the adjacent nodes from the list of source coverage serve like the ad-hoc source then the cycle continues to reached the endpoint.

After completing the process of route identification the data needs to be transferred as well as modeling of threat along with prevention take place.

5.3.2 The Threat Modelling and Prevention

If the transmission of data is successfully enabled, the system can be suffering from security threats with or without it. Two separate attacks were considered in the proposed model named as BHA and SPDA. In the case of a network is comes inside the attack, its impact will start to appear. The architecture of prevention utilizes a two-pronged detection including prevention system. The presented mechanism can understand the importance of nodes, so the nodes are not able to directly identified as an attacker. In this way first of all is to define the path of the entire simulation affected by it. The OBB optimization approach is inspired by the ABC optimization approach is designed and implemented in this presented scheme to identify the route that is affected. The OBB has several benefits as it helps to reduce energy usage, improves optimization as well as minimizes delay too. The suggested technique has also the ability to reduces the overhead imposed in the system of packet delivery that enhances the throughput rate. Basically, OBB can be categorized into three types such as acting bees, monitoring bees along with group bees. The working strategy of these bees is distinct fro another one and here one last bee is also present named as queen bee. The process of monitoring taken place through these bees. The monitoring bees have taken care of the foods that take by acting been through changes in traveling time. If acting bees are able to bring food for monitoring bees then these bees enable the acting bee for searching the food in next time throughput down the food.

$Algorithm$ 3: $OptimalBeeBehaviour$

```
$Input: Simulation_{Routes},$
$Energy\_Consumption\_Route$
$Bee_{Food_{Deposits}} = Energy_{Consumption_{Route}} ForeveryRouteinSimulation_{Route}$
$OBB_{Population} = Bee_{Food_{Deposit}}.Element_{Count};$
```

```
5. $ForeveryBeeinOBB_{Population}Acting_{Bee} = OBB.Population.Bee$
6. $Forthenexttwobees, BeeFoodispreserved.$
7. $GHB.Threshold = Mean( Acting.Bees); Traveltime =$
   $RandomTravelTime.$
8. $IfGHB.threhold.travel_{time} >$
   $Acting_{Bee}Preserve_{Route}ElseSuspectRoute ++$
9. $AppendRoutevaluetoSuspected_{Route};$
```

The faulty routes are provided by the output of OBB that is further passed to the technique of machine learning named as; support vector machine, this classifier can classify the data by behaviors as well as nature. The basic structure of SVM utilized two certain parameters for input. The consumption of bandwidth is considered as the first parameter for every node and the second parameter is packet dump in supposed nodes. The network retains the success of packets corresponds to each route as well as a node. The outputs of the SVM are represented in figure 5.3.

To recognize the novel node in a region through chebyshev method is included in the third part. This method is mathematically explained as;

$$Z_m(y) = Cos[m \arccos(y)] \qquad (5.1)$$

Here Z_m denotes the polynomial with degree m.

The Chebyshev polynomial weights by which its orthogonal behavior is detected $v(y) = (1 - y^2)^{-1/2}$in the ranges of $(-1\ to 1)$. To identify a novel node for entering into a region, the number of variables has been utilized. To compute the detection rate the different order of interpretation has consumed. Apart from this the parameters like (s, t) than interval is managed through modifying variables such as $y \to \frac{1}{2}[(t - s)y + s + t]$.

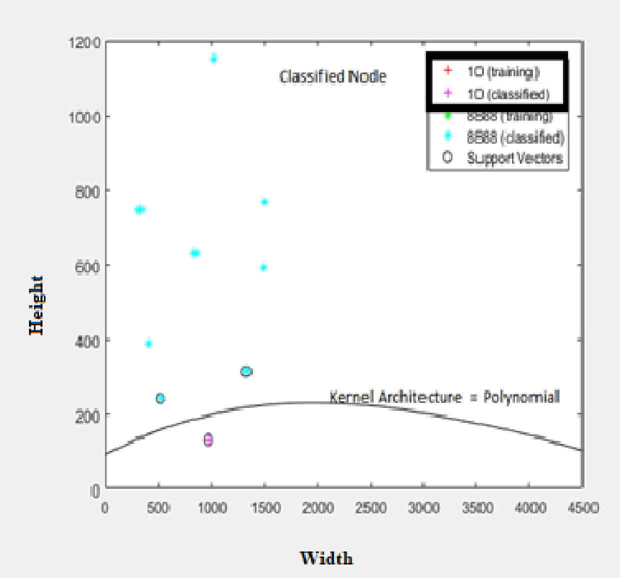


Figure 5.3Classification Architecture

In case of first-order or node the node can be represented in the form of the polynomial for

registering purpose of node is:

$$Z_0(y) = Cos(0) = 1 \qquad (5.2)$$

In similar way to register the 2nd node, the obtained equation is given below;

$$Z_1(y) = Cos(\arccos(1)) = y \qquad (5.3)$$

Algorithm4: **ChebyshevPolynomial**

```
If order=2;   // Order of interpolation
$\mathrm{My}_{\mathrm{VALUE}} = [\ ]$  // initialization of the empty key values
For $i = 1{:}3$   // For 3 vehicles
$\mathrm{counter} = 1;$
$\mathrm{Current}_1$=$\mathrm{Node}_{\mathrm{ID}_\mathrm{I}}$ // Taking the first node as an initial reference
$for\ j = 1; vehicles$
Curr=$\mathrm{Vehicles}_\mathrm{j}$; //for every interpolation, there must be 2- nodes are left
If Curr1~=Curr   // If nodes are not the same
Rest (counter) =curr;
```

```
Counter=counter+1;
End If
End for
Calculate Cheb
$\text{Shared}_{\text{key}} = \text{Share}_{\text{Current}_1} \times \text{My}_{\text{value}}[\text{i}]$
End for
```

In a particular case, if shares result in network key then nodes are enabled to be a part of the network otherwise, it is thrown away.

SUMMARY

The previous chapter covers the different methodologies used for achieving the proposed research work. The current chapter presented the threat as well as the architecture of prevention for transmission of a safe packet in MANET. Here the architecture identifies the affected node through saving the recent nodes through an optimizer that based on SI. The OBBtechnique is utilized for the identification of an affected system that can be considered as input to the SVM. The related work done by a number of scholars as well as researchers in this field of work has been also included here. The next chapter covers to distinguish the Blackhole node and grey hole node and divert the route through the protected node utilizing an altered AODV routing protocol.

CHAPTER 6: MITIGATION OF BLACK HOLE AND GREY HOLE ATTACK USING SWARM INSPIRED ALGORITHM WITH ARTIFICIAL NEURAL NETWORK

6.1 INTRODUCTION

Wireless technology is the most recent advancements in the versatile article, has prompted a MANET, which is an assortment of portable hubs that are speaking with one another without requiring any fixed framework. Because of the dynamic nature with a decentralized framework, these systems are powerless to various assaults, for example, Black Hole Attack (BHA), Smart gray hole attack (GHA), Sink Hole Attack (SHA) and some more. A few scientists have worked for the identification and alleviation of individual assaults, either GHA or BHA hubs. However, the assurance of MANET against a double danger is scant. In this paper, the security against double assaults has been introduced for BHA and GHA by utilizing the idea of Artificial Neural Network (ANN) as a profound learning calculation alongside the multitude based Artificial Bee Colony (ABC) advancement method. The presentation of the framework has been expanded by the determination of fitting and best hubs for information bundles transmission which is clarified in the outcome segment.

For the system structuring and reenactment purposes, MATLAB programming is utilized with correspondence and neural system tool stash. The inspected outcomes show that the introduced mechanism produced better results rather than the current work under a black hole just as gray hole assault condition.

6.2 RELATED WORK

From the last couple of years, several researchers have worked to secure MANET against different types of internal as well as external attacks. Several Intrusion Detection System

(IDS) has been developed by (Shams and Rizaner. 2018; Nadeem et al. 2013; Marchang et al. 2016; Bu et al. 2010) that worked as a safeguard against threats. IDS aims to detect malicious nodes and improve network performance. (Shi et al. 2014) has presented a clustering-based approach to protect the network against the BHA. Clustering is a supervised approach, through which the entire system is divided into subareas, and each sub-area is monitored by a Cluster Head (CH) that helps in the detection of the affected node inside the system. The main drawback through which this research lacks is that with the various CH formations, the overhead increases and also requires high maintenance. (Chang et al. 2014) have utilized cooperative bait detection methods for the identification of affected regions. On the basis of this mechanism, the next hope node has been selected by the transmitting node. The drawback of this work is that only the nearby node has been selected as a bait address, that might be an affected node and hence pass data to that node and thus degrade the network performance. A few researchers such as (Singh et al. 2018 and Nurcahyani and Hartadi. 2018)have worked on DSR protocol to protect the data transmitted using it. Using this protocol, the node's behavior has been examined as per the packet received along with sent. Some nodes have been defined as an affected node if node's values have been exceeded the specified threshold (Mohanapriya and Krishnamurthi 2014). The trust of the node has been evaluated based on the node’s stability, mobility, power remaining, and the pause time (Biswas et al. 2014). Also, an attempt has been made by (Dhaka et al. 2015) to protect MANET against GHA in combination with the BHA using a controlled data packet. The control packet has been transferred through source node to its nearby node as well as based on its response to the activity of the node such as normal and malicious has been determined. An intelligent smart gray hole attack has been identified by using a novel protection mechanism named a mitigating smart gray hole attack mechanism (MGAM). This mechanism worked by analyzing the gray hole node as per the concept of defined value for the threshold. That is the case when the packet drop by the nearby node increases more than the threshold value an Alert has been broadcasted, which declared that the gray hole node has appeared in the network. A dual-threat detection approach precisely for GHA and BHA has been presented by (Ali Zardari et al. 2019) for

MANET. The attacker has been identified based on two features of nodes such as energy and its presence in the blacklist. If it is present in the blacklist then the data is not passed to that node. Existing work only applicable for small network because they only use the concept of energy consumption by nodes as a feature sets to differentiate between normal or malicious node, that means if network size is large, then identification of malicious nodes becomes complicated due to the involvement of similar types nodes and need an optimization approach to segregate the nodes based on the energy consumption, transmission delay, and packet transfer rate according to the fitness function.

To overcome this, a novel fitness function has been designed for the ABC algorithm based on which the nodes are segregated. Based on the segregated node list, the ANN structure is trained, which helps to delivered data with a small delay and high PDR.

6.3 METHODOLOGY

This research aim with providing protection of network for two kinds of attacks named a BHA and GHA. The detection process of these malicious nodes has been performed using ABC (Tareq et al. 2017) as an optimization algorithm along with the ANN (Canêdo et al. 2019) approach. The step by step description is provided below. Initially, a network of certain length and width is created by employing the N-number of nodes within the system (N=50 and 100). The requirement for the network is listed in table 6.1.

Table 6.1Ordinary Measure

Matrix	Range
Node Range	50-100
Area of Network	1000 × 1000 mm2
Coverage Range	25% of the total area
Type of Model	Heterogeneous

The network is designed for a simulated area of 1000 × 1000 mm^2, and each node can communicate within its 25 % of the total area, means that if a node is located with a position of (x,y)= (500,500), then the node can communicate with neighboring nodes up to having maximum position lies in between (525, 525) in both x and y-direction.

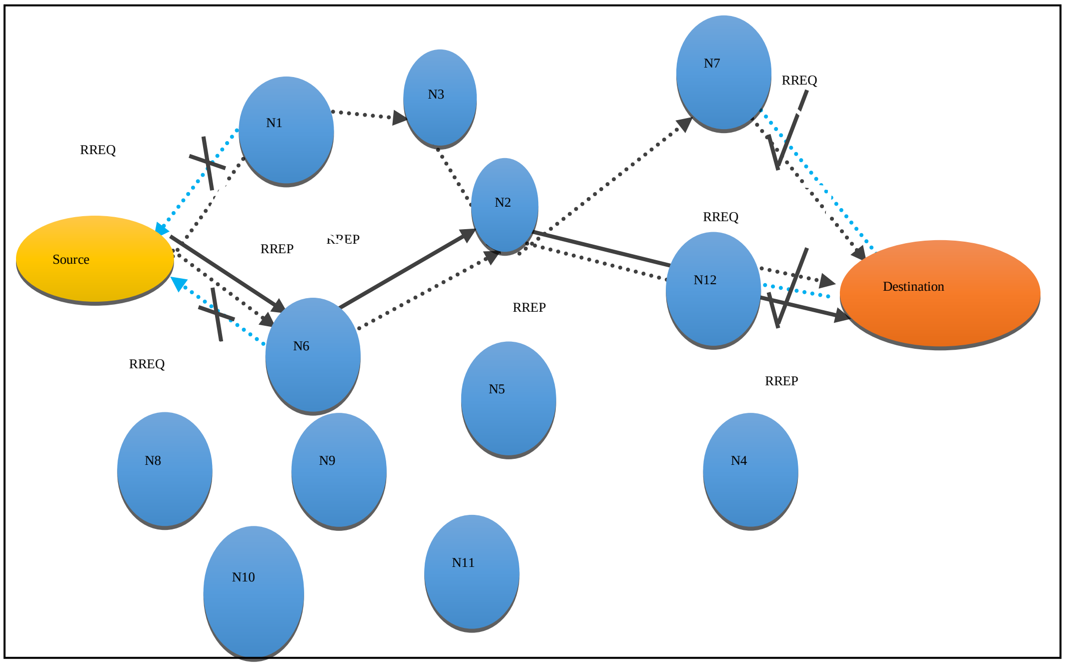


Figure6.1Route Discovery using AODV

Also, a heterogeneous model means that the node's communication capacity range is decided as per the obtained value of distinct parameters such as packet delay, co-ordinates, and energy consumption.

After deploying nodes, the source as well as the target nodes are specified. Then, using AODV routing algorithm, the process of data transmission has been performed. The routing concept is shown in Figure. 6.1.

In AODV, the path is formed only while the data requires to be transmitted. The process is carried out in two steps route request (RREQ) and then route reply (RREP). Whenever one node willing to communicate through another node, a data packet that consists of RREQ message is broadcasted within the source's coverage range of (25 %). After receiving the data packet through the adjacent node, that saves data into the routing table and also matches it with the previous data store, if the data is not matched then forward to its nearby node (Taha et al. 2017; Abusalah et al. 2008). In the AODV protocol, one of the best suitable routes is considered for data transmission among numerous possible routes based on distance measurement (Nakayama et al. 2008). After the data packet is received, the destination node sends back a route response packet towards the transmitting node through the shortest path. The route discovery mechanism is depicted in Figure 6.1. The blue dotted line represents the Route Request sent by the nearby node. The dotted black color line represents the possible route, whereas the solid black color line represents the appropriate route formed between the source and the destination node (Gharavi 2007). The cross clicks represent that the nods that receive the RREQ packet are not the destination node. The right-click represents that the desired destination is obtained, and it responds with the RREP packet (Fapojuwo et al. 2004). The designed algorithm for AODV as a routing mechanism is written below.

Algorithm 1: AODV Routing Protocol

Required Input:

$N_{SN} \leftarrow$ Number of Mobile Sensor Nodes

$N_S \leftarrow$ Source Sensor Node

$N_D \leftarrow$ Destination Sensor Node

Obtained Output: FR $\leftarrow$ Final Route from N_S to N_D

```
Start Routing
Nodes (NSN) start broadcasting of RREQ messages to neighbor nodes
Defined a message for RREQ=[ NS, Hop Count, ND], At initially Hop Count = 0
Route = [] // Initially Route is empty
Route(1st Node) = $N_S$
```

```
6. While $N_D$ not founded
7. 1st Node Broadcast RREQ to Neighbors Sensor Nodes and Record Hop Count
8. Neighbor Nodes Receive RREQ and check requirements
9.  If [NS, Hop Count, ND] == Neighbour Sensor Nodes [NS, Hop Count, VD]
10.     Route = Neighbour NSN is an ND
11.     Each node Send RREP to NS
12.     Hop Count = 1
13. Else
14.     Route = Neighbour NSN
15.     Send RREP to NS
16.     Hop Count = +1
17. End – If
18. Update and repeat step 3 to 13 until ND not founded
19. Possible Route, R = R1, R2, R3,.....RN
20. For r in range of R
21.      Current Route, R = R(r)
22.      Calculate to distance (D) from NS to ND
23.      If D is minimum then
24.          Final route, FR = R(r)
25.      Else
26.          Check next route condition
27.      End – If
28. End – For
29. End – While
30. Returns: FR as a final route from NS to ND
31. End – Function
```

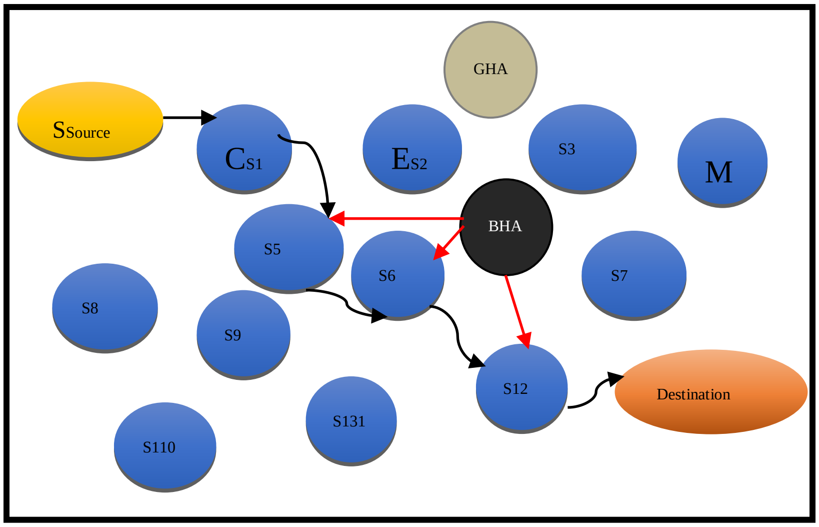


Figure 6.2Network with Blackhole and Smart gray hole attack

After route discovery, the next step is to deploy attacker nodes (Blackhole and Gray hole) as indicated by the black and the gray color, respectively, in Figure 6.2. The attacker nodes are marked based on their properties, such as if a malicious node behaves as a source node in route, and it is not a validated source, then it is defined as a BHA node. In other cases, if the node acts as an intermediate node in route and drops data partially, then it is considered as gray hole node. Based on the properties of the node, the nodes are differentiated into two categories typical and abnormal communicating nodes. Further, abnormal communicating nodes as separated into two subcategories named as a Blackhole and GHA nodes using ABC as an optimization technique with a novel fitness function. Those nodes that satisfy the ABC fitness function is considered as normal node otherwise considered as a malicious node.

6.4 ARTIFICIAL BEE COLONY (ABC)

ABC algorithm is motivated by the forging performance of honey bees that is a robust and swarm intelligence algorithm. It was firstly designed by Karaboga, and has been improved by different researchers by combining with other approaches. It mainly works by using three types of Bees such as (i) scout bee (ii) onlooker bee (iii) employed bee. The working steps are illustrated in (Kalucha and Goyal 2014).

The initial and foremost step of the ABC algorithm is to generate a population on a random basis and hence search for the solution in the search space. The search spaces that are found in its boundary range is determined by equation (6.1);

$$y_i^j = y_{N_s}^j + S^j \times Rand\ (0,1) \qquad (6.1)$$

Where, N_s is the source of nectar with i=1,..., N and j=1...,M, where N, M represents the number of nectar sources and optimization parameters respectively. The minimum and maximum values in dimension j in search space are represented by $y_{min}^j andy_{max}^j$.Now the position of employed as well as onlooker bees are being updated using the equation (6.2);

$$y_i^j = y_i^j + (y_i^j - y_{neighbour}^j) \times rand \qquad (6.2)$$

Here, a neighbor belongs to (1, N), which is being selected randomly and rand comprises of a real number range [-1,1] and is distributed uniformly. When some parameter values generated by this operation exceed the predefined limits in equation (6.3), the parameter is set to the appropriate limit (Karaboga et al. 2012; [13].

$$y_i = \begin{Bmatrix} y_1^i if y_i < y_1^i \\ y_2^i if y_i < y_2^i \end{Bmatrix} \qquad (6.3)$$

The designed fitness function is given by equation (6.4);

$$F(f) = \begin{cases} 1; & if N_{PROP} < Threshold_{PROP} \\ 0; & Otherwise \end{cases} \qquad (6.4)$$

In the fitness function, N_{PROP}: are properties of current sensor nodes which are in FR and $Threshold_{PROP}$ is the threshold properties of all communicating sensor nodes which are defined based on energy, transmission delay, and packet transfer rate. Based upon the fitness function segregated list of nodes (normal, attacker) is created. That node who satisfies the fitness function is considered in the normal list and those who not are considered in the abnormal list.

The algorithm for ABC is written below:

Algorithm 2: ABC

Required Input:	N_{PROP}🡐 Mobile Sensor Nodes Properties in terms of Energy Consumption, Transmission Delay, Packet Transfer Rate, etc. $\boldsymbol{F(f)}$🡐 Fitness function FR 🡐 Final Route using AODV between Source to Destination
Obtained Output:	ON_{PROP}🡐 Optimized Mobile Sensor Nodes Properties

```
1. Start
2. To optimized the FR, ABC Algorithm is used
3. Set up basic parameters of ABC: Population of Bee (B) – Number of Sensor Nodes
                                   Final Route (FR) – Route from NS to ND
                                   Fitness Function using equation 4
4. Calculate Length of Route in terms of R Length
5. Set a variable to store optimized nodes properties, ONPROP = []
6. For i in rang of R Length
7.     EBEE = FR (i) = $N_{PROP}$ // Current Bee from B
8.     OBEE = $Threshold_{PROP}$ // // Mean of all B
9. $F(f) = \ FitFun(E_{BEE}, O_{BEE})$
10.    ONPROP = ABC (F(f), FR (i))
11. End – For
```

```
12. Returns: ONPROP as an optimized mobile sensor node property
13. End – Function
```

Based on the above properties, the network is trained through ANN. During the simulation process, on the basis of the trained architecture of ANN, the system can classify normal, BHA, and GHA nodes and create an optimized and secure path through transmitting to receiving nodes. The developed trained structure along with the designed algorithm for the ANN approach is written below;

Algorithm 3: ANN

Required Input:

N_{SN}← Number of Mobile Sensor Nodes

ON_{PROP}← Optimized Mobile Sensor Nodes Properties on the basis of consumed energy Transmission Delay, the transfer rate of the packet, etc. Concerningnodebehavior

Cat ← Target/Category in terms of Normal and Abnormal Sensor Nodes

N ← Carrier Neurons Number

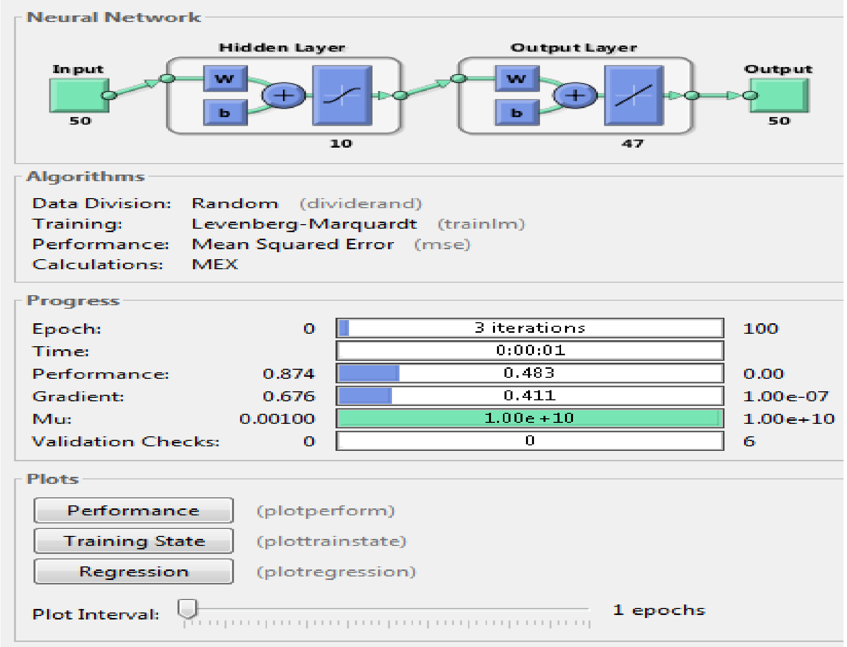
Obtained Output:

OR and BHA/GHA ← Optimized and Validated Route from N_S to N_D with both black hole as well as gray hole nodes. In case if the behaviour of nodes like GH and BH node in route, then ANN identify them and discard that nodes from route

```
1. Start Routing
2. Call and set the ANN using ONPROP properties as training data (T), number of NSN
   as a group (G) and Neurons (N)
```

```
Initialize the ANN: 10 numbers of neurons Epoch
        Defined metrices: MSE, gradient, mutation and validation
        Algorithm for training: levenberg-marquardt
Set, MANET_Structure = NEWFF (T, Group, N)
MANET_Structure = TRAIN (MANET_Structure , T, G) // To train the network based on nodes properties
Current Sensor Nodes, NC = Properties of the current node in MANET //  Current sensor node means which are considered in route during routing and their properties are denoted as NC
Sensor Nodes Characteristics = SIM (MANET_Structure, NC) // To match nodes nature with training structure of ANN
If Sensor Nodes Characteristics is valid then
    OR = Validated
Else
    OR = Need Correction or mark as BHA and GHA Nodes
    If the drop rate is maximum
        Marked as BHA
    Else if drop some and transmit some data packets
        Marked as GHA
    End – If
End – If
Returns: OR as an Optimized and Validated Route from NS to ND with Black Hole and Gray Hole Nodes
End – Function
```

The trained structure for 50 numbers of nodes is represented in figure 6.3 below.



