REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

DEVELOPMENT OF AODV SECURITY AGAINST BLACK HOLE ATTACK IN MOBILE AD HOC NETWORK

Sara Harith Hazim AL-QARAGHULI

Master's Thesis

Supervisor

Asst. Prof. Dr. Mesut ÇEViK

Istanbul, 2023

DEVELOPMENT OF AODV SECURİTY AGAİNST BLACK HOLE ATTACK İN MOBİLE AD HOC NETWORK

Sara Harith Hazim AL-QARAGHULI

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

2023

The thesis titled Development of AODV SECURITY AGAINST BLACK HOLE ATTACK IN MOBILE AD HOC NETWORK prepared by SARA HARITH HAZIM AL- AL-QARAGHULI and submitted on 11/04/2023 has been accepted unanimously for the degree of Master of Science in Electrical and Computer Engineering.

_____

Asst. Prof. Dr. Mesut ÇEViK

Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Mesut ÇEVİK	Electrical and Electronics Engineering, Altınbaş University	_____
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Computer Engineering, Altınbaş University	_____
Assoc. Prof. Dr. Izzet PARUĞ DURU	Medical Imaging Techniques, Istanbul Gedik University	_____

I hereby declare that this thesis meets all format and submission requirements of a master's thesis.

Submission date of the thesis to the Graduate Education Institute: ___/___/___

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Sara Harith Hazim AL-QARAGHULI

Signature

DEDICATION

This study is dedicated to the memory of Thamer Al-Shikhly, my grandfather. he was unable to see my graduation. This is for him.

I dedicated my study to my academic adviser Asst. Prof. Dr. Mesut ÇEViK who guided me in the whole process of research and the committee who's kept me on track.

PREFACE

First and first, I must express my thankfulness to God Almighty for all of his favors, as well as for my patience during the course of this investigation. My heartfelt gratitude and appreciation go to my supervisor Asst. Prof. Dr. Mesut ÇEViK for his supervision, guidance, ideas, and constructive remarks during the whole study time, from start to finish, which has given me a better understanding all along. Lastly, I want to direct my thankfulness to my parent, my entire family and especially to my husband for all of their assistance and ongoing support during this process.

ABSTRACT

DEVELOPMENT OF AODV SECURITY AGAINST BLACK HOLE ATTACK IN MOBILE AD HOC NETWORK

AL-QARAGHULI, Sara Harith Hazim

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Mesut ÇEViK

Date: April/2023

Pages: 62

Security has emerged as one of the most critical concerns to be addressed in MANET (Mobile Ad-hoc Network). Because of the high speed of MANET and the huge amount of nodes, security moved to be a major complicated and too hard challenge in the network, causing it to be unprotected from various kinds of security attacks. In this blackhole attacks were used to be able to evaluate their effects on the MANET. The blackhole attacks are investigated in both single and multiple attack scenarios. They are simulated using NS2 simulator version 2.35 for network simulation. The AODV (standing for Ad-hoc On-Demand Distance Vector) protocol was used to send data messages from one node to another one. Four sets of evaluation used cases were performed in two networks type (static, and dynamic) with (10,20,40, and 60) nodes and speeds ranging from (20-100) MS and implementing appropriate solutions. The R-AODV (Reverse-AODV) and ACO (AntNet Colony Optimization) algorithms are used to eliminate the effect of single blackhole attacks and to improve the MANET under the effect of multiple blackhole attacks, respectively. The full amount of the dropped packets, the ratio of the delivery packet, and the throughputs are calculated and compared to show the change in the efficiency of the AODV protocol improves after implementing solutions to eliminate the impact of blackhole attacks on the network (MANET). The findings show that the attacks of blackhole have a greater effect on

AODV. The efficiency of the network (MANET) is highly affected by the number of nodes and nodes' moving speed, in our performed simulation, network behaviour shows better performance in less number of nodes and high speed. After reviewing the previous studies that related to Ad-hoc networks generally and attacks that target those networks especially I choose the blackhole attack as subject for my study as the blackhole attacks has a higher effect on AODV protocol compared to other attacks like flooding and rushing attacks, from my end I suggest two possible solutions that can help in eliminate blackhole attacks that I will explain it in details and practices in this thesis. R-AODV has a greater impact on reducing attack effect than AntNet solutions for a single blackhole attack.

Keywords: MANETS, Blackhole Attack, AODV, R-AODV, Antnet.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF CHARTS

Pages

ABBREVIATIONS

LANs	:	Local Area Networks
MANET	:	Mobile Ad Hoc Network
VANET	:	Vehicular Ad Hoc Networks
FANT	:	Flying Ad-Hoc Network
SANET	:	Ship Ad-Hoc Network
AODV	:	Ad-Hoc On-Demand Distance Vector
BKH	:	Blackhole
NS2	:	Network Simulator 2
DDOS	:	Distributed Denial of Service
ACO	:	Ant Net Colony Optimization Algorithm
RREQ	:	Route Request
RREP	:	Route Reply
R-AODV	:	Reverse-Ad-Hoc On-Demand Distance Vector
PDR	:	Packet Delivery Ratio
UAV	:	Unmanned Aerial Vehicles
QoS	:	Quality of Service
DSR	:	Dynamic Source Routing
HMAC	:	Hash-Based Message Authentication Code
BPAODV	:	Black Hole Protected Ad-Hoc On-Demand Distance Vector
E2E	:	End-to-End
SAODV	:	Statistical Ad-Hoc on Demand Distance Vector
SVM	:	Support Vector Machine
ANN	:	Artificial Neural Network
TCP	:	Transmission Control Protocol
UDP	:	User Datagram Protocol
DSDV	:	Destination Sequenced Distance Vector
BAN	:	Body Area Network
PAN	:	Personal Area Network
WLAN	:	Wireless Local Area Network
IEEE	:	Institute of Electrical and Electronics Engineers

IP	:	Internet Protocol
INVANET	:	Intelligent Vehicular Ad-Hoc Networks
WRP	:	Wireless Routing Protocol
FSR	:	Fisheye State Routing
ZRP	:	Zone Routing Protocol
OLSR	:	Optimized Link State Routing
Tcl	:	Tool Command Language
MAC	:	Media Access Control
MPS	:	Meter Per Second

1. INTRODUCTION

Wireless networks have evolved quickly in recent years to facilitate mobility. We can categorize mobile wireless networks into two categories based on whether or not they have an infrastructure. A network with infrastructure is the 1st kind, the nearest base station is used by the mobile node to establish a connection within the range of communication. A mobile node is the same as a mobile terminal in such a network. It lacks routing capabilities switching and routing tasks are handled only by mobile switches. Cellular wireless networks, business wireless LANs, and other similar systems are typical instances of this sort of network. A mobile network without infrastructure is the 2nd type. It is a wireless multi-hop autonomous network. There are no fixed routers or equipment throughout the entire network. Each node can maintain touch with other nodes in any fashion and is mobile. due to the terminal's restricted wireless coverage in this scenario, As two terminals' users who are unable to communicate in a direct way can nonetheless transfer packets with the help of another node. since every node is a router, it has to be able to find also keep the route to the rest nodes.

It is a Latin word and this word refers to "for this purpose" Ad-hoc network also referred to local area networks (LANs), link nodes together on their own initiative without the need for any centralized (Base Station) wireless networks. With no Wi-Fi, routers, or access points in a range of 100 meters between each node, the ad-hoc network can be performed where all the nodes' devices (end device) have the ability to communicate with each other without wire connection to get and send the data. The ad-hoc network lacks a fixed topology as an outcome of nodes' mobility. However, the network must have other nodes that work as a router to re-transfer the data to the targeted nodes so any node in the ad-hoc network can transfer the data to other nodes within the ad-hoc network. But there are multiple different kinds of ad hoc networks (wireless) as shown in figure below (Figure 1.1):

a. MANET (Mobile Ad-hoc Network).
b. VANET (Vehicular Ad-hoc Network.
c. FANT (Flying Ad-hoc Network).
d. SANET (Ship Ad-hoc Network).

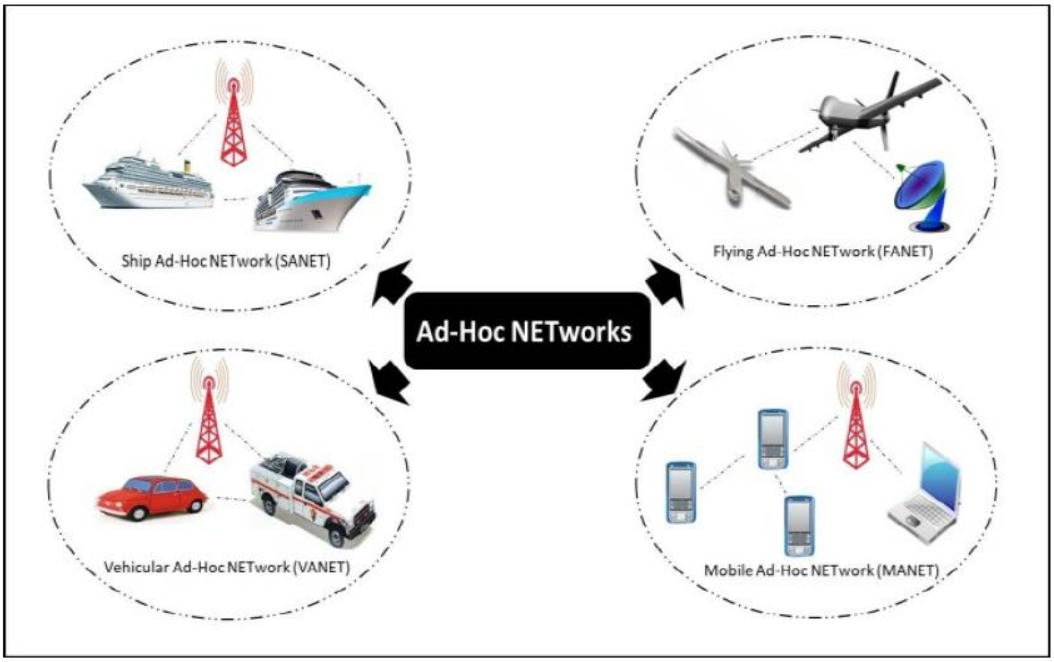


Figure 1.1: Ad-Hoc Network Types [1].

Mobile Ad-hoc Networks (MANETs) are made up of mobile nodes that are constantly moving and that communicate using certain routing protocols. Because of their random structure, unlike conventional networks, they experience constant changes in the courses and routes of communications between nodes. However, because MANETs are scattered and use a variety of routing protocols, there are difficulties and security flaws that can invite assaults [2]. Due to its many applications in data communication, small footprint, quick deployment, low installation cost, and minimal infrastructure needs, it is very well-liked today. The network's nodes can move around and are available to connect/disconnect at any time in the network. The primary MANET's attributes are the non-job, coordinator's several wireless relays, and regular limitations on computing power, bandwidth, and links use of batteries [3]. Each node has a wireless link that allows for direct communication with the others. Each node has the ability to transfer and get data from the nodes beside it also it can serve each other as a host/router. MANET networks are used in many applications kinds, including data collection, seismic research, healthcare, defense, military, search and rescue, wearable technology, and other locations where pre-installed infrastructure is impractical. In MANET, if a user wishes to join the network, it must first be determined whether the user is malicious or not. It must also be determined how much and what kind of resource access permissions

should be granted to the user in order to ensure that the network is not harmed. MANET security is a significant element influencing the network's fundamental operations. Compared to fixed networks, MANET networks are more susceptible to a lot of attacks' kinds because of their dynamic architecture, unclosed media, and finally the gap of un-centralized and monitored management [4]. Blackhole attacks are one of these attacks as the performance at the network layer is particularly will be impacted by blackhole attacks.

1.1 MANET'S FEATURES

MANETs network have the following characteristics Second paragraph [5]:

a. Infrastructure is not required, such as a flat network
b. Network-linked devices act as routers
c. Radio linking - using shared mediums
d. Self-contained nodes
e. Naturally, it has dynamic mobility/topology
f. Needs limited power and a few computing-wise resources.
g. Wireless node connections' unreliability.

1.2 PROBLEM STATEMENT

Security matters are one of the most difficult issues in MANET networks. This is due to the network's nature, which has a lot of network elements (nodes). As a result, maintaining control over the network is more challenging, which increases the potential for network security threats.

1.3 AIMS OF THE STUDY

This work's goal can be summed up as follows:

a. Assess and examine the routing attacks' effect on the functionality of the MANET by using the AODV routing protocol.

b. make relevant suggestions for network routing attacks that will help to reduce their impact and enhance MANET performance.

c. To get around the constraints of earlier works.

d. To decrease MANET security risks.

e. To offer a mechanism that might be updated and changed to thwart more MANET assaults.

1.4 THESIS LAYOUT

Five chapters make up this thesis; the remaining chapters can be summed up as follows:

Chapter two: Contains a MANET's security literature review, as well as information on the classification of security assaults, security needs, network security attacks, and remedies to those attacks.

Chapter three: includes a description of the simulation and three situations classified as follows:

a. Situations where should use the MANET as a routing protocol.
b. Cases that need MANET to be used in conjunction with a blackhole assault.
c. The instances that need MANET to be used after eliminating the security attack.

Chapter four: focuses on the evaluation, analysis, and comparison of the key simulation performance metrics with various applied scenarios.

Chapter five: the conclusions and the recommendations and further studies

2. LITERATURE REVIEW AND THEORY

2.1 INTRODUCTION

This chapter includes the previous studies related to Ad-hoc networks, explaining theoretical part of the MANET, Routing Protocols, and Security Attacks, and explained the blackhole attacks in detail.

2.2 LITERATURE REVIEW

Palak and Rakesh, in 2018 [6] proposed a new technique to prevent DDOS attacks in VANETs. after detecting the malicious nodes in the network then the network security increases. Using the second version of NS2 as a network simulator which used TCL as programming to build the simulations' user interface. In AODV routing protocol, backend is implemented using C++ by NS2. There are a total of 37 nodes, and the simulation area is 800mm by 800mm. The antenna type is omnidirectional. Throughput demonstrates that the number of transferred packets during a DDOS attack is lower than the number of transferred packets during a period in which there was no DDOS attack.

Reyhane and Ghasem, in 2019 [7] Based on the backbone structure, they introduced a geographic routing protocol. instead of using mobile vehicles, they used traffic lights as bridges for assessing routes. The results of the simulation show a huge enhancement in the efficiency of the network, VANET network is got by comparing a protocol similar to VANET named "SCRP".

Krzysztof and Aneta, in 2020 [8] They proved that the SIN algorithm is very useful in finding blackhole attacks. the needed time to find the blackhole attacks depends on the distance between the node and SIN, however, mainly it works by sending a query (RREQ) and then it will be waiting for the response (RREP). and finally, the biggest number of attackers' blackholes will lead to extra needed time to find them all.

Alexey et al, in 2018 [9] This study focused on calculating the FANET's PDR (Packet Delivery Ratio) parameters of 90% percent or more at the designated region (ratio). Every outcome was gathered during the experimental investigation. As a method of study, the simulation modeling was an NS2 based on the network's characteristics created utilizing the

model's simulation. There are details regarding the AODV routing protocol. The connection relies on certain network characteristics, such as the transmission range and the number of nodes that were examined. As a result for the length of the routes and based on the presented parameters' analysis. The simulation's outcomes demonstrated that FANET More than 90% of connectivity with PDR is guaranteed when 50 to 100 nodes are present, and the distance of the transmission is 500 m. Experimental evidence shows that the figuring out factor of the connection of the UAV networks (self-organizing) is the number of all nodes that are distributed over the network area and the transmission's range.

Alpana and shoba, in 2018 [10] Studied the network's proficiency in MANETs under the blackhole attack and using AODV protocol. for simulation using the (NS-2) network simulator with altering the time of the simulation, size of the traffic, nodes' number, and nodes mobility to be considered as the network's factors, performance indicators include throughput, the needed time to deliver the packet from end to end (end-to-end delay), the ratio of the delivered packets, route overloading, and the number of the dropped packets. Results demonstrate that when nodes begin operating maliciously inside the network, will lead to a decrease in the packet delivery ratio and network throughput, which means that the end-to-end delay, number of dropped packets, and routing overload, will be increased in these networks under blackhole attacks as compared to networks with typical AODV.

Deepthi and Vagdevi, in 2018 [11] Examined the effects of reactive routing protocol black hole attacks, such as Distance vector routing for ad hoc situations (AODV). This protocol's effectiveness is evaluated to determine the attacking potential and contrast the results of the attack on AODV with a black hole, AODV, and planned protocols for AODV. The analysis is carried out by using simulations NS-2.35 and Quality metrics like throughput and PDR Additional measurements include Average Energy Consumption in comparison, there has been less data loss caused by rogue nodes. The throughput has increased, which has reduced the delay. The average packet delivery ratio is 99.7%, which is extremely close to 100%. Each node uses an average of 15.78 joules for every packet, for a total energy consumption of 789 joules per 1500-bit packet. Twenty packets were dropped for AODV and none for the suggested AODV technique. With a black hole, throughput is 51.25, whereas using the suggested approach, it is 100%.

Ida and Helmi, in 2018 [12] Investigated the relative merits of DSR and the AODV protocols in the context of a blackhole assault on the MANET. QoS metrics that were employed to evaluate the effectiveness of the packet loss, Throughput, and delay were both of the protocols have the same ratio. The throughput was lower when using the AODV routing protocol. drop in value comparing it to the value in the DSR protocol attacks from both individual and collective black holes that expose. Additionally, the DSR protocol encountered greater lost packets occurring during a cooperating of the blackhole attack when contrasted with the AODV protocol. As a result, When it comes to using AODV because of routing protocols in MANET's networks, essentially if the MANET's network is under the attack of blackholes.

