VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Early warning and detection of malicious nodes and internal attacks in MANET

Submitted by

Reet Bhatia- 20BCT0312

Ojal Shukla- 20BCT0297

Gajula Padmatej- 20BCT0208

Siddhartha Soni- 20BCT0080

Under the guidance of,

Prof. Kalaavathi B

Professor Grade 1

SCOPE

November-2022

TABLE OF CONTENTS

1. ABSTRACT

MANETs are mobile, wireless nodes in an ad hoc network. In a MANET, the mobile nodes self-organize in an arbitrary pattern.

In locations where fixed infrastructure is scarce, these networks can be used to connect people or vehicles.

If the nodes are not within radio range, multi-hop routing can be used to communicate with them.

Because MANET nodes interact across an open-air channel rather than a wired connection, they suffer significant security issues.

This network lacks infrastructure due to the lack of a centralised coordinator and a dynamic path established up between nodes to temporarily transfer packets, a MANET is more vulnerable to various assaults.

Many DOS attacks attempt to target MANET, causing substantial damage to its functionality and connectivity.

So having a good security system to fight such issues is very important and needed.

Black Hole and Wormhole attacks are two such crucial issues which are also part of DOS attacks.

So, this was where the problem was identified and this is where we will work on.

2. INTRODUCTION

A MANET is a collection of wireless points that communicate with each other without the work of a central coordinator. This type of network is useful for establishing communication between nodes that aren't in line-of-sight and aren't within wireless transmission range of one another. Nodes in a MANET won't rely on a central point to coordinate with one another; instead, they work together to transport data between nodes that are far apart.

Because Manet nodes interact across an open-air channel rather than a wired connection, they suffer significant security issues. This network lacks infrastructure due to the lack of a centralised coordinator. A network node with

dynamic topology can easily join or exit the network at any time. Due to the lack of a centralised coordinator and a dynamic path established up between nodes to temporarily transfer packets, a MANET is more vulnerable to various assaults.

In MANET, there are usually 2 sorts of attacks: passive attacks and active attacks.

Active attacks such as black hole attacks, rushing attacks, and wormhole attacks have a significant impact on network performance. A Black hole attack occurs when a node drops all packets and sends forged routing packets to route traffic over itself.

Wormhole attack, two far-flung malicious nodes can join forces using either a physical connection or a directional antenna to make it appear as though they are just one hop apart.

In our proposed project we are going to implement and mitigate both Black hole and Wormhole attacks. We will be working on AODV protocol as it is convenient to use in ns2.35.

3. LITERATURE SURVEY

1. *Examination of existing classical and machine learning methodologies for detecting malicious nodes in MANETs.*

   MANET is a self-configuring, self-organizing network of mobile nodes that does not require any infrastructure.MANETs are especially sensitive to attacks due to their on-the-spot nature, resulting in network performance loss. Special considerations must be made in order to improve MANET's performance by creating more sophisticated algorithms to detect and eliminate these attacks from the network.
   This paper gave a detailed examination of various methods for detecting the existence of malicious nodes in MANET. In different MANET environments, network metrics such as node densities and average node speed differ. As a result, the environment adaptable properties should be

taken into account while creating machine learning-based attack detection techniques.

2. *A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks.*

   They proposed a Intrusion Detection and Prevention System (SA-IDPS) to reduce risks in MANETs using machine learning techniques in this study. At initially, the Trusted Authority uses the one way Hash Chain Function to register mobile users. To validate authentication, each mobile user provides the following information: fingerprint vein biometric, user id, and latitude and longitude. Four entities are used to detect intrusions.

   1. Packet Analyzer
   2. Pre-processing Unit
   3. Feature extraction Unit
   4. Classification Unit.

   A history database is used to categorise packets in this circumstance. Finally, testing is carried out and evaluated in order to determine the performance of the proposed SA-IDPS scheme in terms of detection rate (percent), false positive rate (percent), detection latency (s), and energy consumption (J).

3. *Detecting and isolating black-hole attacks in MANET using timer based baited technique.*

   In this paper, They improved AODV by using a new lightweight technique for detecting and isolating single and cooperative black-hole attacks that uses timers and baiting. The recommended technique allows MANET nodes to detect and isolate black-hole nodes in the network during dynamic topology changes. The proposed technique is implemented with the help of NS-2.35 simulation tools. Baiting and Non neighbor Reply are the two phases of the suggested approach . The suggested technique simulation results show that the results of parameters are all extremely near to the native AODV. They developed a smart black-hole identification and isolation technique in this paper, which should be taken into account while designing and developing any black-hole combat protocols or techniques. They came up with a method that relies on CBDS. During the Bait phase, then the source node picks neighbours at random and sends request with that node's id. The RREP of the bait RREQ is used to construct a list of suspicious nodes in the Reverse Trace phase, after which the other nodes enter into mode to identify if there is any kind of attacker point in the path.

A black-hole alarm is broadcast to neighbour nodes for each black-hole node found in the network. The proposed technique is implemented with the help of NS-2.35 simulation tools. To improve black-hole detection power while maintaining throughput, end delay, and PDR, the proposed TBBT incorporates both approaches. The suggested technique's simulation results show that the results of parameters are all extremely near to the native AODV.

4. *Detection and avoidance of malicious node in MANET.*

In this Paper, they designed a Malicious node that drops packets on a regular basis and investigate its impact on wireless LAN and AODV routing. That is, these organizations are defenceless against a wide scope of assaults at various organization layers. So, Security is very important. In addition, they created an improved AODV that detects and avoids such nodes while establishing a route in AODV.
In Improved AODV, when a packet comes at a node, the routing mechanism finds out whether or not to forward it based on the RREQ packet's sequence number, source and destination addresses, and network diameter. If the packet's source and destination addresses are the identical, the node decides to drop it and adds one to the dropped packets counter before dropping it. This logic is in place. The simulation results suggested that modified AODV improves route discovery time and throughput over standard AODV. OPNET is used for the scenario
In this they have created a 29 model. Once model is created, they create a scenario with the attack and another without the attack. There were 23 nodes and 1 FTP server in the network which they created.
The simulation findings show that in a network without a malicious node, the throughput and route discovery time of AODV is better than in a network with a malicious node. Additionally, when AODV improves, route discovery time and throughput improve. Route Discovery Time and Throughput are some parameters which are used for examination. In the results they have observed that for AODV, Throughput of wireless LAN is very low when the attack is there. The Route Discovery time also increased when the attack is there. But after the AODV is improved, the results for both throughput and Route Discovery time have shown better values.

5. *Wormhole attack detection technique in mobile ad hoc networks.*

In this research paper, they suggested a new wormhole detection technique that calculates the highest end-to-end latency between two nodes within the communication range to identify the wormhole link. There is no requirement for mobile nodes to have GPS, clock synchronisation, or any other form of specific hardware. The results of the simulations show that the suggested system can detect wormhole attacks.
For mobile ad hoc networks, they suggested a safe wormhole detection mechanism. The suggested technique identifies the wormhole link using threshold values rather than special hardware or time synchronisation.
The proposed system can be used to detect and prevent rushed attacks in the future. The suggested technique is first implemented using only AODV, but it can be extended to include other routing protocols as well.