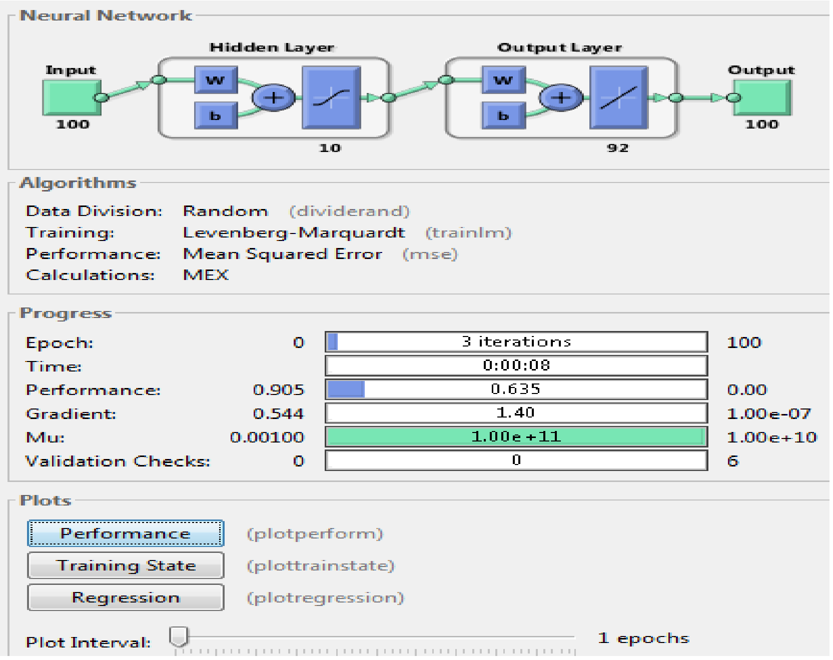
Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

```
Epoch:                  0   3 iterations   100
Time:                       0:00:01
Performance:        0.874   0.483          0.00
Gradient:           0.676   0.411          1.00e-07
Mu:               0.00100   1.00e+10       1.00e+10
Validation Checks:      0   0              6
```

Figure 6.3Training Structure for 50 Nodes



Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

```
Epoch:                  0   3 iterations   100
Time:                       0:00:08
Performance:        0.905   0.635          0.00
Gradient:           0.544   1.40           1.00e-07
Mu:               0.00100   1.00e+11       1.00e+10
Validation Checks:      0   0              6
```

Figure 6.4Training Structure for 100 Nodes

As depicted in figure 6.3 it has to be clear that the input layer comprises 50 numbers of nodes as input data, the information of which such as delay, energy consumption is being carried by10 numbers of neurons as depicted under the hidden layer of Figure 6.3 and Figure 6.4. At the output layer, there are 47 numbers of nodes has been attained, which demonstrates the class of communicating nodes. The network has been trained on energy consumption and the delay produced by the nodes. Later on, these parameters are used to decide that to which node the data is forwarded.

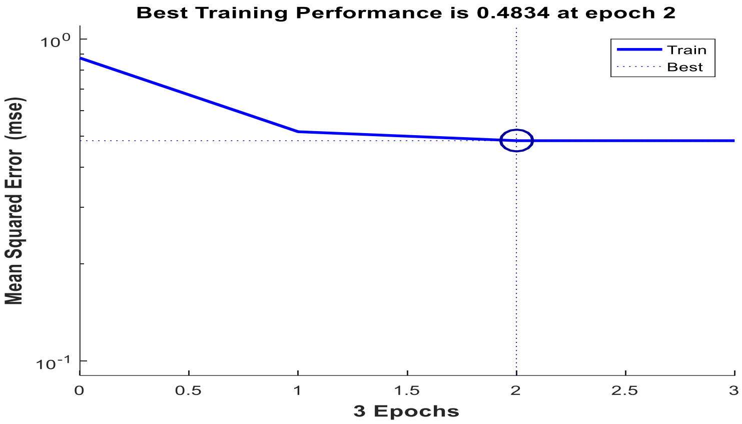


Figure6.5MSE for 50 Nodes

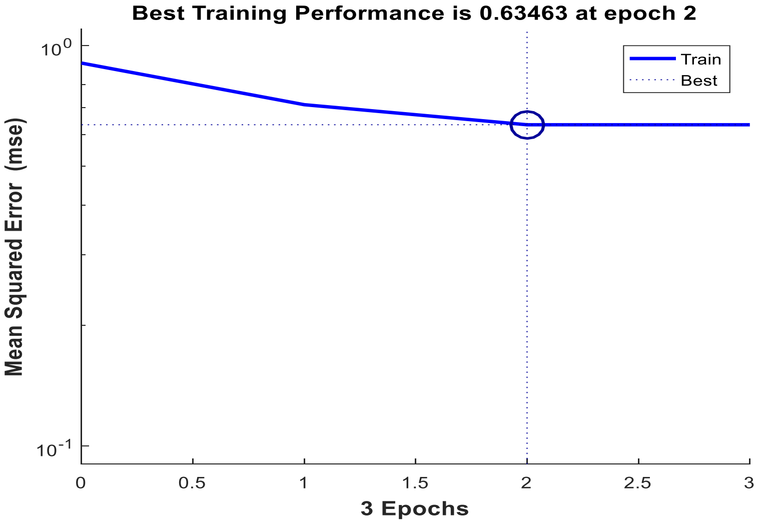


Figure 6.6MSE for 100 Nodes

After clicking on the performance button shown under ANN trained structure as depicted in Figure 6.6, the Mean Squared Error (MSE) graph has been analyzed. From the graph shown in Figure 6.6, MSE value measured at which the ANN structure is trained for 50 numbers of nodes and 100 numbers of nodes is 0.4834 and 0.63463 respectively, which is obtained at the 3rd epoch. For better training, it is desired that the MSE value should by low and near to zero.

Using ANN, the network learns the behavior of participating nodes, which further helps to detect node as a normal and malicious node.

SUMMARY

The previous chapter covers the architecture of threat as well as prevention for secured transmission of a packet in MANET. In this chapter covers to distinguish the Blackhole node and divert the route through the protected node utilizing an altered AODV routing protocol. In this work identifying the node as the black hole has been performed dependent on the energy consumption, delay in transmission of data, and the positioning of nodes in the system. This chapter also includes the previous work related to current work that is done by several researchers and scholars. The next chapter covers the performance of MANET has been affected by many attacker nodes, which becomes a great concern for the research. In this research, an enhanced routing protocol (i.e. AODV) has proposed as well as is utilized in the detection of BHA node. Proposed work is mainly partitioned among three sub-parts. Initially, the routes are created using the AODV routing protocol, the route is optimized using the fitness function of the Artificial Bee Colony algorithm and then classify the nodes based on their properties.

CHAPTER 7: MITIGATION OF MULTIPLE ATTACK USING ARTIFICIAL BEE COLONY USING HYBRID MACHINE LEARNING APPROACH

7.1 INTRODUCTION

Ad Hoc network is identified as an autonomous network which can be built through mobile devices like laptop, mobile phone, and other electronic equipment that can communicate through radio means. These mobile nodes can perform communication among them without utilizing the infrastructure of fixed networks as well as any kind of centralized base station. For certain reasons like dynamically changes in network topology, mutual trust between nodes, dynamic infrastructure for analyzing node behavior, and loss of packet because of malicious nodes, these networks do not provide support against malicious nodes. Among different attacks, the Blackhole attack (BHA) is considered one of the most affecting threats in the Mobile Ad Hoc network (MANET). This attacker node drops entire data traffic and hence degrades network performance. Therefore, it is essential to design an algorithm that can protect the network from the BHA node. This article presented a new updated routing protocol namely; Ad hoc On-Demand Distance Vector (AODV) by using the advantages of the Artificial Bee Colony Algorithm (ABC) along with Artificial Neural Network (ANN) and Support Vector Machine (SVM) technique. The role of ABC is to provide a better route for data transmission between the source and the destination node. Among optimized routes, the selection of the best route is performed by the ANN approach. The properties of an optimized route are fed as input data to the ANN structure and based on those properties ANN learns about the behavior of nodes. The optimized route, suggested by ANN is then passed to the SVM model along with the node's properties. Based on those properties SVM decides as normal and attacker node. The designed algorithm is simulated in the platform of MATLAB. The outcome of this work produces as enhancement in terms of the parameter such as PDR, throughput, and delay.

7.2 RELATED WORK

Shahabi et al. (2016) designed a novel routing algorithm in addition to AODV to secure a network from BHA. Using this strategy, the malicious nodes are identified based on the node's behavior. If detected any, then, delete that node from the route. The experiments also show better Packet Delivery Rate (PDR) with reduced delay. Baadache and Belmehdi (2012) have presented an acknowledgment-based routing approach by which the communicating nodes send acknowledgment whenever the nodes receive the data packet. The algorithm suffers from high routing overhead as each node sends an acknowledgment message to the prior node. In addition to the above problem, Vadhana and Paramasivan (2015) have developed a routing mechanism of trust-based having the behavior of nodes is analyzed based on the dropping rate of packets. But this protocol also suffers from the high overhead because of the additional use of control packets. Gurung and Chauhan (2018) have used the approach of mitigating a gray hole attack (GHA), that takes the help of other nearby nodes known as the nodes of the Intrusion Detection System (IDS) to monitors the performance of other communicating nodes. In the appearance of any malicious node, the packet drop value of the node is higher. In this case, the important message ("ALERT") is transferred among the networks to intimate other nodes to separate attacker nodes. As the algorithm works on the defined threshold therefore proper positioning of special nodes is required. Mohanapriya and Krishnamurthi (2014) have designed a new approach source node is intimates the destination node about the total amount of packets transmitted from all expected routes. Query request has been transmitted by destination node particularly in case if the node cannot obtain the desired packets. In response to this Query Reply message is sent back to the node that is about 2-hop count far as a contrast to the destination node. Once received the message of query reply, the destination node compared its prior received data with the recently received data. In case error appear, then consider that node as the suspected node and add into the list of malicious nodes. The author [13]have presented a combined trust-based bee approach to secure the network against BHA. ABC is used for the detection of a secure route. A new solution has been generated based on the fitness function of bees. The designed algorithm shows enhancement in the PDR and end to end delay. Merlin and Ravi (2019) have presented a new trust-based approach that works on energy-aware routing for MANET. The BHA has been detected for single as well as for multiple routes formed during the data communication process. Medadian et al. (2009) have presented a mechanism in which the source node transmits the route response data packet after processing the node's information, which is later used for BHA detection. Whether the node is genuine or malicious is decided by the intermediate node. On the other hand, Yasin et al. (2018) have used a timer and baiting based method for BHA detection in MANET. Shahabi et al. (2016) have used a security approach to identify a malicious node. Obaidat et al. (2014) have used cryptography approach for data security against BHA.

7.3 PROPOSED WORK

The previous chapter covers to distinguish the Blackhole node and divert the route through the protected node utilizing an altered AODV routing protocol. In this chapter, the identification of multiple threats in the network is a necessary job to enhance the lifetime of the network. Therefore, to improve the performance of the network in the presence of malicious nodes, specifically BHA & GHA nodes, a security mechanism using ABC as a swarm-based approach and ANN as a machine learning technique has been used. This chapter covers the previous works carried out in the relevant field through numerous researchers and scholars. This chapter explains the workflow, too.

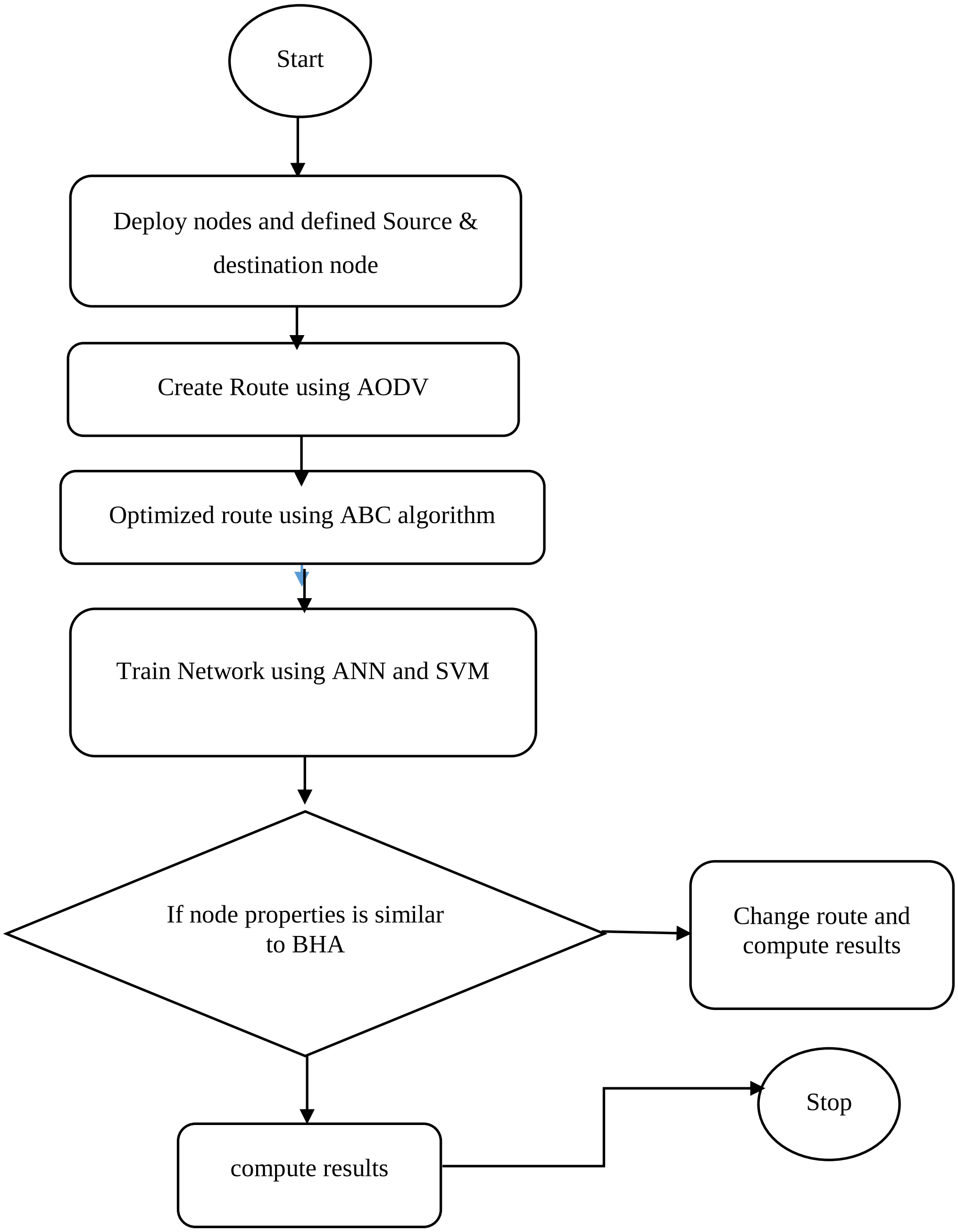

Start
Deploy nodes and defined Source & destination node
Create Route using AODV
Optimized route using ABC algorithm
Train Network using ANN and SVM
If node properties is similar to BHA
Change route and compute results
compute results
Stop

Figure 7.1Flow of Proposed Work

The considered parameters for the system as provided in Table 7.1.

Table 7.1 Simulation Parameters

Running Time	0.2 ms to 1 ms
The number of deployed nodes	100 to 200
malicious nodes Count	1
Simulation environment	1000 × 1000

7.3.1 Deploy nodes and defined source and destination node

Initially, N number of nodes are deployed with defined length and width of (1000 × 1000). Each node is labeled by N1, N2,…..N_n), including the source (N16) and the destination node (N36) where n is the number of deployed nodes.

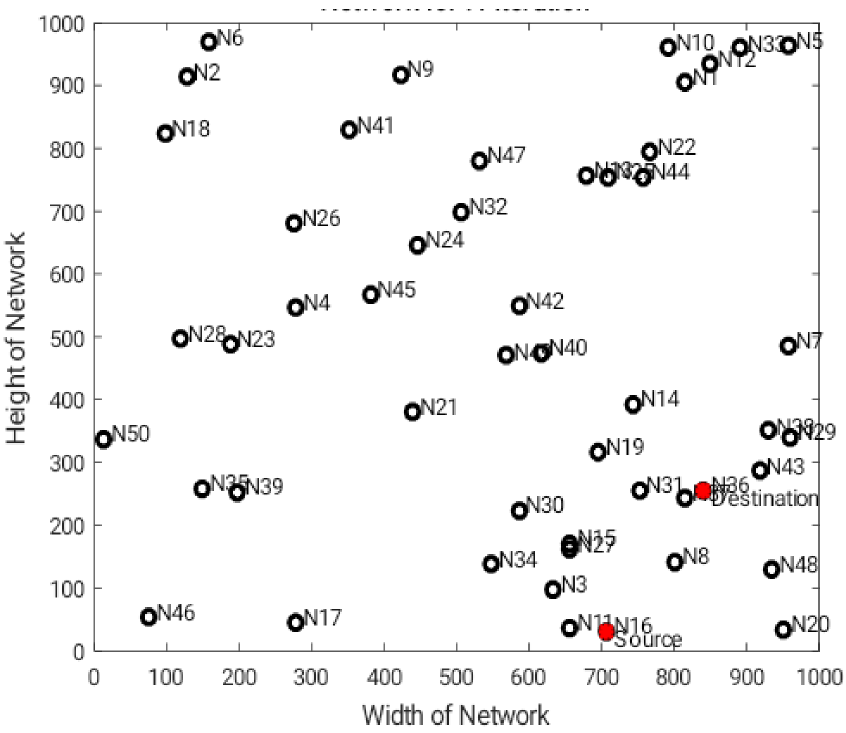
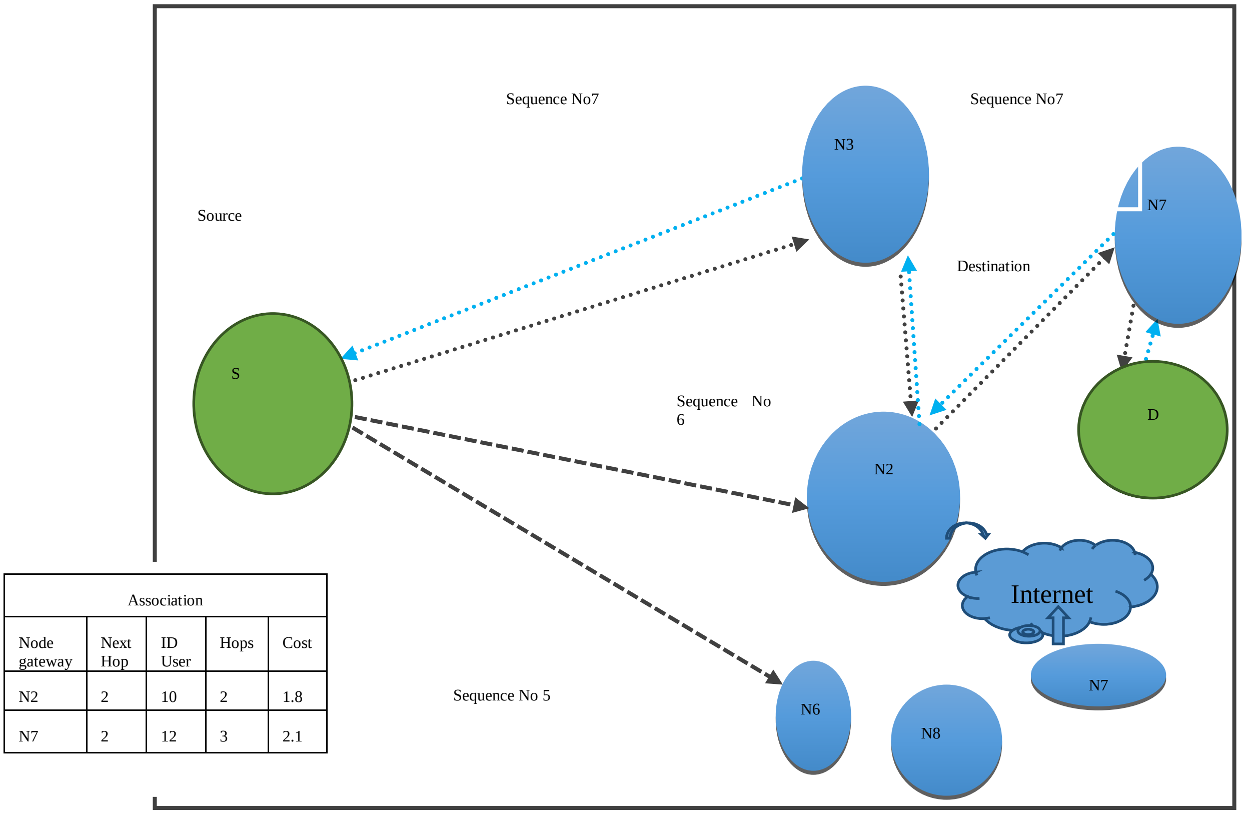


Figure 7.2Node Deployment

7.3.2 Routing Mechanism

The route has been formed using AODV as routing protocol, which establishes route on-demand - basis and hence a reduced number of required broadcasts. Using this protocol, the nodes that are not part of the route have not been needed to manage the information of routing. Thus, it can be known as a pure on-demand basis process of routing. This reduced the routing packet size.



Association				
Node gateway	Next Hop	ID User	Hops	Cost
N2	2	10	2	1.8
N7	2	12	3	2.1

Figure 7.3AODV routing Process

During the route discovery process mainly two packets such as RREQ and RREP are responsible for the route formation. Both control messages contain an essential attribute known as ‘destination sequence number’. The enhanced value of this number determines the best suitable path. As presented in Figure 7.3, the source node (S) broadcasts RREQ messages, which are received by its nearby nodes denoted by N2, N6, and N3 respectively. This process is initiated to determine the destination node (D). After receiving the RREQ message, the nearby nodes (N2, N6, and N3) sent back:

(i) IF the node is identified as a destination node then the RREP message is transferred back to the source node.

(ii) If not, then its routing table needs to be updated by fresh information on the path regarding the destination node.

After reaching the RREQ packet on destination (D), this process is stopped.

Then the node checks the sequence number of destinations from the routing table. If this sequence number is higher as compared to the sequence number of destination then the route has been created through that particular node as shown in Figure 7.3. Node N3 has a higher sequence number than N2 and N6. Therefore, the final route is created by {S, N3, N2, N7, and D}. The algorithm followed for AODV is provided below in pseudo-code.

Algorithm: AODV Routing Protocol

Input Parameters: N->The amount of deployed nodes (50)

Coverage->Wireless communication range (25% of Network Area)

Output Parameters: Route-> ‘S’ to ‘D’ Route

Initialize the variables

‘S’: Corresponds to Source_Node

‘D’: Respect to ‘Destination_Node

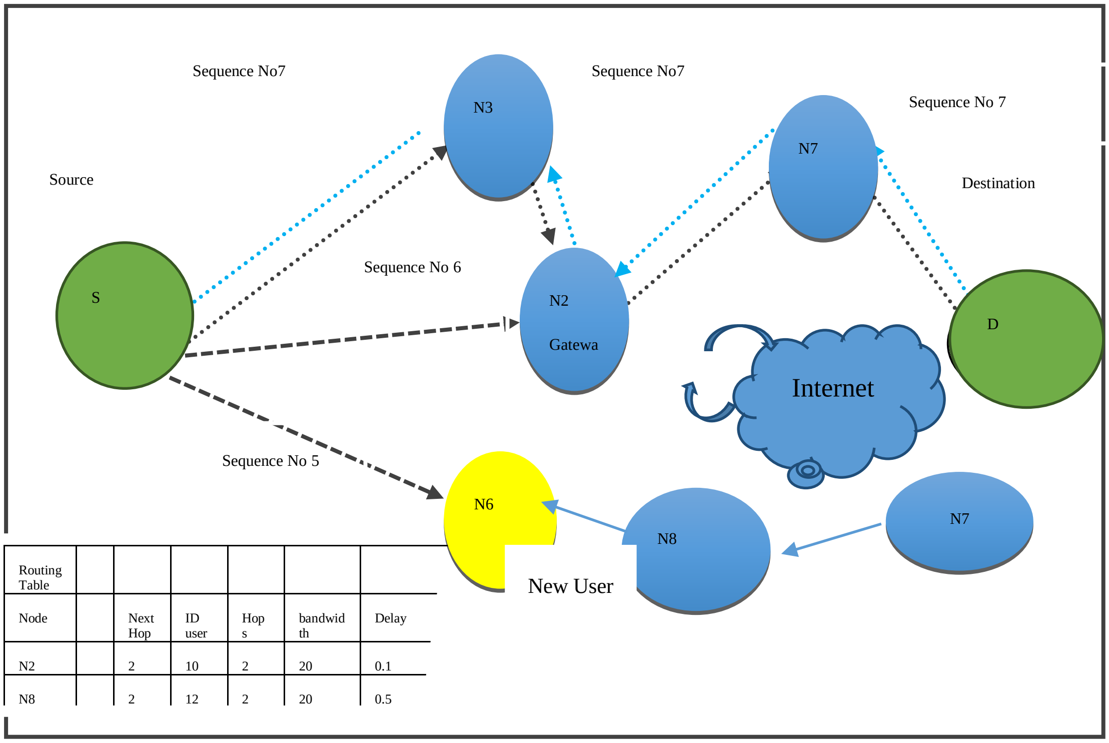
Nb-Add: Address of Nearby_Node

RREQ: Route request control message

RREP: Route reply control message

RP_Table: Maintain Reply Table

```
Start Routing
Route = [] // Create an empty matrix to store Route Nodes
Route (1st Node) = S // Route 1st node is Source
While (D not founded) // Search Next Nodes in Route
    'S' broadcast RREQ within Coverage Area
    If Nb-Add is 'D' then
        RREP acknowledge to the 'S'
        D founded
        Route (Next) = D // Consider D as a next node in the route
    Else
        This broadcasting process is continued until 'D' is not founded
        Route (Next) = Neighbour node with a minimum hop count
    End – If
End – While
RP_Table = Route // Store in the Table
End – Function
```



Routing Table						
Node		Next Hop	ID user	Hops	bandwidth	Delay
N2		2	10	2	20	0.1
N8		2	12	2	20	0.5

Figure 7.4New user Connection request using AODV

The first step is to pre-calculate the optimal route for some pre-existing gateways according to the routing schedule. If a new user-requested for data transmission, the new user must send a request to the nearest node on the network. The scenario of which is shown in Figure 7.4

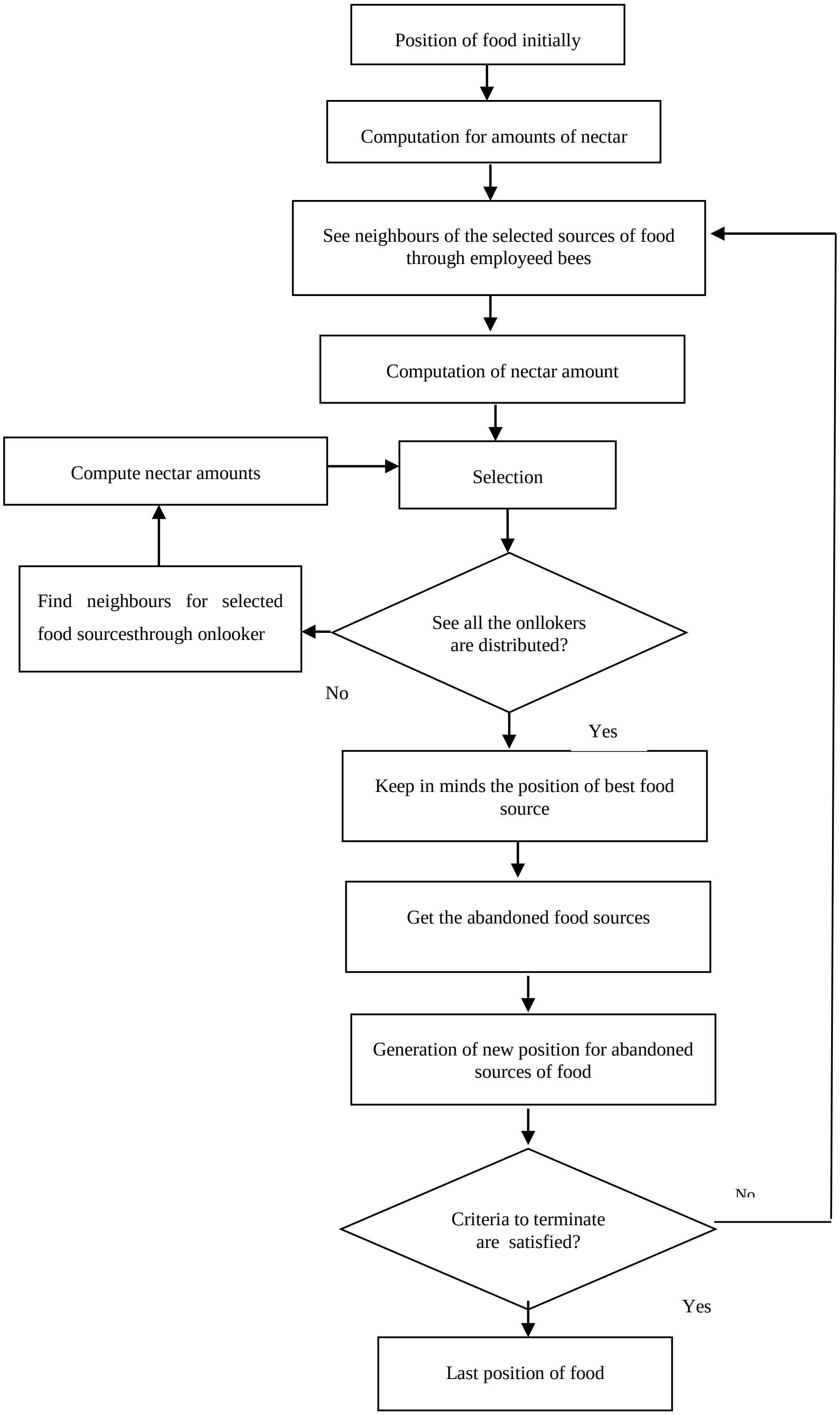
Let node 6 is a new user in the network as denoted by yellow color. After receiving this request, the AODV algorithm must read the routing table as shown in Figure 7 under node A and find the pre-calculated most suitable route to the nearest gateway. In Figure 7.4 (the next gateway 2 has a minimum hop number 2, so it will be used in this situation). The selected route information is sent to the new user (N6), after which connection can be established. As soon as a new user joins, the network topology, as well as network settings, changes. On the move, mobile agents share this information with all nodes in the network.