Nooralhuda et al, in 2019 [13] Find out a novel security system for mobile ad-hoc networks (MANETs). To protect the routing control packets, the suggested technique combined the "Trivium lightweight stream cipher algorithm" with HMAC (SHA-3 as the underlying hash function). The AODV's performance after applying the security scheme has been implemented is compared in this study in terms of end-to-end delay, throughput, jitter sum (end-to-end), and the ratio of the packet loss. Under the attacks of the blackholes, the proposed system performs is bestead than the performance of the original AODV.

Moirangthem et al, in 2019 [14] Focus on the analysis of gray hole attacks of ad-hoc on AODV is one of the routing protocols that depend on the needed distance vector. MANET employs dependability as a primary metric. There is going to be a simulation. utilizing the NS-2.35 which is one of the network simulation software under a variety of different conditions of nodes in the network and a variable amount of gray holes in the network. the simulation's results show a growth in the total number of grey holes in every additional MANET node which leads to a deterioration in the reliability of the MANET.

Sivanesh and Sarma, in 2019 [15] Made a study contrasting rushing and black hole attacks at the network layer using NS-2 simulations. The most susceptible attack can be determined using the delay of transferring the packets from end-to-end, the successfully delivered packets, also Using throughput as a criterion for performance. In this case, the Ad-hoc On-Demand Distance Vector (AODV) protocol is now ready to forward data. The simulation findings show that compared to the rushed assault, the black hole has worse metrics for the ratio of the delivered packets, throughput, delay of transferring the packets from end to end,

and lost packets. Changing values of the malicious nodes in the graph does not affect our observation result (like 5,10, 15, and 20). We draw the conclusion that in MANETs, the attacks of the blackhole are significantly much destructive than the rushing attack.

Sairam and Raghavendra, in 2019 [16] modified the Ad-hoc On-demand Distance Vector (AODV) routing protocol, that was developed for dynamic nodes in the ad-hoc network. The blackhole nodes in the hole network are specified by the AODV's sequence number utilizing the network simulator (NS2) without the usage of any additional packet formats. In this project, the throughput of the MANET, the delay, the load, and the quantity of dropped packets both under attack and with no attack are analyzed. It has been noted that the black hole is attacking the network. parameter deteriorates Considering the expanded network Increases in traffic, throughput, PDR, and packet drops in the absence of an attack. Further, it found that whenever an attacker approaches a source, the impact is more damaging than it is further. comparable to the PDR and throughput increase as the number of black holes rise diminishes. All of the simulations' proximity to the sending node is attacked, and the impact on the blackhole attack causes a reduction in the average latency. The reason for this is the higher number of the sequence's destination RREP with no checking for the route's entry in the table of routing.

Radityo and Suhadi, in 2020 [17] This demonstrates that the black hole assault has a considerable influence on the throughput, PDR, and end-to-end delay. Because of the presents of a blackhole, the received packets number is significantly lower than the transmitted packet number. When compared to SAODV, BPAODV (Black hole Protected) performs poorly (Secure). Both have the ability to dodge the malicious nodes, but they are unable to recover a large amount of dropped packets caused by the nodes that were malicious. However, the default setup of the AODV with a rogue node in the MANET network produces 0% in the packet delivery ratio. As a result, both BPAODV and SAODV can efficiently eliminate the effect of the malicious node in the black holeattack.

Shweta and Varun, in 2020 [18] The proposed method makes use of an ANN (Artificial Neural Network) and SVM (Support Vector Machine) for the classification and detection of attacks caused by the blackhole in the hole network The outcomes are achieved in the midst of the AODV and the blackhole. as well as the mechanism from security wise that offered by SAODV (Safeguard AODV). The outcomes were tested on last, it has a variable number

of nodes tested for 100 nodes that provide a 54.72% reduction in energy use, The throughput is 88.68 kbps, and the ratio of the delivered packets is 92.915%, with a delay from end to end equal to around 37.276ms. The suggested routing model is more secure and efficient. It is also useful for detecting black holes.

Vedant et al, in 2020 [19]TCP analysis against a well-known attack, the black hole attack, is proposed. Under various conditions, the effects of the credible TCP (Transmission Control Protocol) and transport layer protocol are investigated. of the ad hoc network attack The performance has improved. measured using the average of the throughput metrics normalizing the delay from end to end and routing load As a result, inferences were been pulled. The results show TCP's performance and TCP's Vegas with the effecting of the AODV and blackhole AODV with end-to-end delay, medium throughput, and high load in routing density For the network, the throughput value that was achieved falls safely. within the normal range routing load and the delay of transforming from end-to-end increases extremely with a TCP attack (blackhole) TCP's Vegas as well fails to enhance the efficiency when the network is down with a blackhole attack.

Vandana and Suchitra, in 2020 [20] proposed a black hole detection system and performance analysis is performed on the performance metrics to be considered when establishing such mobile networks. We use NS-2.35 to simulate the aftereffects of an AODV with no blackhole attacks, an AODV under blackhole attacks, a DSDV without a black hole, and a DSDV with a black hole attack. Analyze the attack's reactive and proactive routing protocols. A secure sequenced mechanism outperforms the protocol of AODV and the other secure AODV protocol in terms of performance. This is a more effective method to detect nodes that are actually blackhole nodes in mobile ad-hoc networks. The benefit of the key-sharing mechanism especially is to prevent blackhole attacks.

Fahmina et al, in 2020 [21] The proposed solution is targeting to find out and avert the blackhole attacks by leveraging the AODV enhanced recovery route protocol parameters. The suggested algorithm contains two types of non-similar scenarios, one for detection and one for avoidance. The resulted values from the simulation that was performed using NS-2 are used to validate the efficiency of the suggested algorithm in the presence of attacks (blackhole one), with considering the changes in the needed time to end the simulation and the active amount of the attackers' nods. The deployment is graded in reference to the

following metrics: delay in time to deliver the packets, the ratio of the successfully delivered packets, the ratio of the dropped packets, the ratio of forwarding packets, throughput, and overhead. The results recieved from the network's simulator were mapped into a dataset, then it was validated based on the fuzzy modeled system's inference by utilizing MatLab. The results show that the enactment that was proposed for AODV implementation is significantly best, also it increased the amount of the throughput as well as the higher ratio for the delivery of the packet. also, it decreased the delay and overhead, also it lowers the number of drop packets, and resulted in a higher ratio of packet density forwarding in comparison to current ones In addition to that the result of the simulation is supported by a vague inference system that is used to calculate the network is a secure network or not. It strengthens the authentication process of the known approach by rechecking it more with the vague system. Further improvement to the work can be done by detecting cooperative blackhole attacks and utilizing the various delay parameters to find out the malicious nodes and recheck them by the vague logic system inference

Asif Uddin et al, in 2021 [22] Used The source node that utilizes an algorithm that is based on binary partition clustering in order to find out and prevent attackers' nodes (blackhole nods). We evaluated the efficiency of the suggested solution in comparison to the performance of the existing solution by employing the ns2 simulator for simulation and the AODV protocol. The simulation's results which took 200 seconds and had a total of 100 nodes, the max speed level was 30 meters per second, the packet's size was 1024 bytes and demonstrated that the proposed solution is more effective than the one that is currently in use.

Pushpender Sarao, in 2022 [23] The rushing attack, gray hole attacks, and blackhole attacks are used to evaluate the Ad-hoc AODV (On-Demand Distance Vector) protocol. The performance of the network has been evaluated under more than one attack, under one attack, and with no attack. Four different scenarios on this network have been generated by changing the speed, the size of the network, node intensity across the network, and the quantity of nodes that are designed to be attackers. Average throughput, the average of the delay (end-to-end delay), and finally the ratio of the packet delivery, all those factors are considered efficiency factors. The utilized software for the simulation was NS 2 to perform the simulated network using AODV protocol attacks. The results show that multiple attacking

nodes have a greater impact on MANET than a single attacking node. All of the aforementioned attacks are to blame for the network's low throughput, frequent packet drops, and longer delay from end-to-end packet delivery. As attacking nodes grow, so does the throughput. When compared to blackhole and gray hole attacks, rushing attacks have a lower impact on AODV.

After reviewing the previous studies that related to Ad-hoc networks generally and attacks that target those networks especially I choose the blackhole attack as a subject for my study as the blackhole attacks has a higher effect on AODV protocol compared to other attacks like flooding and rushing attacks, from my end I suggested two possible solutions that can help in eliminate blackhole attacks that I will explain it in details and simulations in this thesis.

2.3 MANET ARCHITECTURE

The MANET architecture is depicted in figure below (Figure 2.1)

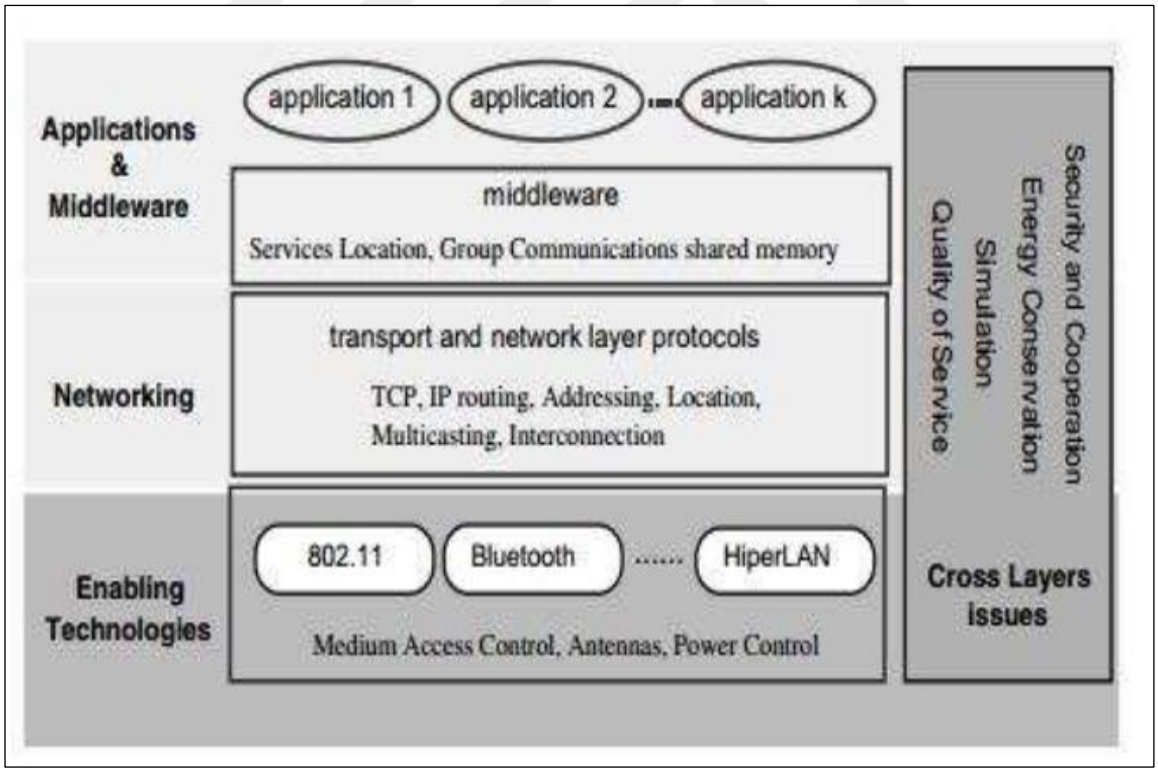


Figure 2.1: MANET Architecture [24].

It is divided into three major sections:

2.3.1 Enabling Technologies

Enabling technologies are further classified based on their scope of application [25].

a. BAN: BAN is stands for Body Area Network for this network the range of communication is 1 to 2 meters. It connects wearable computing devices.

b. PAN: PAN stands for Personal Area Network for this network the range of communication is can reach 10 meters. It allows mobile and stationary devices to be communicated with each other.

c. WLAN: WLAN stands for Wireless Local Area Network for this network the range of communication is 1 hundred up to 5 hundred meters. It can link one building or a group of buildings.

2.3.2 Networking

In MANET architecture, most of the primary networking protocol functionalities must be designed again in a new way for auto-configuring, have the ability for peer-to-peer communication environment, unstable, and dynamic, The initial goal for the protocols of networks is to evolve a credible end-to-end service between both ends (sender and receiver) by utilizing one-hop of the service's transmission that provided by activating technologies. To implement communication between both ends (sender and receiver), the sending end must be located with the receiver end within the network. the primary function of the location service is to automatically map the receiver device's address to its current network location.

2.3.3 Application and Middleware

Application & Middleware Wireless technologies such as Bluetooth, WiFi, WiMAX, IEEE 802.11, and Hyper LAN significantly encourage the deployment of technology of ad-hoc and new networking applications related to ad-hoc, particularly in specific scopes like the services that are emergency, disaster recovery, and environmental monitoring. MANET's adaptability turned it to be suitable for a variety of practical situations, including PAN, home networking, law enforcement operations, applications related to commercial and educational

wise, also networks' sensors. Recently the mobile ad-hoc frameworks were developed to use the methodology of having no middleware, adding relying on every application to treat all of the services it requires.

2.4 TYPES OF MANET

a. VANET: VANET stands for Vehicular Ad-hoc Network and it was built using the principles of MANETs (mobile ad-hoc networks). It allows effective communication between a vehicle with another one, or with the equipment on the roadside.

b. IMANET: it stands for Internet-Based Mobile Ad-hoc Networks which is another kind of wireless ad-hoc network that uses Internet protocols such as TCP/UDP and IP. To connect mobile nodes and automatically establish routes, the IMANET employs a network-layer routing protocol.

c. INVANET: it stands for intelligent vehicular ad hoc networks. this type of network employs artificial intelligence to deal with unlooked-for situations such as car collisions and accidents.

d. FANET: it stands for Flying Ad-hoc Network and it’s made up of unmanned aerial vehicles that provide mobility and connectivity to remote areas.

2.5 MANET APPLICATIONS

Traditionally, MANETs networks were utilized as a wherewithal of communication in harsh and catastrophic environments where it is too hard to set up a full network for communications, such as warfare areas, ruined areas, disaster recovery, saving missions, and others. Because MANET networks are automatically formed, there it does not need physical connections are a centralized station because communication is solely dependent on nodes that comprise a MANET. As mentioned in [26] the nodes will be transceivers, meaning they have the ability to transmit and receive data as well at the same time. figure below (Figure 2.2) shows different applications of the mobile ad-hoc network are listed [27]:

a. Tactical Networks: dynamic battle areas, systems of martial communication, etc.

b. Location-Aware Services: Promotion for the service of specific locations, dynamic forward calls, the guide for travel locations, etc.

c. Sensor Networks: The weather's remote sensors, earth activity, and other purposes.

d. Educational Applications: Creating virtual classrooms, conferences, etc.

e. Emergency Services: militant activities, control and manage the crowds, natural disasters (during floods, earthquakes, and so on), and so on.

f. Entertainment: Robotic pets, multiplayer games, and so on.

Figure 2.2: Applications of MANET.

2.6 ROUTING PROTOCOLS

The below figure (Figure 2.3) shows the types of MANET's routing protocols

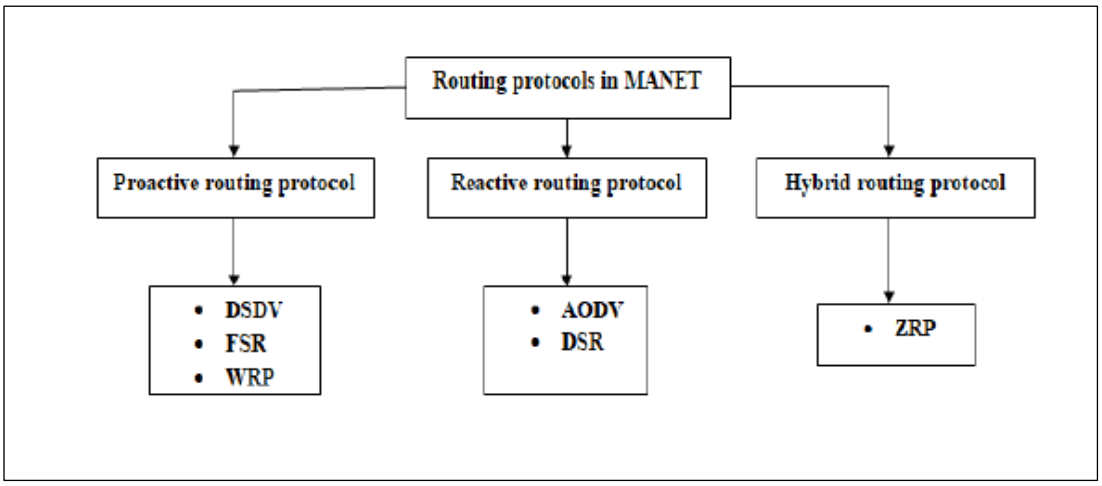


Figure 2.3: MANET Routing Protocols Classification.

a. Proactive Routing Protocols: Table-driven protocols (routing protocols) are used in proactive routing protocols [28]. The target of these table-driven protocols is to keep routing details from every network's node. Furthermore, these routing protocols enable all nodes to store routing information in one or more routing tables. For instance, DSDV, WRP, and FSR.

b. Reactive Routing Protocols: Reactive protocols, also identified as on-demand routing protocols, generate routes only when they are required. once a node requires a path to send information or packets to its destination point, it triggers the path discovery process inside the network. AODV and DSR are two examples.

c. Routing Protocols on Hybrid: Hybrid routing protocols are a mixing of the two protocols above (reactive and proactive). ZRP is an example.