6. *Lightweight detection of malicious nodes in mobile ad hoc networks.*

In this paper, they suggested a lightweight strategy for addressing some issues in MANETs. Their proposed method is simple and does not require the usage of any additional communication or GPS systems. This approach is simple to implement on the Mac layer without the need for additional hardware. Each point in network broadcasts its location claims to a group of witness nodes in this technique. They are using NS-2.35 as the simulator for the model.
The TIMER, threshold, is being used to track the emergence of new identities. If a node's TIMER has expired, a new ID has appeared in the radio range of it; otherwise, it is a recent ID. The goal of this experiment was to see how normal and aberrant nodes behaved. For testing the correctness of our proposed approach,they have used True Positive and False Positive as distinct measures. True positive means an attacker node was accurately discovered, while false positive means a benign node was mistakenly labelled as an attacker.

4. FINDINGS / INFERENCES FROM LITERATURE

Author	Title	Simulator	PDR	End to end delay	Throughput	Year
Sherif, Bismin V P. Salini	Effective and Prominent Approaches for Malicious Node Detection in MANET	NS2 using ubuntu	Yes	Yes	Yes	2021
Adwan Yasin Mahmoud Abu Zant	Detecting and Isolating Black Hole Attacks in MANET Using Timer Based Baited Technique	NS 2.35	Yes	Yes	Yes	2018
M. Islabudeen M. K. Kavitha Devi	A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks Against Security Attacks	NS3	Yes	No	Yes	2020
Kajal S. Patel ,Dr. J. S. Shah	Detection and Prevention of Black -Hole Attack in MANETS	OPNET	No	No	Yes	2015
Parvinder Kaur Dalveer Kaur Rajiv Mahajan	Wormhole Attack Detection Technique in Mobile Ad Hoc Networks	NS-2	Yes	Yes	Yes	2017
Mohsin Ur Rahman, Sohail Abbas and Seemab Latif	Lightweight Detection of Malicious Nodes in Mobile Ad Hoc Networks	NS-2.35	No	No	No	2017

5. PROPOSED SYSTEM

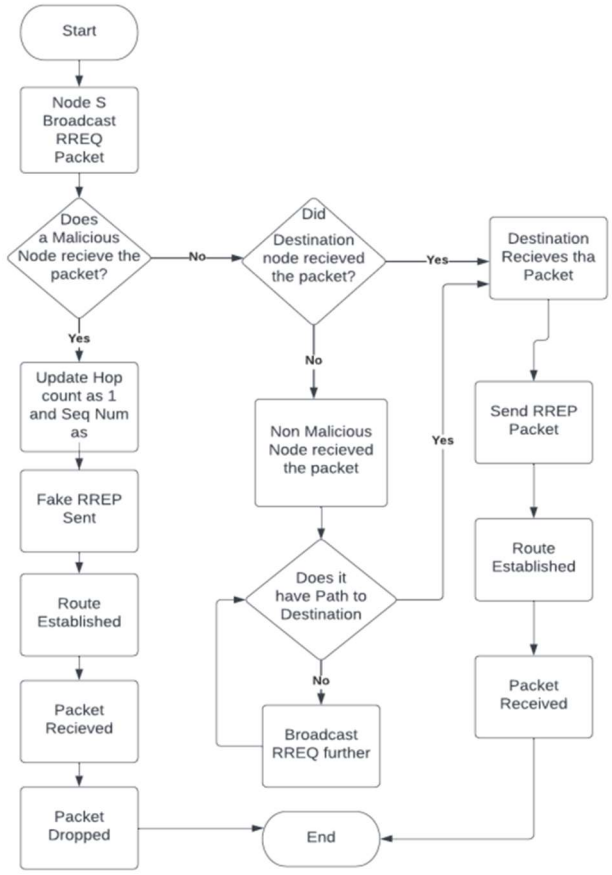
In our proposed project we are going to implement and mitigate both Black hole and Worm hole attacks. We will be working on AODV protocol as it is convenient to use in ns2.35. The main purpose of these simulator (NS2) provides substantial support for simulation of different protocols over wired and wireless networks.

Network Simulator 2 (NS2) provides substantial support for simulation of different protocols over wired and wireless networks. It provides a highly modular platform for wired and wireless simulations supporting different network elements, protocols, traffic, and routing types.

BLACKHOLE ATTACK:

occurs when a node in network drops down all the packets and sends routing packets which are forged to route traffic to itself. A bad node swallows all data packets, similar to how a hole takes everything it comes into contact with. All packets in the network are dropped in this manner.

Flowchart & Algorithm-



- if (Malicious node Received packet)
  - -HopCount and Seq Updated to 1 and Max;
  - -Fake RREP is sent;
  - -Packet is received and Dropped;
  - - END

Else

If (Destination node Received Packet)

-Destination Received the packet;

-RREP Sent;

-Packet Received;

Else

If (non-malicious packet has Destination address)

-Destination Receives the packet;

- END

Else

-RREQ is Further Broadcasted;

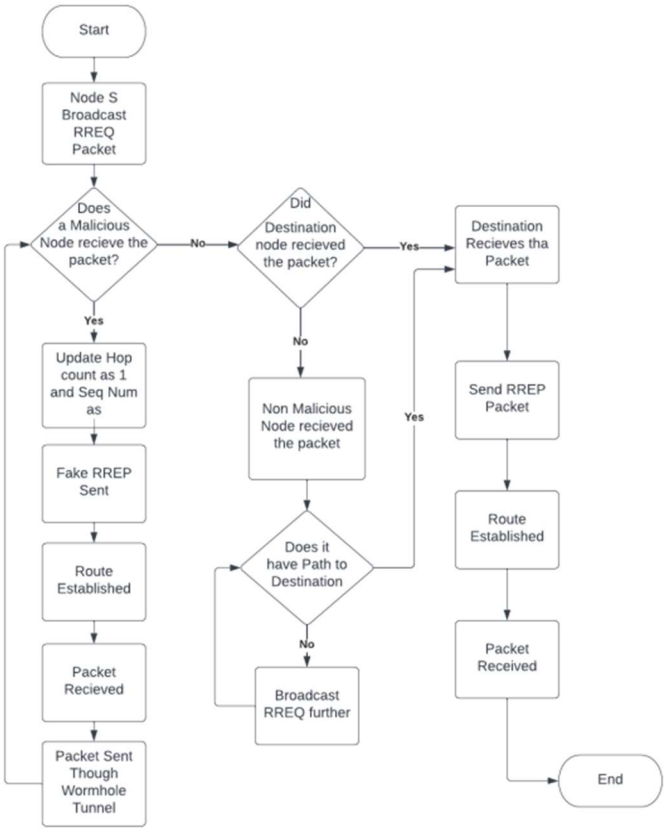
- Checking for Destination loop continues till Destination address is found.

WORMHOLE ATTACK:

two farflung malicious nodes can join forces using either a physical connection or a directional antenna to make it appear as though they are just one hop apart. In both covert and participation modes, wormhole assaults can be launched . So fighting against these attacks is very important for a secure network environment.

So this was where the problem was identified and this is where we will work on.

