Investigate the impact of three wormhole attacks on MANET

Karzan Luqman Ibrahim
Department of Computer Science and Engineering - Software Engineering
University of Kurdistan Hawler, UKH
Erbil, Kurdistan region, Iraq
karzan.iluqman@ukh.edu.krd

Luqman I Azeez
Department of Economics and administrative sciences
Cyprus International University, CIU
Nicosia, Cyprus
21702099@student.ciu.edu.tr

***Abstract*— The ever-growing population of computer and network use introduces the world to many new threats to the security and safety of the data communication and increases the need for more secure and reliable networks. Furthermore, cyber-attacks are evolving rapidly and becoming more intelligent and brutal. This research studies the issues and problems wormhole attacks cause a network by simulating the three different types of wormholes on a single MANET separately. Afterward, the simulation outcomes would be compared to another simulation of the same network but attack free. However, the simulation is divided into different sections and scenarios. The chosen simulation program used is OPNET. Also, the parameters that are simulated and compared include End to End delay, number of hops, the path, packet drop, route discovery time, and Packet delivery ratio. Therefore, in this study, we intend to simulate three types of wormhole attack on an ad-hoc MANET and analyze the effects that these attacks have on the network by comparing their impacts.**

Keywords—ETE delay; packets dropped; MANET; AODV; ad-hoc network; OPNET; PDR; RDT

I. INTRODUCTION

Computer security, cybersecurity, or information technology security is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data and the disruption or misdirection of the services they provide. Furthermore, cybersecurity is a vast topic, and it has various fields and applications. Moving on, one of the popular applications that it is used for is the mobile ad hoc network "MANET". A MANET is a self-configuring network of mobile nodes. It lacks any fixed infrastructure like access points or central stations [1]. MANET like any other network has vulnerabilities and is prone to many forms of attacks.

MANET's flexible infrastructure makes it more exposed to attacks. Therefore, there is a need to strengthen security. Hence, the first step in doing so is to understand the enemy and its effects on our networks. Therefore, this research is conducted on the three variants of wormhole attack and their impacts on MANET. A wormhole attack is a form of attack where two nodes of a network establish a secret fast connection and tunnel data through that tunnel without the knowledge of the other nodes in the network, the connection can be anything as long as it is faster than the network's connection, but it is usually wired connection. The three types of wormhole attacks are closed wormhole, open, and half-open. The closed wormhole has both malicious nodes hidden. However, the open wormhole has both of the malicious nodes visible. Finally, the half-open wormhole has only one of the malicious nodes hidden, meaning it seems as there is only one node. The wormhole has been chosen to be understood, analyzed, simulated, and compare to the effects of all three variants of it on a MANET using OPNET simulation program. By investigating wormholes, we can collect a better understanding of it and ease the way for further research on preventing and defending against it. The study is organized as follows: section 1 introduction, section 2 background overview and related works, section 3 proposed approach, section 4 environment and the wormhole implementation, section 5 results and analysis, and section 6 conclusion.

II. BACKGROUND OVERVIEW AND RELATED WORKS

A. Background overview

1) MANETs

As previously mentioned, Mobile Ad-Hoc Networks "MANET" s are networks with no infrastructure, created by the collaboration of multiple independent nodes that work as hosts and routers at the same time. The nodes are free to move randomly in the network topology. Moreover, MANET have been successful in networking due to their properties of self-maintenance and self-configuration. There are a variety of types of MANETs, which are:

- Vehicular Ad hoc Network "VANET"
- Smart Phone Ad hoc Network 'SPANC"
- Internet-based Mobile Ad hoc Network "iMANET"
- Hub-Spoke MANET
- Flying Ad hoc Networks "FANET"

However, in this research, we are not digging into the types of MANETs.

a) MANET routing protocols

Moving on to MANET routing protocols, they can be divided into three main branches, which are:

ISBN 978-3-903176-42-3

- Pro-active routing protocols

Likewise known as table-driven routing protocols, where each node stores routs to all possible destination mobile nodes in a separate routing table. It has three main subclasses which are: Destination Sequenced Distance Vector Routing Protocol "DSDV", where the destination sequence number is added with every routing entry in the routing table maintained by each node. Next is Optimized Link State Routing "OLSR", where it reduces the size and number of the control packets required, usually used in dense and large networks. Finally, Global State Routing "GSR" where each of the mobile nodes maintains one list and three tables namely, adjacency list, topology table, next hop table, and distance table.