In the second stage of the routing process, a parallel process is activated to assign a route to a new user, so monitoring focuses on the new user's traffic needs and improving bandwidth usage and loading parameters at designated links.

7.3.3 Artificial Bee Colony (ABC)

This research used ABC for obtaining the best or optimized nodes properties of the created route using AODV protocol. ABC is a swarm-based metaheuristic algorithm to solve the combinatorial optimization challenges. To solve the complex problems in different domains, the foraging behavior of honeybees is considered. To establish communication between the bees, waggle dance is required. To collect the knowledge of the outside environment separately is gathered through this dance of waggle. By which the computation of relative merit in multiple patches based on food quality as well as the energy amount to harvest it, is enabled. The observer nodes observe the dance and based on that extract the food. The location for each food source corresponds to the solution that is optimized for the problem. The working flow of ABC is shown in Figure 7.5.

ABC mainly composed of three types of bees such as; onlooker, the forger, and the scout bees. For the selection of sources of food by just watching the waggle dance of two another bees is the key role of onlooker bees. Forger bees have to constantly visit the source of food to obtain nectar. The last one scot bees randomly search for the discovery of novel food sources . The pictorial representation of these three bees searching process of food is illustrated in Figure 7.6.



Position of food initially
Computation for amounts of nectar
See neighbours of the selected sources of food through employeed bees
Computation of nectar amount
Compute nectar amounts
Selection
Find neighbours for selected food sourcesthrough onlooker
See all the onllokers are distributed?
No
Yes
Keep in minds the position of best food source
Get the abandoned food sources
Generation of new position for abandoned sources of food
No
Criteria to terminate are satisfied?
Yes
Last position of food

Figure 7.5Working Flow of ABC

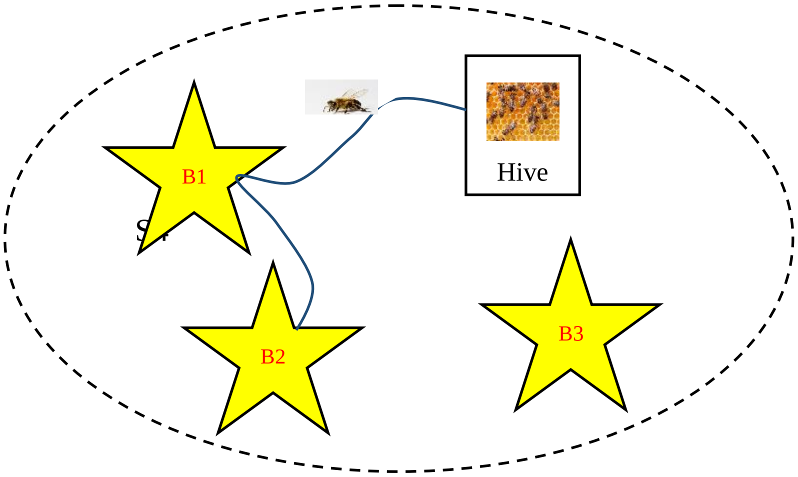


Figure 7.6 Scouting mechanism of ABC

The main process of searching food by bees of ABC is listed in the steps below.

i. Initialization of food sources as per the size of the population.

ii. REPEAT:

   (a) Employed bees visit sources of food to assess the nectar amount based on their memories, and then return to the hive to perform a waggle dance at that location.

   (b) After the food source is exhausted, the onlooker bees start to randomly look for novel sources of food as well as memorize the best sources for food.

iii. The process is repeated until the best food source is obtained.

Every time ABC visits a node (that is, the network topology or several nodes themselves), it computes the energy, delay, and packet drop rate. ABC includes an initialization process along with a search cycle process, iterating through the main search cycle until it finds the best suitability solution acceptable to the best communicating node. After the arrival of the onlooker bees, the algorithm will strictly check to identify the source routing and the number of nodes present in the route performed by the AODV routing mechanism. If there is no source route, it will broadcast the packet and rescan the nodes' properties to crosschecks that whether it is used to transmit outgoing energy or incoming broadcast packets.

ABC with the AODV algorithm enhanced the routing process by selecting the best route in between both the node of source and destination. The role of the scout bee is to measure the energy as well as the distance between two different nodes. More is the distance higher is the transmission delay and results in greater energy loss.

Algorithm: ABC Route Optimization

Input: Final Route from S to D and Mobile Sensor Nodes Properties

Output: Optimized Mobile Sensor Nodes Properties

```
Start Properties Optimization
To optimized the FR, ABC Algorithm is used
Set up basic parameters of ABC: Population of Bee ($P_b$) – Number of Sensor Nodes
```

Final Route (FR) – Route from N_S to N_D

Fitness Function: $F(f) = \{1; \quad if\ N_{PROP} < Threshold_{PROP} 0; \quad Otherwise$

Where N_{PROP} are the properties of the node such as energy consumption, delay, etc.

In the fitness function, N_{PROP}: are properties of current sensor nodes that come in FR as well as$Threshold_{PROP}$ is corresponds to the threshold features for all communicating sensor nodes that define based on energy and distance

```
Computation for the length of Route on the basis of R-Length
Optimized characteristics of nodes are set, $ON_{PROP}$= []
For i in rang of R Length
    $E_{BEE}$ = FR (i) = $N_{PROP}$ // Current Bee from $P_b$
    $O_{BEE}$ = $Threshold_{PROP}$ // // Mean of all $P_b$
$F(f) = FitFun(E_{BEE}, O_{BEE})$
    ON $_{PROP}$ = ABC (F(f), FR (i))
```

```
11. End – For
12. Returns: ON PROP as an Optimized Mobile Sensor Nodes Properties
13. End – Function
```

7.3.4 ARTIFICIAL NEURAL NETWORK (ANN)

ANN is the technique of machine learning that is designed to work like a human brain. The working of ANN is similar to a human brain is works and memorizes from the experience. ANN is a non-linear statistical model, which processed input to discover a new pattern. The ANN consists of three layers as discussed below.

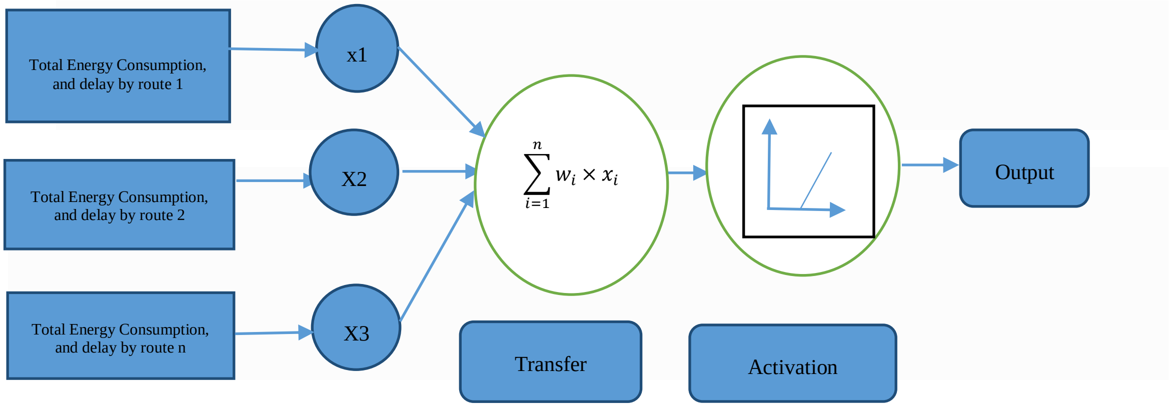

Total Energy Consumption, and delay by route 1
Total Energy Consumption, and delay by route 2
Total Energy Consumption, and delay by route n
x1
X2
X3
$\sum_{i=1}^{n} w_i \times x_i$
Output
Transfer
Activation

Figure 7.7ANN Structure

Input layer: The input regarding the number of the optimized route obtained based on the node’s properties like as packet delay and energy consumed by nodes is provided as input information.

Hidden Layer: This is positioned between the input and output. It can be single or multiple layers can be used. Specifically, this layer processes the input information to know the relationship between the attributes passed on input side.

Output layer: The resultant value after computation is obtained at this layer. The ANN computes the input values and provided the best route with minimum energy consumption and delay. The complete structure of ANN is shown in Figure 7.7.

Depending upon the optimized properties of nodes, the final output has been obtained. The discrepancy between the input values and the output values are obtained in terms of error values. Based upon the error value, the weight of the neuron in the hidden layer is adjusted and that process is known as backpropagation. Each neuron consists of two states that are 0 and 1 corresponds to deactivation and activation of the sigmoid function. Each neuron composed of weight W_{ij}corresponds to its interconnection. In case, if W_{ij}=0, it represents the independency of the neuron, if W_{ij}=W_{JI}shows that weights are symmetric. Every neuron behaves as an individual unit of ANN structure with a non-linear transfer function given by equation (7.5).

$$f(x_i)=Y_i = x_i \qquad (7.1)$$

The neuron's output is fed back to the other interconnected neurons by the linked weight of W=W_{ij}. Also, in the form of hardware, the weight is corresponding to resistance and hence, weight in terms of resistance is given by equation (7.2).

$$W_{ij} = \frac{1}{R_{ij}} \qquad (7.2)$$

The ANN included two inputs one is the external input and the other is the output of network neurons. Therefore, the total input to the neuron can be given by equation (7.3).

$$\sum_{j\neq i} \frac{x_j}{R_{ij}} + In_i \qquad (7.3)$$

R_{ij}Represents the resistance/ interconnection of weight between neurons 'i', and 'j'.

The output is obtained in the output layer of ANN in the forms of two-state values. The output Y_j of output neuron 'j' provides values like Y_j^0 and Y_j^1, which represents values corresponding to 0 and 1 respectively. The output of input neuron (i) of x_i can be represented by equation (7.4).

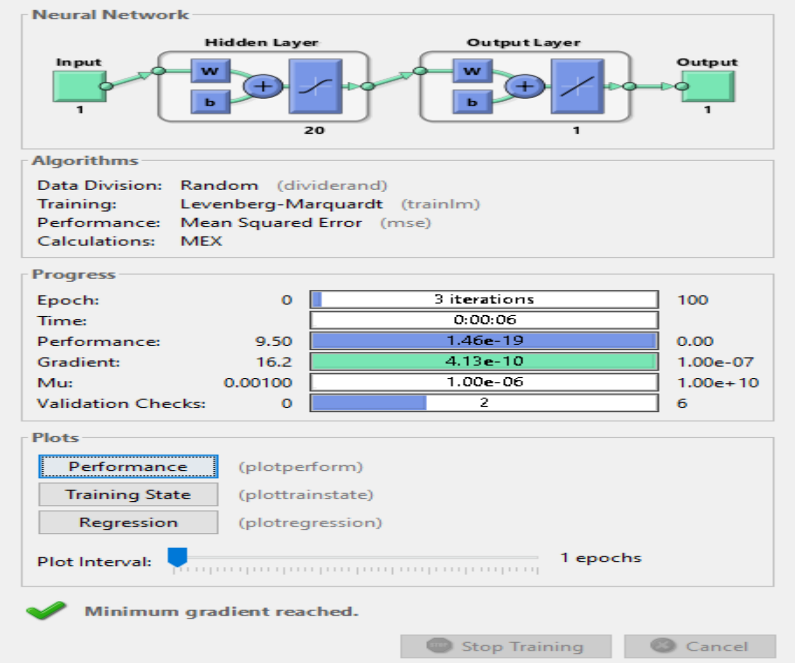
$$If\left(\sum_{j\neq i} \frac{x_j}{R_{ij}} + In_i < x_j\right)\{x_j = x_i^0\} \qquad (7.4)$$

The state of the ANN can be identified by determining the energy function of the neurons. Mathematically, it can be represented by equation (7.5).

$$E = -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{x_i x_j}{R_{ij}} - \sum_{i=1}^{N} In_i x_i \qquad (7.5)$$

The energy varied due to the alteration in the state-run of neurons (i) [33-34]. Therefore, the deviation in energy can be represented by equation (7.6).

$$\frac{\partial E}{\partial x_i} = -\sum_{j=1}^{N}\frac{x_j}{R_{ij}} - \sum_{i=1}^{N} In_i \qquad (7.6)$$



Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

Epoch:	0	3 iterations	100
Time:		0:00:06	
Performance:	9.50	1.46e-19	0.00
Gradient:	16.2	4.13e-10	1.00e-07
Mu:	0.00100	1.00e-06	1.00e+10
Validation Checks:	0	2	6

(plotperform)
(plottrainstate)
(plotregression)

Plot Interval: 1 epochs

✓ Minimum gradient reached.

Figure 7.8Trained ANN

The trained ANN structure and error graph generated during the training process is given correspondingly in Figure 7.8 and Figure 7.9.

The ANN is trained using an optimized node's properties for both normal and abnormal nodes. The nodes' properties are applied as input parameters like energy consumed by nodes and distance covered by nodes. If the output is not as per the desired then the error generated is transferred back to the hidden layer for adjusting the properties of nodes accordingly. In the similar manner, the training of the network is done through minimum error. The network composed of N number of interlinked neurons as indicated by an arrow in Figure 8. These neurons update the activation function of each neuron independently. During training, the error generated by the ANN network is known as the Mean Square error and is represented by Figure 7.9.

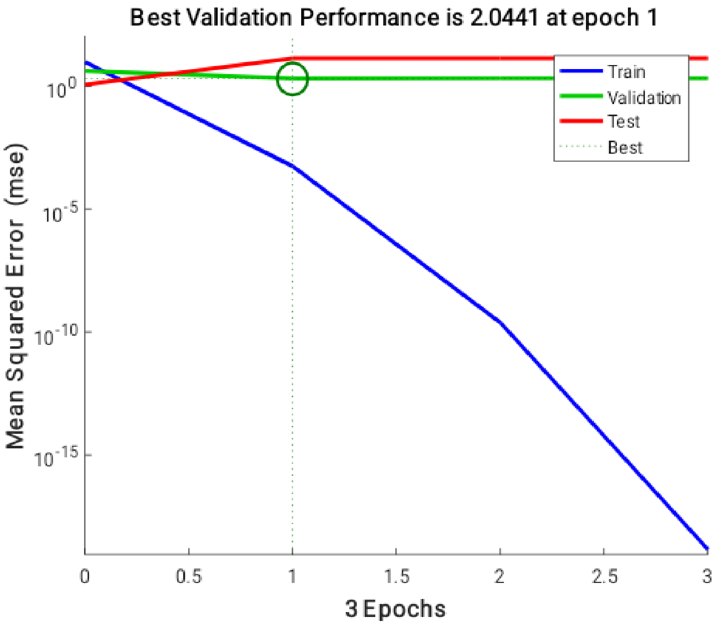


Figure 7.9 MSE

The MSE concerning epochs generated by the ANN algorithm is depicted in figure 7.9. The graph specifically composed of four different values as represented by different colors such as the blue, the green, the red, and the dotted line, which represents the error values of the train, validation, test, and best-obtained solution respectively. Here, the best-trained structure is obtained at first epoch and carrying MSE of 2.0441.

The aim of using ANN is to select the best rout among the number of optimal routes obtained using AODV with the ABC approach. Now, the next step is to identify the black node if it is present in the selected route. To detect node as black hole node, the Support SVM approach is applied. The working of SVM is presented in the next section.

7.3.5 Support Vector Machine (SVM)

SVM is a defined as the supervised model of machine learning (ML), widely recognized because of its incredible performance in performing classification tasks including data of high dimension. In it claimed that SVM is the best alternative for high accuracy as well as reduced error detection of an affected node within IDS framework. The detection module examined in this research has been established through the hybridization of learning approaches i.e. ANN and SVM. The working of SVM is represented by the block diagram as depicted in Figure 7.10.

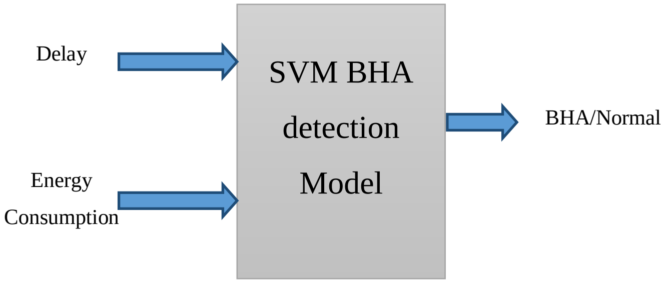


Figure 7.10 Block Diagram of SVM

The nodes' properties of the selected route using the ANN approach are passed as input to the SVM model. The attributes of nodes such as delay and energy consumption are passed to train the module. The training data was collected using the ANN structure for both normal and attacker situation. Based on the energy and delay level, the decision has been taken as a BHA node or a normal node.

Algorithm 2: SVM with ANN

Input Parameters: FR: Final Route

$ON_{PROP:}$ Optimized Nodes Properties as a Training Data (T),

C: Target/Category in terms of communicating and non-communicating node

Output: OR Optimized Route for discovering a route from T_X-Node to R_X-Node and Malicious Nodes (M-Nodes)

```
1.  Start Training
2.  Initialization of the training data for SVM, ONP is denotes the optimization characteristics of overall nodes including RBF as kernel function
3.  For i  is initialized 1 up to every nodes
4.  If nodes property (i) is real
5.  “cat” is defined as a categorization for data of training
6.  $cat_1$= $ON_{PROP}$ (i)
7.  else
8.  $cat_2$ = $ON_{PROP}$ (i)
9.  end - if
10. End – For
11.  Structure of training =SVM_TRAIN (T, cat, kernel_function)
12. OT=Structure of training. Support-Vector //To determine the data of training foANN classifier
13. Initialization for basic parameters of neural network
    –Epoch_amounts(E) // Iterations utilized through neural network
    –Amount of neurons (N) // Utilized as a carrier in a neural network
    – Performance are computed in terms of  MSE, Gradient, Mutation, and Validation
    –Utilized technique: Levenberg Marquardt
    –Division of data: Randomly
14. For i = 1 to OT
15.   If T comes under the nodes communicating features
16. $1^{st}$ group = features of data for training as per the real nodes
17. Else if T comes under the nodes-communicating features
18. $2^{nd}$ group= data_feature (for training as per the non-real nodes)
19.     Else
20.   $3^{rd}$ group = additional features for data of training
21. End_If
```

```
End_For
Initialization of ANN are done by using data for training along with a group
MANET-Net = Newff ($T, Group, N$)
Training parameters are set on the basis of requirements as well as train the system
VoIP = Train (MANET_Network, training_data groups)
Initialized testing:
Present_node = features of present nodes insideMANET_Net
Authentication = simulate (MANET_Net, Current Node)
If Authentication = True
    Genuine Nodes do not consider as a malicious
Else
    M-Nodes = Malicious Node
End – If
Create an Optimized Route, OR = FR (Genuine Nodes)
Return: OR as an optimized Route (OR) and Malicious Nodes (M-Nodes)
End – Function
```

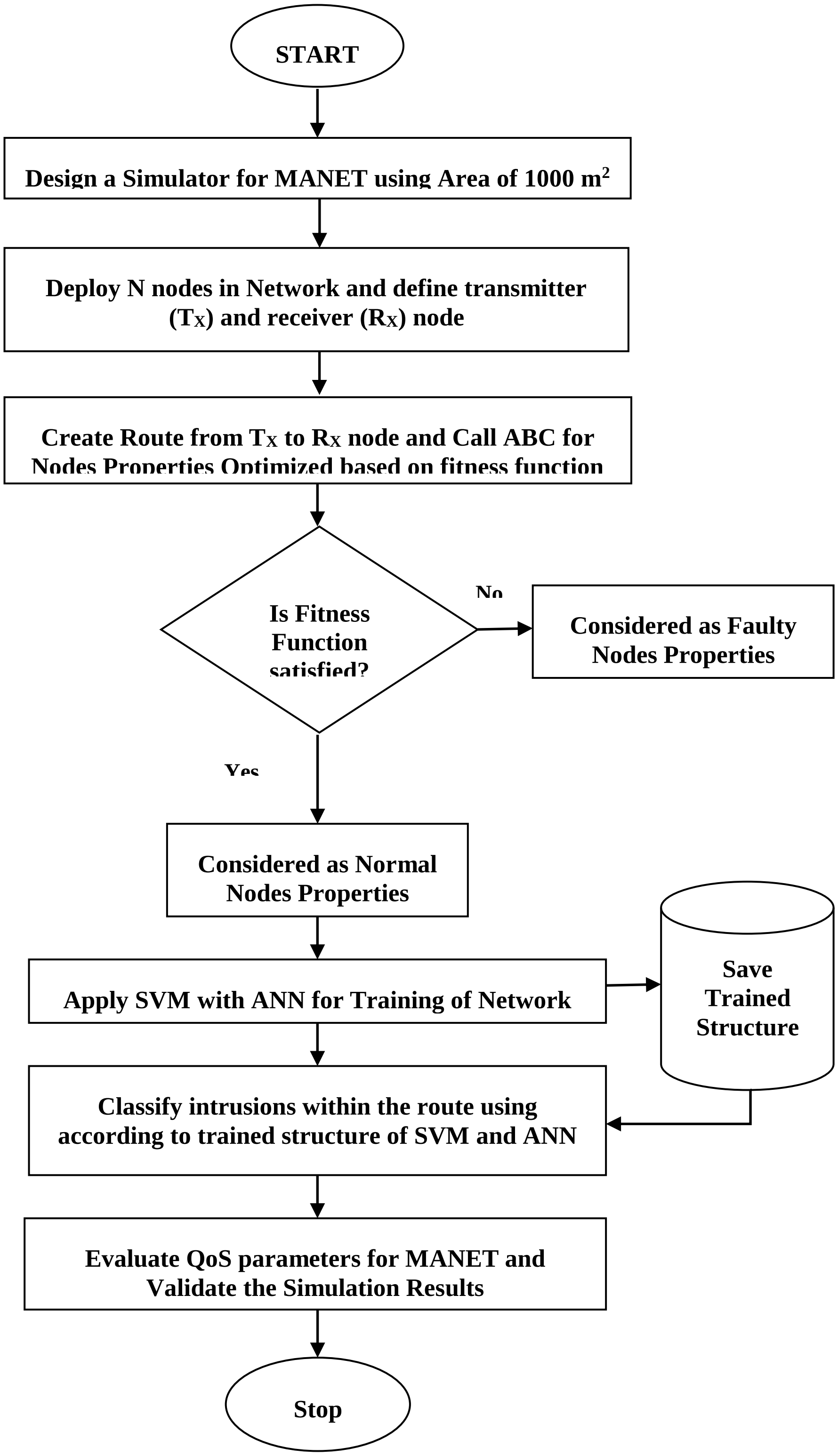

START
Design a Simulator for MANET using Area of 1000 m2
Deploy N nodes in Network and define transmitter (TX) and receiver (RX) node
Create Route from TX to RX node and Call ABC for Nodes Properties Optimized based on fitness function
Is Fitness Function satisfied?
No
Considered as Faulty Nodes Properties
Yes
Considered as Normal Nodes Properties
Apply SVM with ANN for Training of Network
Save Trained Structure
Classify intrusions within the route using according to trained structure of SVM and ANN
Evaluate QoS parameters for MANET and Validate the Simulation Results
Stop

Figure 7.11 Proposed flow of Work

SUMMARY

This chapter detects the blackhole node by using aodv routing protocol and use ABC optimization technique for optimizing the route. After that ANN with SVM is used to identify the route and also detect the malicious node in the network. The next chapter deals with the analysis of outcomes including interpretations of all objectives achieved across various parameter types that have been used in this presented work.

CHAPTER 8: RESULT AND DISCUSSION

This particular section determines the evaluated results for the presented algorithm. This chapter covers the result of the "to analyze the network performance before and after triggering the security attacks" (second objective) of this research work. The entire is divided into three sections; each describes the results obtained by triggering three distinct attacks, namely, BHA, GHA, and SPDA. The findings of this research work done are observed and discussed here. The complete information about the comparative performance of presented work has also been provided with a previous approach to analyze their performance.

8.1 RESULTS WITH AND WITHOUT BHA (BLACK HOLE ATTACK)

The BHA comes under the kind of Denial of Service (DoS) attack.