Flowchart & Algorithm-



- Packet Broadcasted from S
- if (Malicious node Received packet)
  - -HopCount and Seq Updated to 1 and Max;
  - -Fake RREP is sent;
  - -Packet is sent through wormhole tunnel;
  - -Checking for checking Malicious Node received Packet is done
  - - END

Else

If (Destination node Received Packet)

-Destination Received the packet;

-RREP Sent;
-Packet Received;
Else
If (non-malicious packet has Destination address)
-Destination Receives the packet;
- END
Else
-RREQ is Further Broadcasted;
- Checking for Destination loop continues till
Destination address is found.

6. METHODOLOGY/PROCEDURE

For Blackhole attack, we are going to initialise a Trust based Boolean value, based on the trust value, if the value is less than a threshold, then we are going to make it as an attacker node. Else it stays as a normal node. The attacker value is initialized to false, if the node is an attacker node, the attacker value is updated to true and the packet corresponding to that node are dropped. The node first uses such as the
AODV protocol, to say all nodes that it has a correct route to a target. The use of the AODV Protocol route by a node with the goal of interception of packets is bogus. Second, The Node which exploits AODV Protocol route consumes the intercepted packets. If there is no error, the compilation is successful.

For Wormhole attack, the bad point in network is going to receive packets at one point in the network and they are going to be tunnelled to some other part of the network and are now replayed into the network from that node onward. In case of our proposed structure using AODV, this particular attack could be launched by tunnelling every single request to the target directly. When the destination's nearby nodes receive this REQUEST packet, they rebroadcast it and ignore any other REQUESTS for the same route discovery, as per standard protocol.
So, after performing the attack on created scenario, we record the values related to the attack as statistics using a Third-party software like Trace graph.

Later the simulation of a scenario happens with attack mitigated. These values are also recorded by the same software. Then a Comparison of values of both these scenarios (i.e., with attack, With Attack Mitigated) in

both the attacks (i.e., Blackhole attack, Wormhole attack) is done in trace graph with help of graphs and tables.

7. EXPERIMENTAL SETUP

Firstly, For Both the attacks, we need to download a simulator for the work. In this we are using ns-2.35 simulator for the project.
So for that we need to first download ns-allinone-2.35.tar.gz which is the zip file for all packages related to ns-2.35. Before unzipping it, we need to upgrade the packages in the ubuntu.

Installation of ns-2.35:

- For that we are using "sudo apt install build-essential autoconf automake libxmu-dev".
- Next as for the project, we are using ubuntu 16.04, we will get some errors due to compatibility of gcc of latest version in that . So we dowload gcc-4.8 "Sudo apt install gcc-4.8 g++-4.8".
- Next we will unzip the ns-2.35 using "tar zxvf ns-allinone-2.35.tar.gz"
- Next we need to change cc to gcc-4.8 and cxx to g++-4.8 in ns2/makefile.in, nam, otcl-1.14 files.
- To check the installation, go to the directory and use "ns". if we get %, its working.

Type"nam" to open Network Animator.

Installation of Tracegraph –

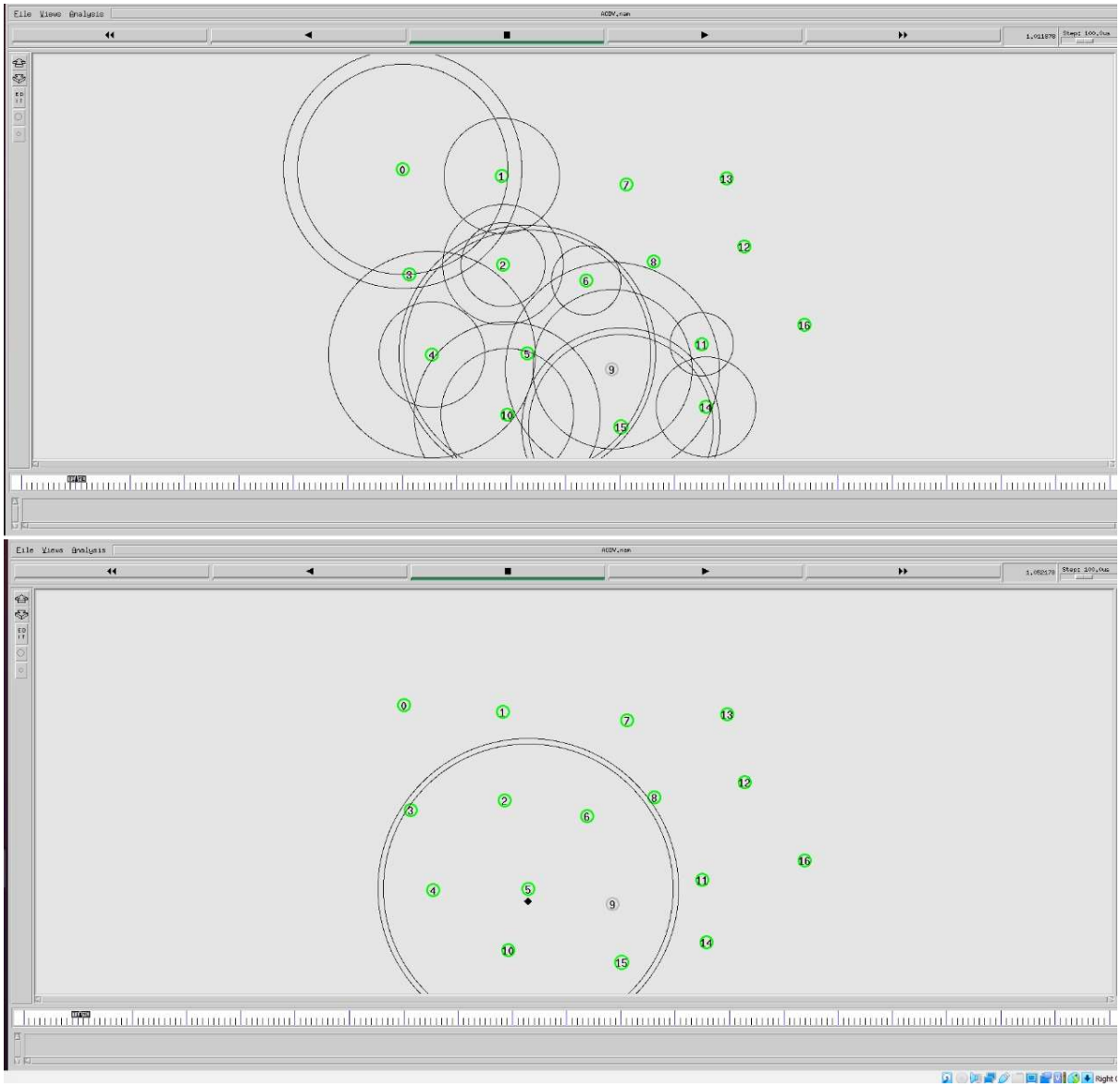
- First we need to download the zip file related to tracegraph202.tar.gz
- We need to unzip using tar xvzf tracegraph202.tar.gz
- After unzipping, go to the directory and run ./trgraph
- This will initiate the tracegraph.
- 3 Windows open for the tracegraph.

After Installing these, we can perform the attacks.

<u>Blackhole Attack:</u>

- First, we are going to edit 2 files in ns-2.35 which we downloaded before.