- Reactive routing protocols

Also Known as the on-demand routing protocol. In this type of routing protocol, the route is discovered only when it is required. It consists of two major phases, route discovery and route maintenance. It has two subclasses: Dynamic Source Routing protocol "DSR", where the discovery occurs by flooding a request packet and find the most optimal path to a destination node, and the route maintenance to fix any failures that happen in the network. Also, Ad-Hoc On-Demand Vector Routing Protocol "AODV", where the AODV is the same as DSR but with the improvement in related to the size of the header by adding a path for each node in the table and not the packet header.

- Hybrid routing protocols

This protocol is considered as a combination of all the advantages of the other two protocols. This protocol is adaptive in nature and adapts itself according to the position and zone of the nodes. It has one subclass of Zone Routing Protocol. This protocol divides all the topology into zones if the source and destination nodes are in the same zone, it uses the proactive protocols. On the other hand, if they were not located in the same zone distribution, the reactive routing protocols are going to be used for transmitting the packets.

With gathering enough background information on MANET and its routing protocols, the AODV protocol has been chosen to be investigated in this research.

2) Wormholes

Moving on, wormhole attack in computer networking consists of two or more malicious nodes that share a faster connection creating a wormhole tunnel. The nodes then receive packets from surrounding nodes and forward them into the wormhole tunnel to another location in the network, while also being able to alter or damage the data being sent. These malicious nodes almost always win the path due to the fast connection they have among themselves. Moreover, the term wormhole came from the space wormholes in astrology, where a hole in space is formed engulfing any matter around it and teleporting it to another point in space. Hence, creating a hole in space. A wormhole in terms of networking and cybersecurity is classified into three main types which are: closed wormhole, half-open wormhole, and open wormhole. Moreover, in a closed wormhole the source and destination nodes see themselves as neighbors. Because the two malicious nodes of the wormhole are hidden from the rest of the network, as shown in figure 1, meaning their IP remains hidden to the surrounding. Moving on to half-open wormholes, as illustrated in figure 2, the source considers only one node of the wormhole. Hence, one side of the attack is visible to the other hidden. Finally, another type of wormhole is where the malicious nodes are visible to the source and destination as shown in figure 3. However, the source and destination perceive them as neighboring nodes even if they were not in reality. Hence, altering the mapping of the network.

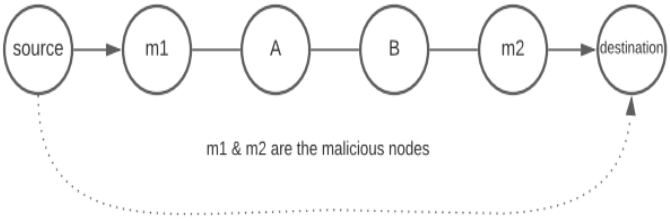

Figure 1 closed wormhole

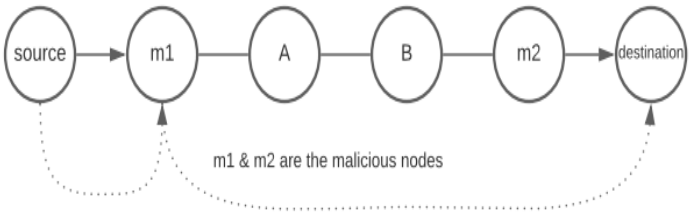

Figure 2 half-open wormhole

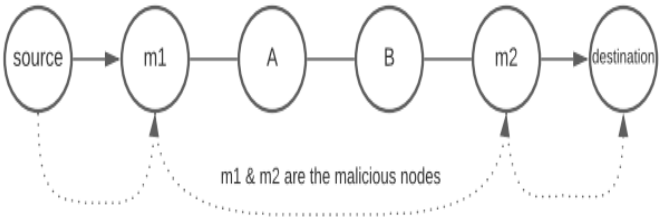

Figure 3 open wormhole

B. Related works

Many studies and researches have been conducted related to wormholes. Few of those researches include defense mechanisms and protocols and analysis of wormhole attacks on a MANET. Some of the most related papers are going to be discussed in this section.