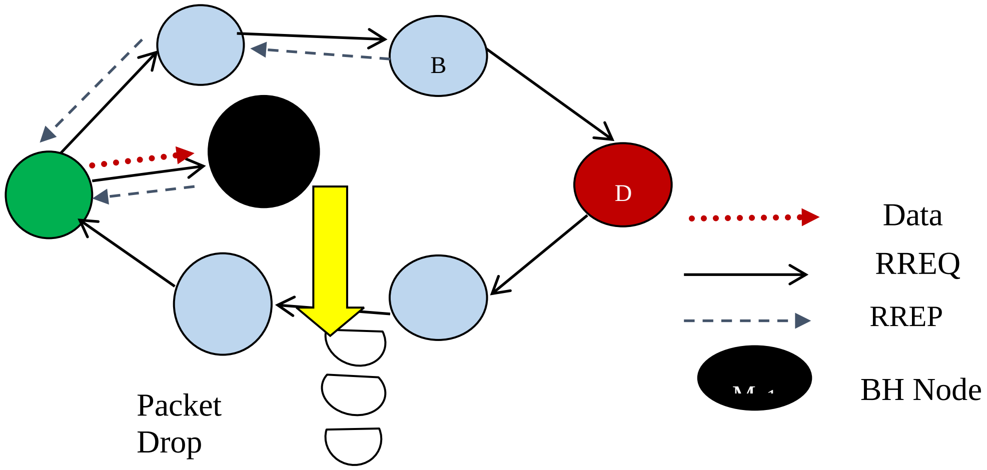


Figure 8.1 Occurrence of BHA in AODV

In which the malevolent node attracts the entire data by behaving like a genuine and shortest route along with the target node. The node with a black hole absorbs the upcoming data without doing forward along with the target node. Let we will discuss its concept with the help of pictorial representation depicted in Figure 8.1 Let node-M is considered as an affected node in this case, as illustrated in Figure 8.1. While the source node is wailings to make communication through the target node, the source side has to broadcast the RREQ packet that is received through nearby nodes that is node-A, node-M, and node-C. As the node-M is a BH node, therefore, it cannot check for the availability of the route towards the node D and hence drop the packet immediately by sending RREP as an acknowledgment message towards the node S before the RREP sends by node A and node C. This process decrease, the PDR. Increase delay as well as consumed energy by the entire network.

8.1.1 Solution to BHA in MANET

To secure MANET from BHA, an improved AODV routing strategy has been constructed by using the concept of ABC with SVM. To lessen the probability of giving data to the BH node instead of genuine node optimization and cross-validation check has been applied using the SVM approach. The results have been evaluated based on the following parameters.

i. Delay

In this presented work, the parameter delay has been taken into regard that defines the rate of the complete amount of delayed received packets through destination up to the amount of packet received by the target node. The data transmission has been initiated by 1000 (number of packets). It is represented mathematically as given below;

$$Delay = \frac{Delayed\ packets\ received\ at\ the\ destination}{total\ count\ of\ packets}$$

It is described as the ratio of packets that are delayed and does not reach at the destination to the total count of the packets reached the destination.

Table 8.1 End to end delay for BHA

Number of nodes	With BHA	Without BHA
20	32	9
40	41	10
60	45	10.22
80	47	14
100	49	14.33

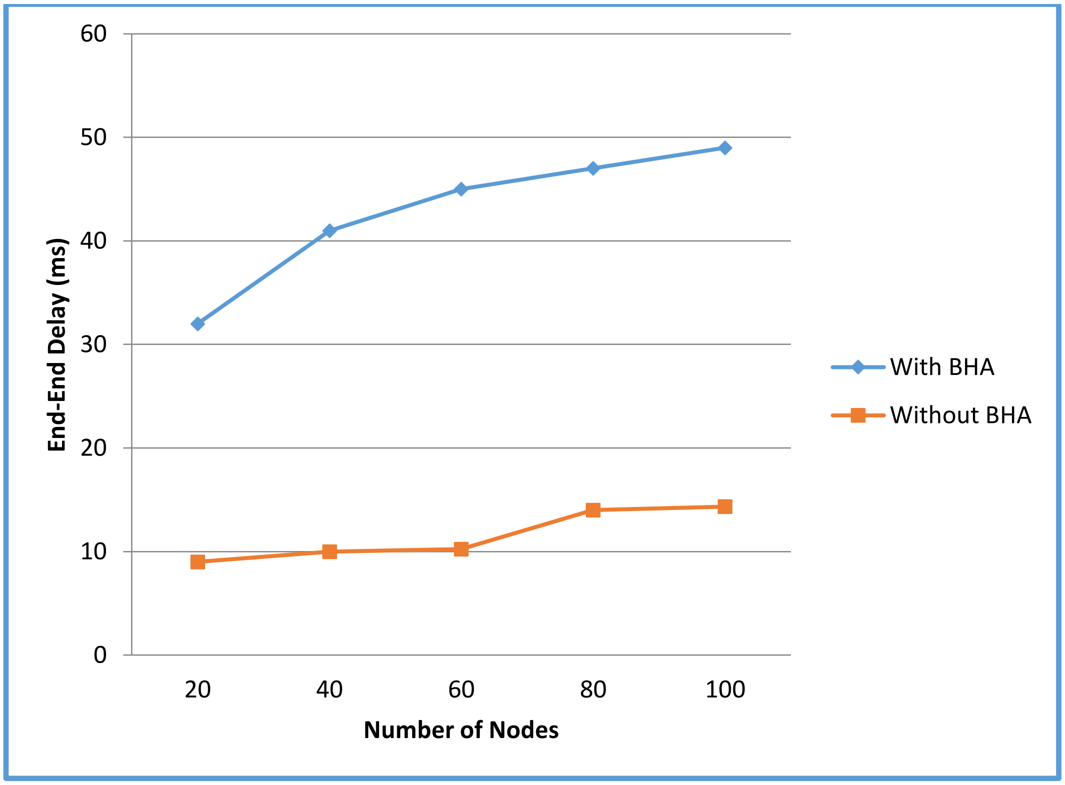


Figure 8.2 Delay for BHA

The table and figure 8.2 dispute that there is a huge difference in the delay in which there is no BHA present inside network topology. When network size is 20, the delay in without BHA is 10, but with BHA, it is 20 more than. Due to enhancing the amount of the node, the slop of with BHA enhanced in a larger amount as compared to without BHA, which is mentioned in the figure.

(ii) Energy Consumption

This parameter is computed on the basis of mobile operation that may have distinct modes of operation, such as transmitting, receiving, idealized, and mode of sleeping. Among them, the mode of transmission and receiving is while the device is in the mode of transaction or operations are doing with packets. When the device is free, it goes to idle mode, but listening to the channel, at last, the sleep mode is while the device is switched off temporarily.

$$Overall\_Energy = \sum_{i=0}^{n-1} (Enegy\_conspumption\_by\_Node(i)))$$

Where i= amount of node and n= total amount of node in the simulation

It is the amount of energy consumed by the nodes when the packets from the adjacent nodes and packets are transferred to the corresponding nodes. When the nodes consume less energy, the network performance improves.

- **Energy uses per packet**

The energy utilization per packet is defined as the rate of total utilized energy through every node by the complete quantity of data packets at the target node that received. The utilization of energy in a greater amount of per packet is the more energy for the successful delivery of packet is necessary. By this parameter, indicates the complete performance of the network protocols at all layers on the basis of energy efficiency.

$$Energy\_per\_packet(\frac{joule}{bit}) = \frac{Overall\_Energy}{Total\_Number\_of\_Recieve\_Packets}$$

In this simulation, we perform the proposed mechanism on an increasing number of mobility nodes for finding the overall energy consumption with or without the presence of a black hole attack. In case if we simulate through minimum nodes amount along with the time of bypassing, we increase it linearly. The outcome of the simulation is detailed in table 8.2 and shown in figure 8.3, which indicates the variance of energy with several nodes.

Table 8.2 Energy Consumption(mj) for BHA

Number of nodes	With BHA	Without BHA
20	14.328	6.753
40	98.2824	75.4373
60	129.55	98.8380
80	157.0053	138.2269
100	174.98	134.98

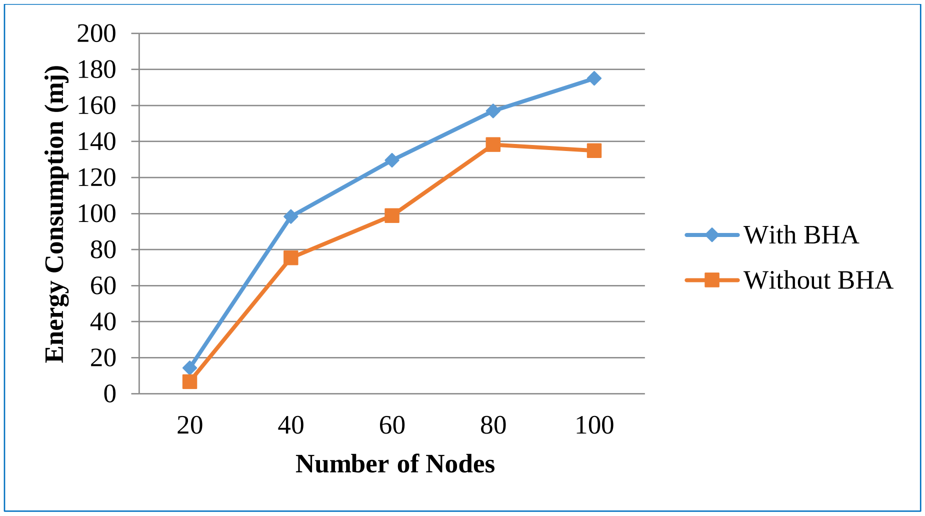


Figure 8.3 End to End Energy Consumption (mJ)

Figure 8.3 shows the connection between vitality utilization and the quantity of hubs with or without a Black Hole assault. In the first place, when the quantity of nodes sent is little, they show very comparative vitality utilization, however as the quantity of nodes builds, connect with the black hole attack consumed more energy as a contrast with the system without a Blackhole attack.

(iii) Throughput

The parameter throughput is described in MANET through the successful delivery of the message or delivery of packets throughout a communication network. Typically throughput is estimated in bit/s or bps. The throughput of the network is the total of the data rates supplied to every terminal inside the network.

$$Throughput(Th) = \frac{Number\ of packet\ recieve}{Total\ time\ interval}$$

A correspondence framework's exhibition that may have been affected by elements, for example, changes factors, including the restrictions of the fundamental physical medium, the adequate handling ability of gadget segments, and the activities of the client.

Table 8.3 Throughput

Number of nodes	With BHA	Without BHA
20	78	81
40	95	100
60	91	97
80	95	100
100	92	93

In view of the various overheads for the convention, the pace of use of the transmitted information might be fundamentally lower than the greatest feasible throughput; the helpful part is normally alluded to as great yield. For better outcomes, throughput ought to be the most extreme conceivable.

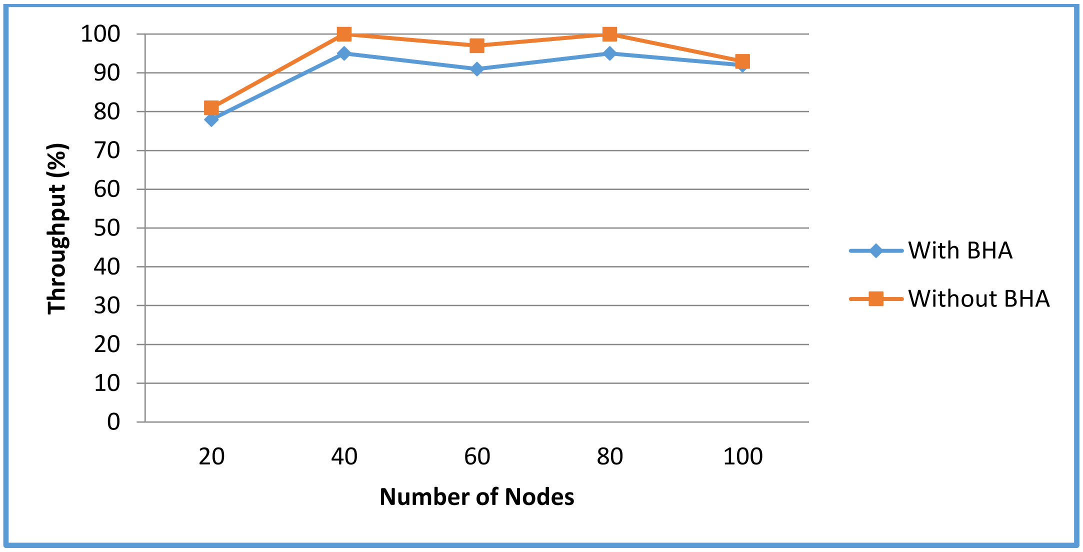


Figure 8.4 Throughput with and without BHA

Figure 8.4 depicted the relation among throughput as well as nodes amount with or without a black hole attack. Initially, if the built-in nodes are present in small amounts, the difference in throughput with or without an attack on the black hole is lower by enhancing the amount of the node inside the network with attacks with a black hole has less throughput due to network errors than compare network without Blackhole attack. However, in the end, they show similar throughput, which means the value of throughput in both cases is 93 corresponds to the 100 number of nodes.

(iii) PDR (Packet Delivery Rate)

This parameter is defined as the rate of data packets gain through the target node and that are produced by the sources. In Mathematical way PDR is represented as;

$$PDR = \frac{Number\ of\ Packet\ receive}{total\ Number\ of\ packet}$$

PDR has an important role, and it shows the actual number of information carrier received by the receiver. The greater the value of PDR, the lesser amount of error inside the network. Ideally, PDR for network topology is 1, which means there is no error in the network that is a hypothetical situation. Also, when PDR is equal to 0 means, there is no packet received by the receiver, which is also a hypothetical situation. For the better result, it will be near to the 1.

Table 8.4 PDR with and without BHA

Number of nodes	With BHA	Without BHA
20	0.9430	0.9835
40	0.9156	0.9504
60	0.8747	0.9447
80	0.8414	0.9214
100	0.8271	0.8805

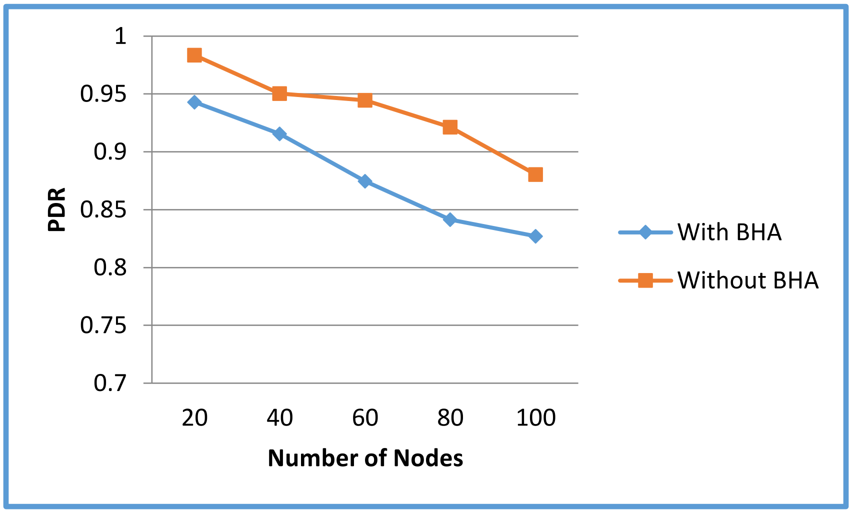


Figure 8.5 PDR with and Without BHA

As depicted in figure 8.5, the relation among the value of packet delivery rate as well as the amount of nodes in two different cases such as including or without including black hole attack. The PDR value corresponds to both the cases is 0.98 without including a black hole attack along with 0.943 is obtained through a black hole attack. Similarly, when the network size increases, both values decrease. When the network size is 100, the result shows a huge difference in Network. PDR without BHA is approx. 0.88 and PDR with BHA are about 0.82, which indicates that the presence of the BHA in-network tropology can affect all the measurement parameters and hence minimizes the outcomes.

8.2 RESULTS IN THE PRESENCE OF GREY HOLE ATTACK(GHA)

GHA is a continuation of the BHA and is used to bluff the transmitting node as well as the entire system by partially forwarding data to the upcoming node. In this scenario, the adjacent node thinks that the previous node is delaying the data packet by some other technical reason. In this way, the Grey hole (GH) node drops data packet based on a selective data packet dropping approach and behaves like a genuine node. GH node involved in the entire communication process started from the discovery of route up to the reception of data by target node and also updated its route as the shortest path in the routing table of the AODV mechanism.

Since GH node collects all incoming data but drops randomly, therefore, it becomes hard for researchers to secure a network from GHA because the reason for dropping the packet might be due to the malicious nature of the node or might be due to overloading and congestion nature. With the aim to compute, the network performance in the presence, as well as when the network is secure from the GHA node using ABC with the SVM approach, is discussed below.

Table 8.5 Delay for GHA

No. of nodes	With GHA	Without GHA
20	28.02	7.12
40	38.35	8.45
60	41.76	9.23
80	45.91	11.25
100	46.24	13.67

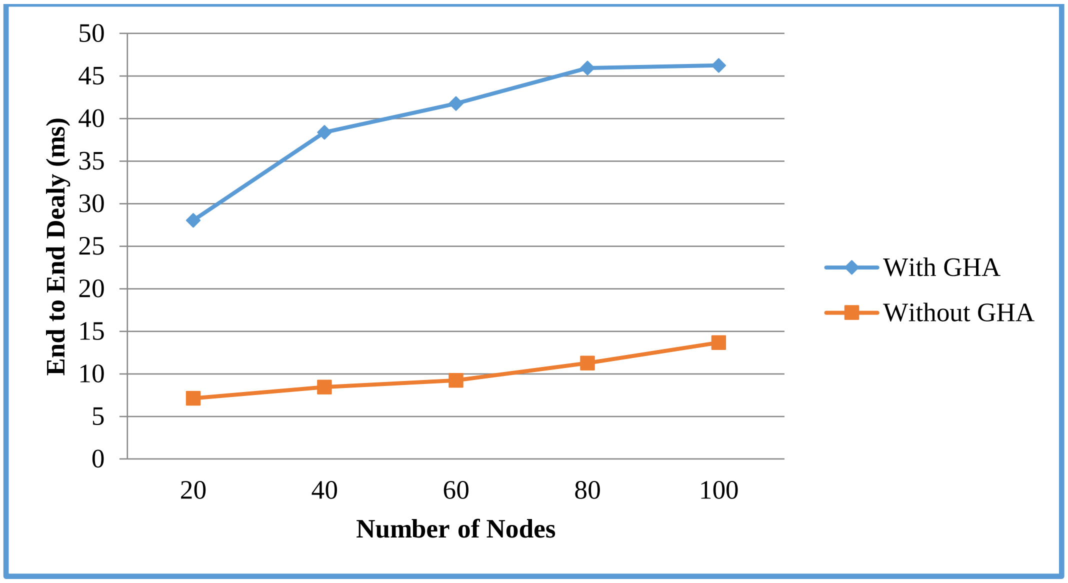


Figure 8.6 Delay for GHA

As shown in figure 8.6 depicts the information about the delay within the network topology in the presence of a Grey hole attack. While the node size is 20, network delay without GHA is 7.12, but in the presence of the GHA, it shows 4 times that of without

GHA, i.e., 28.02. After increasing, the network size both value increases linearly, and at the end, when the network size is about 100, delay without GHA is approx. 13.6, and with GHA, it is 46.24 that is quite higher.

Table 8.6 Energy Consumption for GHA

Number of nodes	With GHA	Without GHA
20	13.138	5.283
40	96.242	72.987
60	124.87	97.189
80	155.051	132.761
100	174.98	134.98

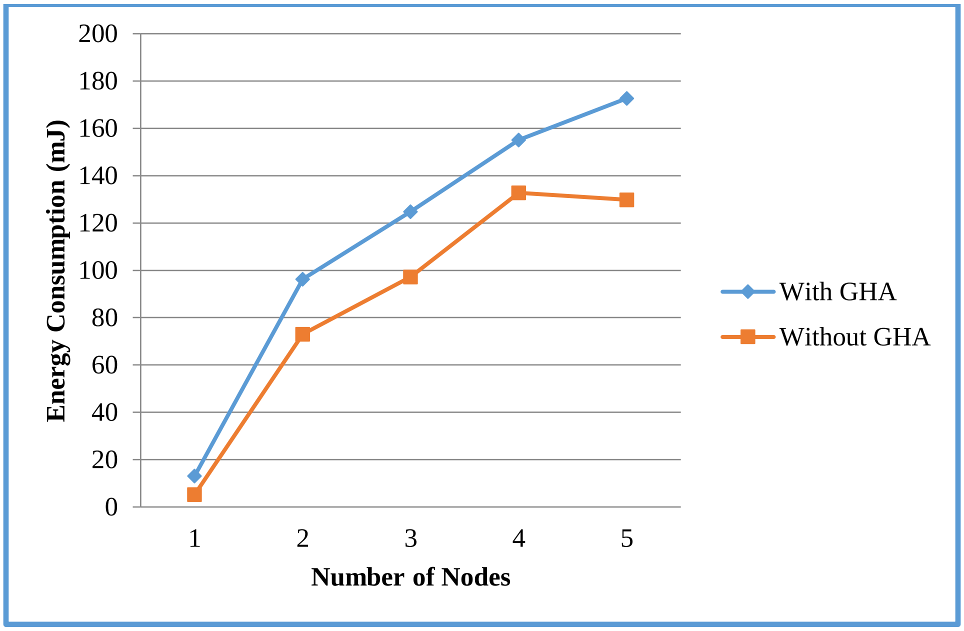


Figure 8.7 Energy Consumption with and without GHA

Figure 8.7 shows the relation among the energy consumption and several nodes in network simulation with or without GHA. At the stating when node size is 20, the energy consumption with GHA is 13.138, while without GHA, it is 5.283 that is half off with GHA. Through increasing the sizes of nodes, the energy consumption of tropology is also enhanced, as well as at the end, when node size is 100, energy consumption with GHA is 174.98, and without GHA, it is 134.98.

(i) Throughput

Table 8.7 Throughput with and without GHA

Number of nodes	With GHA	Without GHA
20	80	88
40	96	100
60	92	98
80	96	100
100	93	96

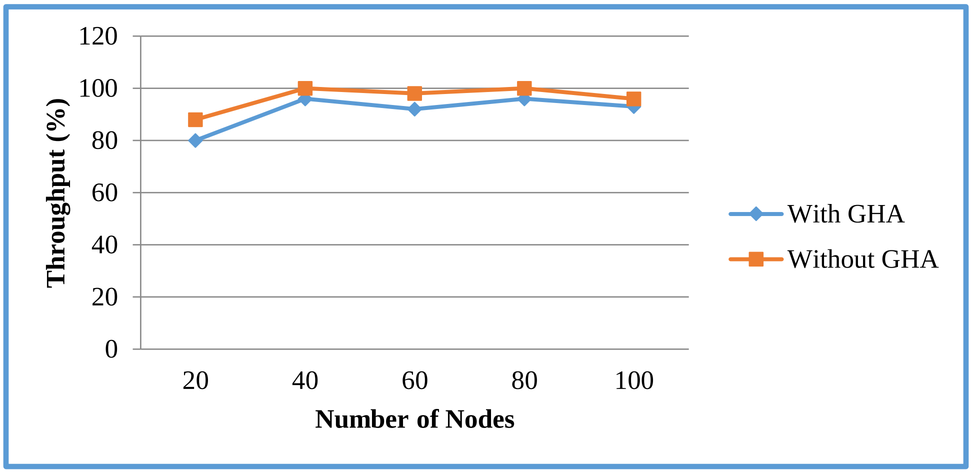


Figure 8.8 Throughput with and without GHA

Figure 8.8 represented the coordination among throughput and amount of nodes with or without Grey Hole Attack. In the beginning, while the amount of nodes deployed is smaller(i.e., size of the node is 20), the difference in throughput with or without a BHA is small (with GHA, it is 80, and without GHA it is 88). Due to increasing the node amounts, the amount of attackers nodes is increased as well as throughput is decreased. However, in the end, they show quite a similar throughput, i.e., if the node amount is 100, the throughput in both cases is 93 and 96 (without GHA).

(ii) Packet Delivery Ratio (PDR)

Table 8.8 PDR with and without GHA

Number of nodes	With GHA	Without GHA
20	0.9512	0.9912
40	0.9203	0.9543
60	0.8967	0.9423
80	0.8852	0.9298
100	0.8376	0.8823

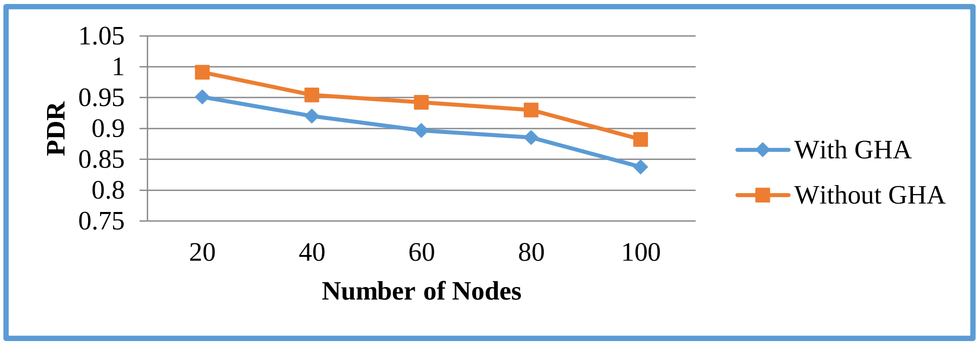


Figure 8.9 PDR with and without GHA

Figure 8.9 depicts the relationship between PDR and node amounts with or without a grey hole attack. In the case of a smaller size of the network, PDR without a grey hole attack is 0.991, while with a grey hole attack, it is 0.95. Similarly, when the network size increases, both values decrease. When the network size is 100, the result shows a huge difference in Network. PDR without GHA is approx. 0.88 and PDR with GHA are about 0.837, which indicates that the presence of the GHA in-network tropology can affect all the measurement parameters and hence minimizes the outcomes.

8.3 RESULTS IN THE PRESENCE OF SELECTIVE PACKET DROP(SPD)

The selective Packet Discard (SPD) techniques in MANET are used to manage the process-level input laws on the Route Processor (RP). The main motive of SPD is to give priority to routing protocol packages and other important traffic control layers by keeping them alive during periods of process-level congestion.

SPD is a kind of DoS attack, which relay packets instead of dropping the packets. For detection as well as prevention of network from attack, ABC, in combination with SVM, has been used and the results obtained before and after the prevention algorithm are discussed in the following section.

(i) Delay for SPD

Table 8.9Delay SPD

Number of nodes	With SPD	Without SPD
20	44	12
40	67	23
60	79	35
80	82	68
100	91	74

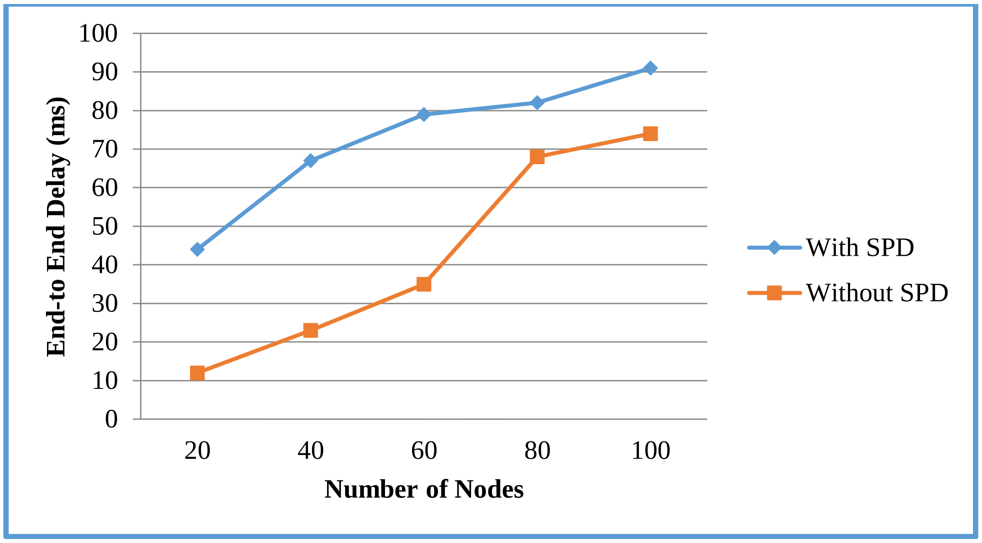


Figure 8.10 End to End Delay with and without SPD

Table 8.9 and figure 8.10 demonstrate the information regarding delay as well as its change in behavior by node amounts are increases in the presence of SPD network tropology. In particular, a case in which is a small amount of nodes are present, delay with SPD is 44, and delay without SPD is 12 that is three times lesser than the with SPD. By increasing the size of network cases increase, the dealy for both cases is increased linearly, and at the end, when the number of nodes is about 100 delay with SPD is 91 and delay without SPD is 74.