2.7 AODV ROUTING PROTOCOL

Because it is one of the most efficient routing protocols, the AODV protocol is used in this project to send safety messages between nodes. AODV is considered as a reactive routing protocol that create connections between nodes only when source nodes request it. It keeps the routes alive if the sources require it. The network remains silent in this protocol until a connection is required. The below figure (Figure 2.4) depicts the protocol's algorithm, which includes the following steps [29]:

a. First, the node that wishes to transmit data checks the route; if it is available, it will send an RREQ (Route Request) message to find the end point destination, otherwise, it will send an RREQ letter to find a path among other nodes.

b. If the received node is a destination node and is ready to transmit data, it will respond to the source with an RREP (Route Reply) message to begin data transmission; otherwise, it will activate a local route search to find an available route over neighbouring nodes to the destination.

c. Finally, if the transmission is not successful, the route maintenance will be reactivated to restart the route discovery procedure.

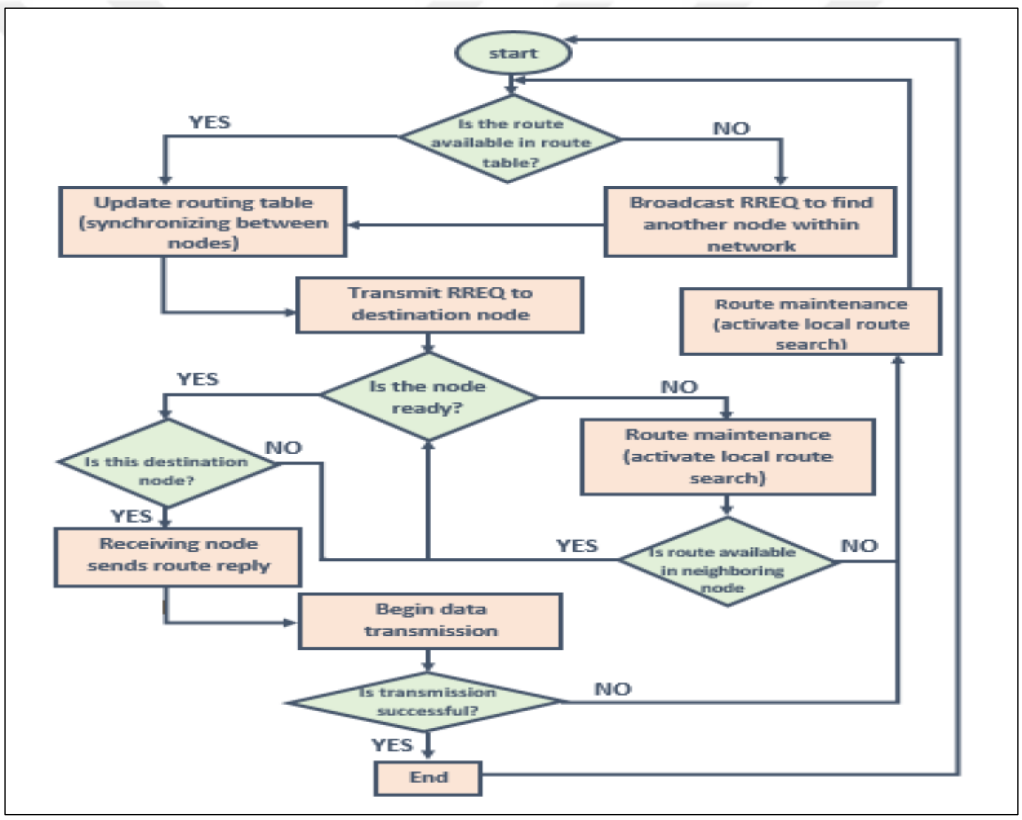


Figure 2.4: Flowchart of AODV.

2.8 SECURITY ISSUES AND CHALLENGES IN MANET

The MANET (mobile ad hoc network) is a network with no infrastructure in which every node has the ability to be functioning as a router, which allows the network to dynamic topology in which the single nodes can move freely. Ad-hoc Networks are considered very

fast growing networks due to the proliferation of portable, affordable, and technologically advanced devices on the market [30]. MANET is vulnerable to malignant attacks and security infringements due to its lack of physical organization [31]-[32]. These attacks can be classified in nature into [33]:

a. External attacks: include refusal of service, overcrowded links, and incorrect routing data attacks.

b. internal attacks: include malignant nodes impersonating systematic nodes in order to reach secret data [34]. This is doable to be done after the malignant node has established itself in the network because it will at first take part in all network activities as an original node.

c. Active Attacks: Active Attacks achieve the attacker for duplicate; transformation and removal of exchange and also attempt to modify protocol behaviour. A number of times, identify the active attack; however, an attacker uses active attacks less frequently. Essentially, an active attack modifies data packets, injects packets, and drops packets.

d. Passive Attacks: Passive attacks are difficult to detect. A routing packet and an attacker may learn about a node [35]. The passive attack aims to compromise the network's privacy and complete the communication prototype among nodes.

These are some of the attacks that have the ability to occur in the MANET networks:

a. DDoS (Denial of Service) attack: In this case, the assailants intend to obstacle the node or the whole network, resulting in no available attacked node or non-attacked node. the signals of the radio are used to disable the prey node, resulting in an unavailable node as well as a battery drain [36].

b. Eavesdropping: It’s classified as a passive offensive because the malignant node examines all the packets of data that pass out of it in order to earn prudence inside the network. assailants are typically concerned with various kinds of data, like passcodes, locations, etc.

c. Impersonation: Impersonation occurs once the assailant node poses like a legitimate node in the network in order to gain dependability and credit. If the verification mechanism

fails, the assailant has the ability to bypass it, gaining the reach to secret information too as the ability to monitor the traffic of the network.

2.9 SECURITY REQUIREMENTS

The fundamental security requirements are outlined below:

a. Availability: Nodes should maintain their ability to deliver all of the designed services, regardless of their security state or the safety area that was compromised during a denial of service attack, and every authorized node should assess the data.

b. Authentication: Authentication establishes the trustworthiness of communication between two distinct nodes. Because the identity of the source node is ensured, the necessary participant ensures your identity. One method of providing this service is through certifications; however, in the absence of a central control unit, key allocation, and key management are questionable.

c. Confidentiality of data: Each node or application specifies the services and permissions to access. Because MANET networks have no centric management, key distribution is too hard, if not impossible in some cases.

d. Integrity: When messages are transmitted than integrity grantee identity in MANET, only authorized nodes can create editor delete packets, according to integrity security service.

e. Authorization: The authorization process is commonly used to assign different access rights to different levels of users.

f. Privacy: ensures that the node's personal information is not disseminated by the node or the system software, ensuring that contact is unknown.

2.10 MANET NETWORK LAYER SECURITY ATTACKS

MANET networks can be affected by attacks in a variety of ways. Some of them may cause network delays by sending traffic packets to non-optimal paths or sending them to non-existent paths, causing them to be lost. Some attacks may cause routing loops and network congestion, while others may prevent the source's node from determining the path to the end destination node. Network layer attacks are categorized according to the phase of the routing

operation. Most attacker nodes attempt to exploit routing protocol vulnerabilities, which can be either proactive or reactive. At the network layer, there are various types of attacks. There are several:

a. Wormhole attack: Wormhole attacks collaborate with each other to degrade network performance. A wormhole node pairs with another wormhole node in the same network or could be a different network. In the case of wormhole attacks, the packets of the data are transferred via a wormhole tunnel. Following route capture, wormhole nodes have the ability to store, modify, or turn the packets of the data, causing network overcrowding, spoofing the lost packet, and eavesdropping [37].

b. Grayhole Attacks: A gray hole attack is a most stealthy attack form than a blackhole attack. In a gray-hole attack, the attacker drops some incoming packets from different nodes but selectively forwards other incoming packets from other network's nodes. A secure routing protocol is not going to be able to stop grayhole attacks very easily [38].

c. Rushing Attacks: On-demand routing protocols are particularly vulnerable to this type of attack as they depend on deleting repeats in their functionality except for the first request for a route being performed by the nodes, and the repeated packets that reach later on are removed. This technique is used to decrease the expense of discovering the route. As a result, in order to be part of the founded out routes, malignant nodes utilize the rushing attack by rapidly publishing route request packets. Rushing attacks have the ability to carry out in a variety of methods, including utilizing the high power of transmission levels in wireless communication, discarding the delays in the routing layers or MAC, accomplishing the wormhole attack, and maintaining other nodes' queues of transmission full [39].

d. Byzantine attacks: The "Byzantine problem" is the spot attitude of several faulty and corrupted group members that causes a system malfunction. The byzantine attack in MANETs are resulted from one or more malignant intercede nodes working together to launch attacks like removing selective packets, initiation of routing loops, and, resulting in an obstruction or degeneration of services transferring packets routing via non-optimal paths.

e. Replay attacks: Because of the recurrent nodes' dynamic moving in MANETs, the topology of the network is unstable. The on-ground topology of the network going to vanish in an instant. In the replay back attack, a malignant node copies the previous correct value of control messages and then inserts the control messages into the network (in the case of OLSR protocol the messages will be TC). The nodes' tables of routing will then get these letters and they will be modified according to corrupted data. The attack's replay could be utilized to steal the identity, deactivate the routing, or perform requesting data by a duplicated packet.

f. Link spoofing attacks: This type of attack advertises fake links with non-neighbors in order to disrupt routing operations. The malicious node creates a link with the fewest hop neighbors, causing the goal node to choose this malignant node as a multipoint relay for it, allowing it to obtain data or route traffic while modifying or dropping it.

g. Routing Table Poisoning Attacks: By varying the routes in the table of routing, attacker venoms the routing table. Another option is to add an RREQ packet with a high arrangement number and delete a packet with a low sequence number. Routing protocols keep tables that include the network's routes in the correct order.

h. (Denial of Service) attack: It is forbidden for a node to send and receive packets of data to its targeted destination or to use resources of the network. This is accomplished by sending a huge amount of routing packets to the prey node. Other nodes' packets have no ability to be received or sent by the victim node [40]. DoS attackers utilize one-node connectivity to spate the targeted node with bogus RREQ, commonly in a try to result in a large value of resources and bandwidth. disseminate refusal of service (DDoS) attacks, on the other hand, are performed from many malignant nodes spread through the network.

i. Jellyfish attacks: Is one of the DoS attack types that are too hard to be detected due to its unusual attitude. Jellyfish is one of the attacks that it's almost undetectable and, like blackhole attack, degrades MANET performance. The essential distinction is that in the Jellyfish attack, the malicious node causes a delay in packet forwarding, while, in a blackhole attack, the malignant node drops all data packets. Jellyfish attacks are classified into three types: delay variance attacks, periodic dropping attacks, and reorder attacks [41]. The packets are too delayed in tyrannical order in a delay variance attack. In a cyclic

dropping attack, the attacker nodes are dropping the packet on a regular basis. The jellyfish reorder attack reorders transmissions between both the destination and source nodes. In this project, the safety applications are selected, and depending on the routing protocols used, they may be sent in either a proactive or reactive manner. The AODV routing protocol will be used to send safety messages to and from the nodes in the network. However, it does not possess any security mechanisms to protect against breaches in network security. In addition, the blackhole attacking the network's layer of the MANET is utilized in order to test the effect that these protocols have on AODV.

2.11 BLACKHOLE ATTACKS

The malignant node utilizes the discovery procedure of the routing protocol route in this attack to announce itself as a shorter path to the targeted node that wants to take its packets. It informs other nodes in the network about the availability of new routes despite the check of it'a own routing table. As a result, the malignant nodes (attackers nodes) are permanently available to respond to route requests and intercept and retain data packets. The blackhole attack can be divided into two kinds [42]:

a. A single blackhole attack: This is common in MANETs [43]. In a single blackhole attack, one node only will act maliciously within the network.

b. In a collaborative blackhole attack: multiple blackhole nodes attacking in the network and acting as malignant nodes.

If a node within the network tries to send packets, the node must first send a route request letter to all neighbor nodes, including the attacker node. The responses will come from the attacker node to the source node by quickly sending back the route reply message. When it receives an RREP, it routes the packets to the attacker node. The blackhole node begins dropping all incoming packets after receiving them [44]. The blackhole's function is the attacker node depicted as shown in the below figure (Figure 2.5) Node S, the first node (source node) wishes to transmit packets to the end node (destination node) D, so it first transmits an RREQ letter to all neighbor nodes (nodes C, B, and A). Assuming that node A has a path to node S, Node A will first transmit an RREP letter to node S. Prior to this, the malignant node M transmits an incorrect RREP letter to node A informing it that it has a higher sequence number than the end node (destination node), so node S considers node A

to be the shorter path to the destination node and distributes packets among it. The malicious node M will then receive the packets and discard them [44].

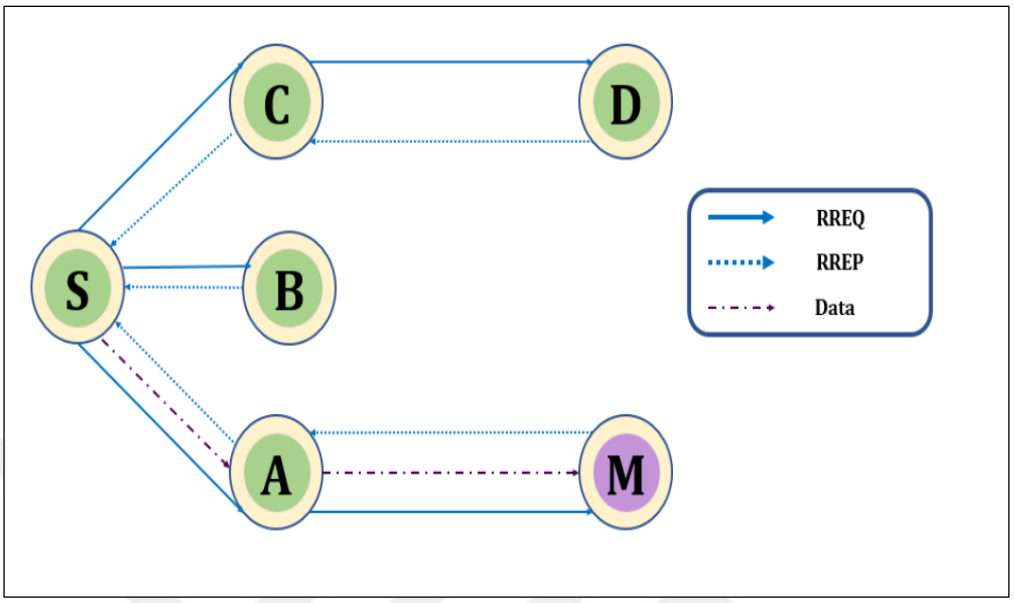


Figure 2.5: Ad-Hoc Network Black Hole Attacker Node Function.

2.12 SOLUTIONS USED FOR NETWORK LAYER ATTACKS

The following solutions were used in this thesis to eliminate the effect of network layer attacks and enhance the AODV Routing protocol security side in MANET networks.

a. R-AODV: It is an AODV modification that is used in this thesis to eliminate the effect of a single black hole attack by using reverse route discovery. A reverse AODV protocol is a type of routing protocols that are utilized on need. once a first node (source node) needs to find a path, it transmits RREQ letters to all nodes that are neighboring it. However, unlike the original AODV protocol, the end node (destination node) doesn't unicast the RREP to the first node (source node) back, instead, once the end node (destination node) receives a route request from the first node (source node), it broadcasts a reverse route request to the first node (source node). once the first node (source node) gets a reverse route request, it begins sending information packets to the destination[45].

b. AntNet Colony Optimization Solution: ACO is a member of the development family's algorithm which depends on the behaviors of true ants. The ants are software agents were used to find out the network and detect the best paths for data packets to reach their

destinations. Ants maintain routing tables and use them to communicate with one another. This solution's prevention of attacks and improvement of network efficiency will be briefed as [46]:

a. First, using the AODV features, determine the initial path for transmitting data from source to destination.

b. using the Ant Net algorithm to detect anomalies in attacks if they exist.

c. Then, using the Ant Net colony optimization algorithm, rediscover the path.

3. SIMULATION OF MANET SECURITY

This chapter introduces the evaluation of the simulation of the AODV (routing protocol) in MANET, attacks, and scenarios of attacks solutions.

3.1 MANET SIMULATION DESIGN

The below figure (Figure 3.1) depicts the overall design of the MANET simulation, which includes both the generation of the MANET simulation through the use of NS2 version 2.35 as well as the implementation of MANET scenarios. Operating system Ubuntu 14.04.3 LTS Desktop serves as the platform for the simulator's installation.