Firstly, Devi and few other researchers[2] conducted an analysis about a wormhole assault on a MANET. The MANET protocol used for the simulation is AODV. Although

two routing protocols of MANET, which are Proactive or Table-Driven routing protocols "DSDV", and Reactive or On-Demand routing protocols "AODV", mentioned in this paper, only one of them is used in regards to the analysis and simulation. The simulation consists of two identical scenarios where one of the two is injected with the one malicious node that are introduced to the node network, and then the other malicious node. The research's testing parameters of this paper are throughput, jitter, packet delivery ratio, and packet dropped. The researchers only introduce one malicious node into the network and record the date and graph of the testing parameters. Afterward, another node is introduced into the network, and then again, the testing parameters are observed and recorded. In this research, each malicious node that receives any packet discards it. The results of the simulation and conclusion of the study are analyzed using ANOVA tool. The results of the analysis show that with the increase in the number of malicious nodes, the testing parameters are more affected negatively. This research is pretty similar to the current research we are conducting. However, there are few shortcomings to be tested. One of the shortcomings of this research is that it is mostly related to the effects of number of nodes. Moreover, the researchers' goal and objective of the study was to monitor the behavioral changes that happen as more nodes are introduced to the network. In addition, there is only one type of wormhole being used in the research.

Another research done by N. Al-Bulushi and his colleagues[3] is pretty similar to the previously mentioned article. One of the differences is that it uses static and mobile nodes for the MANET. Therefore, we will not dig too deep into it. Moreover, the main difference is in the scope of the research, because it concerns the routing protocols and not the attack types.

Next, research done by Kadian and Singh[4] regarding Wireless Sensor Networks and the wormhole attacks on them. "Wireless Sensor Network "WSN" as a part of MANET consists of a large number of tiny sensor nodes that continuously monitor the environmental conditions[4]." In this research, the sensor nodes "SN" are the nodes that are prone to attacks in this network. Because the sensor nodes have strictly limited resources such as power and memory. Moreover, the use of WSNs in part of MANET here in this study is mentioned in a scenario where the nodes are placed in dangerous locations and are not protected physically. Therefore, they are already at risk of loss and destruction. Also, being prone to assaults such as wormhole assaults makes the use of WSNs in part of a MANET a useless technique.

The researcher Kadian and Singh [4] define a wormhole attack as a denial-of-service attack and moves on further by mentioning the other classifications of a wormhole. Moreover, the three classifications used in this research are open wormhole, half-open wormhole, and closed wormhole. Later on, the mode of wormhole attacks is mentioned which are Packet encapsulation, Out-of-band Channel, High Power transmission capability, Packet relay, and protocol Distortions. These attacks have different minimum node requirements, which are two, two, one, one, and one respectively. The researcher goes on by mentioning the difficulty of detecting wormhole assaults in WSN MANET. Finally, few methods used to minimize the effect of wormhole attacks on WSN MANETs are discussed. This research is also informative regarding wireless sensor networks as sub-networks of MANET and wormhole attacks in it.

In another research conducted related to wormhole attacks on a MANET, the authors[5] analyze the previously written papers in regards to wormhole attacks in MANET. Moreover, the researchers focus mostly on wormhole detection methods and techniques. Few of the techniques that are mentioned in this research are location-based, time-based, hop count based, neighborhood-based, data pack-based, route reply based, and route-request based. In addition, the main issues with these detection techniques are mentioned such as congestion, routing delay, resource overuse, special hardware requirements, and mobility issues. Finally, The researchers[5] mention that the techniques based on route request "RREQ" and hop count are better than other techniques to detect wormhole attacks.

Another research similar to Imran the research provides a more informative view in regards to MANET and wormholes. "In this paper, we have condensed the endeavors already done, our point here is to give the analysts a stage where they can locate a total reference to all past work done as to the wormhole assault [6]." As stated by the researchers, this paper does not contribute any detection, analysis, nor recovery mechanism in regards to MANET and wormholes. It only collects information regarding previous researches.

Additionally, another study in regards to wormhole detection in ad hoc networks is done where the researchers[7] use TIK and temporal packet leashes. This research has been done in 2006, therefore it is having been updated and improved over the years. To simply explain the work, TIK uses n keys for n nodes and uses a small storage size and doesn't require a lot of CPU and high internet speed to perform.