(ii) Energy Consumption for SPD

Table 8.10 Energy Consumption for SPD

Number of nodes	With SPD	Without SPD
20	19.20	10.753
40	110.23	83.29
60	133.24	104.86
80	168.98	142.976
100	177.90	145.981

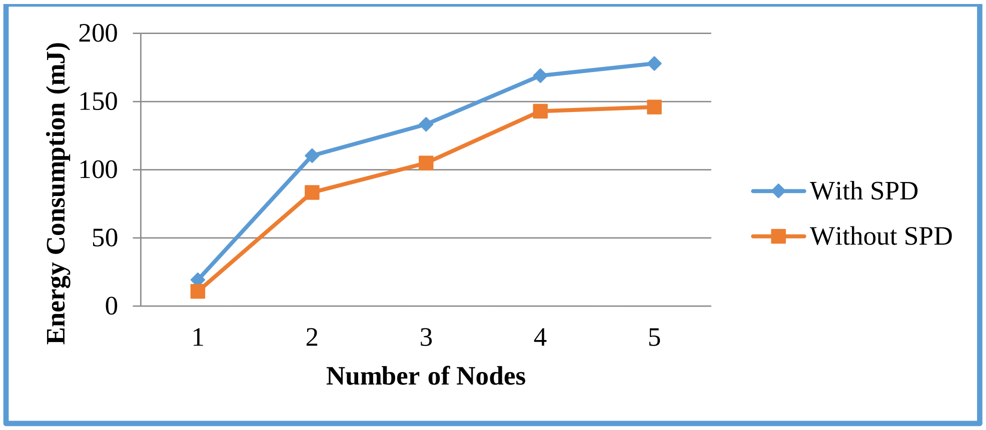


Figure 8.11 Energy Consumption with and without SPD

Table 8.10 and Figure 8.11 demonstrate the information about energy consumption and its change in behavior through the amount of the node in the presence of SPDA. When the amount of nodes is small, delay with SPD is 19.20, and delay without SPD is 10.73 that is lesser than with SPD. By increasing the size of the network, the delay in both the cases has been increased linearly, and at the end, if the number of nodes becomes 100, the obtained consumed energy with SPD is 177.9, and energy consumption without SPD is 145.98.

(iii) Throughput

Table 8.11 Throughput with SPD

Number of nodes	With SPD	Without SPD
20	65	78
40	87	90
60	86	93
80	82	96
100	80	97

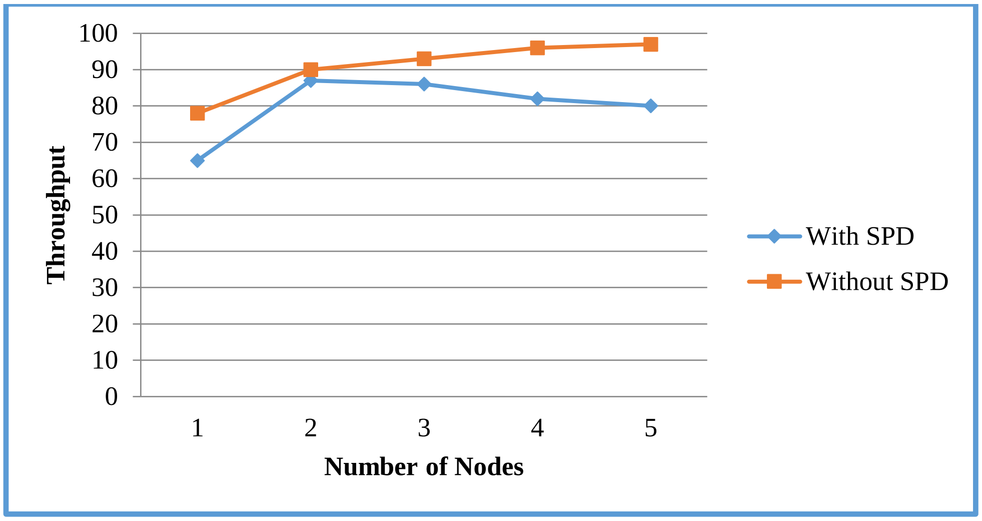


Figure 8.12 Throughput with and without SPD

Figure 8.12 represented the relation between throughput and node amounts with or without SPD. In the beginning, while the number of deployed nodes is small (i.e., size of the node is 20), the difference in throughput with or without a black hole attack is small (with SPD it is 65, and without GHA it is 87).

Table 8.12 PDR with and without SPD

Number of nodes	With SPD	Without SPD
20	0.9212	0.9723
40	0.9012	0.9398
60	0.8509	0.9109
80	0.8312	0.8924
100	0.8012	0.8746

There is an increment in the amount of attacker node, including reduced throughput value through increasing the amount of the node. However, in the end, they show quite a similar throughput, i.e., if the node amount becomes 100, the throughput in both cases is 80 and 97 (without SPD).

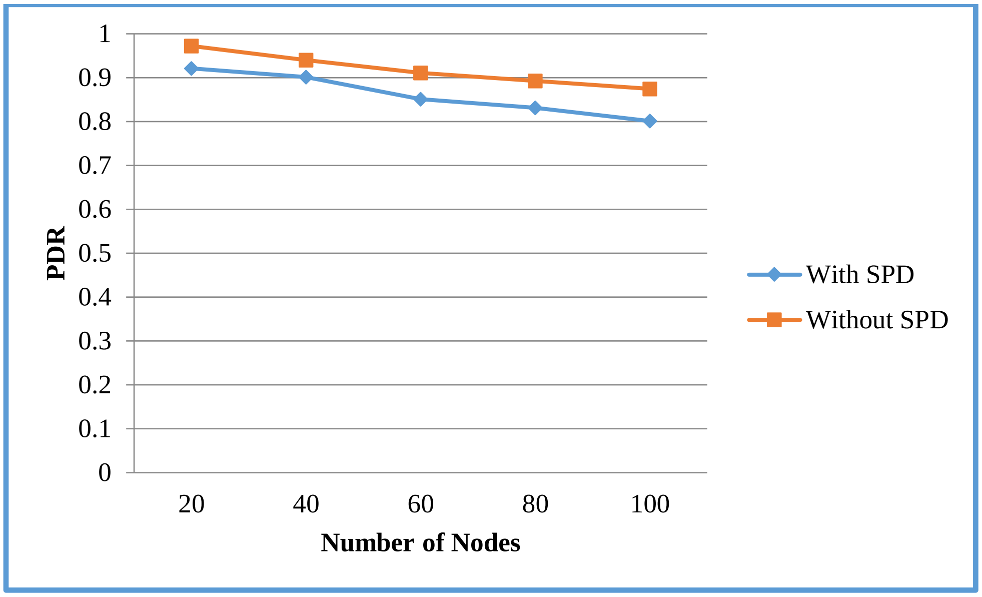


Figure 8.13 PDR with and without SPD

Figure 8.13 rendered the relation among the PDR along with the number of nodes with or without SPD. If node size is small, PDR without SPD is 0.972, while with SPD, it is 0.921. Similarly, when the network size increases, both values decrease linearly. When the network size is 100, the result shows a huge difference in Network. PDR without SPD is approx. 0.87 and PDR with SPD are about 0.801, which indicates that the presence of the SPD in network topology can affect all the measurement parameters and hence minimizes the outcomes.

8.4 RESULT OF ABC+SVM

The effectiveness of the presented technique is described by developed mechanisms. They take into account the following parameters. The results have been assessed using linear and polynomial grain. The framework of the assessment taken is pre and post-attack. The assessment is carried out while retaining the following limitations.

a) Delay

The parameter delay is defined as the ratio of received delayed packets incomplete amount through the target node to the amount of packets got through a destination. It is represented mathematically as given below;

$$Delay = \frac{Total\ delayed\ packets\ received\ at\ the\ destination}{number\ of\ packets\ received\ \ at\ the\ destination}$$

Table 8.13 Delay (in seconds)

Number of nodes	Delay (in seconds) of the Presented approach	Delay (seconds) obtained by past approch[13]	Delay obtained in [16]
20	9	28	10.01
40	10	32	11.11
60	10.22	38	13.43
80	14	44	14.55
100	14.33	48	15.03

The contrast of the delayed packets provided in table 8.13 with end to end. The provided table is vivid that perhaps the delay implemented for various sensor nodes has been reduced. The delay for 20-100 nodes has been enhanced from 9 to 14.33. Nevertheless, the delay introduced by the proposed technique is smaller than that of the traditional approaches.

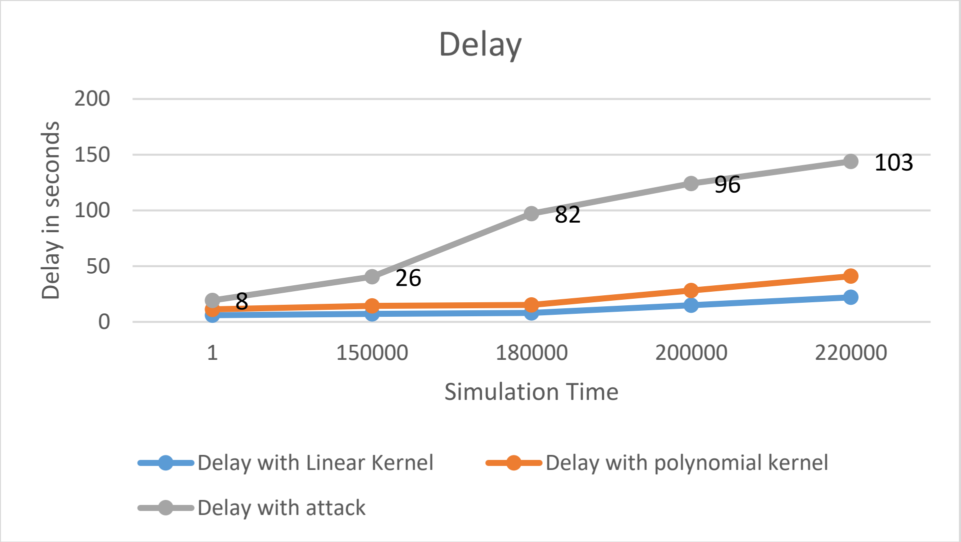


Figure 8.14 Delay computation

Figure 8.14, given, indicated that the delay is lower in contrast to the previous approach. This parameter has grown by increasing the sensor nodes with the amount of 20. In this presented approach, the dealy value in the average amount is approx 11.52, whereas this value fo past mechanism is 38 corresponds to [13] and 12.82 for [17]. Thus, the delay has been improved by $\frac{38-11.51}{38} \times 100 = 69\%$ obtained corresponds to work presented as compare to past approach, i.e. [13] and 10% for [16].

b) Consumption of energy

The energy that consumed through network nodes during packets is received through neighboring nodes along with the transmission of packets up to respective nodes. The performance of the network has been increased due to less consumed energy.

It makes clear from the given figure 8.15 that the presented approach utilized lower consumed energy as compare to the existing approach [17]. The amount of energy on average consumed through the presented approach, and past work is 626250 and 713750 correspondingly. Therefore, the complete consumed energy through the presented work is enhanced by $\frac{713750-626250}{713750} \times 100 = 12\%$.

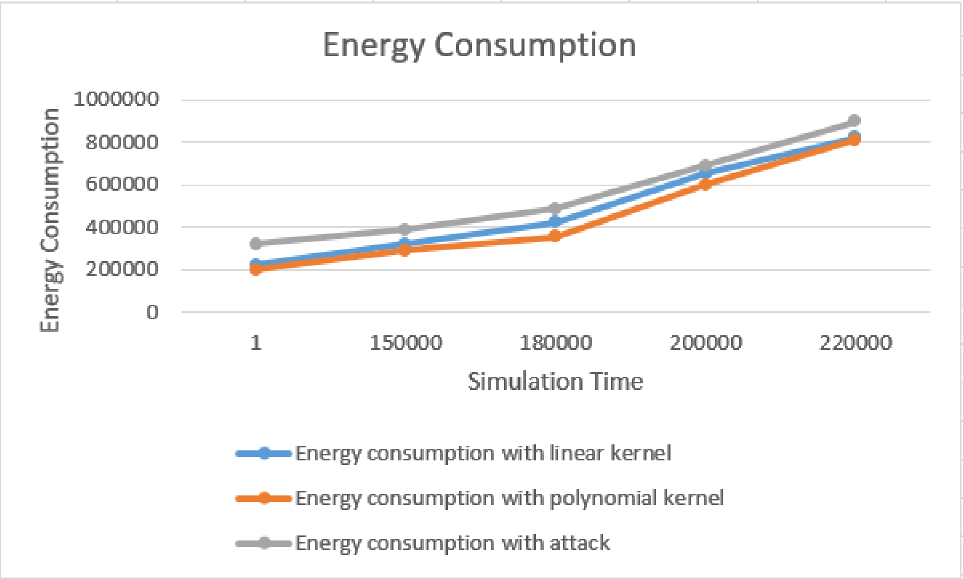


Figure 8.15 Energy Consumption

c) Throughput

This parameter is explained as the delivered ratio of complete amounts of packets to the destination in every corresponding time frame. The complete amount of delivered packet is represented through T_{Pd}, and throughput, as well as the time frame, is indicated by T and t, respectively.

$$T = \frac{T_{Pd}}{t}$$

Table 8.14 Throughput

Total No. of Simulations	Throughput (With Attack)	Throughput (by Linear Kernel)	Throughput (by the polynomial kernel)
100	10000	20000	20000
200	20000	40000	40000
300	40000	60000	60000

400	57000	76000	77000
500	59000	81000	85220

The throughput of the presented approach is provided in table 8.14 by using a linear along with the polynomial kernel. Here, the findings have been analyzed through 500 simulations that are in a repeating manner for computation of throughput value for this approach. The obtained value through polynomial kernel has seen as enhanced contrast with a linear kernel. The higher attained throughput in this presented approach corresponding to the linear and polynomial kernel is 55400 and 56444, respectively. On the other side, the obtained throughput without prevention is 37200. It has to be clear from the result the rate of throughput by applying polynomial kernel is improved as a contrast with linear kernel and without the prevention system.

In figure 8.16 provide the representation of throughput for the present approach that is analyzed through both polynomials as well as linear kernel. The findings of the presented scheme are enhanced as a contrast to the values with the attack; it makes clear that the performance of the polynomial kernel is enhanced as compared to the linear kernel. The obtained rate of throughput on average is 56444, and 55400 corresponds to polynomial as well as linear kernel. Therefore, the throughput rate of the network has been enhanced through a polynomial kernel corresponding to 500 simulation rounds is $\frac{56444-55400}{56444} * 100 = 1.8\,\%$. With the intrusion effect, the network performance of the network becomes very low.

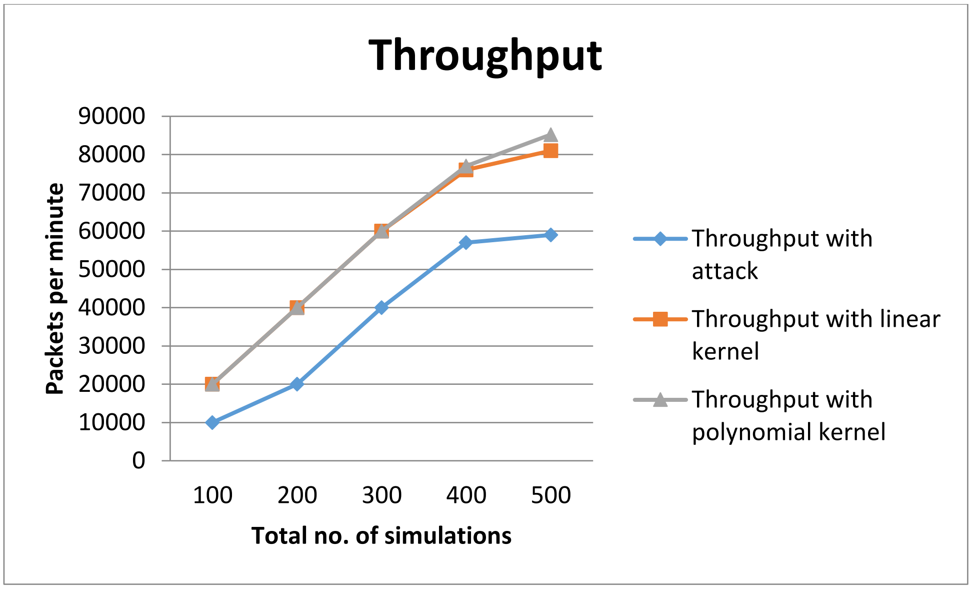


Figure 8.16 Throughput Evaluation

The model depicted only 37200 (units) of packet transfer in every minute for the same set of simulation architecture. Due to the high packet dump, the value of throughput under intrusion is very less. The minimum value of PDR, along with higher consumption of bandwidth results in high packet dumps.

d) PDR (Packet Delivery Ratio)

This parameter is described through the ratio of the complete amount of received packets to the complete amount of packets transferred. Also, say the $_{Received}$ is denoted the total received packets and $T_{ransmitted}$ is corresponds to the packets transmitted.

$$PDR = \frac{T_{received}}{T_{transmitted}}$$

Table 8.15 PDR EVALUATION

Number of Simulations	PDR (under threat)	PDR (after prevention with linear Kernel)	PDR (after prevention for polynomial Kernel)
100	0.23	0.6	0.93
200	0.26	0.60	0.94
300	0.30	0.633	0.95
400	0.33	0.69	0.97
500	0.35	0.80	0.99

Table 8.15 represents the PDR for the presented approach by utilizing linear as well as polynomial kernel. This work performance has been examined by 500 simulations that are repeated for validation of results.

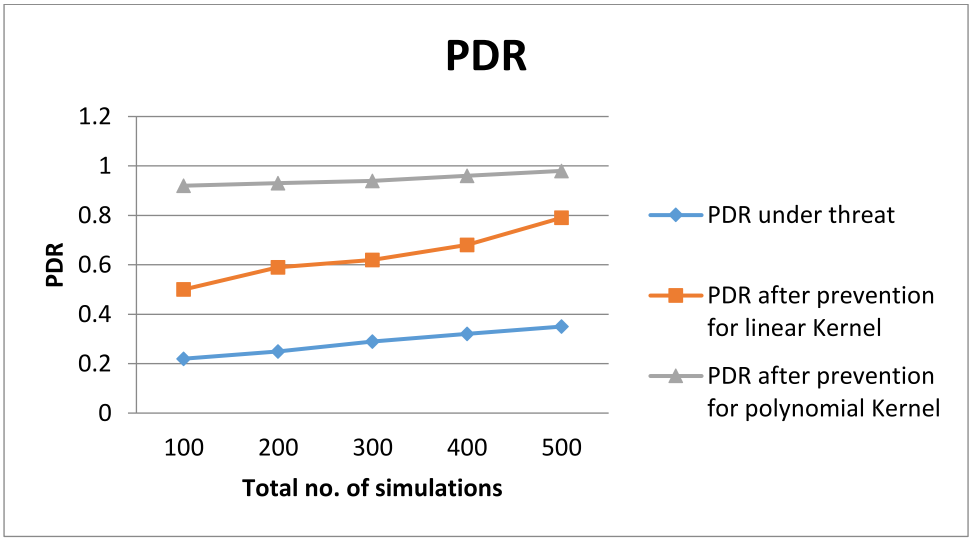


Figure 8.17PDR Evaluation

In figure 8.17 represents the PDR for the current approach obtained by utilizing linear along with the polynomial kernel. It has to be analyzed from the given figure; the under threat is around 0.30 that comes under the very low range, i.e., with 0.2 - 0.36. After prevention by utilizing linear kernel of SVM classification mechanism, the value of PDR is obtained in the range of 0.5 – 0.8 is 0.639 for 100 – 500 simulations.

The average value of the polynomial kernel is considered around 0.94. This produced value is indicated that the delivery rate of the packet using the polynomial kernel is improving through considering the prevention framework in the network. Likewise, for experiments of 100 to 500 iterations, PDR utilizing SVM prevention architecture for polynomial kernels is between 0.6 and 0.94.

8.5 RESULT WITH ABC AND ANN

In this first we compare the parameter for four different conditions, such as under threat (GHA and BHA) node, AODV, AODV with ABC, and after preventing the network using ANN. After the simulation, the performance has been evaluated, and the comparison with the existing approach presented by Ali Zardari et al. 2019 has been shown. The entire work has been conducted in MATLAB simulator.

Table 8.16 PDR (%)

Number of Nodes	Under Threat	AODV	AODV with ABC	After Prevention
100	44	58	82	94.7
200	48	60	84	95.8
400	52	64	87	96.9
600	55	67	88	97.1

800	58	68	90	97.7
1000	60	70	92	98.24
2000	62	72	93	98.66

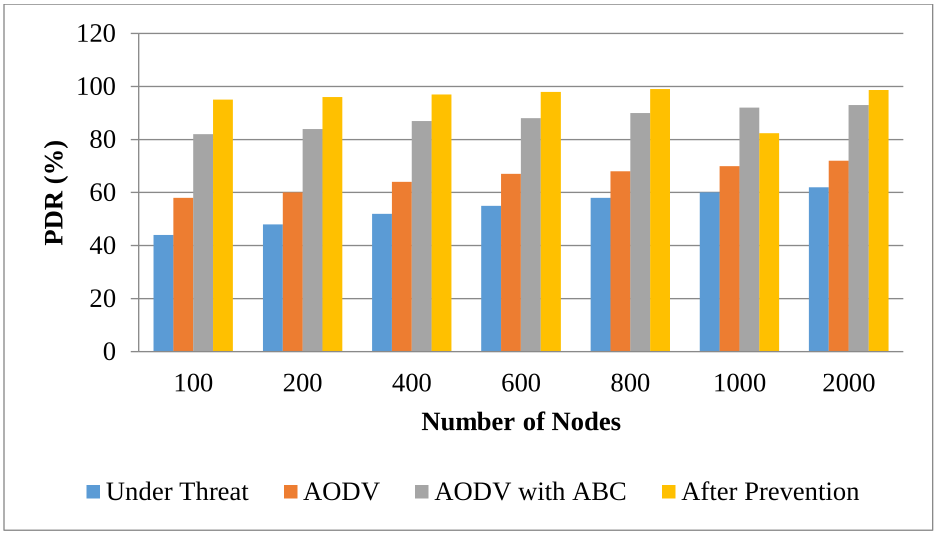


Figure 8.18PDR

Figure 8.18 represents the values examined for the PDR parameter for four different conditions, such as under threat (GHA and BHA) node, AODV, AODV with ABC, and after preventing the network using ANN. From the Figure, the highest PDR of about 98.66 % has been examined for 2000 nodes. This is because, after preventing the MANET against BHA and GHA node, packets are delivered efficiently as well as at high speed to the target node. After the implementation of the proposed algorithm in hybridization that is AODV with ABC and ANN approach, the PDR rate has been increased slightly compared to the remaining three conditions, as indicated by the blue, the red, and the green color respectively. Also, the observed values of PDR are indexed in Table 8.16.

Table 8.17 Throughput (Kbps)

Number of Nodes	Under Threat	AODV	AODV with ABC	After Prevention
100	58.97	68.02	80.25	85.64
200	60.25	72.94	82.59	86.98
400	62.57	75.36	85.25	88.02
600	63.87	78.75	87.94	89.64
800	65.94	79.25	88.92	90.57
1000	66.32	80.25	89.25	91.89
2000	67.85	82.67	90.04	92.96

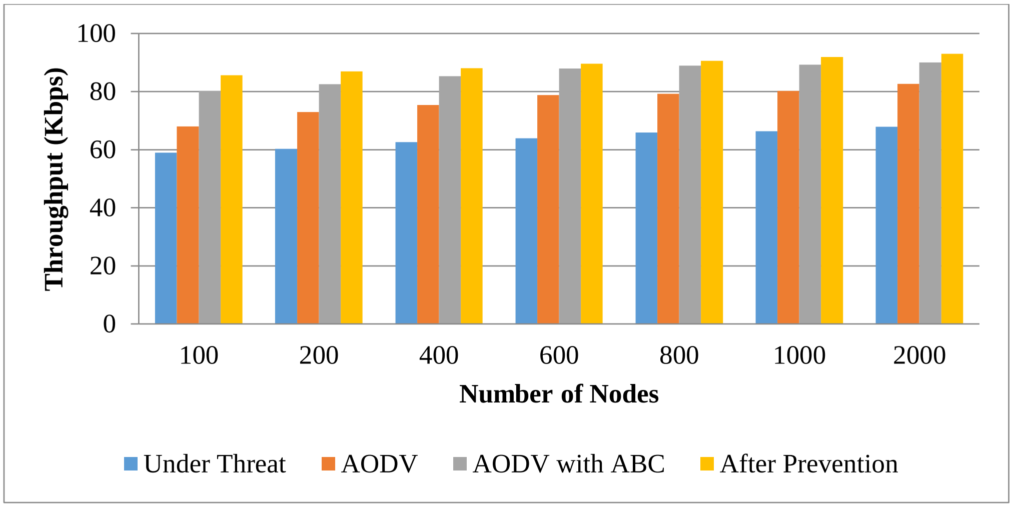


Figure 8.19Throughput

The throughput values analyzed under threat, after prevention from (GHA and BHA), AODV, AODV with ABC as well as the values observed by proposed work (after prevention) has been depicted in Figure 8.19. The case when the nodes are usually communicating, and their communication is disturbed by the attacker node by sending the false request or by claiming that the route through the attacker node is the exact route or the shortest path, the throughput gets degraded. The performance has been increased by identifying the affected node and passing the data to the user node, which has been done using GA with the ANN approach. The values examined using the proposed technique after prevention, under threat, and AODV, AODV with ABC are listed in table 8.17.