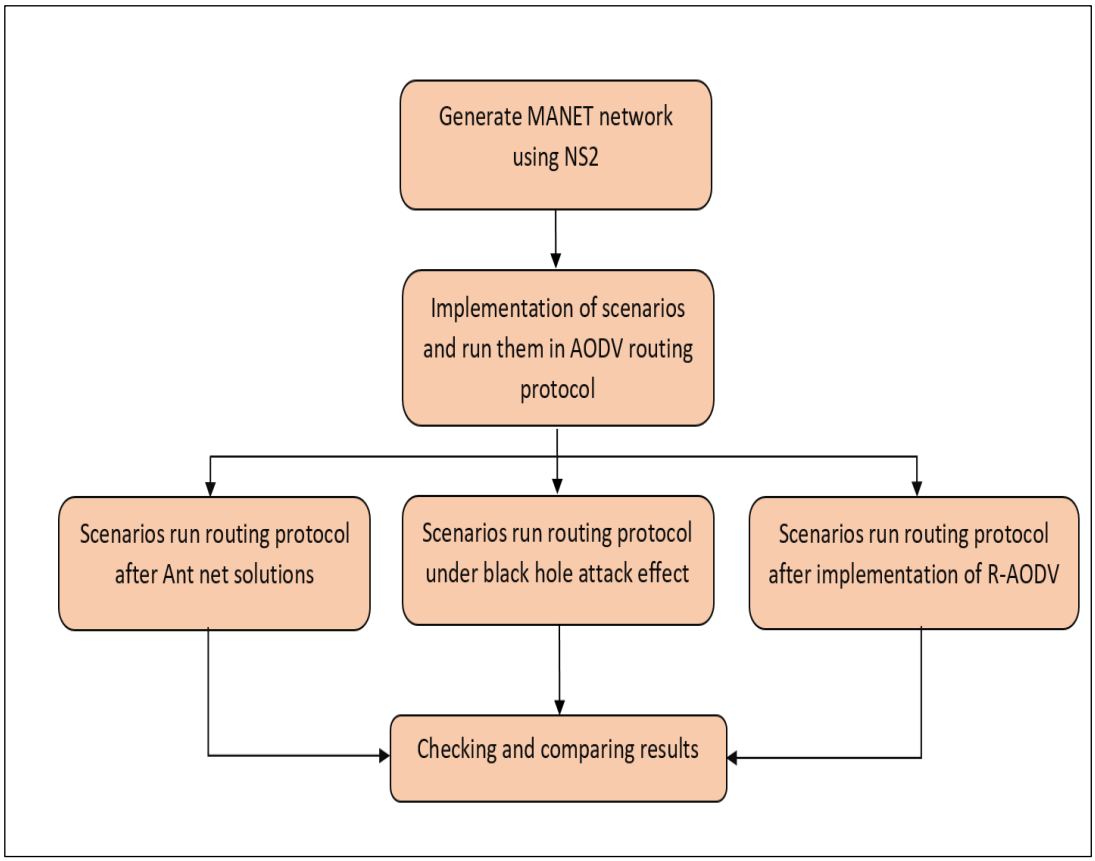


Figure 3.1: MANET Simulation Design Steps.

3.2 GENERATING MANET NETWORK SIMULATION

The MANET simulation part is generated using NS2 by creating a Tcl (tool command language) format file that includes the main simulation parameters. Modeling each node based on the parameters of the ad-hoc network has the ability used to configure a wireless environment. Node configuration is essentially the process of defining the various node characteristics. They may include defining network components for nodes, enabling or disabling the options trace at the Agent/MAC/the levels of the router, and choosing the kind of ad-hoc routing protocol for non-wire connected nodes. The parameters that use in the simulation are shown in Table 3.1 below. The AODV routing protocol is used, a wireless channel is used for connection, signals are propagated using an omnidirectional antenna, two ray ground propagation models are used, and a number of nodes (10,20,40,60) are placed over a (1000*1000) meter2 area, the time of simulation is 600 seconds, and the MAC 802.11 (Media Access Control) protocol is used.

Table 3.1: Network Simulation Parameters.

Parameters	Values
Type of channel	Wireless channel
Type of antenna	Omnidirectional
Propagation Model	Two Ray Ground
Packet Length	512 Byte
Transport Protocol Type	UDP
Simulation Time	600 sec.
Routing Protocols	AODV
MAC Type	802.11
No. of nodes	10,20,40,60
Speeds (m/s)	20,100
Simulation area (m^2)	1000*1000

The Tcl file also includes instructions for creating simulation nodes and moving them. It entails creating a traffic message as shown in below figure (Figure 3.2), which is a safety message that is sent between nodes. To generate traffic messages, we used UDP (User Datagram Protocol).

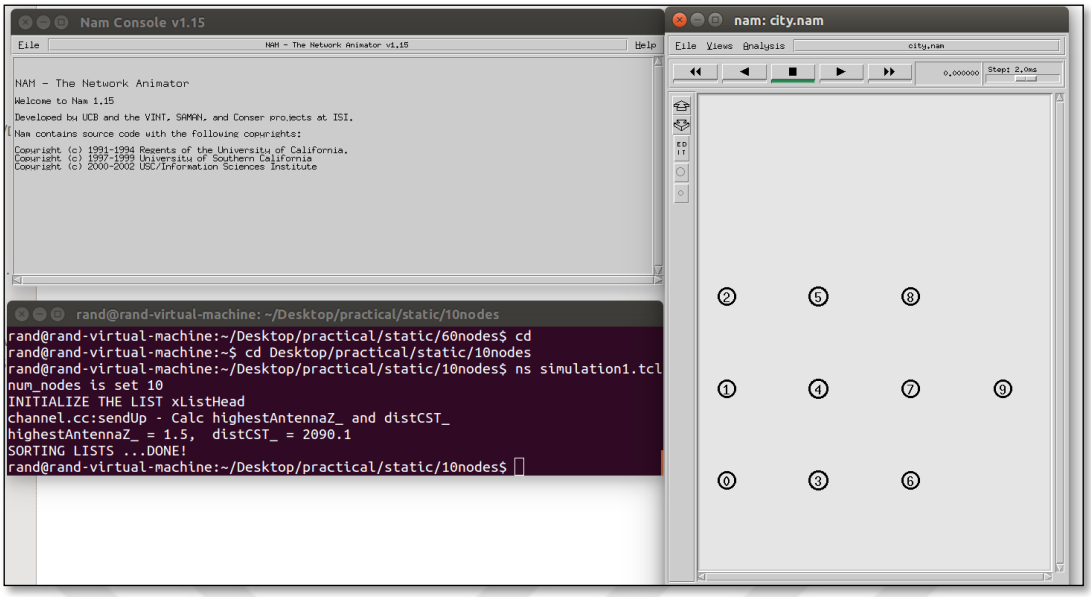


Figure 3.2: Implemented Simulation in NS2.

3.3 IMPLEMENTATION OF SIMULATION SCENARIOS

In this thesis, the simulation is implemented on two types of networks. The first type of network is consisting of multiple numbers of static nods and the second type of network consists of multiple numbers of dynamic nods that are moved at different speeds, the performed scenarios for each type are explained below:

3.3.1 Set of Scenarios for Static and Dynamic Nodes

Four sets of scenarios are used. At each simulation runs through the network (static and dynamic) the number of nodes is changed with values (10,20,40,60). And for dynamic networks the speed is varying as well with those values (20,100) MPS, below are the sets that performed in each case:

a. The initial set of scenarios involves running a simulation of the routing protocol (AODV) in the types of network types (dynamic and static) to observe the network performance.

b. The second set of scenarios includes running a simulation of the AODV routing protocol under single and multiple blackhole attacks to see how attacker nodes affect the performance of the networks.

c. The third set of scenarios includes running a simulation of the routing protocol (AODV) in the types of network types (dynamic and static) under single and multiple blackhole attacks with applying AntNet solutions to see how attacker nodes affect network performance.

d. The fourth set of scenarios includes running a simulation of the routing protocol (AODV) in the types of network types (dynamic and static) under a single blackhole attack and RAODV solution to see how attacker nodes will affect the network's performance.

3.3.2 Simulation Scenarios with Solutions

AntNet colony optimization solution (ACO): The algorithm of ACO is utilized to eliminate the effect of the malicious node by distinctive amidst the attacker nodes and normal nodes based on the definition of the characteristics of these attacks and quickly finding a suitable route to send the packet from the source node to the destination node. This solution is used for single and multiple blackholes. The below figure (Figure 3.3) depicts the algorithm for eliminating the effect of attacks using the AntNet colony optimization solution, which includes the following steps:

a. In the beginning, the node that wants to send data will send an RREQ message in order to locate the node at the destination.

b. If the received node is an attacker node and ACO algorithm was used, it will detect the attacker node and rediscover a suitable path to the destination. Otherwise, network performance will suffer.

c. The data transmission will finally begin without any difficulties after the attack effect has been eliminated.

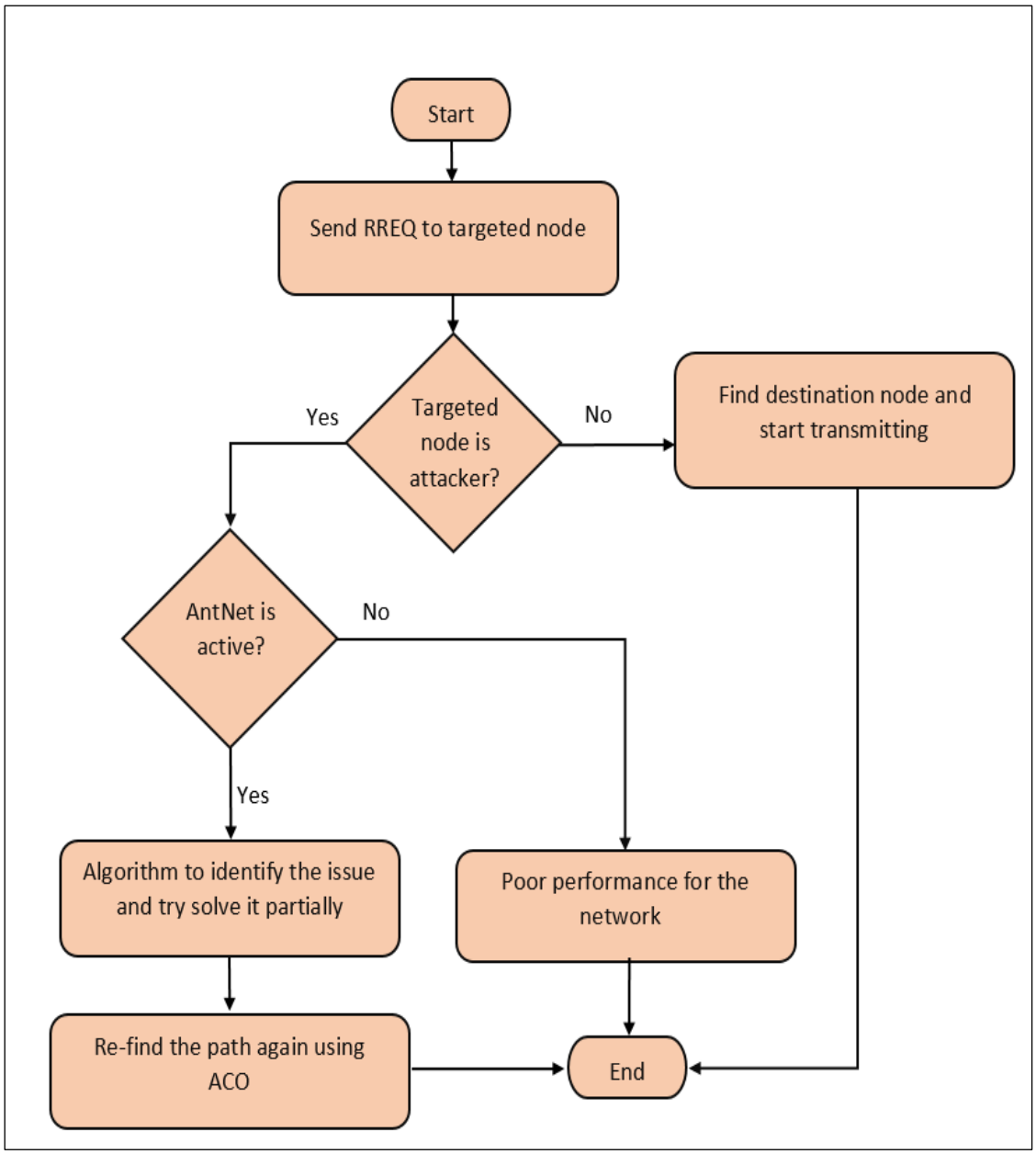


Figure 3.3: An Algorithm for Eliminating The Effect of Blackhole Attack Using The ACO Solution.

R-AODV: This technique is utilized to counteract the single blackhole attack node effect. R-AODV is a multipath routing protocol R-AODV is a modification of the AODV routing protocol, which is used to eliminate the blackhole attacks effect by discovering routes on-demand using a reverse route discovery procedure. The below figure (Figure 3.4) depicts the algorithm for eliminating the blackhole attack effect using the R-AODV solution, which includes the following steps:

a. To begin, the node wishing to transmit data will send an RREQ message to determine the destination.

b. Using the R-AODV solution, the effect of a blackhole attack is eliminated by detecting the attack via a reverse route (R-AODV). Otherwise, data will be transmitted into the blackhole attack path, which will discard all incoming data.

c. Finally, after removing the blackhole attack effect, the RREQ message will be sent again to find a suitable path before beginning data transmission and ensuring that it completes successfully. Route maintenance will be activated otherwise.

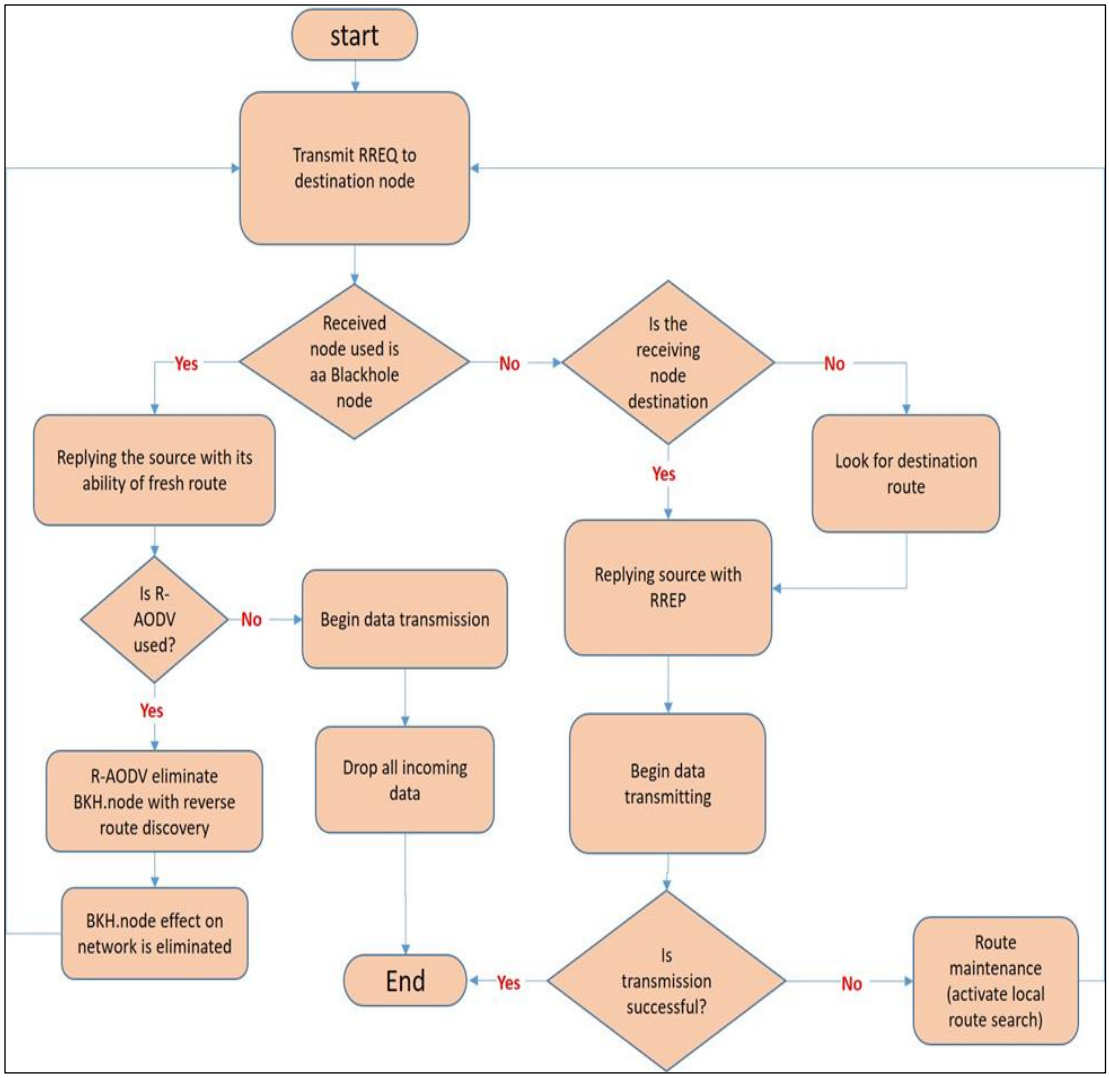


Figure 3.4: An Algorithm for Eliminating The Effect of Blackhole Attack Using The R-AODV Solution.

4. RESULTS OF MANET ATTACKS AND SOLUTIONS

This chapter describes the evaluation performance metrics of the MANET in a set of situations evaluated during the study of this thesis, including the results of MANET networks scenarios that implement the routing protocol (AODV), MANET networks scenarios' results, and the results of network scenarios with the effect of Blackhole attacks after implementing solutions that eliminate the effect of the Blackhole attacks. Following that, a comparison of these results is presented.

4.1 PERFORMANCE METRICS

The following are the metrics that were used to obtain the performance results of MANETs that use the AODV routing protocol:

a. Dropped Packets' Number: It's equal to the difference between the received packets' number and the sent packets' number.

b. Throughput: The received packets' number per second between both nods (source and destination).

c. Packet Delivery Ratio: The number of sent packets from by source node against the total received packets at the destination node side.