Moreover, in this research done S. Majumder and M. A. Hussain [8], three types of attacks are implemented and their effects on the throughput of the networks are studied at different data rates in a MANET. The MANET routing protocol used for all these attacks is On-Demand Routing Protocol "AODV". The researchers explain an AODV as whenever there is a need for a table for the routing path, one is created using a route request packet being broadcasted to the neighbors and each neighbor broadcasting it until finally getting all the nodes and recording them in a table[8]. Moreover, the researchers explain a set of attacks briefly such as passive eavesdropping attack, selfish existence attack, grey hole attack, black hole attack, impersonation attack, modification attack, against routing tables attack, sleep deprivation torture attack, and wormhole attack. In addition, codes for implementing blackhole attacks are given. In reality, grey hole attack is similar to blackhole attack. Therefore, only little differences have been done to a blackhole code. In an attempt of wrapping this research review up, there is very little research done related to a wormhole, even in the simulations and resulting graphs compared to a black hole attack.

Therefore, it is fair to say that there is not much effort given to the wormhole assault. [8] Finally, many kinds of research regarding wormholes and MANETs have been conducted over the course of many years. Those studies are detection-related, informative-related, and simulation and analysis related. However, the only type of study related to my research is the simulation and analysis, which has not implemented all three types of wormholes and analyze each induvial type's impacts on a network.

III. PROPOSED APPROACH

One of the most common methods of research in the fields of networking and security is simulation and evaluation of the scope of the study in different kinds of network-based scenarios. As previously mentioned, this research aims to create two network scenarios and injecting an Open wormhole, half-open wormhole, and closed wormhole into one of them separately. However, one copy of the scenario will be left out, which is going to be used as a benchmark to compare the impacts and effects of the assaults on the network. The networks under test are going to be MANET consisting of 20 to 30 nodes being mobile nodes. The routing protocol between the nodes of the MANET is going to be Ad hoc On-Demand Distance Vector Routing "AODV". The environment for the implementation and simulation of the scenarios and the attacks is the Optimized Network Engineering Tool "OPNET". "It is a network simulator which is used to provide multiple solutions for managing networks and applications such as research and development, network operation and engineering, planning and performance management." [9]. The variables that are going to be compared in each scenario are end to end delay, number of hops, packet delivery ratio "PDR", route discovery time "RDT", and packet drop, which are explained briefly:

The number of hops is the value of hops each packet took node by node from source to destination. Using this variable helps in determining the impact of wormholes on winning the path. Next, the path shows the route that the traffic went through from the source to the destination. Moreover, the path displays the nodes that a packet took from the source of the traffic to the destination. Moving on to End to End "ETE" delay, ETE is the time taken for the transmitted traffic to reach its destination. ETE delay is selected to demonstrate the impact of wormholes in regards to time consumption and delaying of traffic transition. Packet delivery ratio "PDR" is the ratio between the packets sent and packets received. The purpose of this variable is to demonstrate the rate of successful transmissions. This variable helps to determine the impact of the wormhole's malicious nodes in dropping packets. It is worth mentioning that OPNET does not return the value of PDR, therefore it is calculated using the ratio of delivered packets by sent packets. The route discovery time "RDT" is the time that the network takes in terms of finding the path to use that path to transfer the data, during this time the table is created for AODV protocol. Moreover, RDT is calculated by the average of both traffics being sent from each corner nodes that are implemented with the OPNET program. Finally, packet drops refers to the packets that are being dropped due to the malicious nodes of the wormhole.

The analysis for this research will be conducted in the following manner:

- Comparing the path with delay and route discovery time and the number of hops of a scenario injected with an open wormhole with the attack free of the same scenario.
- Comparing the number of hops and packet delivery rate, route discovery time, packet drop, and ETE delay of three scenarios each injected with an open, half-open, and closed wormhole with the attack free of the same scenario.
- Comparing the packet delivery ratio of two scenarios one with an open wormhole and one with no wormhole, using a different number of nodes, comparing the impact of the number of nodes on MANETs.
- Comparing the packet delivery ratio of two scenarios one with an open wormhole and one with no wormhole, using different date rates, comparing the impact of the different data rates on MANETs.

```
Variable : source_node          // altering previous node
Variable : my_address
WH // the variant of the wormhole
If (WH ==2)    // wormhole variant both nodes hidden "closed wormhole"
{   if ( source_node == specific source address1 AND
          my_address == malicious_node2 address ) {
        previous_node_address = malicious node1 address }
     else  if ( source_node == specific source address 2  AND
               my_address == malicious_node1 address ) {
        previous_node_address = malicious node2 address  } }
If (WH ==1)                // wormhole variant half open
{   if ( source_node == specific source address1  AND
          my_address == malicious_node2 address ) {
        previous_node_address = malicious node1 address } }
```