Table 8.18 Average Delay (S)

Number of Nodes	**Under Threat**	**AODV**	**AODV with ABC**	**After Prevention**
100	0.13	0.11	0.099	0.059
200	0.19	0.13	0.12	0.062
400	0.22	0.145	0.133	0.065
600	0.26	0.159	0.142	0.068
800	0.28	0.167	0.151	0.075
1000	0.29	0.174	0.158	0.18
2000	0.30	0.179	0.162	0.22

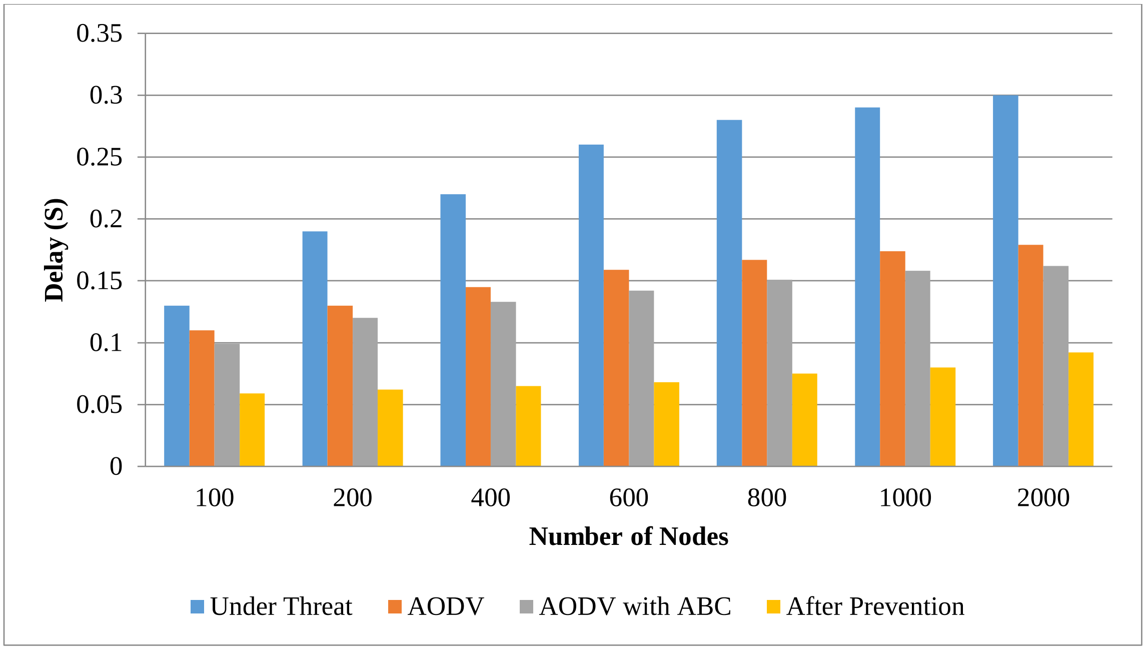


Figure 8.20Delay

The interval of time taken by the communicating nodes to send the data packet from the source to the destination node successfully within the time frame is represented by delay. From the Figure, it has been observed that the delay analyzed under the malicious node (BHA and GHA) nodes is high as indicated by the blue bar because of the drop-down of a data packet during the communication process. From the graph shown in Figure 8.20, there is a constant increase in the delay that has been observed with the amplification of deployed nodes. Also, it is clearly observed that the delay followed by ABC with the ANN approach performs better in contrast to existing work.

Table 8.19 Energy Consumption (mJ)

Number of Nodes	**Under Threat**	**AODV**	**AODV with ABC**	**After Prevention**
100	15.024	7.265	5.267	2.325
200	17.0325	8.257	6.257	2.758
400	18.014	8.574	8.365	3.254
600	19.025	9.236	9.157	4.257
800	20.274	11.325	10.357	5.698
1000	21.368	12.365	11.325	6.742
2000	22.658	12.875	11.987	7.478

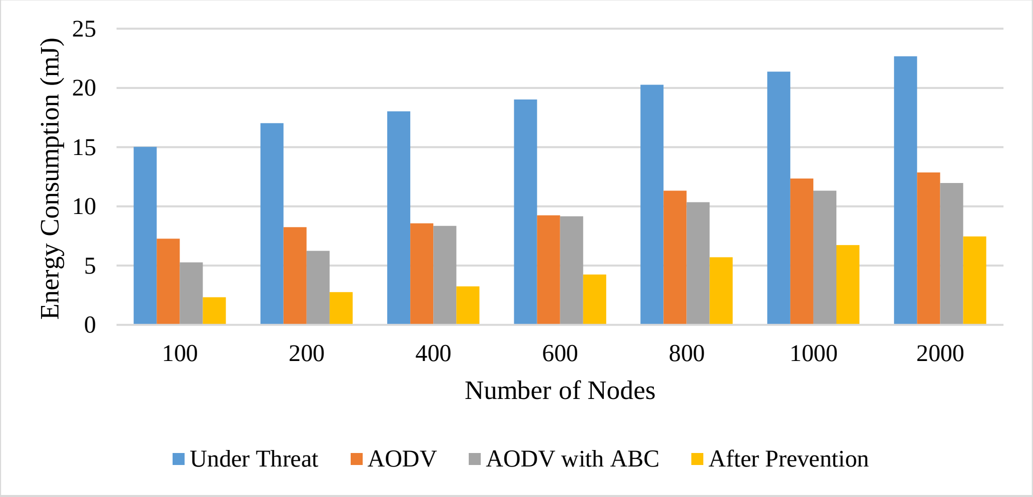


Figure 8.21 Energy Consumption

In figure 8.21 shows the total consumed energy through nodes in different scenarios rendered through blue, the orange, the grey, and yellow bar. The graph indicates that using the proposed technique, the overall consumed energy through communicating nodes is smaller compared with the rest of the scenarios. Here, in this presented scheme, the average value of consumed energy is 4.64mJ.

8.6 COMPARISON OF PROPOSED WORK WITH EXISTING WORK

For the efficiency analysis purpose of the designed secure MANET system, the comparison has been made by past mechanisms presented through Ali Zardari et al. 2019. The comparison has been made based on average values examined for PDR, Throughput, and delay, as depicted in Table 8.20.

Table 8.20 Comparative Analysis for examined Parameters

PDR (%)		**Throughput (Kbps)**		**Delay (s)**		**Energy Consumption (mJ)**	
Proposed	**Ali Zardari et al. 2019 [103]**	**Proposed**	**Ali Zardari et al. 2019 [103]**	**Proposed**	**Ali Zardari et al. 2019 [103]**	**Proposed**	**Ali Zardari et al. 2019 [103]**
97.55	96.94	89.38	79.08	0.071	0.087	4.64	5.02

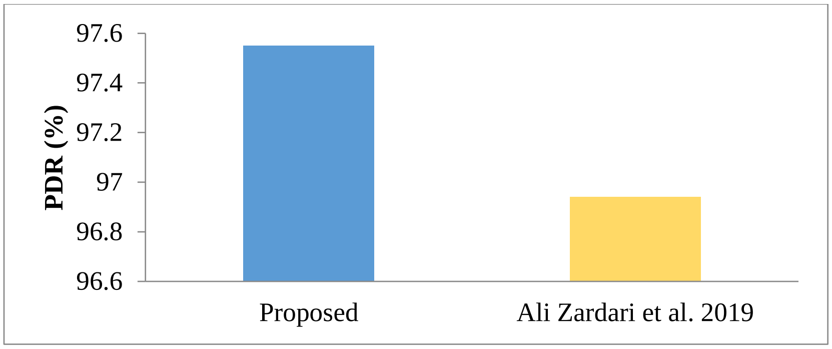


Figure 8.22 Comparison of PDR

The comparison of PDR against Ali Zardari's work is shown in figure 8.22. The graph has shown an enhancement of about 0.63 % while using ANN with the ABC algorithm. This is because in [103], the authors have used a traditional approach named CDS (connected Discriminant Set) approach, in which a set of nodes has been created based on their energy. The authorization of the node has been checked based on the energy. During this process, the chances of packet drop increase because each node contains a data packet for a long time. To overcome this problem, we create a model using the concept of AI for detection of intrusion in the network automatically, and the achieved average PDR is of 97.55%.

Using AI technique, intermediate nodes transfer the data packet different nodes without any delay, then the rate of data delivery, as well as the speed of data delivery rate increases, which is represented in terms of the Throughput parameter, as shown in Figure 8.23.

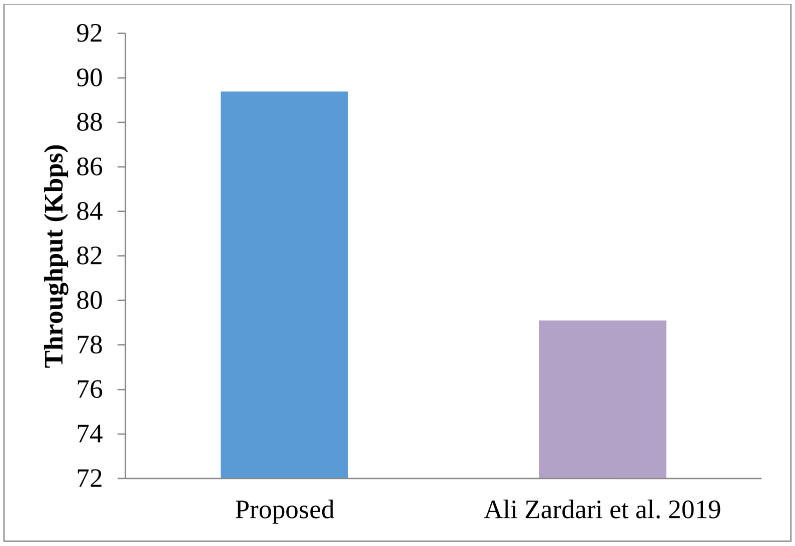


Figure 8.23 Comparison of Throughput

The obtained throughput of the presented work has been examining by deploying nodes (N= 100, 200, 400, 600, 800, 1000, 2000) in the proposed work against the existing work [103]. Figure 5.19 indicates the throughput examined for this work is better compared to the [103]. Also, there is an enhancement of $\{(\frac{89.38-79.08}{79.08})\ \times 100\}$ =13.02 % has been observed compared to the [103] work.

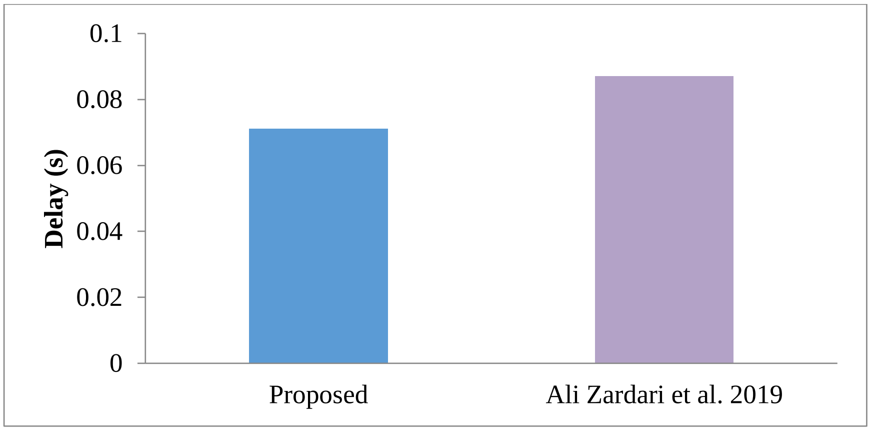


Figure 8.24 Comparison of Delay

The comparison of delay produced during the communication process in [103] with the presented approach is depicted in figure 8.24. Using the swarm-based approach in combination with the AI approach, the speed of data transmission has been increased, and the percentage reduction in the data transmission observed compared to the [103] work is calculated as; $[(\frac{0.087-0.071}{0.071} \times 100)]$=18.39%. This is because the list of affected nodes and the normal node is created by an ABC algorithm on the basis of which accurate route is selected by the ANN algorithm. This process helps to enhance the speed and hence reduce the delay.

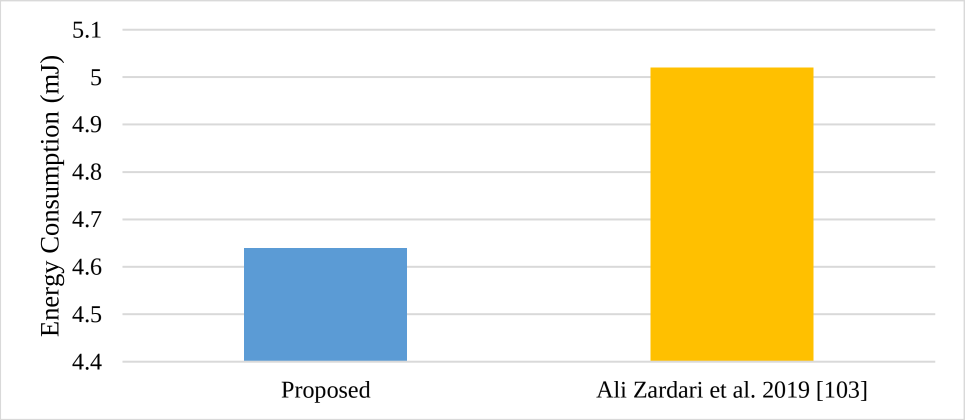


Figure 8.25 Energy Consumption

Here, the comparison of consumed energy through nodes during the process of communication against the existing work is shown in Figure 8.25. From the graph, it is clearly seen that in this presented scheme, the consumed energy is less in contrast with existing work. Therefore, the percentage of energy saved obtained using the proposed approach of 7.57 % has been obtained against the exiting work [103].

8.7 RESULTS WITH ABC+ANN+SVM APPROACH

The results have been computed in MATLAB simulator that offers a simple platform for network simulation. The nodes are deployed in range of {N=100, 200, 400, 600, 800, 1000, 2000}. The results have been computed based on parameters such as throughput, PDR, and Delay. The obtained outcomes are examined using AODV along with ABC with the ANN approach. To analyze the effectiveness of the presented work, the comparative has also been done.

Table 8.21 PDR

Number of Nodes	Under Threat	AODV without Threat	AODV with ABC	After Prevention
100	42.5	48.52	84.55	96.45
200	51.25	57.41	85.22	96.47
400	56.75	65.22	88.13	98.75
600	60.66	66.27	89.72	98.76
800	65.37	69.47	91.67	98.74
1000	67.2	72.24	93.74	99.17
2000	69.77	75.47	94.72	99.38

In table 8.21represented the computed values examined for the designed network based on PDR metrics, its graph is illustrated in figure 8.26. PDR represents the rate of reception for the complete amount of packets to the transmission quantity of packets that are transmitted. The graph shows four different values:

- AODV under Threat
- AODV with Threat
- AODV with ABC
- AODV with ABC, ANN & SVM (After Prevention)

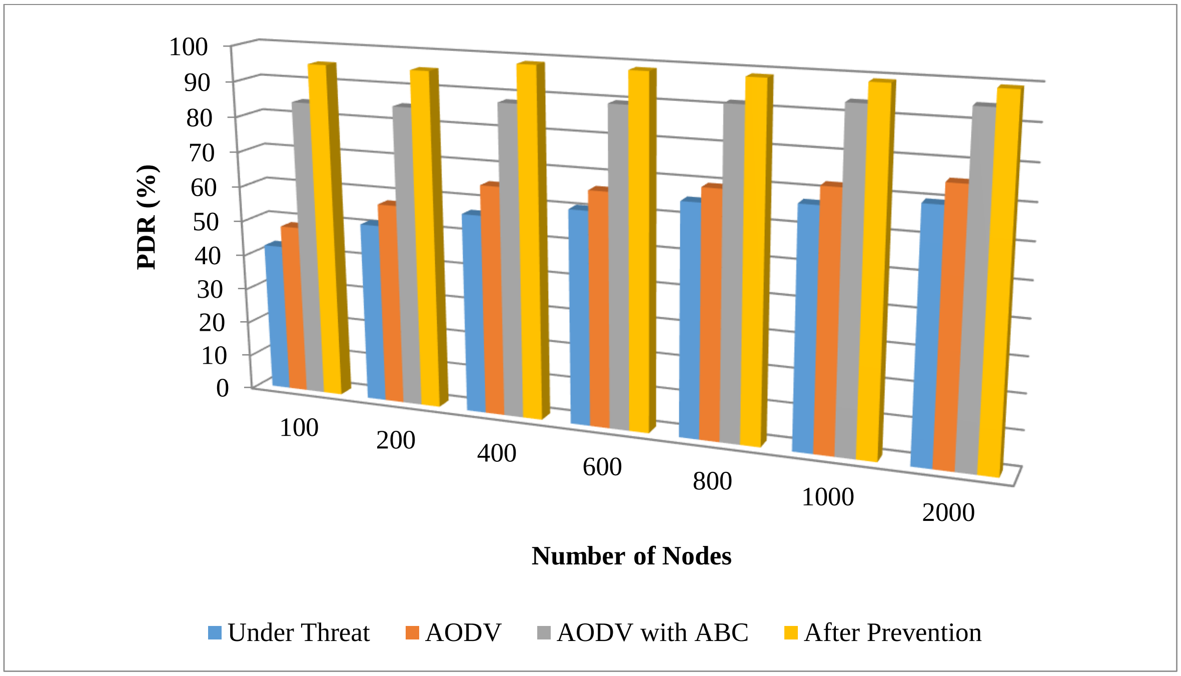


Figure 8.26 PDR

As per the given graph in Figure, it makes clear that the proposed approach (modified AODV) using ABC and ANN with the SVM method has been performed well. The values are analyzed with respect to the quantity of nodes as indicated towards the horizontal axis. To show the enhancement compared to the other considered scenario, the average value for each has been calculated. The average value analyzed with AODV under Threat, AODV without Threat, AODV with ABC, and after prevention are 59.07, 64.94, 89.67, and 97.96, respectively. Therefore, the highest PDR has been examined for the proposed work.

Table 8.22 Throughput (Kbps)

Number of Nodes	**Under Threat**	**AODV**	**AODV with ABC**	**After Prevention**
100	53.02	67.8	82.7	89.2
200	54.83	70.67	84.22	89.8
400	61.3	73.13	87.08	91.79
600	62.9	76.17	89.51	92.92
800	64.29	77.09	90.87	94.3
1000	66.34	79.2	93.3	95.22
2000	67.02	80.82	93.33	96.23

Throughput represents the transmission information of packets in a network. The analyzed values for four distinct situations, including the nodes with varying amount i.e., 100, 200, 400, 600, 800, 1000, and 2000 are listed in Table 8.22. The graphical representation of throughput is depicted in Figure 8.27.

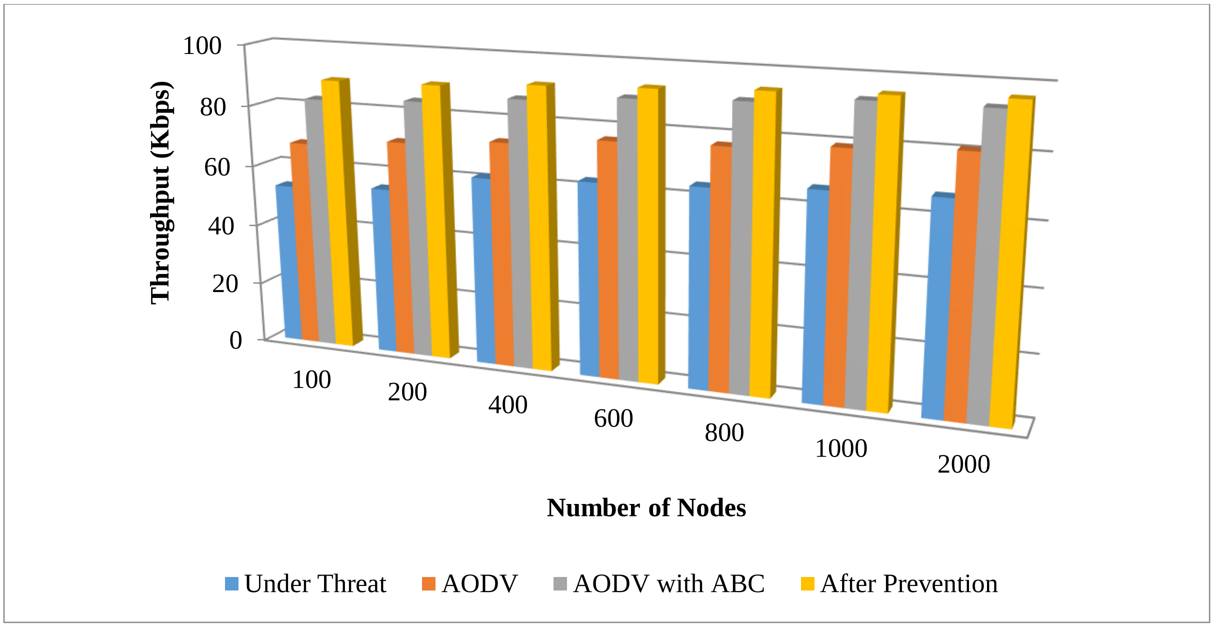


Figure 8.27 Throughput

It is clearly seen that throughput for proposed work is higher for all causes compared to the other three cases AODV under Threat, AODV with Threat and AODV with ABC. The network performance has been degraded through the appearance of BHA inside the network. To overcome this problem, AODV is utilized as a routing protocol by taking the advantages of ABC with a dual scenario of SVM with the ANN approach. Using ABC in combination with ANN and SVM, the route is optimized, and the attacker node is detected. Hence, it increased throughput. The average values analyzed for AODV under Threat, AODV, AODV with ABC, and After prevention are 61.38, 74.98, 88.71, and 92.78, respectively.

Table 8.23 Average Delay (sec)

Number of Nodes	Under Threat	AODV	AODV with ABC	After Prevention
100	0.123	0.112	0.062	0.033
200	0.1504	0.123	0.0694	0.036
400	0.2416	0.135	0.0767	0.043
600	0.2527	0.145	0.0781	0.0431
800	0.2718	0.156	0.892	0.0433
1000	0.2781	0.17	0.904	0.0437
2000	0.2956	0.178	0.922	0.0439

Delay represents the total consumed time through packets to arrive at the target or destination node via source node. The analyzed values of delay are shown in Table 8.23.

Figure 8.28 represents the values of delay analyzed on the basis of numbers for different techniques. The values of delay under threat, AODV, AODV with ABC, and After prevention from BHA are represented through blue, orange, gray, and yellow-colored, respectively.

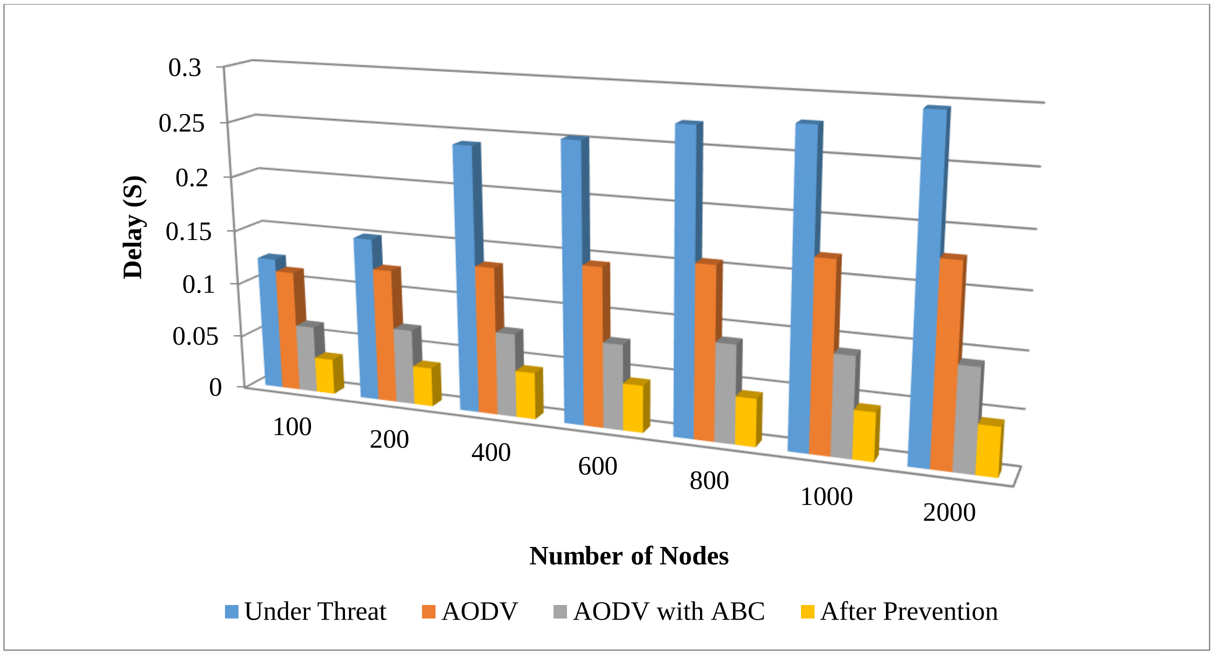


Figure 8.28 Delay

The average values of delay using AODV in under threat, AODV without threat, AODV with ABC, and After prevention are 0.2304 s, 0.145 s, 0.079 s, and 0.04 s, respectively.

Table 8.24 Energy Consumption (mJ)

Number of Nodes	**Under Threat**	**AODV**	**AODV with ABC**	**After Prevention**
100	14.97	7.211	5.22	2.288
200	16.9785	8.203	6.21	2.721
400	17.96	8.52	8.318	3.217
600	18.971	9.182	9.11	4.22

800	20.22	11.271	10.31	5.661
1000	21.314	12.311	11.278	6.705
2000	22.604	12.821	11.94	7.441

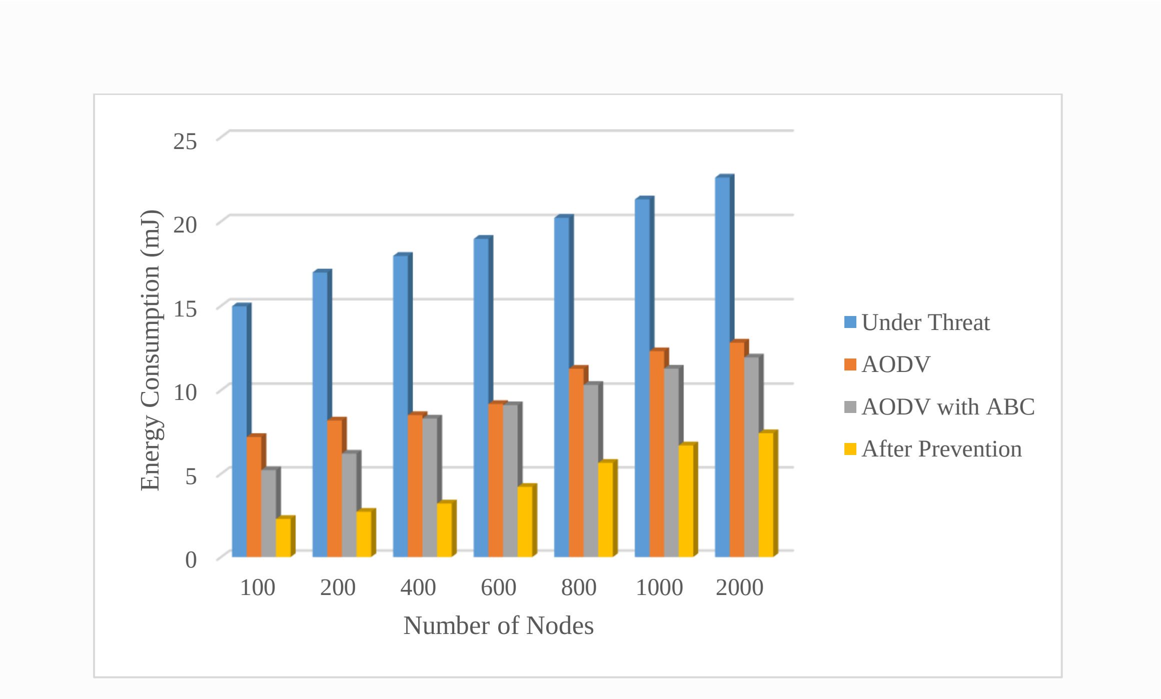


Figure 8.29 Energy Consumption Using ABC with ANN

The energy consumed by the nodes inside the network when deployment of the system by utilizing a varying amount of nodes N=100, 200, 400, 600, 800, 1000, and 2000 is depicted in figure 8.29. As per the diagrammatical information, it has to be analyzed that the energy consumed by nodes using the proposed technique that is ABC with ANN and SVM is less compared to AODV with ABC, single AODV, and under threat condition. The overall energy consumption of the nodes for four different scenarios, such as under threat, AODV, AODV and ABC, AODV, ABC, and ANN approach, are 18.94 mJ, 9.87mJ, 8.86 mJ, and 4.57 mJ respectively. Therefore, energy consumption can be saved to a great extent using the proposed approach (ABC with ANN and SVM).