We will be using aodv.h and aodv.cc . We are going to modify these files according to the black hole attack.
- We created an attacker variable with a trust value. It is initalized to false.
- Later we configure the code such that what happens to attacker variable if the node is attacker.
- Later we write the code for actions of node when its attacker. We added code to showcase how the packets are being dropped.
- Then we created a TCL file to create a network topology with number of nodes as our wish.



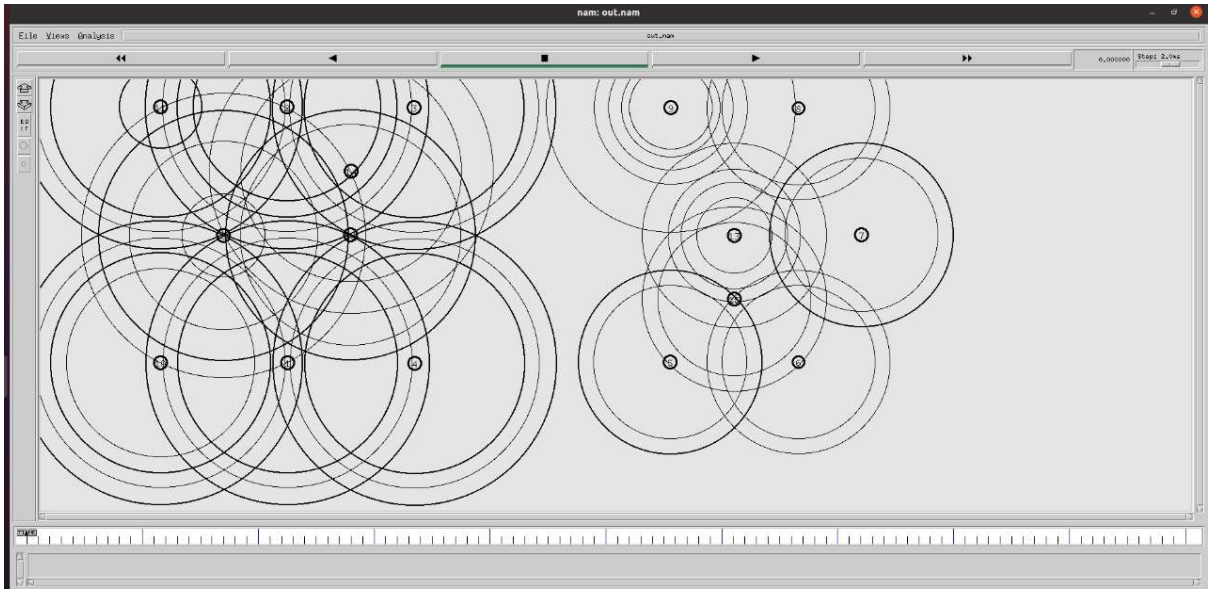
```
nishanth@nishanth-VirtualBox:~/Downloads/ns-allinone-2.35/ns-2.35/aodv$ ns AODVb
lack.tcl
num_nodes is set 17
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Packets dropped by node number 5 is 0
Packets dropped by node number 5 is 1
Packets dropped by node number 5 is 2
nishanth@nishanth-VirtualBox:~/Downloads/ns-allinone-2.35/ns-2.35/aodv$ Cannot c
onnect to existing nam instance. Starting a new one...
```

- Later once the attacker node is enabled and code is ready, we are going to see the demo of how this works using ns-2.35 network animator.

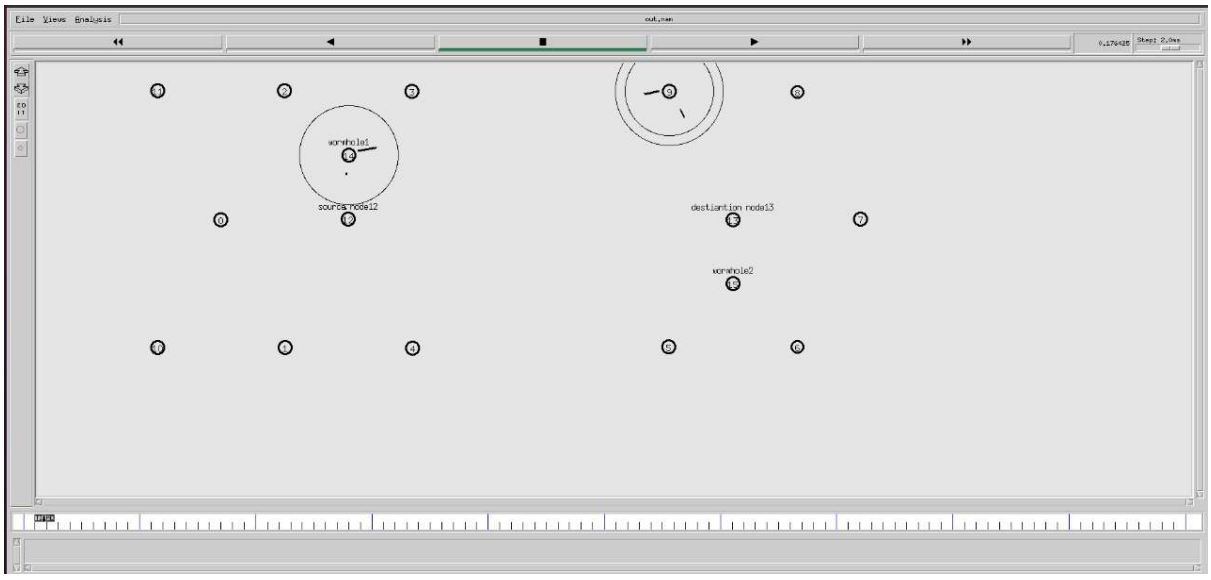
Here After the attack is performed, If we check the terminal , it shows the statements about packets dropping. In our code, we kept Node 5 as malicious node. So that's the reason Node 5 is dropping packets in the network.

Wormhole Attack –

- First, we are going to edit 2 files in ns-2.35 which we downloaded before. We will be using arp.cc, ll.cc, ll.h we are going to modify these files according to the black hole attack .
- Here in arp.cc, we will be adding codes related to the wormhole attack. We are going to specify some actions to do during the attack.
- In ll.cc also we are going to add some code like to initiate the wormhole peer list head and also specifying some actions during attack.
- In ll.h , we specified some codes related to defining of elements for wormhole peer list . In this we are going to enable class LL.
- Once all the codes are done, we have to run the demo by creating a topology in TCL file. We are going to specify the number of nodes.