Figure 4 pseudocode of previous node altering

```
Variable : my_address      // altering next node
Variable : WH              // the variant of the wormhole
If (WH ==2)                // wormhole variant closed
  {    if (my_address == malicious_node2 address )
            neighbor_ next_ address =  malicious_node1 address
       else  if (my_address == malicious_node1 address )
            neighbor_ next_ address = malicious_node2 address   }
If (WH ==1)                //  wormhole variant half open
  {    if (my_address == malicious_node2 address )
            neighbor_ next_ address = malicious_node1 address
```

Figure 5 pseudocode of next node altering

Scenarios	Network	Time (min)	Variables		Observed parameters			
			No. of nodes	Data rate (Mbps)				
Scenario 1	Open WH vs No WH	30	30	11	No. of hops		Path (delay & RDT)	
	All WH vs No WH	30	30	11	No. of hops	Packets dropped	RDT	PDR
Scenario 2	No WH vs Open WH	20	30,25,20,15,10	11	PDR			
	No WH vs Open WH	20	30	6,12,18, 24,32	PDR			

Table 1 specifications or the simulations

IV. ENVIRONMENT AND THE WORMHOLE IMPLEMENTATION

A. Wormhole implementations

The wormhole is one of those malicious attacks that take advantage of the routing protocol to display itself as the shortest path from a source to a destination. The way a wormhole works is based on replying to the RREQ messages in the AODV protocol. Within the AODV routing protocol, a node requests a route to a specific destination, through flooding RREQ messages to all its neighbors and they reply with the PREP. The wormhole due to the fast ethernet connection it has between both of its malicious nodes, will always reply faster and win the route. Moreover, the design of the wormhole consists of three main parts, referencing the previous node, referencing the next node, and dropping the packets

Regarding the design of the wormhole in OPNET, three pieced of code was inserted into the AODV protocol code in (aodv_rte_reqq_pkt_arrival_handle) function of the aodv_rte. The inserted lines were related to referencing the previous node, referencing the next node, and dropping packets. See figures 4,5, and 6 for the pseudocode of the pieces of code inserted.

```
Variable : WH // the variant of the wormhole    //dropping packets
If  (WH ==2 or 1 or 0 )
{   if ( simulation_time > 60 sec)
{   if  ( my_address == malicious_node2 address OR malicious_node1 address)
        Drop the packets
} }
```

Figure 6 pseudocode of dropping packets

B. Scenarios

The scenarios for the wormholes are divided into 2 main parts, one focusing on the impact of the wormholes regarding the path and the other focusing on the performance impact of wormholes. These scenarios are each divided into two different sub-scenarios. All the scenarios are set up per the specifications of table 1.

1) Scenario 1

The first scenario consists of four variations of an identical 30-node network using the AODV protocol. The four variants of the network are differentiated by the wormhole nodes stationed in them. Three of the four simulations performed contain one of the three types of wormhole attacks and the fourth simulation contains no wormhole. The wormholes are open wormhole, half-open wormhole, and closed wormhole. The wormhole-free simulation is used as a benchmark to compare the specified parameters to determine the impact of the wormholes on Mobile Ad-Hoc Networks following the AODV protocol. All the specifications in table 1 are used in the setup of all the simulations of scenario-1. The traffic used is IP-unicast full mesh between the node MN_1 and node MN_30, for more clarity check figures 7 and 8. Moreover, two traffics will be sent one from MN_1 to MN_30 and vice versa. The simulation time for this scenario is 30 minutes. However, the objective of observation and data collection of this scenario will be divided into two simulations.

a) Scenario1 sub-scenario 1

The first sub-scenario is concentrated on the impact of a wormhole in winning the path from nodes MN_1 to MN_30 also from MN_30. to MN_1, the number of hopes, the path, delay, and RDT are chosen parameters and will be observed and analyzed in the next section. Moreover, this section of the first scenario contains the comparison of the two networks, one wormhole free and the other containing the open wormhole.

b) Scenario 1 sub-scenario 2

The second sub-scenario of scenario-1 focuses more on the impact of each type of wormholes on a MANET. Accordingly, PDR, and number of hops, ETE delay, route discovery time "RDT", and packet drop are chosen as the parameters and will be researched and analyzed in the next section.