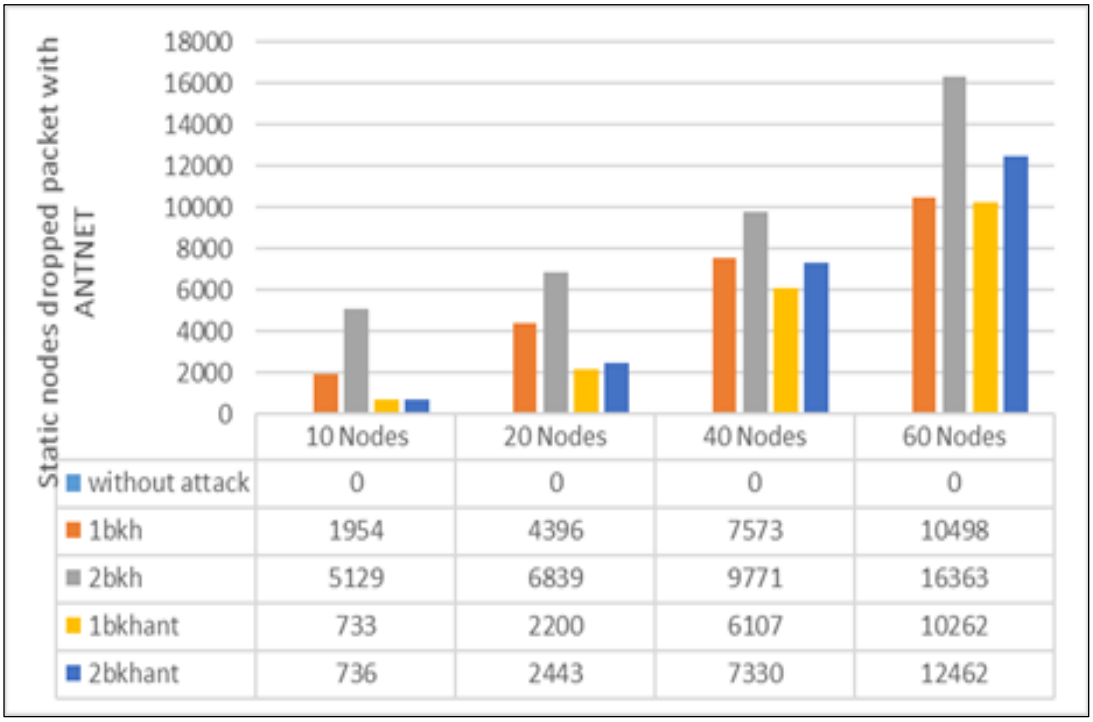
By changing the nodes' number and speed values, the UDP traffic type is used to evaluate the simulation and evaluation results of the simulation scenarios.

4.2 SIMULATION RESULTS USING STATIC NODES

4.2.1 Dropped Packets Simulation Results

The results of the total drop packets metrics show a comparison study between the performance of the MANET before and after the effect of the single and multiple blackhole attacks, and their improvement after implementing R-AODV/AntNet solutions to those attacks. In all situations, the numbers nodes 10, 20, 40, and 60 were used. below are the simulation results for each situation. After applying the AntNet solution in both single and multiple blackhole attacks the solution has reduced the blackhole effect, the same scenarios were applied but with using the R-AODV

solution, for more simulation results, please check the below charts that show the dropped packets under attacks and under proposed solutions in the below Charts (Chart 4.1 Static nodes dropped packet with ANTNET) and (Chart 4.2 Static nodes dropped packet with R-AODV)



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	0	0	0	0
1bkh	1954	4396	7573	10498
2bkh	5129	6839	9771	16363
1bkhant	733	2200	6107	10262
2bkhant	736	2443	7330	12462

Chart 4.1: Static Nodes Dropped Packet with ANTNET.

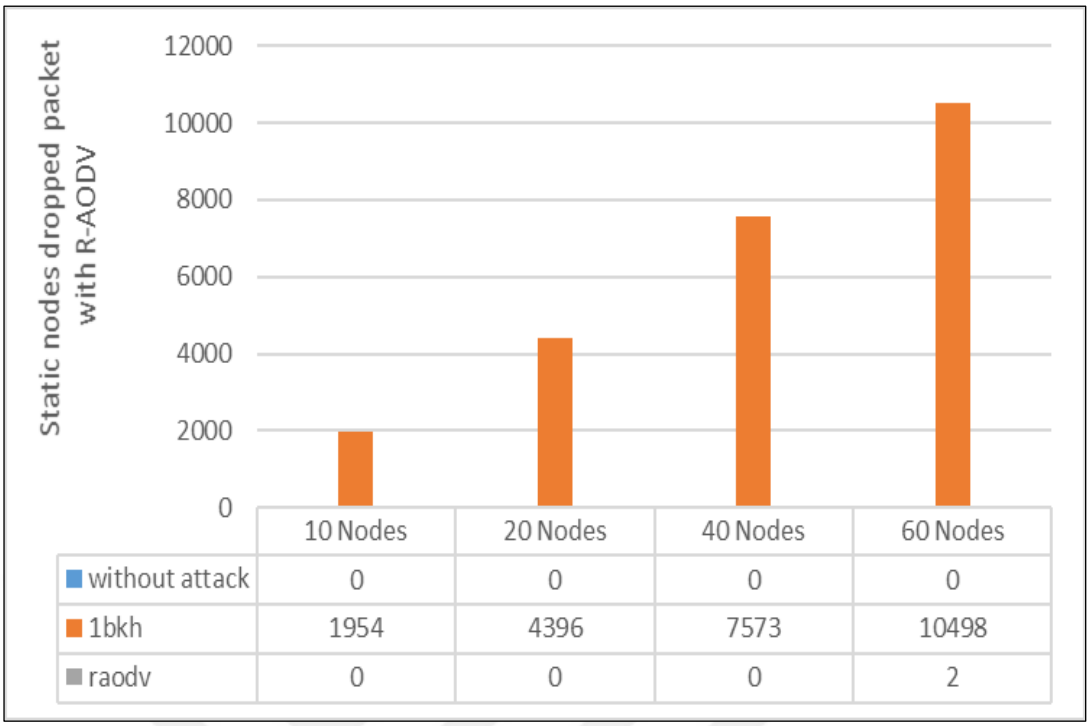


Chart 4.2: Static Nodes Dropped Packet with R-AODV.

4.2.2 Packet Delivery Ratio Simulation Results

The results that were evaluated also show a comparison study between the performance of the MANET before and after the effect of the single and multiple blackhole attacks, and their enhancement after implementing R-AODV, AntNet, in this scenario we also obtained the simulation with 10,20,40,60 nodes for all situations that were used. This metric pertains to the packet delivery ratio. Below are the simulation results for applying both solutions under different scenarios. When we apply the AntNet solution, we noticed that the solution reduced the blackhole effect, below are the charts that show performance for each scenario (Chart 4.3 Static nodes packet delivery ratio with AntNet) and (Chart 4.4 Static nodes packet delivery ratio with R-AODV)

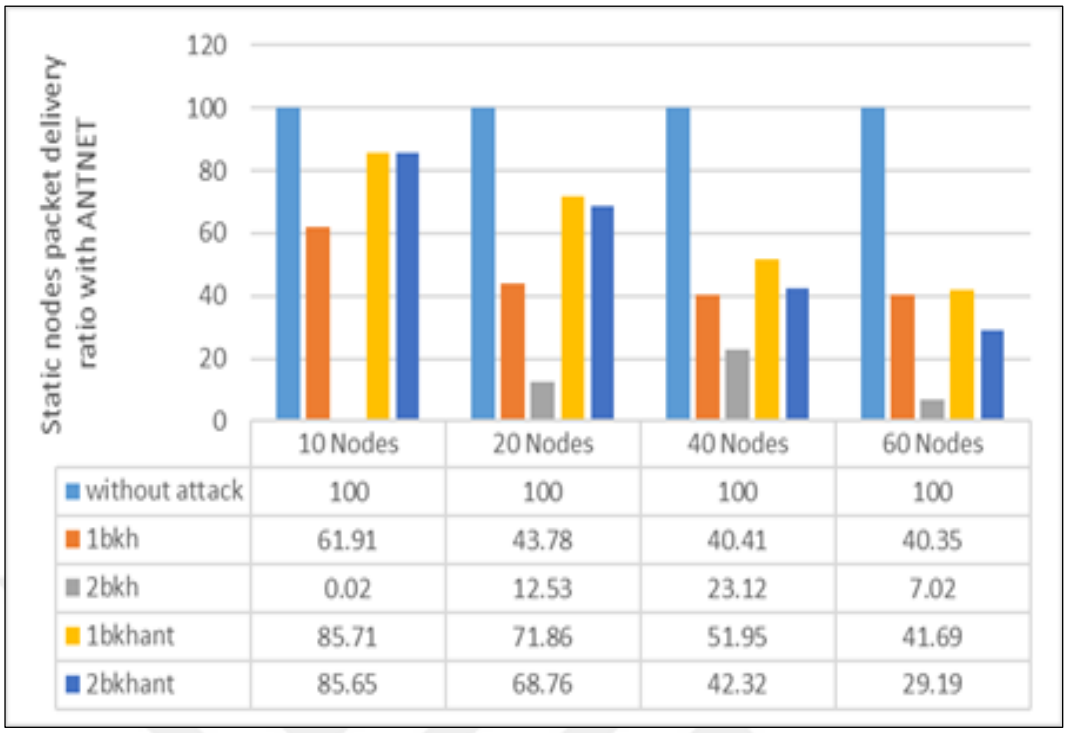


Chart 4.3: Static Nodes Packet Delivery Ratio with Antnet.

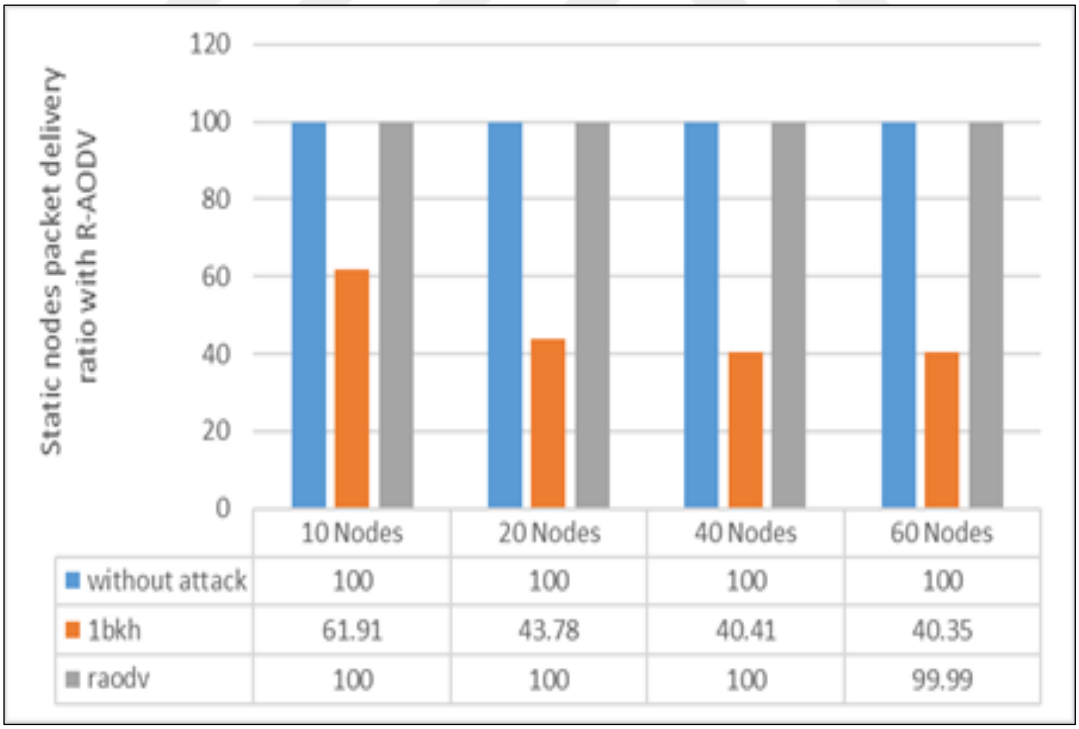
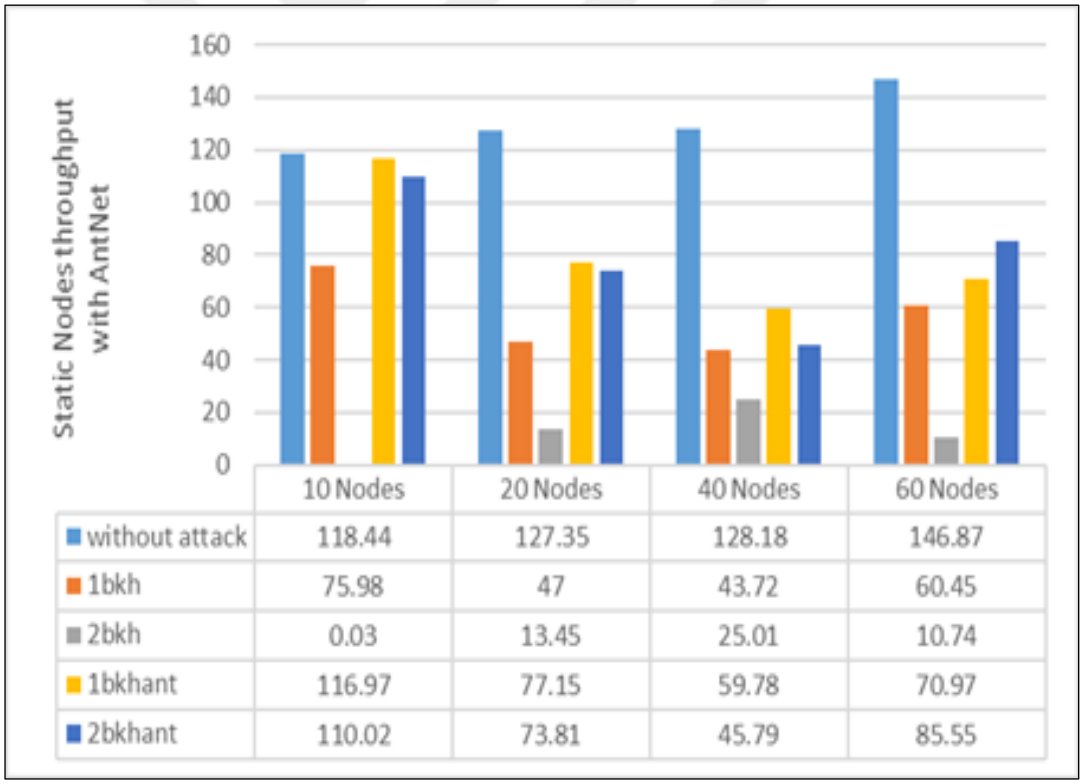


Chart 4.4: Static Nodes Packet Delivery Ratio with R-AODV.

4.2.3 Throughput Simulation Results

The results that were evaluated also show a comparison study between the performance of the MANET before and after the effect of the single & multiple blackhole attacks, and their enhancement after implementing R-AODV, AntNet, and is also obtained with 10,20,40,60 nodes for all of the situations that were used. This comparison study was carried out using the evaluations that were carried out. This metric is concerned with the amount of throughput. Again after applying the AntNet solution in both signal and multiple blackhole attacks, demonstrating that AntNet has mitigated the blackhole effect in signal and multiple blackhole attacks and as expected from our old experience R-AODV performs extremely well under a single blackhole attack, the below charts (Chart 4.5 Static Nodes Throughput with AntNet) and (Chart 4.6 Static Nodes Throughput With R-AODV) are explaining the results of each scenario in numbers.



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	118.44	127.35	128.18	146.87
1bkh	75.98	47	43.72	60.45
2bkh	0.03	13.45	25.01	10.74
1bkhant	116.97	77.15	59.78	70.97
2bkhant	110.02	73.81	45.79	85.55

Chart 4.5: Static Nodes Throughput with AntNet.