So here if we see, Node 12 is sending packets to destination node in network . In AODV protocol, the node sends data by sending it to nearby nodes. This is done so that to ensure only some packets are dropped. But in the simulation, it is observed that in between source node 12 and Destination node 13, Node 14 is sending packets. So here it is the wormhole node.



```
nishanth@nishanth-VirtualBox:~/Downloads/ex-wormhole-1-20221107T133749Z-001/ex-w
ormhole-1$ ns 2worm14.tcl
num_nodes is set 16
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 0.2,  distCST_ = 763.1
SORTING LISTS ...DONE!
nishanth@nishanth-VirtualBox:~/Downloads/ex-wormhole-1-20221107T133749Z-001/ex-w
ormhole-1$
```

8. RESULTS AND DISCUSSION

BLACKHOLE ATTACK-

Before the attack is performed

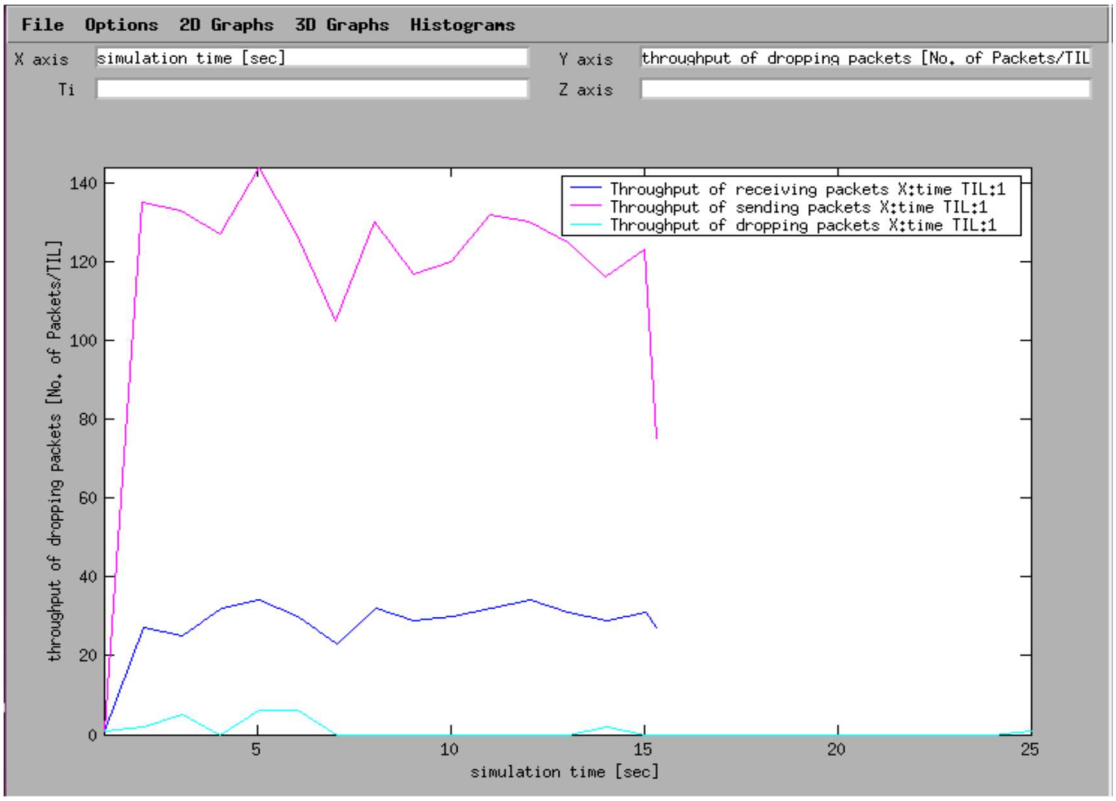


Fig - 1(a) Tracegraph Simulation of Network before Attack is Performed

Contains Graphical comparision between Throughputs of Receiving packets , Sending packets , Dropping packets .This is done using Tracegraph. In the TCL file , Removing the attack and keeping the TR file as GoodAODV.tr , we can run the simulationusing command " ./tracegraph202/trgraph GoodAODV.tr" . This will result in the tracegraph simulation of network saved before the attack. The Pink Line Shows the Throughput of Sending packets,Blue line represents Thorughput of Receiving packets , Cyan Line represents Throughput of Dropping Packets. This is done by Ovelay of graph.

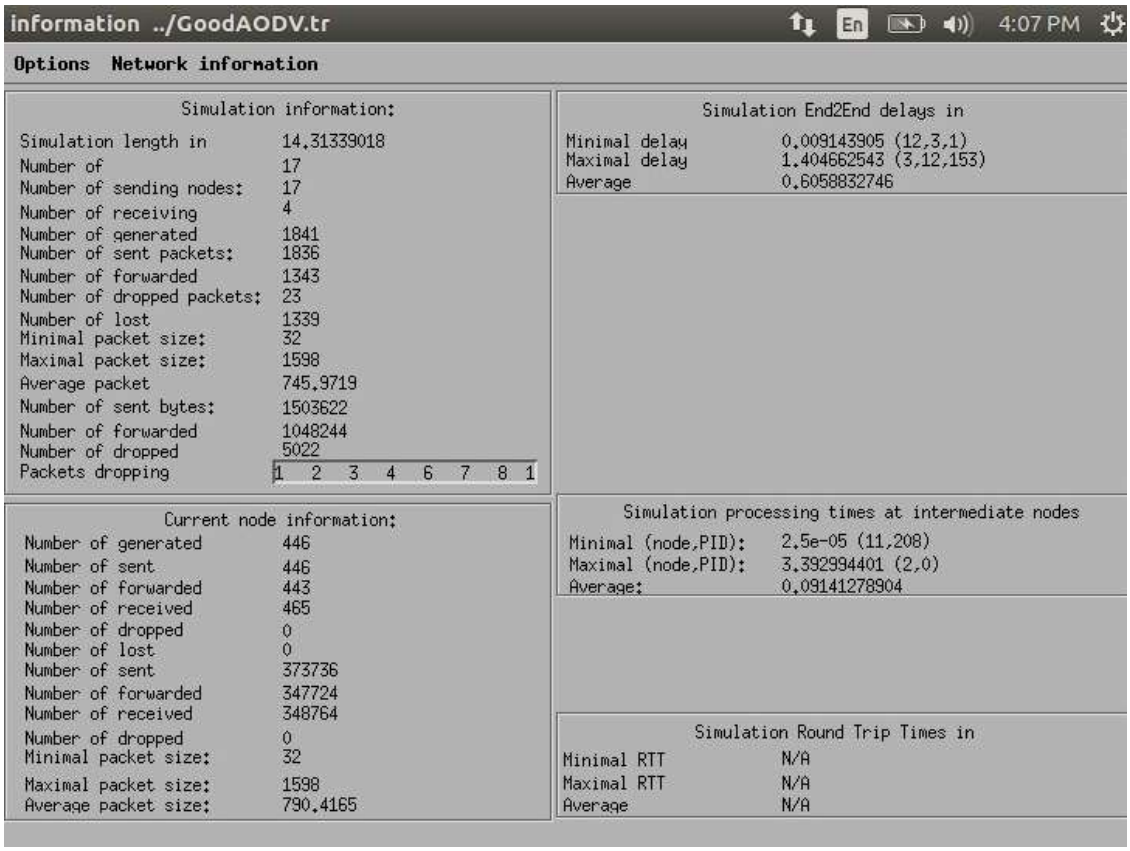


Fig 1(b) - Network Information of the Network when no attack is performed

To get the simulation information related to packets, we can open the Network Information window and select the required parameters information. In **Fig-1(b) ,**We haveused parameters like Simulation Information , Current Node Information , End-to-End Delay ,