2) Scenario 2

The second scenario also consists of 2 main sub-scenarios. The purpose of these scenarios is to observe and simulate the performance impact of wormholes on a MANET AODV with different number of nodes and different data rates. The simulations are conducted with nodes scattered around within a 2x2km area and the setup specifications in table 1. The traffic used is IP-unicast full mesh between the node MN_1 and node MN_30, the two corner nodes. The simulation time for both of the sub-scenarios of this scenario are 20 minutes. Furthermore, for both of the simulations, the parameter PRD will be observed.

a) Scenario2 sub-scenario 1

The specifications of this sub-scenario are visible in table 1. The only main significance of this scenario is the removal of 5 random nodes and the repetition of the simulation to observe the effect of the number of nodes on PDR.

b) Scenario 2 sub-scenario 2

The second simulation of scenario-2 also focuses on the performance impact different data rates have on the two networks mentioned in the previous simulation. Moreover, the difference regarding the implementation of the simulation is that the fixed number of nodes in addition different data rates selected per tables 1.

V. Results and Analysis

A. Scenario 1

As previously mentioned, this scenario is divided into two sub-scenarios and their results are as shown below:

1) Scenario 1 Sub-scenario 1

The results shown in table 2, the traffic in the simulation of the network with a wormhole has a lower average for the number of hops taken from destination to source. The network with the open wormhole took an average of 5.0655 hops whereas the network with no wormhole took an average of 8.53615 hops to get to the destination. The data demonstrates that the network with the open wormhole wins the path due to the smaller number of hops it takes.

Route	Open wormhole	Wormhole free
MN_1 -->30	5.0659	8.52
MN_30 -->1	5.0651	8.5523
Average	5.0655	8.53615

Table 2 number of hops taken for open wormhole and wormhole free

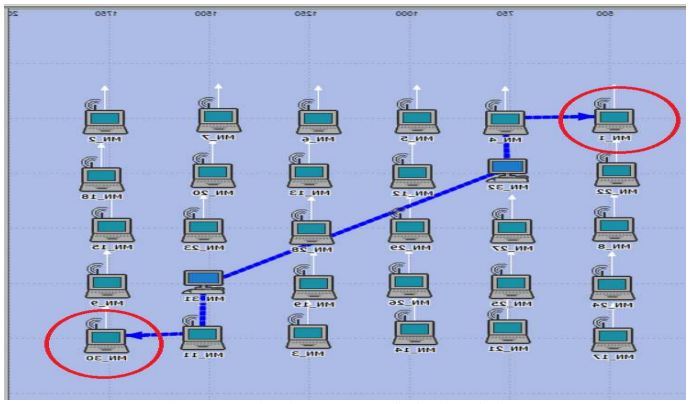

Figure 7 path of open wormhole simulation

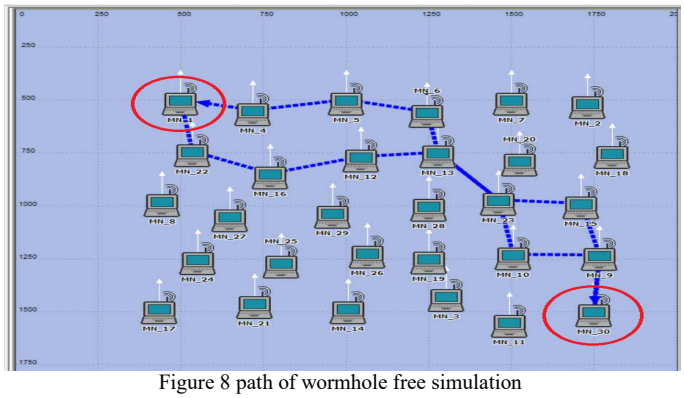

Figure 8 path of wormhole free simulation

As the path is shown in figures 7 and 8, the open wormhole network took a shorter path whereas the wormhole free network took a longer path. The paths are visible in figures 7 and 8 and the results are visually concluded that the network with a wormhole wins the path due to taking a shorter path due to the ethernet connection between the wormhole malicious nodes. Moreover, the RDT in table 3 shows the results as the open network takes less in terms of the time of route discovery that will guaranty the win of the path with the smaller delay shown in the same table.