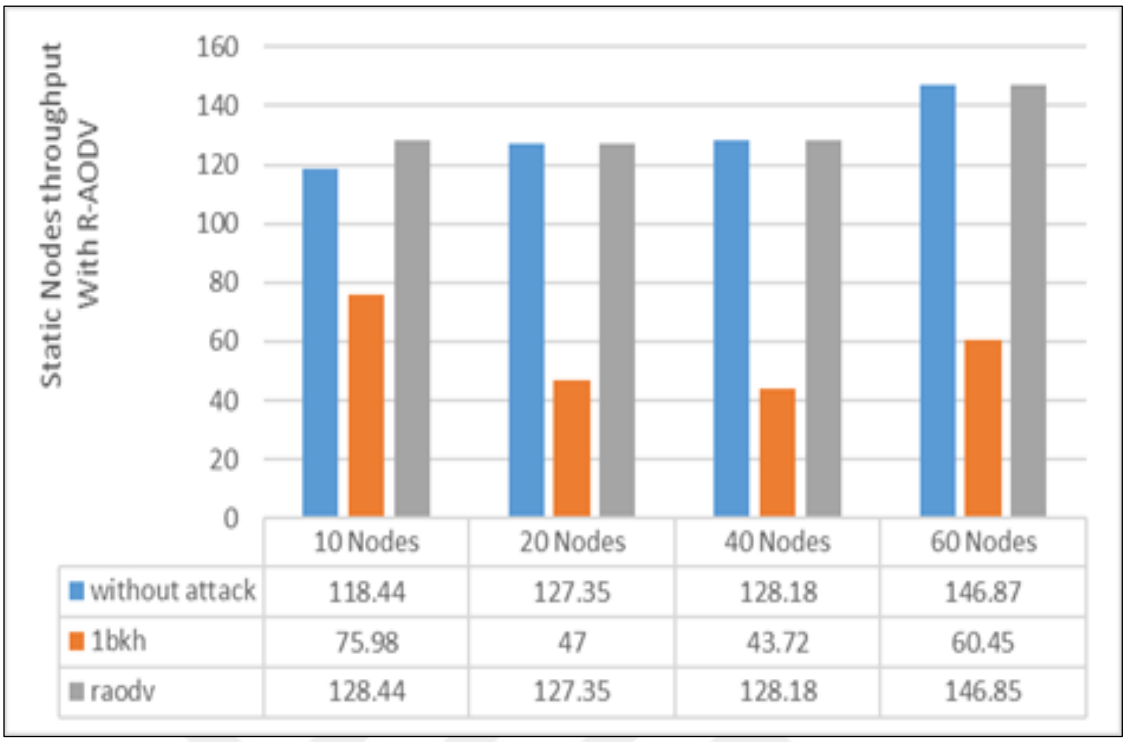


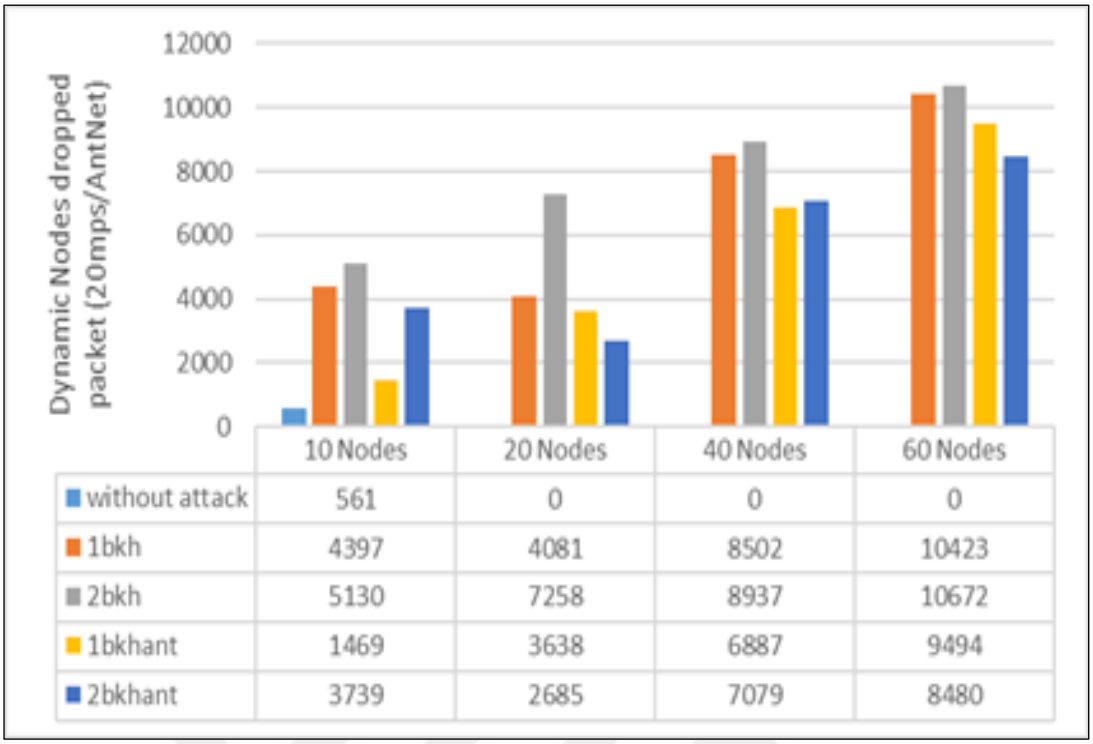
Chart 4.6: Static Nodes Throughput with R-AODV.

4.3 SIMULATION RESULTS USING DYNAMIC NODES

4.3.1 Dropped Packets Simulation Results

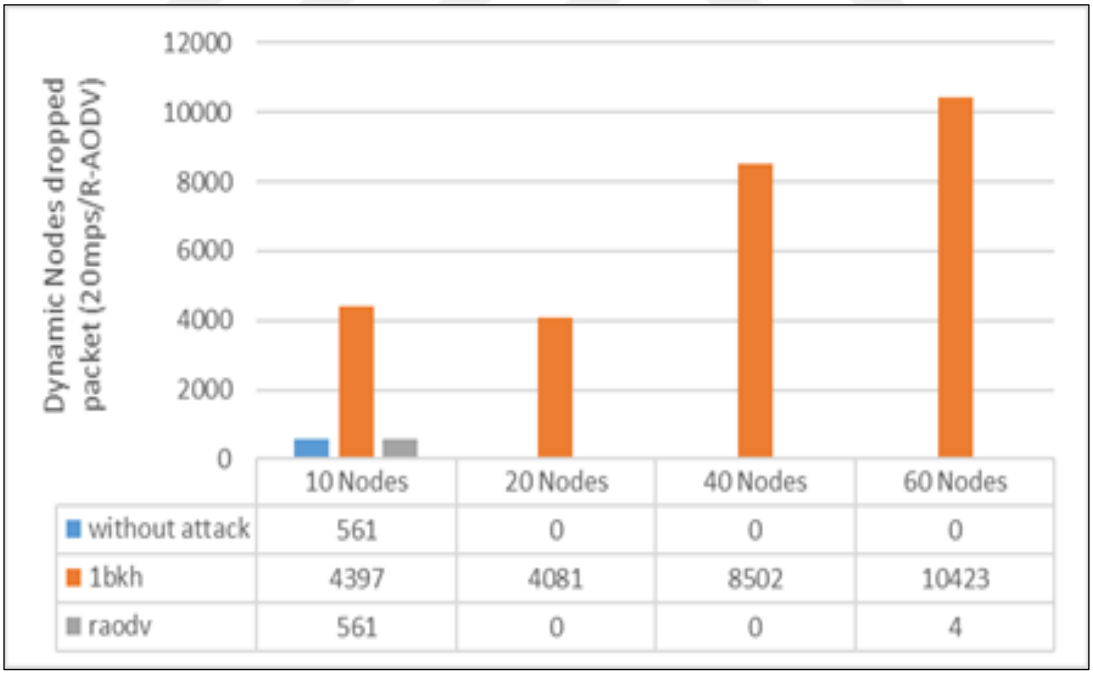
Another simulation was performed using dynamic nodes to check the MANET performance before and after the effect of single and multiple blackhole attacks, as well as their improvement after implementing R-AODV/AntNet solutions to those attacks. The numbers of nodes used in all situations were 10, 20, 40, and 60, and the speed was 20-100 MPS. the simulation results for each situation are shown below:

Moving at 20 MPS: A network was prepared to consist of 10, 20, 40, and 60 nodes moving at 20 MPS, after applying the scenarios on the above network, we noticed that the AntNet solution has reduced the blackhole effect in signal and multiple blackhole attacks and again the R-AODV shows a great performance under the single attack, the below charts (Chart 4.7 Dynamic Nodes Dropped Packet (20mps/AntNet)) and (Chart 4.8 Dynamic Nodes Dropped Packet (20mps/ R-AODV)) are explaining the results of each scenario in numbers.



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	561	0	0	0
1bkh	4397	4081	8502	10423
2bkh	5130	7258	8937	10672
1bkhant	1469	3638	6887	9494
2bkhant	3739	2685	7079	8480

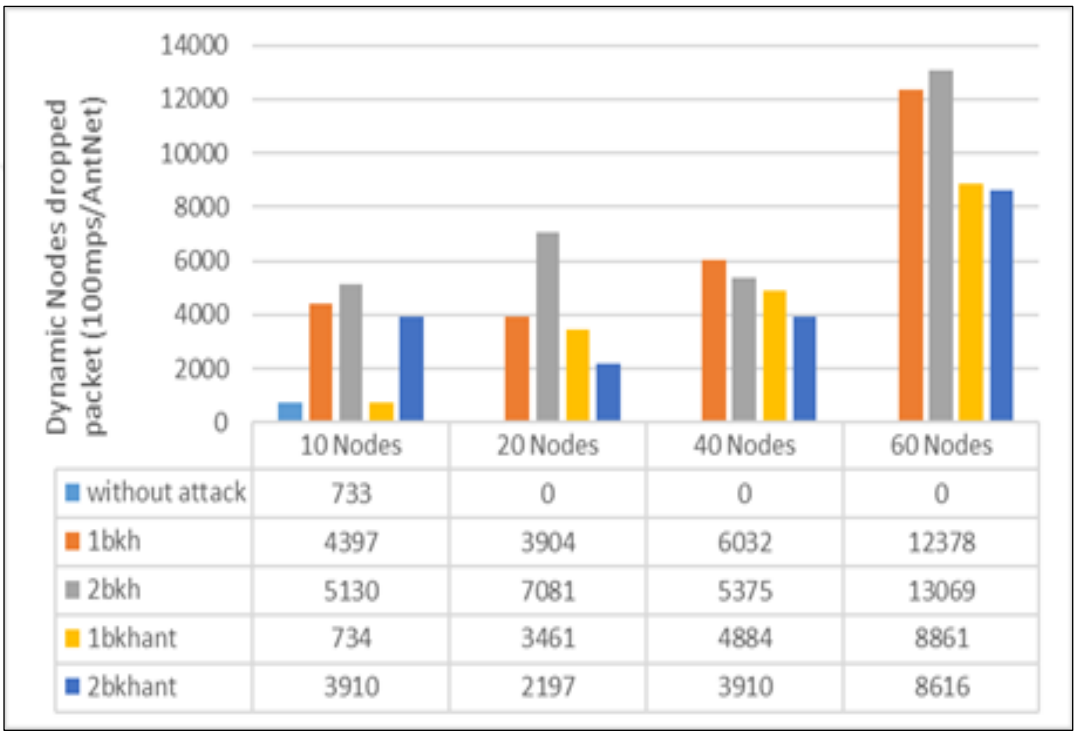
Chart 4.7: Dynamic Nodes Dropped Packet (20mps/AntNet).



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	561	0	0	0
1bkh	4397	4081	8502	10423
raodv	561	0	0	4

Chart 4.8: Dynamic Nodes Dropped Packet (20mps/ R-AODV).

Moving at 100 MPS: Another network was prepared to consist of 10, 20, 40, and 60 nodes but the moving speed was increased to 100 MPS, and we re-applied the scenarios on the above network, we noticed that the AntNet solution has better performance on a higher speed in signal and multiple blackhole attacks and again the R-AODV shows a great performance under the single attack, the below charts (Chart 4.9 Dynamic Nodes Dropped Packet (100mps/AntNet)) and (Chart 4.10 Dynamic Nodes Dropped Packet (100mps/ R-AODV)) are explaining the results of each scenario in numbers.



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	733	0	0	0
1bkh	4397	3904	6032	12378
2bkh	5130	7081	5375	13069
1bkhant	734	3461	4884	8861
2bkhant	3910	2197	3910	8616

Chart 4.9: Dynamic Nodes Dropped Packet (100mps/AntNet).

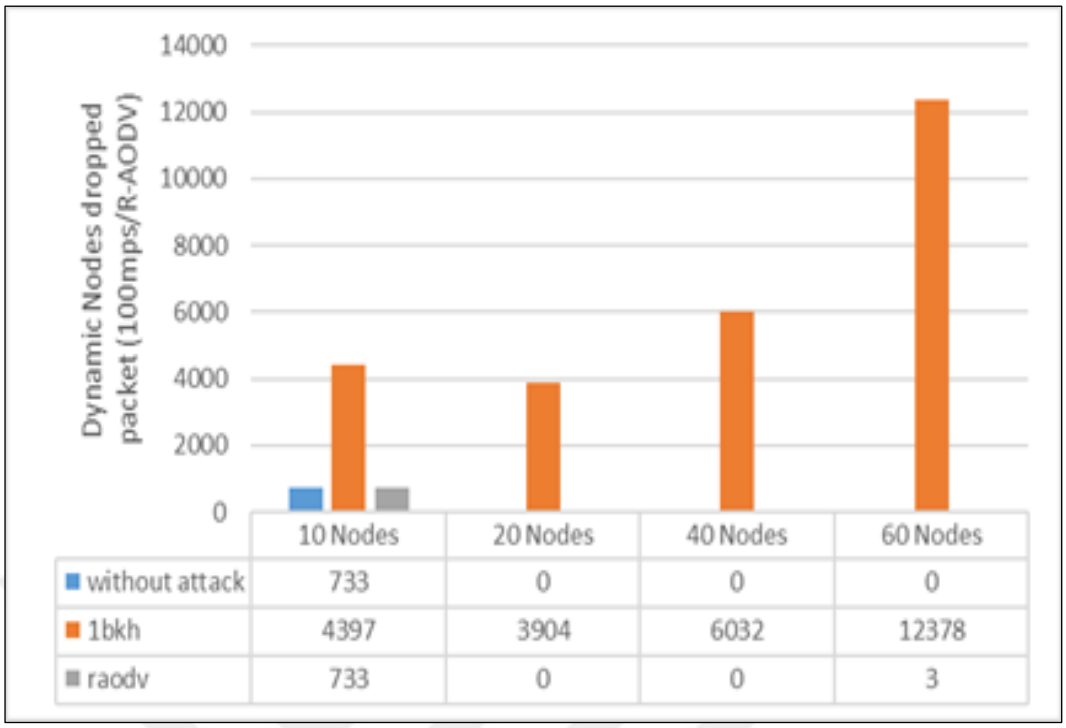
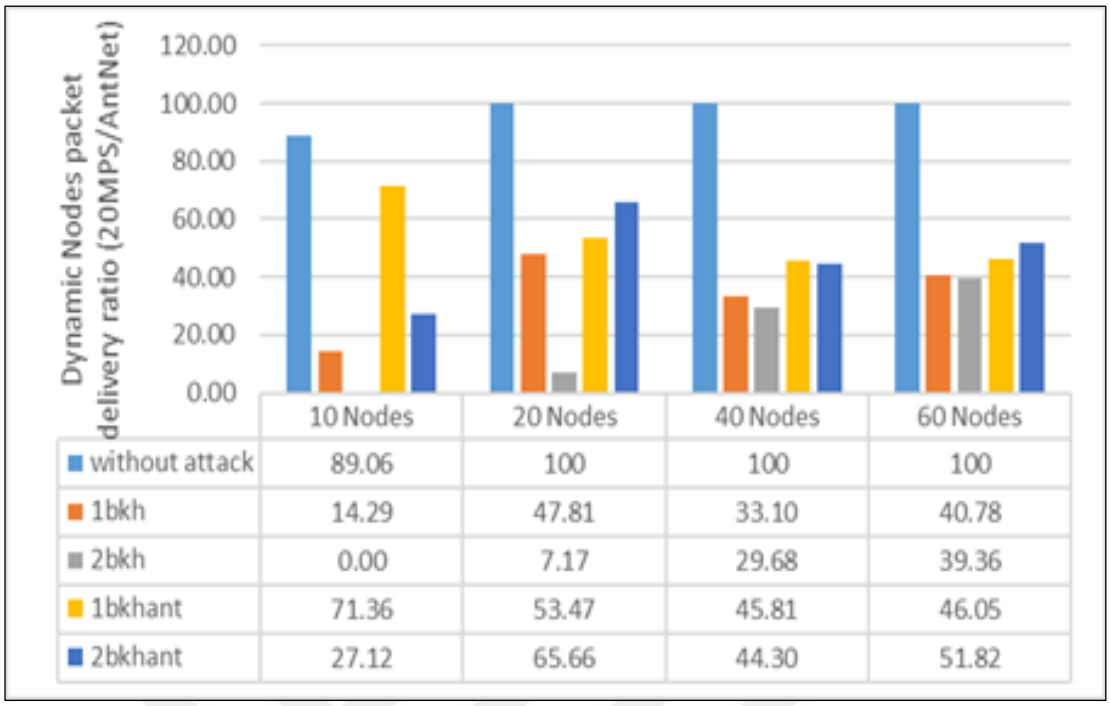


Chart 4.10: Dynamic Nodes Dropped Packet (100mps/ R-AODV).

4.3.2 Packet Delivery Ratio Simulation Results

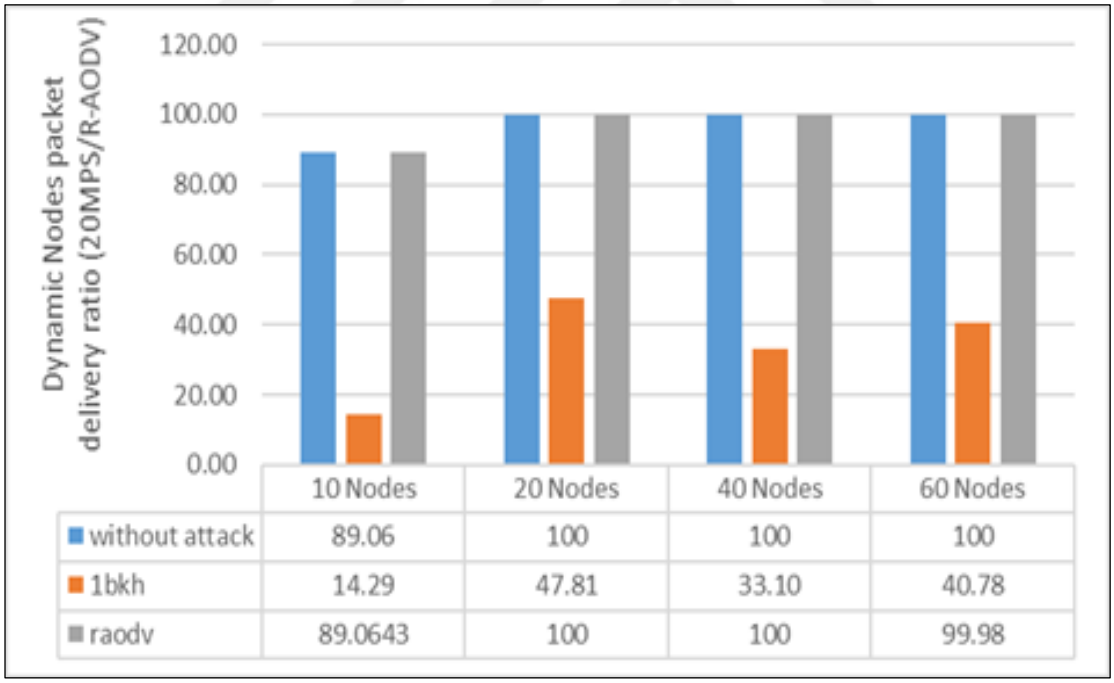
This simulation was executed with dynamic nodes to be able to test the efficiency of the MANET both before and after the effect of single and multiple blackhole assaults, as well as their improvement after the use of R-AODV/AntNet solutions to counteract the effects of those attacks. In every scenario, 10, 20, 40, and 60 nodes were employed, and the speed ranged from 20 to 100 MPS. below are the simulation results for each scenario:

Moving at 20 MPS: A new network was built which consist of 10, 20, 40, and 60 nodes moving at 20 MPS, then we applied the same scenarios on this network, and we noticed that the AntNet solution reduced the blackhole effect in signal and multiple blackhole attacks and again the R-AODV shows a great performance under the single attack, the below charts (Chart 4.11 Dynamic Nodes Packet Delivery Ratio (20mps/AntNet)) and (Chart 4.12 Dynamic Nodes Packet Delivery Ratio (20mps/R-AODV)) are explaining the results of each scenario in numbers.