8.8 COMPARATIVE ANALYSIS

In order to show the efficiency of the designed secure MANET against BHA, the analyzed performance has been contrasted with the previous work i.e., proposed by Ali Zardari et al. 2019 [103] and Gupta et al. (2019) [195]. Based on the average values of PDR, Throughput (Kbps) and Delay (s)computed for proposed work are compared to the average PDR, throughput, and delay of existing works as listed in table 8.25.

Table 8.25 Comparative Parametric Values

PDR (%)			**Throughput (Kbps)**		**Delay (s)**			**Energy Consumption(Mj)**	
Proposed	**[103]**	**[195]**	**Proposed**	**[195]**	**Proposed**	**[195]**	**[39]**	**Proposed**	**[103]**
97.96	96.94	95.14	92.78	79.08	0.04	0.087	0.035	4.6	5.02

Here, the performance of the presented work is a contrast with a past approach, such as [103], and [195]. It has been observed that the designed hybrid AI approach (SVM with ANN) performed better in contrast to the existing work. This is because in [103], the authors have used a traditional approach named as CDS (connected Discriminant Set) approach, through which the data transmission has been performed based on by considering only one property of node that is the utilized energy through nodes. Whereas, in the proposed work, an intelligent approach is used by which ANN and SVM are trained using two different distinct characteristics of networks as an example consumed energy and data transmission delay. In the past work [103], the chances of packet drop increase because each node contains a data packet for a long time. To overcome this problem, we create a BHA detection model, which uses the concept of AI for detection of intrusion in the network automatically and the achieved average PDR, throughput, the delay and energy consumption is of 97.96%, 92.78 kbps, 0.04s and 4.6 mj respectively.

In [195], the authors have used the strategy of reliability factor, by which the reliability factor corresponds to every node is calculated, and if the computed value is high, the data is forwarded otherwise recheck the data for its malicious behavior through transferring FRREQ. If the node is malicious, then it responds to the FRREQ and declares it as a malicious node. The process is time-consuming and provides PDR at a low rate. Therefore, to enhance the work, routing using AODV is enhanced by utilizing an optimization approach with hybrid classification techniques, and we have obtained enhanced performance of networks per the obtained throughput along with delay. The comparison of results is explained below.

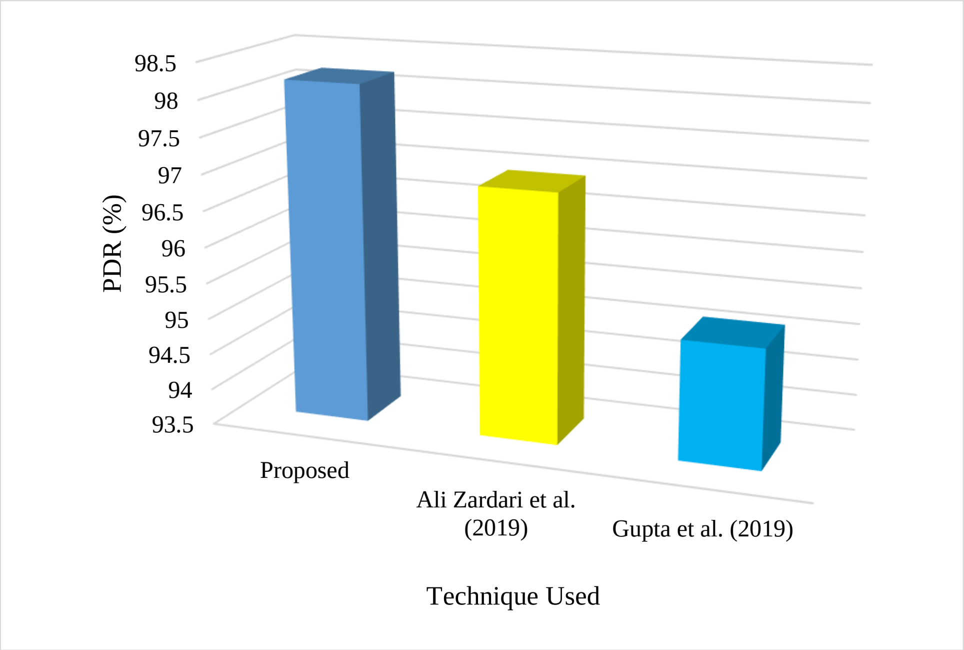


Figure 8.30 Comparison of PDR

In depicted figure 8.30 shows PDR comparison against the existing approach performed by [196] and [197]. From the graph, an improvement of 1.29 % and 3.21 % respectively have been analyzed against [196], and [197] approach. This improvement comes because of nodes selection inappropriate manner while creating routes among source and destination nodes. The existing approach [196] worked on the energy consumption of nodes properties, whereas, in [197] work, the nodes are identified using a reliability score. In the proposed work, as three nodes properties have been considered for the identification of BHA nodes; therefore, it performs better compared to existing approaches.

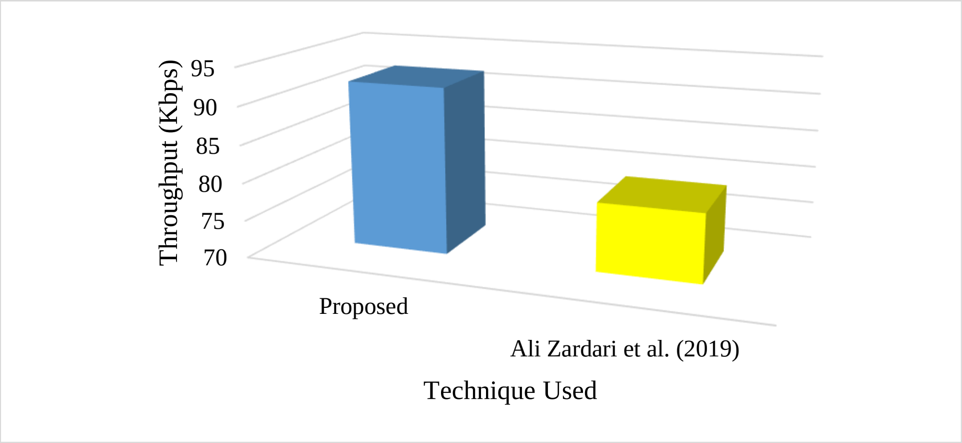


Figure 8.31 Comparison of Throughput

In figure 8.31 illustrated the comparative graph for analyzed throughput against [196] work. The improvement in the throughput using the proposed approach has been indicated the blue bar in Figure 14. The percentage increase in the throughput is calculated, and the improvement of $\left(\frac{92.13-79.08}{79.08}\right)\times 100=16.5\ 5$ has been examined compared to the [196 and 197] work.

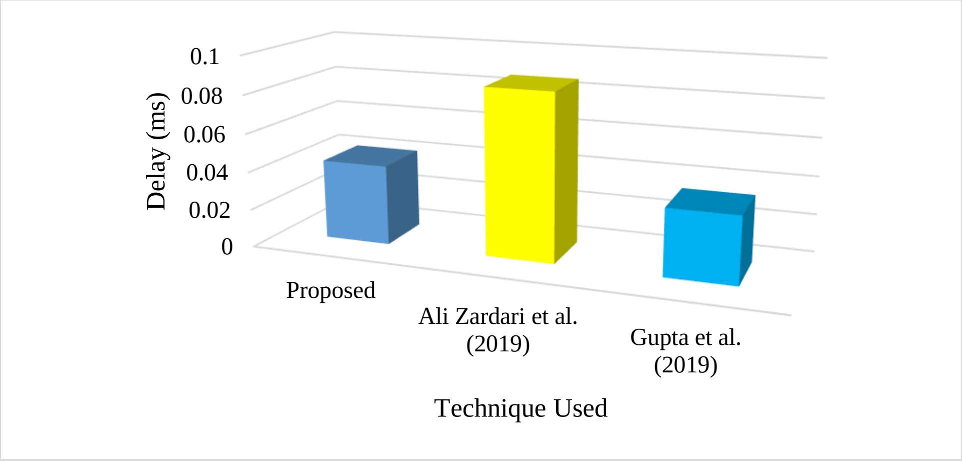


Figure 8.32 Comparison of Delay

The average delay observed for the proposed work as compared to the past approach performed by [196] and [197] is 0.087 ms and 0.035 ms, respectively. The enhancement is seen by the graph presented in Figure 8.31. To know the percentage enhancement against existing work, the percentage decrease has been calculated. $\left(\frac{0.087 - 0.042}{0.087}\right)$×100=51.72 % from the [196], and $\left(\frac{0.035 - 0.042}{0.035}\right)$×100= 20 % against [197] improvement in the proposed work has been obtained.

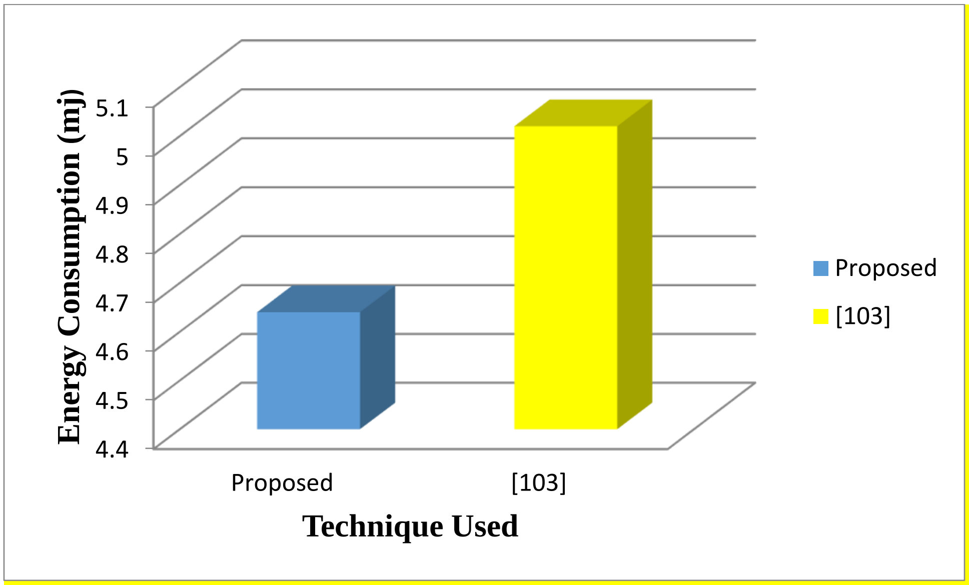


Figure 8.33 Energy Consumption (Mj)

In figure 8.33 illustrated the comparative graph for analyzed Energy Consumption (Mj) against [103] work. The improvement in Energy Consumption (Mj) using the proposed approach has been indicated the blue bar in figure 8.33. The average Energy Consumption (Mj) observed for the proposed work as compared to the past approach performed by [103] is 5.02 Mj.

SUMMARY

Here, in this chapter covers the findings of the research work done has observed and discussed in this chapter. The obtained outcome of this presented work is done with the previous approach to evaluate their performance. This chapter demonstrated the observations and discussions that corresponds to the presented research work. The contrast for the results with the traditional algorithms is shown, and proposed algorithms are showing better performance. The next chapter covers the conclusion of the research work, along with its future work.

CHAPTER 9: CONCLUSION AND FUTURE SCOPE

9.1 CONCLUSION

Security is an essential function for deploying MANET. A new scheme to detect the number of threats i MANETs has designed and implemented here using a machine learning approach. In proposed method detects threats and creates a separate list of both normal and malicious nodes. Because of the dynamical behaviors of MANET, wireless has fewer infrastructures, and it has proved to be vulnerable to various attacks. In addition to all these hazards, there are also secure routing protocols that make the ultimate goal of Ad-hoc networks to achieve immediate network security, regardless of the type of node or environment. These routing protocols enable Ad-hoc nodes to make them more secure and error-free. Mobile ad hoc networks can dynamically set up systems in harsh environments where traditional network infrastructure may not be deployed. Whether the ad hoc network has great potential still has many challenges to overcome.

The review of literature is specifically divided into Routing in MANET, including attacks in MANET. In which summarises the literature survey of enormous kinds of routing techniques likely approach based on thresholding, Fuzzy-based secure multicast to detect the authentication of nodes, location-aware routing protocol, dynamic energy (DE) ad-hoc on-demand distance vector routing protocol (AODV) along with refined trust-based energy effective (ReTE –AODV) to minimize the packet delay, improved durability of the system along with minimizes power consumption. After discussing the routing in MANET part of literature here, go through the attacks included in MANET that needs to detect and overcome. The techniques are utilized to select a system for intrusion detection through a connected dominating set (CDS) for dual attack detection for black and smart gray hole attack (DDBG). To enhance the performance of work, the optimizer i.e., genetic algorithm (GA), is combined with fuzzy logic, including neural network (NN), including support vector machine (SVM) is also utilized for classification mechanism.

The covered objectives of this work, as well as hypotheses, are given. An innovative mechanism has been designed for a BHA, GHA, and SPDA, and all the related schemes presented work is described through flowcharts, including algorithms. In the first part of the methodology, "An Optimal Security Mechanism to prevent Multi-Threat in MANET using Bee Algorithm" utilized optimal bee behavior (OBB) technique inspired through artificial bee colony (ABC) algorithm, this OBB technique is utilized for detection of malicious nodes that are passed to SVM as input.

In the next methodology i.e., "Mitigation of Black Hole and grey hole attack using swarm inspired algorithm with artificial neural network" covers to distinguish the Blackhole node and divert the route through the protected node utilizing an altered AODV routing protocol. The identification of multiple threats in the network is a necessary job to enhance the lifetime of the network.

Therefore, to improve the network performance while the malicious nodes are present, specifically BHA & GHA nodes, in the third methodology "Mitigation of attack using artificial bee colony using Hybrid machine learning approach" in which a security mechanism using ABC as a swarm-based approach and ANN as a machine learning technique has been used. According to the experiment results, it has been observed that data in the proposed work has been transmitted with little delay. Also, the implementation of AODV and threat detection is a simple and easy process. The designed network detects affected nodes using swarm inspired ABC approach. The normal, as well as the affected nodes, are taken as input by the SVM and ANN, respectively. The SVM determines the consumed bandwidth by the affected nodes, as well as the amount of dumped packets through the node. Also, the Chebyshev polynomial function of SVM is used for new node registration. The identification of multiple threats in the network is necessary for improving the efficiency of the system. ABC utilized the intelligent behavior of honeybees, which has been used to segregates the nodes based on their properties, such as into two lists named healthy and affected nodes lists.

Furthermore, the attacker nodes list is subdivided into BHA nodes and the GHA nodes list. Based on these properties, for the training of network ANN is utilized along with for classification purposes, utilize the SVM approach. The performance has been analyzed based on PDR, throughput, delay, and energy consumption. The improvement against PDR, throughput, delay, and energy consumption compared to existing work such as 0.63 % 13.02 %, 18.39 %, and7.57% have been attained compared to existing work.

9.2 FUTURE SCOPE

On the basis of network performance of the proposed method for detection and isolating multiple attacks from the network it has been observed that our result are better from others, here are the following recommendations for future directions:

- The proposed concept can be applied for real life.
- The proposed concept can be integrated with other swarm intelligence-based concepts to improve further results.
- Other machine learning techniques also intergrated with swarm intelligence techniques.

REFERENCES

1. Brindha, V., Karthikeyan, T., &Manimegalai, P. (2019). Fuzzy enhanced secure multicast routing for improving authentication in MANET. Cluster Computing, 22(4), 9615-9623.
2. Yang, H., Li, Z., & Liu, Z. (2019). A method of routing optimization using CHNN in MANET. Journal of Ambient Intelligence and Humanized Computing, 10(5), 1759-1768.
3. Jamaesha, S. S., &Bhavani, S. (2019). A secure and efficient cluster-based location-aware routing protocol in MANET. Cluster Computing, 22(2), 4179-4186.
4. Rajesh, M.,&Gnanasekar, J. M.(2016). Path observation-based physical routing protocol for wireless ad hoc networks. International Journal of Wireless and Mobile Computing, 11(3), 244-257.
5. Deepa, J., &Sutha, J. (2019). A new energy-based power-aware routing method for MANETs. Cluster Computing, 22(6), 13317-13324.
6. Venkanna, U., Agarwal, J. K., &Velusamy, R. L. (2015). A cooperative routing for MANET based on distributed trust and energy management. Wireless Personal Communications, 81(3), 961-979.
7. Sherin, Z., &Soni, M. K. (2015). Secure routing in MANET through crypt-biometric technique. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 (pp. 713-720). Springer, Cham.
8. Bhattacharyya, D., Chatterjee, A., Chatterjee, B., Saha, A. K., &Santra, A. (2018, January). A novel approach to energy-efficient low-cost routing in MANET by a reduction in packet size. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 679-684). IEEE.
9. Balamurugan, K., Chitra, K., &Jawahar, A. (2018). Enhanced hierarchical cluster based routing protocol with optical sphere in FSO MANET. In Optical And Microwave Technologies (pp. 1-8). Springer, Singapore.

10. R.Nandakumar, and K. Nirmala, “Anonymity-based intra–inter and multiple layer service dependent security-aware packet scheduling algorithm (AIIMLSDSPS)”, International Journal of Computers and Applications, pp.1-9, 2018.
11. Pathak, S., & Jain, S. (2016). A novel weight based clustering algorithm for routing in MANET. Wireless Networks, 22(8), 2695-2704.
12. Sethuraman, P., &Kannan, N. (2017). Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. Wireless Networks, 23(7), 2227-2237.
13. Keerthika, V., &Malarvizhi, N. (2019). Mitigate Black Hole Attack Using Hybrid Bee Optimized Weighted Trust with 2-Opt AODV in MANET. Wireless Personal Communications, 106(2), 621-632.V.
14. Brindha, V., Karthikeyan, T., &Manimegalai, P. (2019). Fuzzy enhanced secure multicast routing for improving authentication in MANET. Cluster Computing, 22(4), 9615-9623.
15. Rath, M., &Pattanayak, B. K. (2019). Prevention of Replay Attack Using Intrusion Detection System Framework. In Progress in Advanced Computing and Intelligent Engineering (pp. 349-357). Springer, Singapore.
16. Prasad, A. Y., &Balakrishna, R. (2019). Implementation of optimal solution for network lifetime and energy consumption metrics using improved energy efficient LEACH protocol in MANET. Telkomnika, 17(4), 1758-1766.
17. Panda, N., &Pattanayak, B. K. (2018). Energy aware detection and prevention of black hole attack in MANET. International Journal of Engineering and Technology (UAE), 7(2.6), 135-140.
18. Ramkumar, K. R., & Singh, R. (2017). Key management using Chebyshev polynomials for mobile ad hoc networks. China Communications, 14(11), 237-246.
19. Mukherjee, S., Chattopadhyay, M., &Chattopadhyay, S. (2015, February). A novel encounter based trust evaluation for AODV routing in MANET. In 2015

Applications and Innovations in Mobile Computing (AIMoC) (pp. 141-145). IEEE.

20. Ullah, K., Das, R., Das, P., & Roy, A. (2015, September). Trusted and secured routing in MANET: An improved approach. In 2015 International Symposium on Advanced Computing and Communication (ISACC) (pp. 297-302). IEEE.
21. Usman, M., Jan, M. A., He, X., & Nanda, P. (2018). QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Generation Computer Systems.
22. Shams, E. A., &Rizaner, A. (2018). A novel support vector machine based intrusion detection system for mobile ad hoc networks. Wireless Networks, 24(5), 1821-1829.
23. Zakaria, A. H., Saman, M. Y. M., Noor, A. S. M., & Hassan, H. (2015). Finding shortest routing solution in mobile ad hoc networks using firefly algorithm and queuing network analysis. Jurnal Teknologi, 77(18).
24. Alsumayt, A., Haggerty, J., &Lotfi, A. (2018, April). Evaluation of detection method to mitigate DoS attacks in MANETs. In 2018 1st International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE.
25. Chhabra, M., & Gupta, B. B. (2014). An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET). Research Journal of Applied Sciences, Engineering and Technology, 7(10), 2033-2039.
26. Khan, S., Gani, A., Wahab, A. W. A., & Singh, P. K. (2018). Feature selection of denial-of-service attacks using entropy and granular computing. Arabian Journal for Science and Engineering, 43(2), 499-508.
27. Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 4.
28. Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L., &Gaiti, D. (2014, November). Denial of service (dos) attacks detection in manets using bayesian

classifiers. In 2014 IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT) (pp. 7-12). IEEE.

29. Anbarasan, M., Prakash, S., Antonidoss, A., &Anand, M. (2018). Improved encryption protocol for secure communication in trusted MANETs against denial of service attacks. Multimedia Tools and Applications, 1-21.
30. Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications, 34(1), 107-117.
31. Weerasinghe, H., & Fu, H. (2007, December). Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In Future generation communication and networking (fgcn 2007) (Vol. 2, pp. 362-367). IEEE.
32. Jain, A. K., Tokekar, V., &Shrivastava, S. (2018). Security enhancement in MANETs using fuzzy-based trust computation against black hole attacks. In Information and Communication Technology (pp. 39-47). Springer, Singapore.
33. Doss, S., Nayyar, A., Suseendran, G., Tanwar, S., Khanna, A., & Thong, P. H. (2018). APD-JFAD: accurate prevention and detection of jelly fish attack in MANET. Ieee Access, 6, 56954-56965.
34. Cheng, B. N., & Moore, S. (2012, October). A comparison of MANET routing protocols on airborne tactical networks. In MILCOM 2012-2012 IEEE Military Communications Conference (pp. 1-6). IEEE.
35. Schweitzer, N., Stulman, A., Shabtai, A., &Margalit, R. D. (2015). Mitigating denial of service attacks in OLSR protocol using fictitious nodes. IEEE Transactions on Mobile Computing, 15(1), 163-172.
36. Bhuvaneswari R., and R. Ramachandran, “Denial of service attack solution in OLSR basedmanet by varying number of fictitious nodes,” Cluster Computing, pp. 1-11, May 2018

37. MANET Characteristics and Features, 2018. [Online]. Available:https://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/. [Last Accessed:10-Jan-2019].
38. Bhuvaneswari, R., &Ramachandran, R. (2019). Denial of service attack solution in OLSR based manet by varying number of fictitious nodes. Cluster Computing, 22(5), 12689-12699.
39. Ahn, J. H., & Lee, T. J. (2014). Multipoint relay selection for robust broadcast in ad hoc networks. Ad Hoc Networks, 17, 82-97.
40. Duan, Q., Al-Shaer, E., Chatterjee, S., Halappanavar, M., &Oehmen, C. (2018). Proactive routing mutation against stealthy Distributed Denial of Service attacks: metrics, modeling, and analysis. The Journal of DefenseModeling and Simulation, 15(2), 219-230.
41. Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 4.
42. Zhang, X. M., Zhang, Y., Yan, F., &Vasilakos, A. V. (2014). Interference-based topology control algorithm for delay-constrained mobile ad hoc networks. IEEE Transactions on Mobile Computing, 14(4), 742-754..
43. Arora, S. K. (2016). Detection and Performance Analysis of Wormhole Attack in MANET using DELPHI Technique. International Journal of Security and Its Applications, 10(10), 321-330.
44. Abraham, A. (2005). Artificial neural networks. Handbook of measuring system design.
45. Wang, S. C. (2003). Artificial neural network. In Interdisciplinary computing in java programming (pp. 81-100). Springer, Boston, MA.
46. Anuradha, M., & Mala, G. A. (2017). Cross-layer based congestion detection and routing protocol using fuzzy logic for MANET. Wireless Networks, 23(5), 1373-1385.

47. Chadha, K., & Jain, S. (2014, May). Impact of black hole and grayhole attack in AODV protocol. In International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014) (pp. 1-7). IEEE.

48. Culpepper, B. J., & Tseng, H. C. (2004, October). Sinkhole intrusion indicators in DSR MANETs. In First International Conference on Broadband Networks (pp. 681-688). IEEE.

49. Tseng, H. C., & Culpepper, B. J. (2005). Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators. Computers & Security, 24(7), 561-570.

50. Ghaffari, A. (2017). Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms. Wireless Networks, 23(3), 703-714.

51. Feng, F., Liu, X., Yong, B., Zhou, R., & Zhou, Q. (2019). Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. Ad Hoc Networks, 84, 82-89.

52. Walia, M., &Challa, R. K. (2010, April). Performance analysis of cross-layer mac and routing protocols in manets. In 2010 Second International Conference on Computer and Network Technology (pp. 53-59). IEEE.

53. Misra, S., Dhurandher, S. K., Obaidat, M. S., Verma, K., & Gupta, P. (2010). A low-overhead fault-tolerant routing algorithm for mobile ad hoc networks: A scheme and its simulation analysis. Simulation Modelling Practice and Theory, 18(5), 637-649..

54. Kout, A., Labed, S., &Chikhi, S. (2018). AODVCS, a new bio-inspired routing protocol based on cuckoo search algorithm for mobile ad hoc networks. Wireless Networks, 24(7), 2509-2519.

55. Ramya, P., &Gopalakrishnan, V. (2019). Proficient algorithms for enhancing topology control for dynamic clusters in MANET. Cluster Computing, 22(4), 9715-9726.