Parameter	Open wormhole	No wormhole
RDT (sec)	0.326	0.699
Delay (sec)	0.0498	0.9675

Table 3 RDT and delay (sec) for wormhole and no wormhole AODV networks

Route	Open wormhole	Half open wormhole	Closed wormhole	Wormhole free
MN_1 -->30	5.0659	5.1115	5.1115	8.52
MN_30 -->1	5.0651	5.104	5.104	8.5523
Total average	5.0655	5.10775	5.10775	8.53615

Table 4 number of hops taken for all the simulations

Parameter	Open wormhole	Half-open wormhole	Closed wormhole	No wormhole
Delay (sec)	0.0498	0.036	0.036	0.9675

Table 5 delay (sec) for the variations of wormhole and the no wormhole from the simulation

2) Scenario 1 Sub-scenario 2

Within this sub-scenario, the number of hops, end-to-end delay, packet delivery ratio "PDR", route discovery time "RDT", and packets dropped will be analyzed.

As the results are shown in table 4, the network with the open wormhole took an average of 5.0655 hops whereas the networks with the half-open wormhole, closed wormhole, and wormhole free took an average of 5.10775, 5.10775, and 8.53615 hops to get to the destination respectively. The data demonstrates that the network with the open wormhole takes the shortest path due to the smallest number of hops it takes aided by the ethernet connection between nodes MN_31 and MN_32.

End to End "ETE" delay has been recorded in table 5 for each open wormhole, half-open wormhole, closed wormhole, and no wormhole. The results show that delay with a wormhole overall is less than with no wormhole. In addition, the half-open and closed wormholes, have the least delay and they are equivalent. The reason for that is the mechanism of hiding the nodes of the previous and/or next node is very similar, therefore, no extra delay has occurred.

Moving on to PDR, the rate of received packets in bits over sent packets in bits. To calculate PDR, we must divide the Traffic Received by Traffic Sent. The results of the simulation were collected and were as such: 0.134, 0.144, 0.1515, and 0.612 for the open wormhole, half-open wormhole, closed wormhole, and no wormhole respectively. From the results, we can conclude that the network with the no wormhole has the highest PDR rate meaning that it had the highest success transaction and least packets drops. Moreover, the networks with wormholes had the lowest PDR meaning that they had the most packet drops. The reason for that is the networks with wormholes start dropping packets after the network discovery time by 60 seconds and during data transition.

Parameter	Open wormhole	Half-open wormhole	Closed wormhole	No wormhole
RDT (sec)	0.326	0.351	0.351	0.699

Table 6 RDT (sec) for all the networks

Parameter	Open wormhole	Half-open wormhole	Closed wormhole	No wormhole
Packet drop(pkts)	2090.15	2465.55	2465.55	314.81

Table 7 packets dropped (pkts) for each of the networks simulated

Next, RDT, the time the network nodes take to discover the route in which they send the traffic. during the simulation, the RDT for all the four networks was collected and the results are shown in table 6. The results of the table show that the open wormhole takes the least time for the route discovery, followed by the half-open and closed wormholes with equivalent route discovery time, lastly is the wormhole-free network. The reason for that is wormholes provide a better time with less delay due to the ethernet connection they have.

Finally, the dropping of the packets is mostly due to the malicious nodes. The results are shown in table 7. Moreover, the results indicate that the wormholes have a higher packet dropping compared to the no wormhole situation. The justification for that is due to the negative impact of the malicious nodes for dropping packets after route discovery.

B. Scenario 2

Similar to scenario 1, the results of this scenario are also divided into two scenarios and they are analyzed below:

1) Scenario 2 Sub-scenario 1

By calculating PDR, we understand more clearly the impact of the number of nodes on the networks. The results are shown in figure 9. The results of the simulation were collected and were as such: From the results, we can conclude that the network with the open wormhole has the lower PDR over the no wormhole network. This indicates that the number of dropped packets, meaning success rate, in the wormhole network was more than the wormhole free network. Moreover, as the number of nodes decreases the ratio of packets received to packets dropped increases, indicating that the number of nodes is indirectly proportional to the PDR for both of the situations.

We can conclude That decrease in the number of nodes is helpful for MANET AODV networks with and without wormholes. However, overall, the PDR of the wormhole-free network is more than the PDR of the network with the open wormhole. This is predicted due to the dropping of packets done with the malicious nodes of the wormhole. For clarity check the figure below.