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	89.06	100	100	100
1bkh	14.29	47.81	33.10	40.78
2bkh	0.00	7.17	29.68	39.36
1bkhant	71.36	53.47	45.81	46.05
2bkhant	27.12	65.66	44.30	51.82

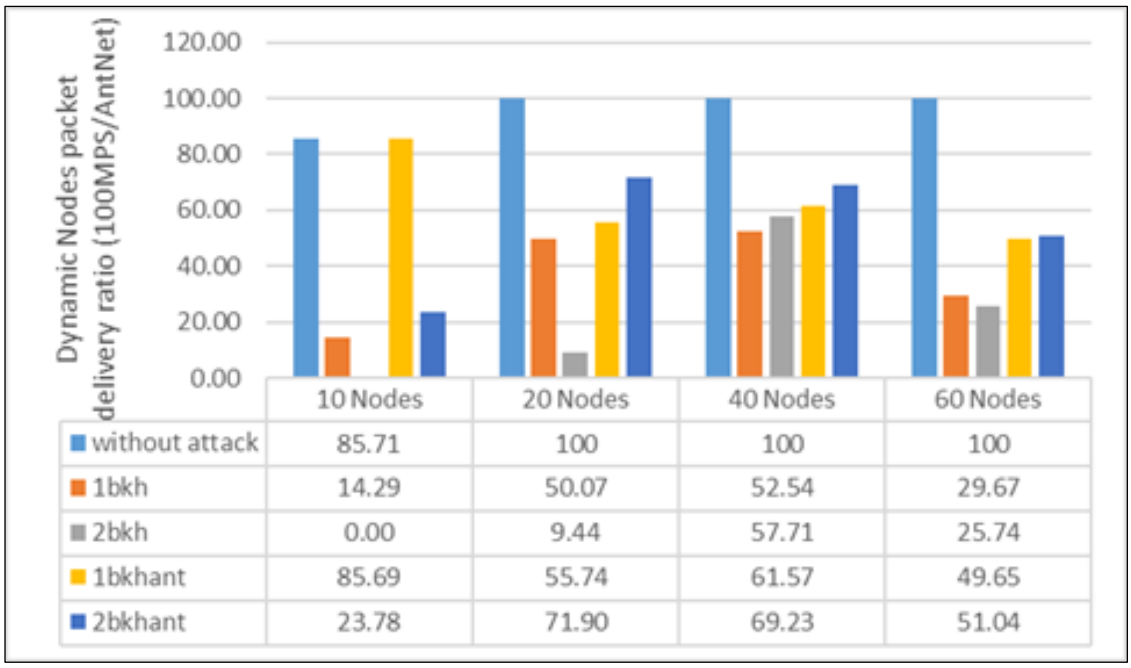
Chart 4.11: Dynamic Nodes Packet Delivery Ratio (20mps/AntNet).



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	89.06	100	100	100
1bkh	14.29	47.81	33.10	40.78
raodv	89.0643	100	100	99.98

Chart 4.12: Dynamic Nodes Packet Delivery Ratio (20mps/R-AODV).

Moving at 100 MPS: Another network was prepared and again consist of 10, 20, 40, and 60 nodes but the moving speed was increased to 100 MPS, and we re-applied our scenarios again, we noticed that the AntNet solution has better performance at a higher speed in signal and multiple blackhole attacks and again the R-AODV shows a great performance under the single attack, the below charts (Chart 4.13 Dynamic Nodes Packet Delivery Ratio (100mps/AntNet)) and (Chart 4.14 Dynamic Nodes Packet Delivery Ratio (100mps/R-AODV)) are explaining the results of each scenario in numbers.



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	85.71	100	100	100
1bkh	14.29	50.07	52.54	29.67
2bkh	0.00	9.44	57.71	25.74
1bkhant	85.69	55.74	61.57	49.65
2bkhant	23.78	71.90	69.23	51.04

Chart 4.13: Dynamic Nodes Packet Delivery Ratio (100mps/AntNet).

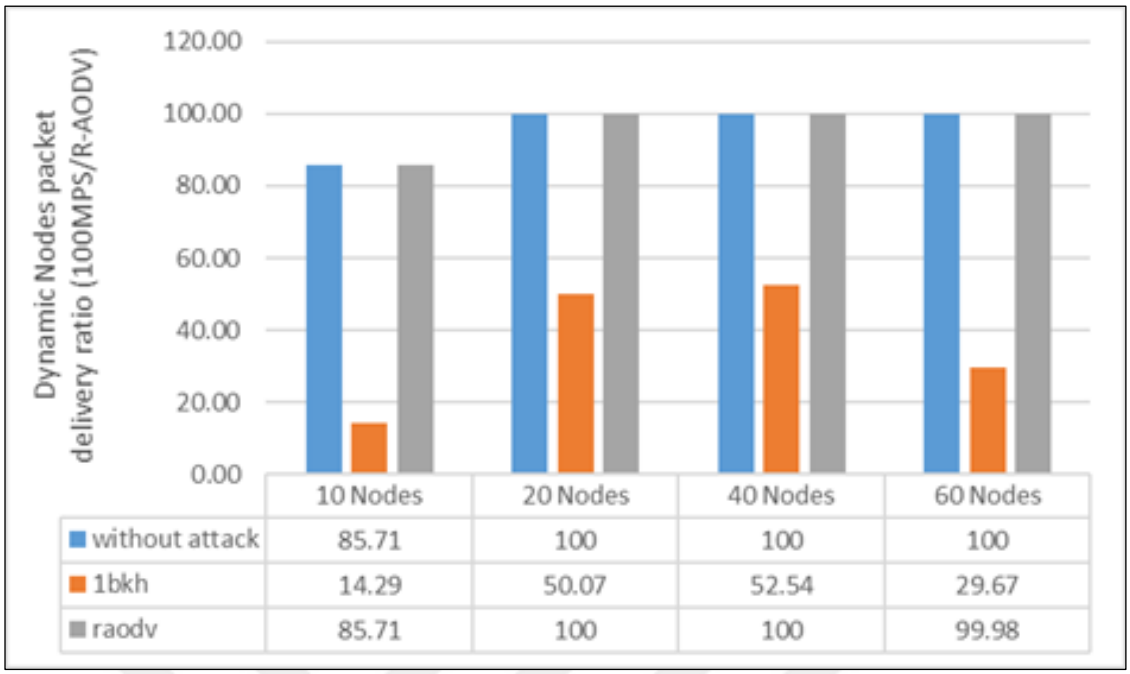


Chart 4.14: Dynamic Nodes Packet Delivery Ratio (100mps/R-AODV).

4.3.3 Throughput Simulation Results

The performance of the MANET was tested before and after the impact of single and multiple blackhole assaults, as well as their improvement following the employment of R-AODV/AntNet solutions to mitigate the consequences of those assaults. This simulation was run with dynamic nodes. 10, 20, 40, and 60 nodes were used in each scenario, and the speed varied from 20 to 100 MPS. The simulation results for each scenario are listed below:

Moving at 20 MPS: A new network was built which consist of 10, 20, 40, and 60 nodes moving at 20 MPS, then we applied the same scenarios on this network, and we noticed that the AntNet solution reduced the blackhole effect in signal and multiple blackhole attacks and again the R-AODV shows a great performance under the single attack, the below charts (Chart 4.15 Dynamic Nodes Throughput (20mps/AntNet)) and (Chart 4.16 Dynamic Nodes Throughput (20mps/R-AODV)) are explaining the results of each scenario in numbers.

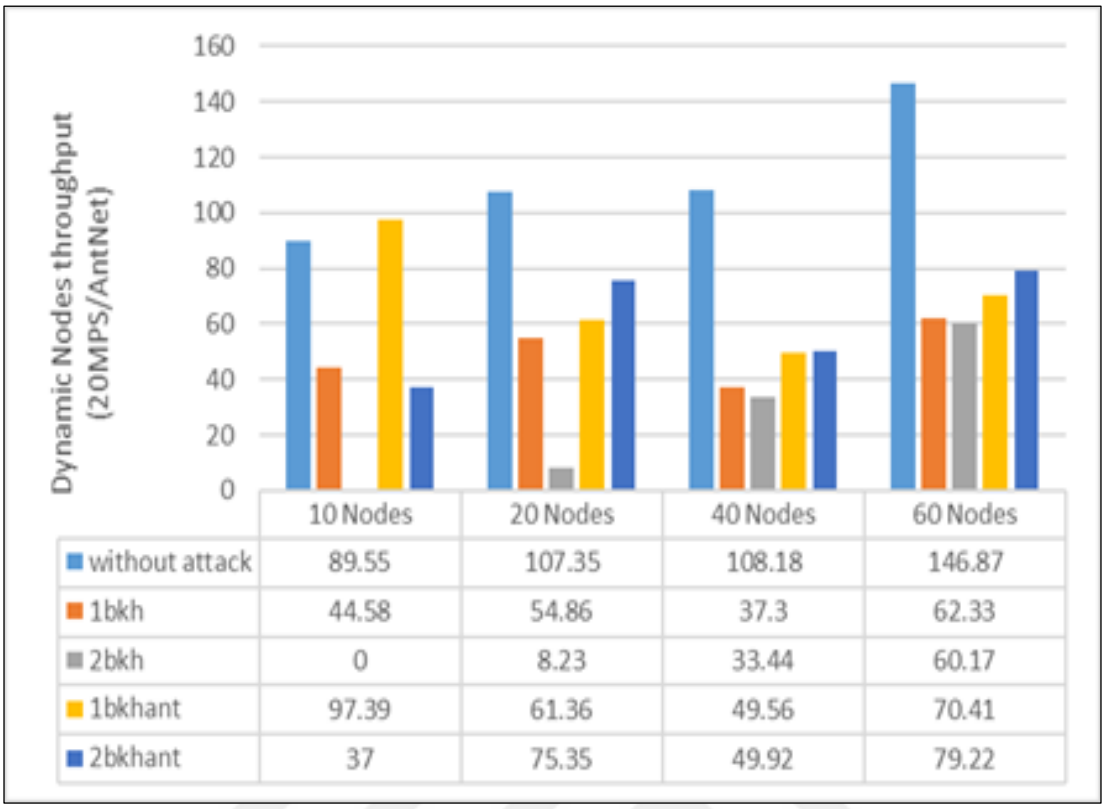


Chart 4.15: Dynamic Nodes Throughput (20mps/AntNet).

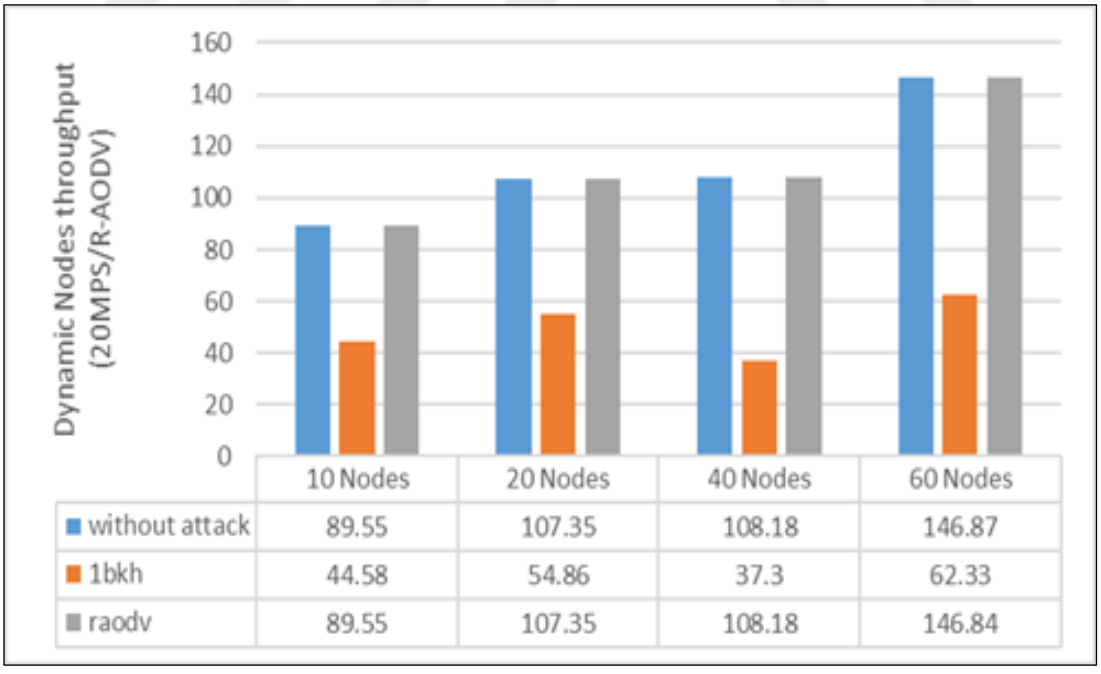
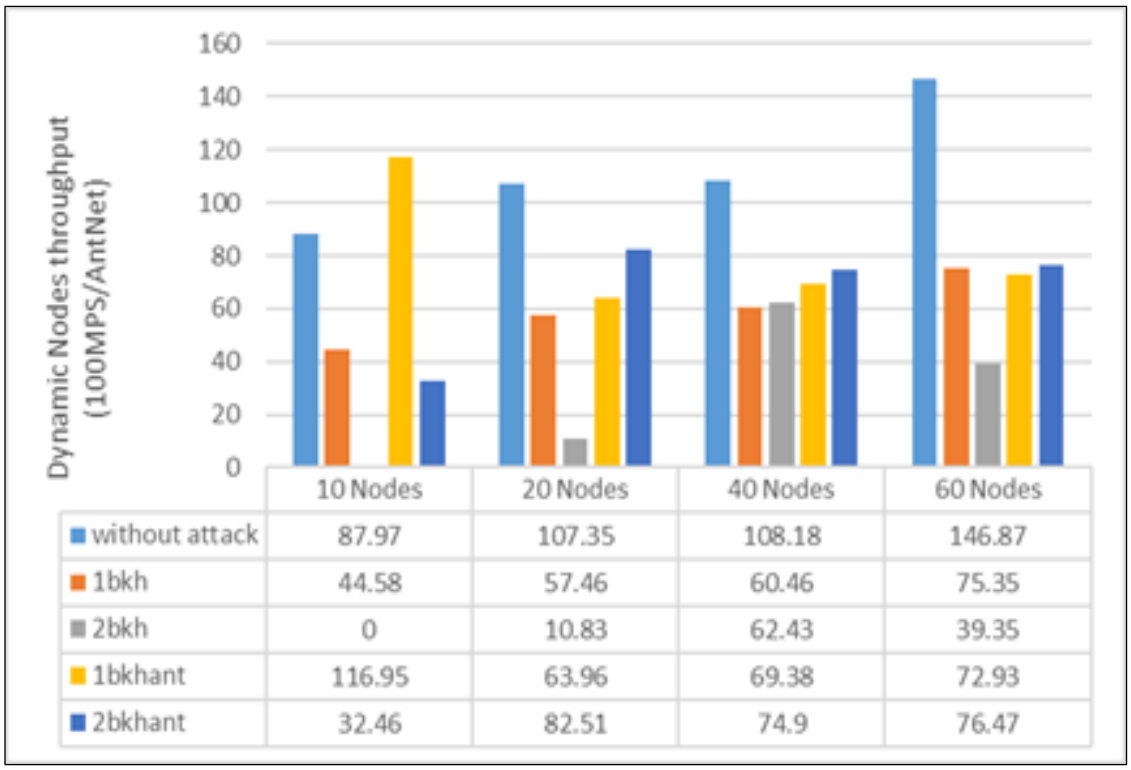


Chart 4.16: Dynamic Nodes Throughput (20mps/R-AODV).

Moving at 100 MPS: Another network was prepared and again consist of 10, 20, 40, and 60 nodes but the moving speed was increased to 100 MPS, and we re-applied our scenarios again, we noticed that the AntNet solution has better performance at a higher speed in signal and multiple blackhole attacks and again the R-AODV shows a great performance under the single attack, the below charts (Chart 4.17 Dynamic Nodes Throughput (100mps/AntNet)) and (Chart 4.18 Dynamic Nodes Throughput (100mps/R-AODV)) are explaining the results of each scenario in numbers.