Simulation Processing Time , RoundTrip Times. Here if we observe the number of packets dropped at the current node , it is 0 . So as there is no attack, The Number of packets dropped are minimal. So using these kind of parameters is useful for comparison

After Blackhole Attack is Performed:

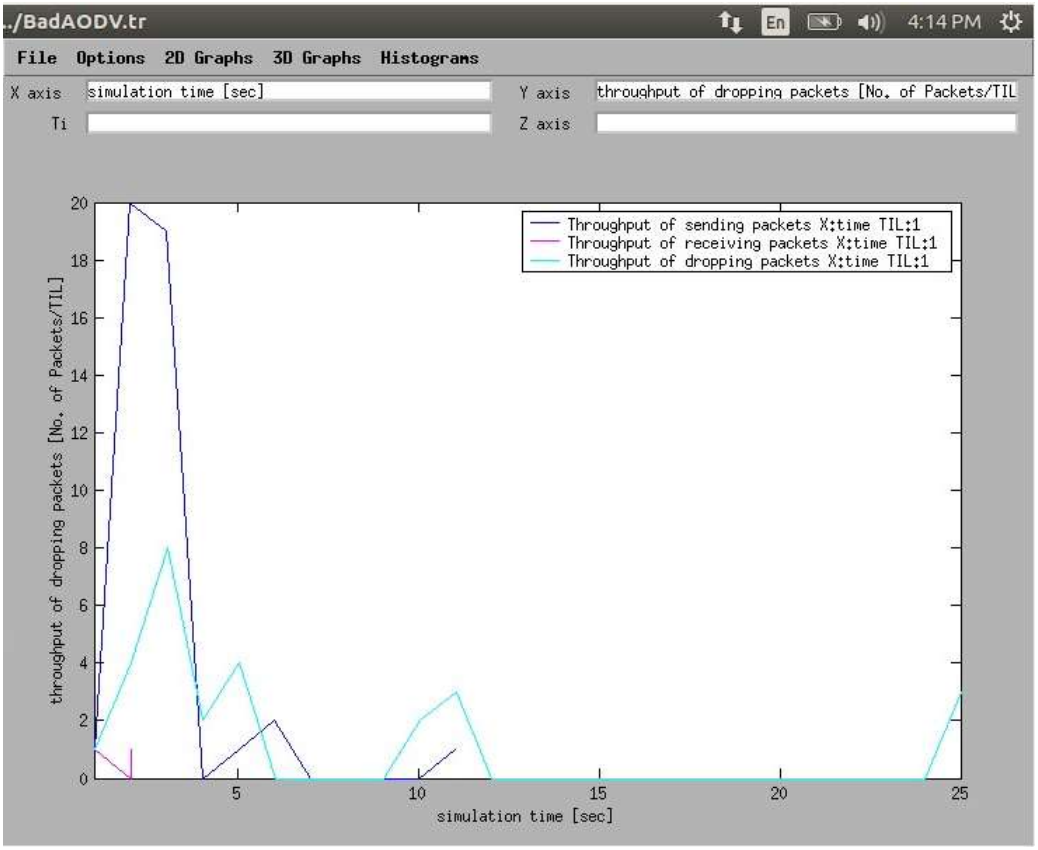


Fig -2(a) - Tracegraph Simulation of Network After Attack is Performed

Fig-2(a) Contains Graphical comparision between Throughputs of Receiving packets , Sending packets , Dropping packets .This is done using Tracegraph. In the TCL file , Removing the attack and keeping the TR file as BadAODV.tr , we can run the simulation using command " ./tracegraph202/trgraph BadAODV.tr" . This will result in the tracegraph simulation of network saved before the attack. The Blue Line Shows the Throughput of Sending packets,Pink line represents Thorughput of Receiving packets , Cyan Line represents Throughput of Dropping Packets.This are done by Ovelay of graph. So here comparing the Throughput with those before the attack , The Throughput of packethad varied much . This variation is due to the

attack.

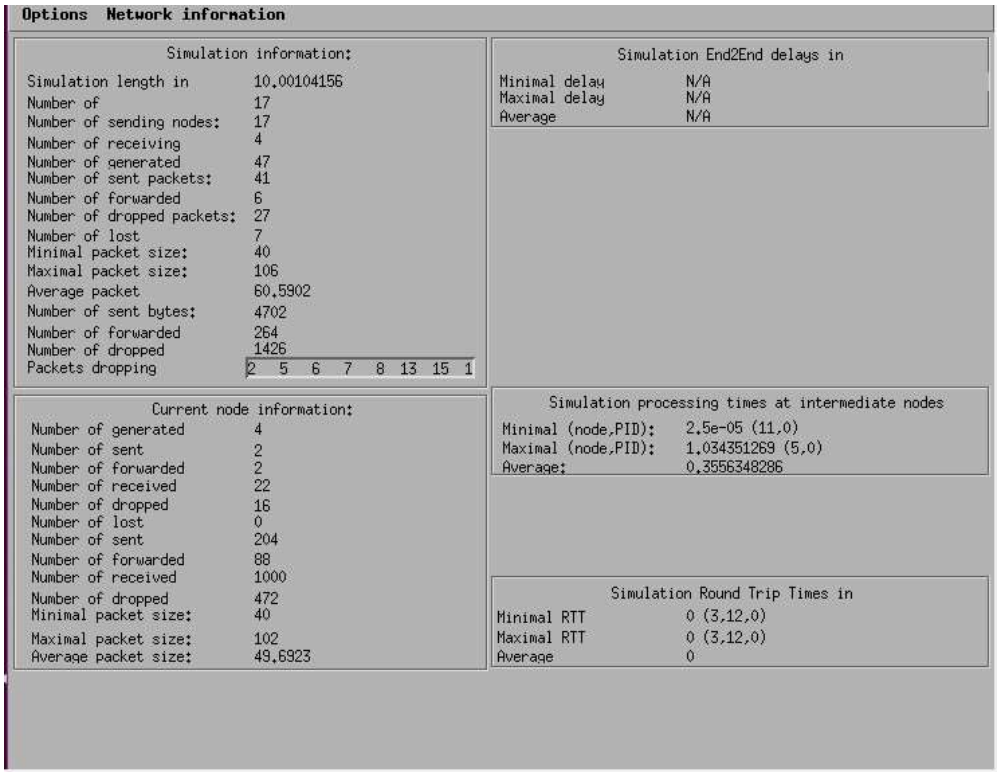


Fig-2(b) - Network Information of the Network After attack is performed

To get the simulation information related to packets, We can open the Network Information window and select the required parameters information. In **Fig-2(b)** We haveused parameters like Simulation Information, Current Node Information, End-to-End Delay, Simulation Processing Time, Round-trip Times. Here if we observe the number of packets dropped at the current node , it is 472 . So as there is attack, The Number of packetsdropped have increased from 0 to 472. So this rise of number of Dropping packets will prove the attack is performed

WORMHOLE ATTACK:

Before Attack is Performed :