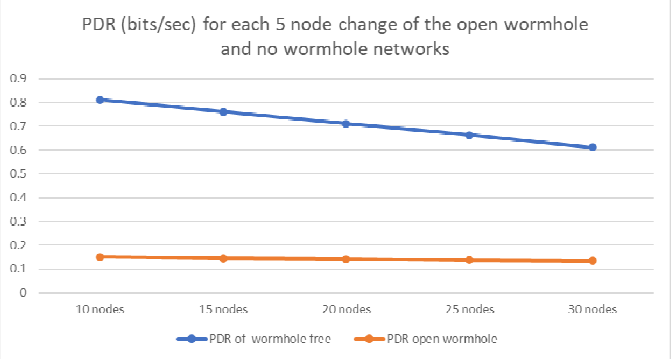

Figure 9 PDR of all the networks vs number of nodes

2) Scenario 2 Sub-scenario 2

The results of sub-scenario-2 of scenario-2 are shown in figure 10. From the results, we can conclude that the AODV networks meaning not having any wormhole has a higher PDR than the AODV networks with the open wormhole attack. Moreover, higher PDR indicates that the number of dropped packets is less as predicted for the networks with no wormhole. Overall, for the wormhole-free network, as the data rates increase the PDR decreases. On the contrary, the AODV network with the wormhole malicious nodes has lower PDR, meaning more packets dropped due to the packet dropping of the malicious nodes.

VI. CONCLUSION

Mobile ad-hoc networks "MANET"s are interesting networks and are applicable for the future of communications. Because MANET is capable of creating networks without worrying about topology. This dynamic method reduces many costs financially and timewise. This being said, there is a drawback when it comes to MANETs and it is regarding its security. Any node can enter the network and as the wormhole by winning the path, and it can be a huge security risk. Using the three varieties of the wormhole, tests for winning the path and performance impacts were made on MANET with AODV protocol.

Using the OPNET modeler, scenarios for the networks were created and observed. With the help of the simulations and the scenarios, we can conclude Wormhole wins the path during the route discovery as it provides better route discovery time with less delay but it drops packet during the data transmission, the results confirm that wormhole is hard to detect, increasing security issue, as it does not provide any indication during route discovery of any malicious nodes then during data transmission drops packets harming the network.

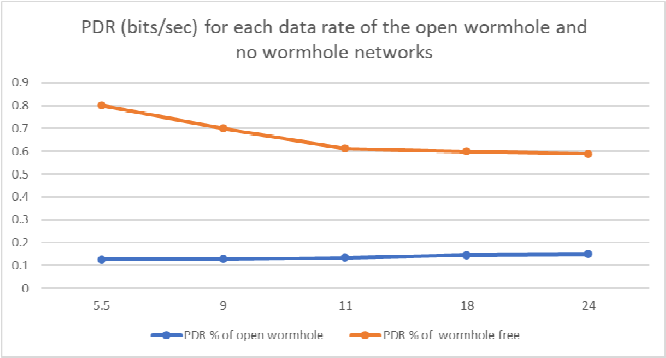

Figure 10 PDR of all the networks vs different data rates

REFERENCES

[1] A. Bhattacharyya, A. Banerjee, D. Bose, H. N. Saha, and D. Bhattacharjee, "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques," *URL: arxivweb3. library. cornell. edu/pdf/1111.4090,* 2011.

[2] B. R. Devi, N. kaylyan Chafravarthy, and M. Faruk, "Analysis of Manet Routing Protocol in Presence of Worm-Hole Attack Using Anova Tool," *International Journal of Pure and Applied Mathematics,* vol. 117, no. 15, pp. 1043-1054, 2017.

[3] N. Al-Bulushi, D. Al-Abri, M. Ould-Khaoua, and A. Al-Maashri, "On the Impact of Static and Mobile Wormhole Attacks on the Performance of MANETs with AODV and OSLR Routing Protocols," in *2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2020, pp. 1064-1069: IEEE.

[4] G. Kadian and D. Singh, "Review Paper on Wormhole Attack," *International Journal of Computer Applications,* vol. 975, p. 8887, 2015.

[5] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs," *Procedia Computer Science,* vol. 56, pp. 384-390, 2015.

[6] P. Roshani Verma, R. Sharma, and U. Singh, "Wormhole Attacks in MANET."

[7] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE journal on selected areas in communications,* vol. 24, no. 2, pp. 370-380, 2006.

[8] S. Majumder and M. A. Hussain, "Attack Patterns for Black Hole, Gray Hole and Worm Hole Attack on Adhoc Networks," *International Journal of Mobile &Adhoc Network,* 2011.

[9] Y. Sarwar and M. A. Ali, "Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions," ed, 2011.