	10 Nodes	20 Nodes	40 Nodes	60 Nodes
without attack	87.97	107.35	108.18	146.87
1bkh	44.58	57.46	60.46	75.35
2bkh	0	10.83	62.43	39.35
1bkhant	116.95	63.96	69.38	72.93
2bkhant	32.46	82.51	74.9	76.47

Chart 4.17: Dynamic Nodes Throughput (100mps/AntNet).

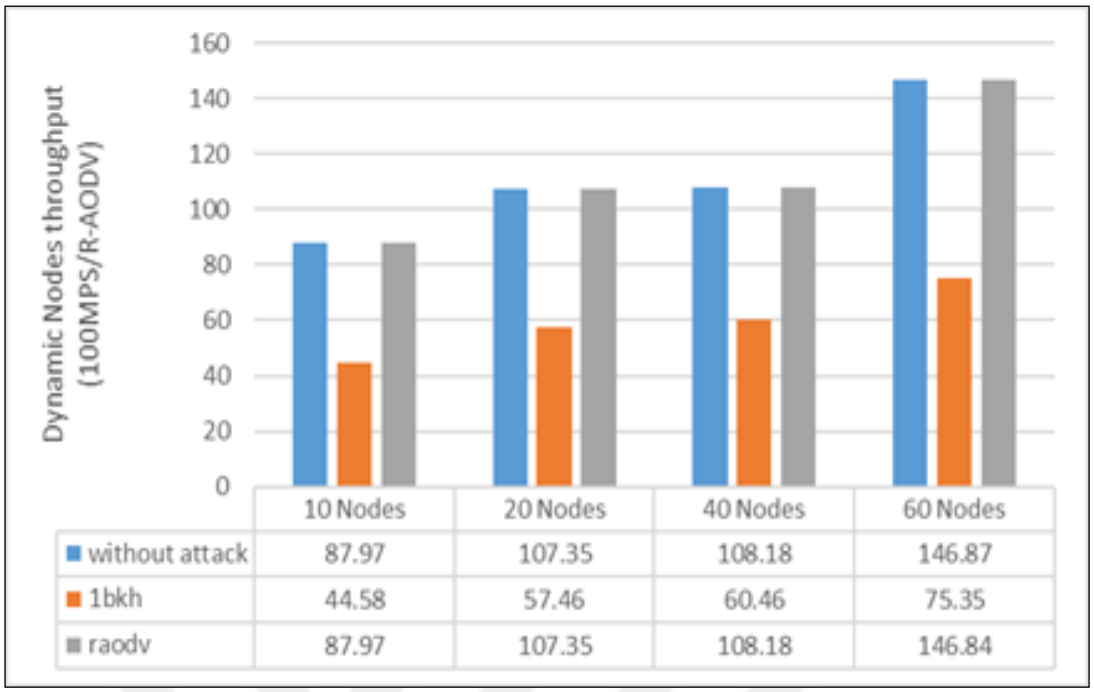


Chart 4.18: Dynamic Nodes Throughput (100mps/R-AODV).

4.4 DISCUSSION OF RESULTS

After computing and analyzing the results of all dropped packets' number, PDR, and the throughput for (10,20,40, and 60) nodes with all situations implemented, a comparison of results was performed and discussed to demonstrate how network security attacks affect the efficiency of the AODV routing protocol in MANET networks based on the below tables (Table 4.1: Dropped Packets in each scenario), (Table 4.2: Packet Delivery Ratio in each scenario), and (Table 4.3: Throughput in each scenario). Below are summary of how the implementation of solutions eliminated the effect of these attacks as follows:

a. The dropped packets percentage in dynamic nodes is higher than the static nodes.

b. Increasing the speed of nodes from 20 MPS to 100 MPS will negatively affect AntNet solution performance.

c. R-AODV is better than AntNet in mitigating blackhole attack effect.

d. In static and dynamic nodes, we noticed that when the drop packet percentage increased the packet delivery ratio and throughput decreased.

e. Raising the blackhole nodes' number will lead to increasing the effect of the blackhole on the network.

Table 4.1: Dropped Packets.

	Static Nodes				**Dynamic Nodes (20 mps)**				**Dynamic Nodes (100 mps)**			
	10	20	40	60	10	20	40	60	10	20	40	60
without attack	0	0	0	0	561	0	0	0	733	0	0	0
1bkh	1954	4396	7573	10498	4397	4081	8502	10423	4397	3904	6032	12378
2bkh	5129	6839	9771	16363	5130	7258	8937	10672	5130	7081	5375	13069
1bkhant	733	2200	6107	10262	1469	3638	6887	9494	734	3461	4884	8861
2bkhant	736	2443	7330	12462	3739	2685	7079	8480	3910	2197	3910	8616
RAODV	0	0	0	2	561	0	0	4	733	0	0	3

Table 4.2: Packet Delivery Ratio.

	Static Nodes				**Dynamic Nodes (20 mps)**				**Dynamic Nodes (100 mps)**			
	10	20	40	60	10	20	40	60	10	20	40	60
without attack	100	100	100	100	89.06	100	100	100	85.71	100	100	100
1bkh	61.91	43.78	40.41	40.35	14.29	47.81	33.10	40.78	14.29	50.07	52.54	29.67
2bkh	0.02	12.53	23.12	7.02	0.00	7.17	29.68	39.36	0.00	9.44	57.71	25.74
1bkhant	85.71	71.86	51.95	41.69	71.36	53.47	45.81	46.05	85.69	55.74	61.57	49.65
2bkhant	85.65	68.76	42.32	29.19	27.12	65.66	44.30	51.82	23.78	71.90	69.23	51.04
RAODV	100	100	100	99.99	89.06	100	100	99.98	85.71	100	100	99.98

Table 4.3: Throughput.

	Static Nodes				**Dynamic Nodes (20 mps)**				**Dynamic Nodes (100 mps)**			
	10	20	40	60	10	20	40	60	10	20	40	60
without attack	128.4	107.3	108.1	146.8	121.5	107.3	108.1	146.8	116.9	107.3	108.1	146.8
1bkh	103.9	47	43.72	60.45	44.58	54.86	37.3	62.33	44.58	57.46	60.46	45.35
2bkh	0.03	13.45	25.01	10.74	0	8.23	33.44	60.17	0	10.83	62.43	39.35
1bkhant	116.9	77.15	59.78	70.97	97.39	61.36	49.56	70.41	116.9	63.96	69.38	72.93
2bkhant	110.0	73.81	45.79	45.55	37	75.35	49.92	79.22	32.46	82.51	74.9	76.47
RAODV	128.4	107.3	108.1	146.8	121.5	107.3	108.1	146.8	116.9	107.3	108.1	146.8

5. CONCLUSIONS AND SUGGESTIONS FOR FUTURE WORK

5.1 CONCLUSIONS

Following the security implementation for the AODV routing protocol in MANET, computing and comparing the results of all cases utilized in this thesis, the following conclusions are reached:

a. By increasing the nodes' number, the drop packet percentage will be increased and the ratio of the packet delivery and throughput will be reduced.

b. The R-AODV solution has a significant impact on mitigating the impact of a single blackhole attack because it employs reverse route discovery, which decreases the lost packets' number.

c. The MANET network performance is highly affected by the number of nodes and nodes' moving speed, in our performed simulation, network behavior shows better performance in less number of nodes and low speed.

d. The suggested solutions are performing better in static nodes than the dynamic nodes because in the static network, the nodes are fixed and the space between nodes is not changing.

e. AntNet efficiency is effected negatively by increasing nodes number and increasing the speed.

f. Blackhole attacks can significantly affect the network because they work by hacking and deleting everything in their path.

g. All dropped packets and average throughput amount have inversely proportional. The average throughput decreases because the total drop packets' number increases.

5.2 SUGGESTIONS FOR FUTURE WORK

Future work ideas include:

a. Establishing security on the multicast-AODV to compare security between normal and multicast-AODV.

b. Improving security in MANET networks by modifying the application or transport layers.

c. Other types of network security assaults, such as Sybil and wormhole attacks, are being implemented and solved in order to eliminate their effects on the MANET network.

d. We intend to provide a find-out and prevention solution for the multiple blackhole attack in the future as the RAODV is not appropriate for multiple blackhole attacks and Anetnet is acceptable for performing multi attacks, maybe it’s good to try the IDS-AODV solution as it well performing on both blackhole attacks types.

REFERENCES

[1] M. A. Al-Absi, A. A. Al-Absi, M. Sain, and H. Lee, “Moving ad hoc networks—A comparative study,” *Sustainability*, vol. 13, no. 11, p. 6187, 2021.

[2] Y. Ebazadeh and R. Fotohi, “A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold,” *Secur. Priv.*, vol. 5, no. 1, p. e183, 2022.

[3] G. Li, Z. Yan, and Y. Fu, “A study and simulation research of blackhole attack on mobile adhoc network,” in *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1–6.

[4] V. Khandelwal and D. Goyal, “BlackHole attack and detection method for AODV routing protocol in MANETs,” *Int. J. Adv. Res. Comput. Eng. \& Technol.*, vol. 2, no. 4, pp. 1555–1559, 2013.

[5] A. Singhal, V. Jha, S. Virmani, and P. Jain, “Towards the study of a living mobile backbone: VANET,” in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, 2018, pp. 1–6.

[6] P. Shandil and R. Kumar, “Security Analysis of Vehicular Ad Hoc Network,” in *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, 2018, pp. 1–5.

[7] R. Gazori and G. Mirjalily, “Sbgrp as an improved stable cds-based routing protocol in vehicular ad hoc networks,” in *2019 27th Iranian Conference on Electrical Engineering (ICEE)*, 2019, pp. 1979–1983.

[8] K. St\kepień and A. Poniszewska-Marańda, “Security methods against Black Hole attacks in Vehicular Ad-Hoc Network,” in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, 2020, pp. 1–4.

[9] A. V Leonov, G. A. Litvinov, and E. V Shcherba, “Simulation and comparative analysis of packet delivery in flying ad hoc network (FANET) using AODV,” in *2018 19th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, 2018, pp. 71–78.

[10] A. Kumari and S. Krishnan, “Simulation Based Study of Blackhole Attack Under AODV Protocol,” in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018, pp. 1–6.

[11] V. S. Deepthi and S. Vagdevi, “Behaviour analysis and detection of blackhole attacker node under reactive routing protocol in MANETs,” in *2018 International Conference on Networking, Embedded and Wireless Systems (ICNEWS)*, 2018, pp. 1–5.

[12] I. Nurcahyani and H. Hartadi, “Performance analysis of ad-hoc on-demand distance vector (AODV) and dynamic source routing (DSR) under black hole attacks in mobile ad hoc network (MANET),” in *2018 International Symposium on Electronics and Smart Devices (ISESD)*, 2018, pp. 1–5.

[13] N. waheed Aziz, S. N. Alsaad, and H. kadhum Hmood, “Implementation of lightweight stream cipher in AODV routing protocol for MANET,” in *2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019, pp. 210–215.

[14] M. M. Singh and J. K. Mandal, “Gray hole attack analysis in AODV based mobile adhoc network with reliability metric,” *2019 IEEE 4th Int. Conf. Comput. Commun. Syst. ICCCS 2019*, pp. 565–569, 2019, doi: 10.1109/CCOMS.2019.8821671.

[15] S. Sivanesh and V. R. Sarma Dhulipala, “Comparitive analysis of blackhole and rushing attack in MANET,” *Proc. 2019 TEQIP - III Spons. Int. Conf. Microw. Integr. Circuits, Photonics Wirel. Networks, IMICPW 2019*, pp. 495–499, 2019, doi: 10.1109/IMICPW.2019.8933192.

[16] T. S. Vamsi, E. R. P. Kumar, and T. Sruthi, “Performance Analysis of Aodv Routing Protocol in Manet under Blackhole Attack,” *Int. J. Eng. Res. Appl.*, vol. 9, no. 5, pp. 58–63, 2019.

[17] R. Anggoro, W. Suadi, A. M. Shiddiqi, R. Ijtihadie, S. Lili, and D. W. L. Pamungkas, “The Development Of Blackhole Attack In AODV Routing Protocol,” in *2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM)*, 2020, pp. 309–314.

[18] S. Pandey and V. Singh, “Blackhole attack detection using machine learning approach on MANET,” in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2020, pp. 797–802.

[19] V. Sharma, T. Shree, and others, “An adaptive approach for Detecting Blackhole using TCP Analysis in MANETs,” in *2nd International Conference on Data, Engineering and Applications (IDEA)*, 2020, pp. 1–5.

[20] V. Suchitra, “Performance Analysis of Blackhole Attack in MANETs.”

[21] F. Taranum, Z. Abid, and K. U. R. Khan, “Legitimate-path Formation for AODV under black hole attack in MANETs,” in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2020, pp. 806–813.

[22] A. U. Khan, R. Puree, B. K. Mohanta, and S. Chedup, “Detection and Prevention of Blackhole Attack in AODV of MANET,” in *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2021, pp. 1–7.

[23] P. Sarao, “Performance Analysis of MANET under Security Attacks.,” *J. Commun.*, vol. 17, no. 3, pp. 194–202, 2022.

[24] A. J. Joseph, N. Sani, K. S. Kumar, T. A. Kumar, R. Nishanth, and others, “Towards a Novel and Efficient Public Key Management for Peer-Peer Security in Wireless Ad-Hoc/sensor Networks,” in *2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, 2022, pp. 1–4.

[25] S. Mirza and S. Z. Bakshi, “Introduction to MANET,” *Int. Res. J. Eng. Technol.*, vol. 5, no. 1, pp. 17–20, 2018.

[26] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, “A survey on MANETs: architecture, evolution, applications, security issues and solutions,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 832–842, 2018.

[27] B. U. I. Khan, N. F. Zulkurnain, R. F. Olanrewaju, G. Nissar, A. M. Baba, and S. A. Lone, “JIR2TA: Joint Invocation of Resource-Based Thresholding and Trust-*Intelligent Systems Conference (IntelliSys) 2016: Volume 2*, 2018, pp. 689–701.

[28] K. P. Manikandan, R. Satyaprasad, and D. K. Rajasekhararao, “A survey on attacks and defense metrics of routing mechanism in mobile ad hoc networks,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 3, 2011.

[29] R. S. Majeed and M. A. Abdala, “Improving the AODV Routing Protocol Against the Route-Request Flooding Attack Using AntNet Algorithm in VANETs.”

[30] A. O. Bang and P. L. Ramteke, “MANET: History, challenges and applications,” *Int. J. Appl. or Innov. Eng. \& Manag.*, vol. 2, no. 9, pp. 249–251, 2013.

[31] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, “Modified AODV routing protocol to improve security and performance against black hole attack,” in *2016 International Conference on Information Technology for Organizations Development (IT4OD)*, 2016, pp. 1–7.

[32] B. Ul Islam Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, “A survey on MANETs: Architecture, evolution, applications, security issues and solutions,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 832–842, 2018, doi: 10.11591/ijeecs.v12.i2.pp832-842.

[33] R. F. Olanrewaju, B. U. I. Khan, A. R. Najeeb, K. N. Zahir, and S. Hussain, “Snort-based smart and swift intrusion detection system,” *Indian J. Sci. Technol.*, vol. 11, no. 4, pp. 1–9, 2018.

[34] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, and A. Shah, “Manifestation and mitigation of node misbehaviour in adhoc networks,” *Wulfenia J.*, vol. 21, no. 3, pp. 462–470, 2014.

[35] I. A. Sumra, P. Sellappan, A. Abdullah, and A. Ali, “Security issues and challenges in MANET-VANET-FANET: A survey,” *EAI Endorsed Trans. Energy Web*, vol. 5, no. 17, pp. e16--e16, 2018.

[36] A. Alharbi, “Security issues in wireless sensor networks,” *Indian J. Sci. Technol.*, vol. 10, no. 24, pp. 1–5, 2017.

[37] G. Kadian and D. Singh, “Review Paper on Wormhole Attack,” *Int. J. Comput. Appl.*, vol. 975, p. 8887, 2015.

[38] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, “Security challenges and attacks in dynamic mobile ad hoc networks MANETs,” in *2019 IEEE jordan international joint conference on electrical engineering and information technology (JEEIT)*, 2019, pp. 28–33.

[39] O. Sbai and M. Elboukhari, “Classification of mobile ad hoc networks attacks,” in *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, 2018, pp. 618–624.

[40] W. Ahmed and M. Elhadef, “DoS Attacks and Countermeasures in VANETs,” in *Advanced Multimedia and Ubiquitous Engineering: MUE/FutureTech 2018 12*, 2019, pp. 333–341.

[41] S. Doss *et al.*, “APD-JFAD: accurate prevention and detection of jelly fish attack in MANET,” *Ieee Access*, vol. 6, pp. 56954–56965, 2018.

[42] N. Gupta, S. Das, and K. Singh, “A comprehensive survey and comparative analysis of black hole attack in mobile ad hoc network,” *Int. J. Comput. Inf. Eng.*, vol. 8, no. 1, pp. 192–201, 2014.

[43] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” *Human-centric Comput. Inf. Sci.*, vol. 1, no. 1, pp. 1–16, 2011.

[44] J. Kumar, M. Kulkarni, and D. Gupta, “Effect of Black hole Attack on MANET routing protocols,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 5, p. 64, 2013.

[45] M. B. Dsouza and D. Manjaiah, “Congestion aware reverse AODV routing protocol for MANET,” *Int. J. Sci. Res. Netw. Secur. Commun.*, vol. 8, no. 1, pp. 10–13, 2020.

[46] S. Pal, K. Ramachandran, I. D. Paul, and S. Dhanasekaran, “A review on anomaly detection in manet using antnet algorithm,” *Middle-East J. Sci. Res.*, vol. 22, no. 5, pp. 690–697, 2014.