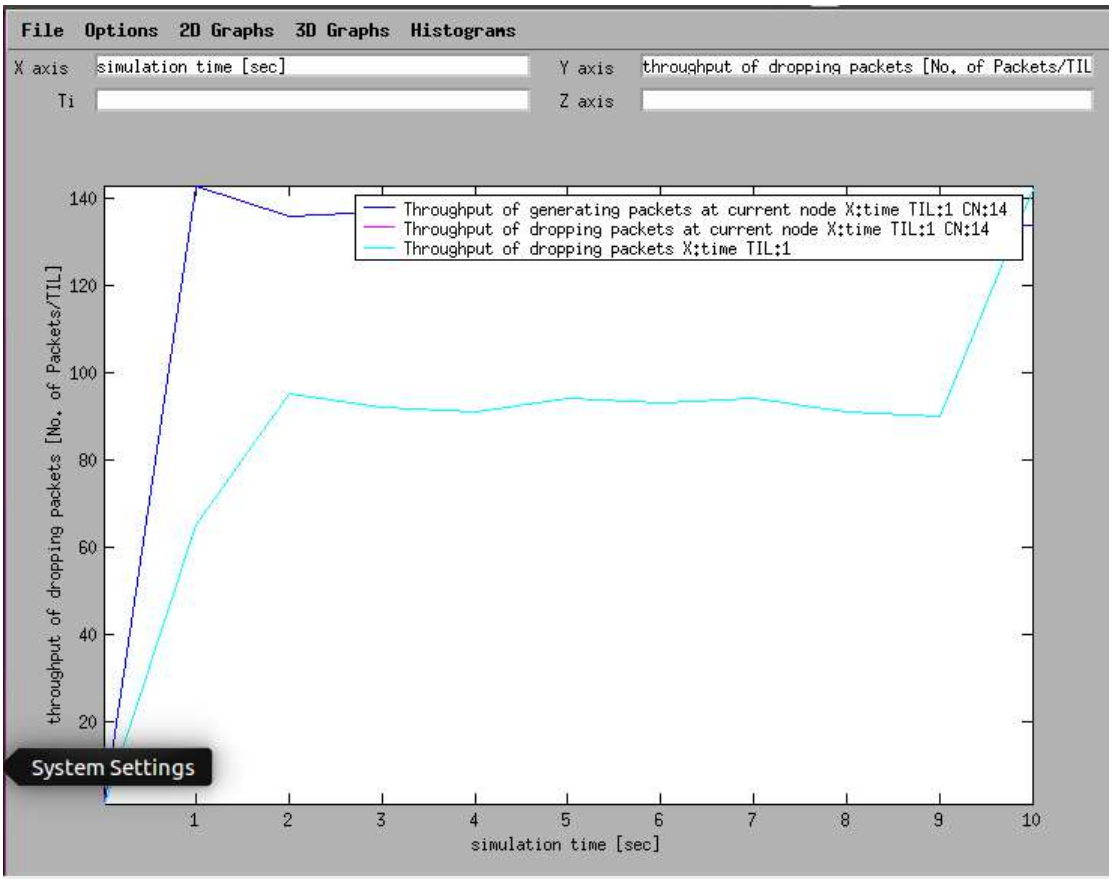
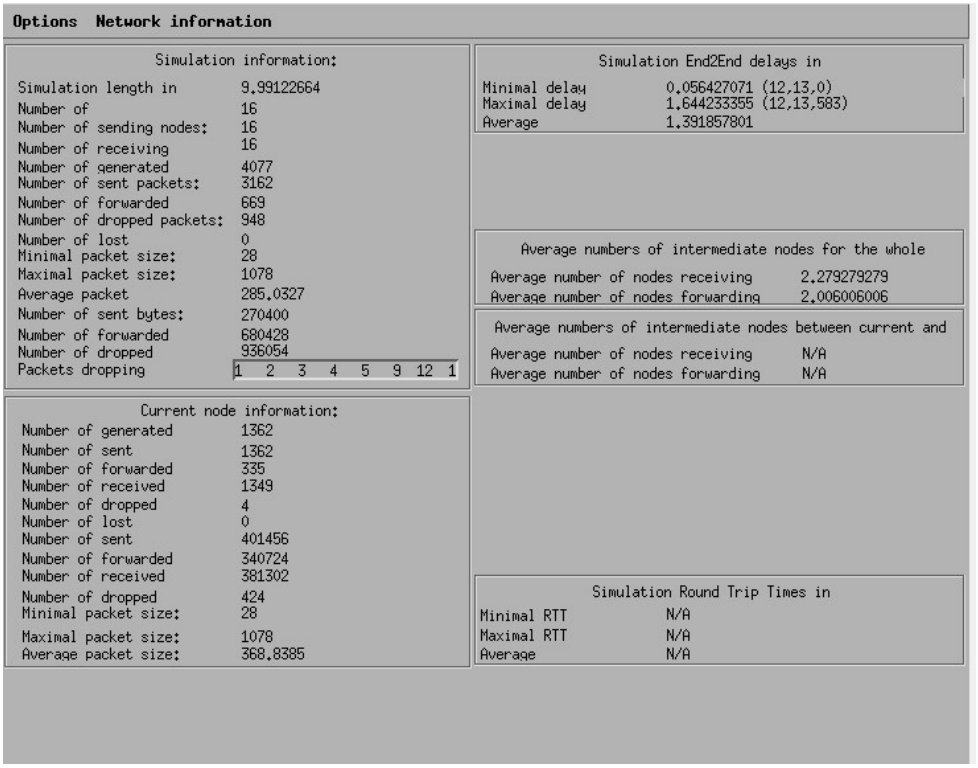


Fig-3(a) - Tracegraph Simulation of Network Before Attack is Performed

Fig-3(a) Contains Graphical comparision between Throughputs of Receiving packets , Sending packets , Dropping packets .This is done using Tracegraph. In the TCL file , Removing the attack and keeping the TR file as wormgood.tr , we can run the simulation using command " ./tracegraph202/trgraph wormgood.tr" . This will result in the tracegraph simulation of network saved before the attack. The Pink Line Shows the Throughput of Dropping packets at current node ,Blue line represents Thorughput of Generating packets at current node , Cyan Line represents Throughput of Dropping Packets. This

are done by Overlay of graph.



To get the simulation information related to packets, We can open the Network Information window and select the required parameters information. In **Fig-3(b),** We haveused parameters like Simulation Information , Current Node Information, End-to-End Delay, Average numbers of intermediate nodes, RoundTrip Times. So, using these kind of parameters is useful for comparison.