56. Srivastava, P., & Kumar, R. (2018). A timestamp-based adaptive gateway discovery algorithm for ubiquitous internet access in MANET. In Next-generation networks (pp. 153-162). Springer, Singapore.
57. Feed-Forward Neural Networks, 2018. [Online]. Available:https://towardsdatascience.com/recurrent-neural-networks-and-lstm-4b601dd822a5. [Last Accessed: 31-Jan-2019].
58. Hinds, A., Ngulube, M., Zhu, S., & Al-Aqrabi, H. (2013). A review of routing protocols for mobile ad-hoc networks (manet). International journal of information and education technology, 3(1), 1.
59. Ahmad, M., Aydın, N., Boeloeni, L., Boukerche, A., Turgut, D., &Turgut, B. (2011). Routing protocols in ad hoc networks: A survey.
60. Cheng, B. N., & Moore, S. (2012, October). A comparison of MANET routing protocols on airborne tactical networks. In MILCOM 2012-2012 IEEE Military Communications Conference (pp. 1-6). IEEE.
61. Culpepper, B. J., & Tseng, H. C. (2004, October). Sinkhole intrusion indicators in DSR MANETs. In First International Conference on Broadband Networks (pp. 681-688). IEEE.
62. Luo, J., & Xiang, L. (2011). Prolong the lifetime of wireless sensor networks through mobility: A general optimization framework. In Theoretical Aspects of Distributed Computing in Sensor Networks (pp. 553-588). Springer, Berlin, Heidelberg.
63. Razaque, A., Abdulgader, M., Joshi, C., Amsaad, F., &Chauhan, M. (2016, April). P-LEACH: Energy efficient routing protocol for Wireless Sensor Networks. In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (pp. 1-5). IEEE.
64. Abdel-Azim, M., Salah, H. E. D., &Eissa, M. E. (2018). IDS Against Black-Hole Attack for MANET. IJ Network Security, 20(3), 585-592.

65. Le Fessant, F., Papadimitriou, A., Viana, A. C., Sengul, C., & Palomar, E. (2012). A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis. Computer communications, 35(2), 234-248.
66. Tseng, H. C., & Culpepper, B. J. (2005). Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators. Computers & Security, 24(7), 561-570.
67. Melamed, R., Keidar, I., &Barel, Y. (2008). Octopus: A fault-tolerant and efficient ad-hoc routing protocol. Wireless Networks, 14(6), 777-793.
68. M. M. Ozcelik, E. Irmak, & S. Ozdemir, (2017, May). A hybrid trust based intrusion detection system for wireless sensor networks. In 2017 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE
69. V. R. Prabha& P. Latha, (2017). Enhanced multi-attribute trust protocol for malicious node detection in wireless sensor networks. Sādhanā, 42(2), 143-151.
70. S. Otoum, B. Kantarci& H. T. Mouftah (2017). Detection of known and unknown intrusive sensor behavior in critical applications. IEEE Sensors Letters, 1(5), 1-4.
71. Z. Zhang, H. Zhu, S. Luo, Y. Xin, ,& Liu, X. (2017). Intrusion detection based on state context and hierarchical trust in wireless sensor networks. IEEE Access, 5, 12088-12102.
72. A. Basan, E. Basan, & O. Makarevich (2017, October). A trust evaluation method for active attack counteraction in wireless sensor networks. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 369-372). IEEE.
73. M. Wazid, & A. K. Das (2017). A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks. Wireless Personal Communications, 94(3), 1165-1191.
74. R. Singh, J. Singh, & R. Singh, (2017). Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks. Wireless Communications and Mobile Computing, 2017.

75. Abu TahaZamani, S. Z. (2014). Key management scheme in mobile Ad Hoc networks. International Journal of Emerging Research in Management &Technology, 3(4), 157-165.

76. Ozdemir, S., Peng, M., & Xiao, Y. (2015). PRDA: polynomial regression based privacy preserving data aggregation for wireless sensor networks. Wireless communications and mobile computing, 15(4), 615-628.

77. Kurundkar, S., Joshi, S., &Waghmare, L. M. (2017). Modeling and statistical analysis of scenario metric parameters of ad hoc on demand distance vector routing protocol. Wireless Personal Communications, 96(1), 183-197.

78. Zhou, J., Cao, Z., Dong, X., Xiong, N., &Vasilakos, A. V. (2015). 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Information Sciences, 314, 255-276.

79. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50.

80. Ghugar, U., Pradhan, J., Bhoi, S. K., Sahoo, R. R., & Panda, S. K. (2018). PL-IDS: physical layer trust based intrusion detection system for wireless sensor networks. International Journal of Information Technology, 10(4), 489-494.

81. Shanthi, S., &Rajan, E. G. (2016, October). Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks. In 2016 2nd International Conference on Next Generation Computing Technologies (NGCT) (pp. 426-431). IEEE.

82. Martínez, V. S., Buchsteiner, M., Gray, P., Nielsen, L. K., &Quek, L. E. (2015). Dynamic metabolic flux analysis using B-splines to study the effects of temperature shift on CHO cell metabolism. Metabolic Engineering Communications, 2, 46-57.

83. Wang, L., &Olariu, S. (2004). A two-zone hybrid routing protocol for mobile ad hoc networks. IEEE transactions on Parallel and distributed systems, 15(12), 1105-1116.

84. To, M. A. (2016). A proactive approach for strip interoperability in wireless ad hoc routing protocols. IEEE Latin America Transactions, 14(6), 2543-2549.

85. Le Minh, H., Sexton, G., &Aslam, N. (2014). Self-adaptive proactive routing scheme for mobile ad-hoc networks. IET Networks, 4(2), 128-136.

86. Wang, Z., Chen, Y., & Li, C. (2011). A new loop-free proactive source routing scheme for opportunistic data forwarding in wireless networks. IEEE Communications Letters, 15(11), 1184-1186.

87. Schweitzer, N., Stulman, A., Shabtai, A., &Margalit, R. D. (2015). Mitigating denial of service attacks in OLSR protocol using fictitious nodes. IEEE Transactions on Mobile Computing, 15(1), 163-172.

88. Marimuthu, M., &Krishnamurthi, I. (2013). Enhanced OLSR for defense against DOS attack in ad hoc networks. Journal of communications and networks, 15(1), 31-37.

89. Rajani, K. C., Aishwarya, P., &Meenakshi, S. R. (2016, April). A review on multicasting routing protocols for mobile ad-hoc wireless networks. In 2016 International Conference on Communication and Signal Processing (ICCSP) (pp. 1045-1052). IEEE.

90. Kalwar, S. (2010). Introduction to reactive protocol. IEEE potentials, 29(2), 34-35.

91. Xu, H., Wu, X., Sadjadpour, H. R., & Garcia-Luna-Aceves, J. J. (2010). A unified analysis of routing protocols in MANETs. IEEE Transactions on communications, 58(3), 911-922.

92. Johnson, D. B., Maltz, D. A., &Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5(1), 139-172.

93. Johnson, D., Hu, Y. C., &Maltz, D. (2007). The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4 (Vol. 260). RFC 4728.

94. Xiaochuan, X., Gang, W., Keping, W., Gang, W., &Shilou, J. (2008). Link reliability based hybrid routing for tactical mobile ad hoc network. Journal of Systems Engineering and Electronics, 19(2), 259-267.

95. Haas, Z. (1998). The zone routing protocol (ZRP) for ad hoc networks. IETF Internet draft, draft-ietf-manet-zone-zrp-01. txt.

96. Ramasubramanian, V., Haas, Z. J., &Sirer, E. G. (2003, June). SHARP: A hybrid adaptive routing protocol for mobile ad hoc networks. In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing (pp. 303-314)..

97. Zhao, Z., Hu, H., Ahn, G. J., & Wu, R. (2011). Risk-aware mitigation for MANET routing attacks. IEEE Transactions on dependable and secure computing, 9(2), 250-260.

98. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2014). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE systems journal, 9(1), 65-75.

99. Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. IEEE communications surveys & tutorials, 15(4), 2027-2045.

100. Abbas, S., Merabti, M., Llewellyn-Jones, D., &Kifayat, K. (2012). Lightweight sybil attack detection in manets. IEEE systems journal, 7(2), 236-248.

101. Liang, Y., Poor, H. V., & Ying, L. (2011). Secrecy throughput of MANETs under passive and active attacks. IEEE transactions on information theory, 57(10), 6692-6702.

102. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., &Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. IEEE Wireless communications, 14(5), 85-91.

103. Ali Zardari, Z., He, J., Zhu, N., Mohammadani, K. H., Pathan, M. S., Hussain, M. I., &Memon, M. Q. (2019). A dual attack detection technique to identify black and grayhole attacks using an intrusion detection system and a connected dominating set in MANETs. *Future Internet, 11*(3), 61.

104. Gurung, S., &Chauhan, S. (2019). A novel approach for mitigating grayhole attack in MANET. Wireless Networks, 24(2), 565-579.

105. Singh, V., Singh, D., & Hassan, M. M. (2019). Survey: Black Hole Attack Detection in MANET. Malik Mubasher, Survey: Black Hole Attack Detection in MANET (March 12, 2019).

106. Trivedi, M. C., &Malhotra, S. (2019). Identification and Prevention of Joint Gray Hole and Black Hole Attacks. International Journal of Ambient Computing and Intelligence (IJACI), 10(2), 80-90.

107. Saudi, N. A. M., Arshad, M. A., Buja, A. G., Fadzil, A. F. A., &Saidi, R. M. (2019). Mobile Ad-Hoc Network (MANET) Routing Protocols: A Performance Assessment. In Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017) (pp. 53-59). Springer, Singapore.

108. Jain, S., Patel, H., Prajapati, A., Jain, S., Patel, H., &Prajapati, A. (2019). Advancement of Network Performance using Improved AOMDV Protocol in MANET. International Journal, 5, 58-64.

109. 109. Gorine, D., &Saleh, R. (2019). Performance Analysis of Routing Protocols in ManetUnder Malicious Attacks. International Journal of Network Security & Its Applications (IJNSA) Vol, 11.

110. Muhammad, H. A., Yahiya, T. A., & Al-Salihi, N. (2019, June). Comparative Study Between Reactive and Proactive Protocols of (MANET) in Terms of Power Consumption and Quality of Service. In International Conference on Computer Networks(pp. 99-111). Springer, Cham.

111. Kumar, S., Goyal, M., Goyal, D., &Poonia, R. C. (2017, December). Routing protocols and security issues in MANET. In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS) (pp. 818-824). IEEE.

112. Aldaej, A., &Ahamad, T. (2016). AAODV (aggrandized ad hoc on demand vector): a detection and prevention technique for manets. International Journal of Advanced Computer Science and Applications (IJACSA), 7(10), 2016.

113. Khanpara, P., &Trivedi, B. (2017). Security in mobile ad hoc networks. In Proceedings of International Conference on Communication and Networks (pp. 501-511). Springer, Singapore.

114. Chahal, P., Tak, G. K., &Tomar, A. S. (2015). Comparative analysis of various attacks on manet. International Journal of Computer Applications, 111(12).

115. Mahajan, K., & Singh, H. (2016). MANET, its types, Challenges, goals and Approaches: A Review. International Journal of Science and Research (IJSR), 5(5), 1591-1594.

116. Brar, S., & Angurala, M. (2016). Review on grey-hole attack detection and prevention. International Journal of Advance research, Ideas and Innovations in Technology, 2(5), 1-4.

117. Brajević, I., & Ignjatović, J. (2018). An upgraded firefly algorithm with feasibility-based rules for constrained engineering optimization problems. Journal of Intelligent Manufacturing, 1-30.

118. Wang, H., Wang, W., Cui, L., Sun, H., Zhao, J., Wang, Y., &Xue, Y. (2018). A hybrid multi-objective firefly algorithm for big data optimization. Applied Soft Computing, 69, 806-815.

119. Wang, Sun-Chong. (2003). Artificial neural network." Interdisciplinary computing in java programming. Springer US,. 81-100.

120. Park, Dong C., et al. "Electric load forecasting using an artificial neural network." IEEE transactions on Power Systems vol.6,1991, pp. 442-449.Manufacturing, 1-30.

121. Abraham, A. (2005). Artificial neural networks. handbook of measuring system design.

122. He, X., & Xu, S. (2010). Artificial neural networks. Process Neural Networks: Theory and Applications, 20-42.

123. Bajpai, S., Jain, K., & Jain, N. (2011). Artificial neural networks. International Journal of Soft Computing and Engineering (IJSCE), 1(NCAI2011).

124. Z. Li and Y. Wu(2017). Smooth Mobility and Link Reliability-Based Optimized Link State Routing Scheme for MANETs, in IEEE Communications Letters, vol. 21, no. 7, pp. 1529-1532.

125. Y. H. Chen, E. H. K. Wu & G. H. Chen.(2017). Bandwidth-Satisfied Multicast by Multiple Trees and Network Coding in Lossy MANETs, in IEEE Systems Journal, vol. 11, no. 2, pp. 1116-1127.

126. Y. Fang, Y. Zhou, X. Jiang & Y. Zhang.(2017). Practical Performance of MANETs Under Limited Buffer and Packet Lifetime, in IEEE Systems Journal, vol. 11, no. 2, pp. 995-1005.

127. Ahmed, D., & Khalifa, O.(2017). An overview of MANETs: applications, characteristics, challenges and recent issues. IJEAT, 3, 128.

128. L. Prashar & R. K. Kapur.(2016). Performance analysis of routing protocols under different types of attacks in MANETs, 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, pp. 405-408.

129. D. Kim, H. Bae & C. K. Toh.(2007). Improving TCP-Vegas Performance Over MANET Routing Protocols, in IEEE Transactions on Vehicular Technology, vol. 56, no. 1, pp. 372-377.

130. Z. Wang, Y. Chen & C. Li.(2014). PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks, in IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 859-868.

131. L. Wang and S. Olariu.(2017). A two-zone hybrid routing protocol for mobile ad hoc networks, in IEEE Transactions on Parallel and Distributed Systems, vol. 15, no. 12, pp. 1105-1116.

132. M. A. To.(2016). A Proactive Approach for Strip Interoperability in Wireless Ad hoc Routing Protocols, in IEEE Latin America Transactions, vol. 14, no. 6, pp. 2543-2549.

133. T. T. Son, H. Le Minh, G. Sexton & N. Aslam.(2015). Self-adaptive proactive routing scheme for mobile ad-hoc networks, in IET Networks, vol. 4, no. 2, pp. 128-136.

134. Z. Wang, Y. Chen & C. Li.(2011). A New Loop-Free Proactive Source Routing Scheme for Opportunistic Data Forwarding in Wireless Networks, in IEEE Communications Letters, vol. 15, no. 11, pp. 1184-1186.

135. N. Schweitzer, A. Stulman, A. Shabtai & R. D. Margalit. (2016). Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes, in IEEE Transactions on Mobile Computing, vol. 15, no. 1, pp. 163-172.

136. M. Marimuthu & I. Krishnamurthi.(2013). Enhanced OLSR for defense against DOS attack in ad hoc networks, in Journal of Communications and Networks, vol. 15, no. 1, pp. 31-37.

137. S. Kalwar.(2010). Introduction to reactive protocol, in IEEE Potentials, vol. 29, no. 2, pp. 34-35.

138. Y. Liang, H. V. Poor & L. Ying.(2011). Secrecy Throughput of MANETs Under Passive and Active Attacks, in IEEE Transactions on Information Theory, vol. 57, no. 10, pp. 6692-6702.

139. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato & A. Jamalipour.(2017). A survey of routing attacks in mobile ad hoc networks, in IEEE Wireless Communications, vol. 14, no. 5, pp. 85-91.

140. Patel, N. J. K., &Tripathi, K. (2018). Trust Value based Algorithm to Identify and DefenseGray-Hole and Black-Hole attack present in MANET using Clustering Method.

141. Shalika, E., Bal, J. S., & Dhir, V. (2018). A Review on Implementation of AODV Technique for Isolation of Gray Hole Attack in MANET.

142. M. Mohanapriya ,Ilango Krishnamurthi.(2014).Modified DSR protocol for detection and removal of selective black hole attack in MANET, Computers & Electrical Engineering 40, no. 2,pp. 530-538.

143. Gupta Anuj K., Sadawarti Harsh, & Anil K. Verma.(2011). A review of routing protocols for mobile ad hoc networks. SEAS Transactions on Communications 10, no. 11, pp. 331-340.

144. Abusalah, Loay, Ashfaq Khokhar, & Mohsen Guizani.(2008). A survey of secure mobile ad hoc routing protocols. IEEE communications surveys & tutorials10, no. 4.

145. Siddharth, Sandeep, & Mukul. (2016). Black hole attack detection and prevention mechanism for mobile ad-hoc networks, In Computing for Sustainable Global Development (INDIACom), pp. 2993-2996. IEEE.

146. Ziming Zhao, Hongxin Hu, Gail-JoonAhn & RuoyuWu.(2012). Risk-aware mitigation for MANET routing attacks. IEEE Transactions on dependable and secure computing 9, no. 2,pp. 250-260.

147. Sarkar, S., & Datta, R. (2017). An adaptive protocol for stable and energy-aware routing in MANETs. IETE Technical Review, 34(4), 353-365.

148. Simon, D.(2008). Biogeography-based optimization, IEEE transactions on evolutionary computation, 12(6), 702-713.

149. Karaboga, D. (2005). An idea based on honey bee swarm for numerical optimization (Vol. 200), Technical report-tr06, Erciyesuniversity, engineering faculty, computer engineering department.

150. Back, T., Hammel, U., & Schwefel, H. P. (1997). Evolutionary computation: Comments on the history and current state, IEEE transactions on Evolutionary Computation, 1(1), 3-17.

151. Dorigo, M., Maniezzo, V., & Colorni, A. (1996). Ant system: optimization by a colony of cooperating agents, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 26(1), 29-41.

152. Clerc, M. (2010), Particle swarm optimization (Vol. 93), John Wiley & Sons.

153. Karaboga, D., Gorkemli, B., Ozturk, C., & Karaboga, N. (2014). A comprehensive survey: artificial bee colony (ABC) algorithm and applications, Artificial Intelligence Review, 42(1), 21-57.

154. Alex Hinds, Michael Ngulube & Shaoying Zhu. (2013). A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET), International Journal of Information and Education Technology, Vol. 3, No. 1.

155. Biradar Arun. (2013). Effectiveness of Genetic Algorithm In Reactive Protocols For MANET, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2, Issue 7.

156. Azzedine Boukerchea & Begumhan Turgut.(2011). Routing protocols in ad hoc networks: A survey", 2011 Elsevier doi:10.1016/j.comnet.05.010

157. Bow-Nan Cheng & Moore, S.(2012). A comparison of MANET routing protocols on airborne tactical networks, in Military Communications Conference – (MILCOM'12), vol., no., pp.1-6.

158. Khetmal Chetana, Shailendra & Nilesh. (2013). MANET: Black Hole Node Detection in AODV, International Journal of Computational Engineering Research, Vol. 03.

159. Singh Gurpinder.(2012). MANET: Issues and Behaviour Analysis of Routing Protocols, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, ISSN: 2277 128X.

160. Harjeet, Varsha & Manju.(2013). A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review, in International Journal of Computer Science and Information Technologies, (IJCSIT), Vol. 4 (3), pp. 498-500.

161. K. Chadha & S. Jain.(2014). Impact of black hole and grey hole attack in AODV protocol, in International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-7, Jaipur.

162. Singh Tejinderdeep & Arora Harpreet.(2013). Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2.

163. Fabrice Le Fessant, Antonis Papadimitriou, AlineCarneiroViana, CigdemSengul, & Esther Palomar.(2012). A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis, Computer Communications vol.35, pp. 234–248.

164. B. J. Culpepper & H. C. Tseng.(2004). Sinkhole intrusion indicators in DSR MANETs, First International Conference on Broadband Networks, pp. 681-688.

165. E. C. H. Ngai, J. Liu & M. R. Lyu.(2006). On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks, IEEE International Conference on Communications, Istanbul, pp. 3383-3389.

166. D. Sheela, C. N. Kumar & G. Mahadevan.(2011). A non cryptographic method of sink hole attack detection in wireless sensor networks, International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, Tamil Nadu, pp. 527-532.

167. Tseng, H. Chris & B. Jack Culpepper.(2005) Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators. Computers & Security vol.24, pp. 561-570.

168. Rana E. Ahmed.(2011). A Fault-Tolerant Routing Protocol for Mobile Ad Hoc Networks, Journal of advances in Information Technology, Vol. 2, No. 2.

169. V. Jayalakshmi & D R. Ramesh.(2012). Multipath fault tolerant routing protocol in MANET, International Journal on Ad Hoc Networking Systems (IJANS) Vol. 2, No. 1.

170. Suldip, Sanjay K. Dhurandher, Mohammed S.Obaidat, Karan Verma & Pukhar Gupta.(2010). A low overhead default tolerant routing algorithm for mobile Ad Hoc networks: A scheme and its simulation analysis, Simulation modelling practice and theory 18, pp. 637-649, Elsevier publications.

171. Roie Melamed, Idit Keidar, & Yoav Barel.(2005). Octopus: A Fault-Tolerant and Efficient Ad-Hoc Routing Protocol, Reliable Distributed Systems, P-ISBN: 0-7695-2463-X pp.39-49.

172. Anjali, & Singh Maninder.(2012). Performance Analysis of Proactive, Reactive and Hybrid MANET Routing Protocols on IEEE 802.11 Standard, International Journal of Computer Applications (0975 – 8887) Volume 54– No.12, September 2012.

173. Bow-Nan Cheng & Moore, S. (2012). A comparison of MANET routing protocols on airborne tactical networks, in Military Communications Conference, 2012 - MILCOM 2012, vol., no., pp.1-6.

174. john, P.M. & Vivekananda, P.(2012). A framework for secure routing in Mobile Ad hoc Networks, in Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on , vol., no., pp.453-458, 30-31.

175. Kaur Kiranveer & Kaur Surinderjit.(2014). Throughput Analysis of Proactive and Reactive MANET Routing Protocols International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-3).

176. K. Mahajan, D. Malik, M. A. Rizvi & D. S. Karaulia.(2014). Event Driven Dynamic Path Optimization for AODV in MANET, 2014 International Conference on Computational Intelligence and Communication Networks, Bhopal, pp. 448-452.

177. R. Kumar & M. Gupta.(2014). Route stability and energy aware based AODV in MANET, 2014 International Conference on High Performance Computing and Applications (ICHPCA), Bhubaneswar, pp. 1-5.

178. H. C. Jang & C. C. Hung.(2010). Direction based routing strategy to reduce broadcast storm in MANET, 2010 International Computer Symposium (ICS2010), Tainan, pp. 445-450.

179. A. H. Moon, U. Iqbal, G. M. Bhat & Z. Iqbal. (2016). Simulating and analyzing RREQ flooding attack in Wireless Sensor Networks, 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, pp. 3374-3377.

180. H. Han, M. Wu, Q. Hu & N. Wang.(2014). Best Route, Error Broadcast: A Content-Centric Forwarding Protocol for MANETs, 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall), Vancouver, BC, pp. 1-5.

181. Devi S. S. & Sikamani K. T.(2013). Improved route error tolerant mechanism for AODV routing protocol in MANET, 2013 International Conference on Current Trends in Engineering and Technology (ICCTET), Coimbatore, pp. 187-190.

182. Jenn-Wei Lin, Jichiang Tsai & Chao-Ying Chiu.(2005). An efficient approach to tolerating route errors in mobile ad hoc networks, 11th Pacific Rim International Symposium on Dependable Computing (PRDC'05), pp. 8 pp.-

183. M. Guerroumi, A. Derhab & K. Saleem. (2015). Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink, 2015 12th International Conference on Information Technology - New Generations, Las Vegas, NV, pp. 307-313.

184. D. Sheela, C. N. Kumar & G. Mahadevan.(2011). A non cryptographic method of sink hole attack detection in wireless sensor networks, 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, Tamil Nadu, pp. 527-532.

185. Agrwal L. S., Khandelwal R., P. Sharma & Gupta S. K.(2016). Analysis of detection algorithm of Sinkhole attack & QoS on AODV for MANET, 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, pp. 839-842.

186. Khatri S. K. & Dixit M. (2015). Reducing Route discovery latency in MANETs using ACO, 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, pp. 1-5.

187. S. Nath, S. Banik, A. Seal & S. K. Sarkar.(2016).Optimizing MANET routing in AODV: An hybridization approach of ACO and firefly algorithm, 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, pp. 122-127.

188. Prabaharan S. & Ponnusamy R.(2016). Secure and energy efficient MANET routing incorporating trust values using hybrid ACO, 2016 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, pp. 1-8.

189. Kojić, N., Reljin, I., & Reljin, B.(2014). A neural networks-based hybrid routing protocol for wireless mesh networks, Sensors vol. 12, no 6, pp. 7548-7575.

190. Shah S. K. & Vishwakarma D. D.(2012). FPGA implementation of ANN for reactive routing protocols in MANET, 2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat), Bali, pp. 11-14.

191. M. R. Masillamani, A. Jamalipour & G. V. Uma. (2007). Intelligent MANET, 2007 International Conference on Intelligent and Advanced Systems, Kuala Lumpur, pp. 408-413.

192. Shivhare, M., & Gautam, P. K. (2017). Prevention of black hole attack in MANET using indexing algorithm. Int. J. Eng. Sci, 12603, 12603-12606.

193. Jain, A. K., Tokekar, V., & Shrivastava, S. (2018). Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks. In Information and Communication Technology (pp. 39-47). Springer, Singapore.

194. Chhabra, A., Vashishth, V., & Sharma, D. K. (2018). A fuzzy logic and game theory based adaptive approach for securing opportunistic networks against black hole attacks. International Journal of Communication Systems, 31(4), e3487.

195. Gupta, Prakhar, Goel Pratyaksh, Pranjali Varshney, & Tyagi Nitin.(2019). Reliability factor based AODV protocol: Prevention of black hole attack in MANET. In Smart Innovations in Communication and Computational Sciences, pp. 271-279.

196. Tareq, M., Alsaqour, R., Abdelhaq, M., & Uddin, M.(2017) Mobile ad hoc network energy cost algorithm based on artificial bee colony, Wireless Communications and Mobile Computing.

197. https://www.researchgate.net/figure/256846143_fig1_Fig-3-CGSR-routing-from-nodes-2-4-6-and-7form-a-single-cluster.

List of publication

1. “Mitigation of Blackhole and Gray hole Attack using Swarm Inspired Algorithm with Artificial Neural Network” Pooja Rani, Dr. Kavita published in IEEE ACCESS, SCI with impact factor 4.098 online ISSN: 2169-3536, Digital Object Identifier: 10.1109/ACCESS.2020.3004692.
2. “Mitigation of Black Hole Attack using Artificial Bee Colony and Hybrid Machine Learning Approach in IoT” Pooja Rani, Dr. Kavita submitted in SCI(MDPI SENSOR with impact factor 3.25).
3. “An optimal Security Mechanism to Prevent multi-threat in MANET using Bee Algorithm” Pooja Rani, Dr. Tanupreet Singh published in Volume-8 Issue-11, September 2019, Page No. 1960-1967. of ‘International Journal of Innovative Technology and Exploring Engineering (IJITEE)’ Scopus, ISSN: 2278–3075.
4. “Effect on the performance of MANET Network using multiple attacks “ Pooja Rani, Dr. Tanupreet Singh” Pooja Rani, Dr. Tanupreet Singh published in 11-3 Volume-2 Issue-2, Page no. 37-42 of ‘International conference of advances in science and technology(ICAST 2018) 978-93-86823.