After Attack is performed:

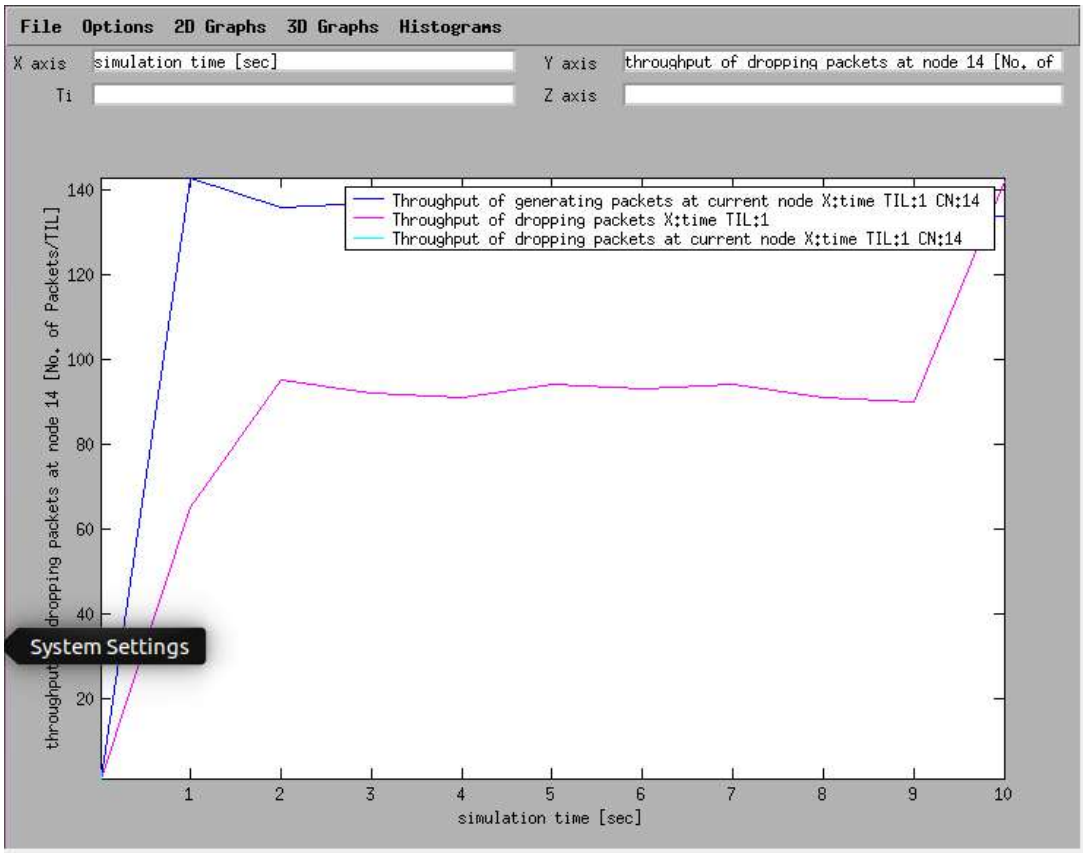


Fig -4(a) - Tracegraph Simulation of Network After Attack is Performed

Contains Graphical comparision between Throughputs of Receiving packets , Sending packets , Dropping packets .This is done using Tracegraph. In the TCL file , Removing the attack and keeping the TR file as wormattack.tr , we can run the simulationusing command " ./tracegraph202/trgraph wormattack.tr" . This will result in the tracegraph simulation of network saved before the attack. The Cyan Line Shows the Throughput of Dropping packets at current node, Blue line represents thorughput of Generating packets at current node, Pink Line represents Throughput of Dropping Packets.This are done by Ovelay of graph. So here comparing the Throughput with those before the attack, The Throughput of packet had varied much. This variation is due to the attack.

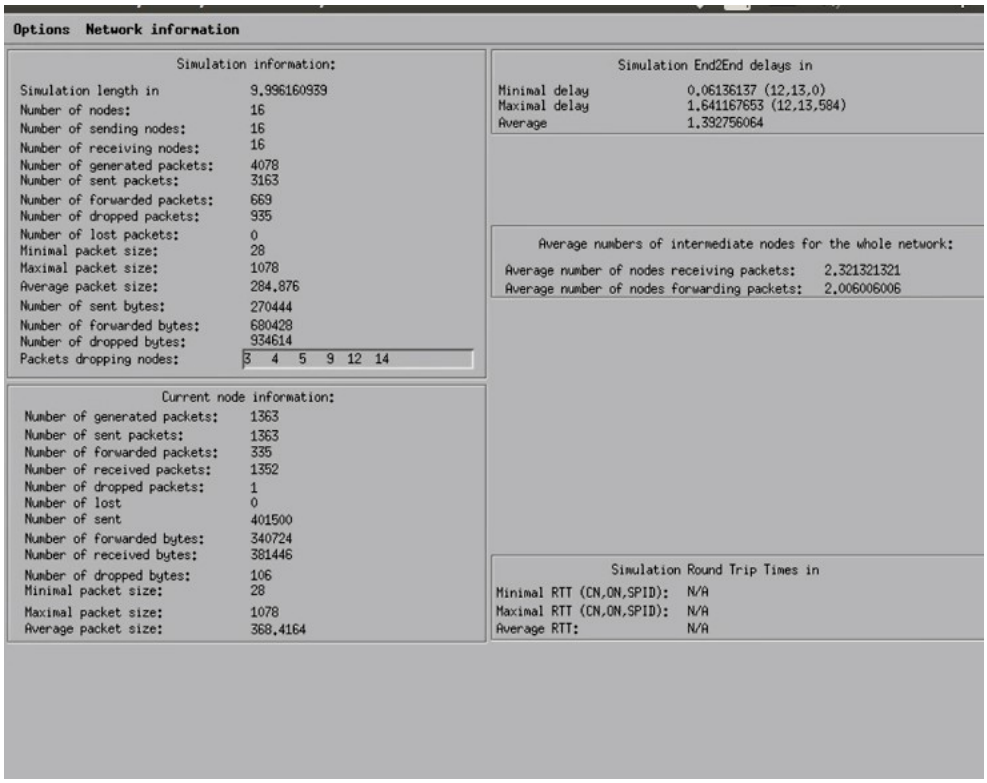


Fig-4(b) - Network Information of the Network After attack is performed

To get the simulation information related to packets, we can open the Network Information window and select the required parameters information. In **Fig-4(b) ,** We haveused parameters like Simulation Information, Current Node Information, End-to-End Delay, Average numbers of intermediate nodes, RoundTrip Times .

9. FINDINGS

We used parameters like Simulation Information, Current Node Information, End-to-End Delay, Simulation Processing Time, RoundTrip Times. Here, we observe the number ofpackets dropped at the current node , before and after the attack.

In blackhole attack, we observe the number of packets dropped before and after the attack, so at the current node, it is 472. After the attack, the

Number of packets dropped increased from 0 to 472. So, this rise of number of dropping packets will prove the attack is performed.

In wormhole attack, the receiver node does not receive any packets, instead redirects all the packets to some other node.
Throughput using trace graph has also been recorded for both the attacks which shows that there is a sudden change after the attack(represented by pink and blue lines)

10. CONCLUSION AND FUTURE WORK

In our Project, by implementing certain improvements to AODV, we were able to provide adequate protection against Black hole attacks; the activities to be performed in each node are very simple; the algorithm is based on asynchronous and autonomous communication of agents; it is self-organising, thus robust and fault tolerant; it is inherently traffic adaptive without the need for complex metrics; and it is self-organising.

The black hole attack is not only identified, but also avoided, by applying a threshold factor to AODV. As a result, utilising AODV(with predefined threshold factor) as a routing scheme in MANETS ensures that black hole attacks are avoided.

Our protection approach detects rogue nodes, separates them from active data transmission and routing, and alerts their neighbours by issuing ALARM packets. We also believe that with additional in-depth study and some AODV add-on capabilities, other security dangers may be recognised and, to some degree, averted, similar to how we suggested for the black hole assault. Our research combines a lot of works in the field of mobile and ad hoc networks in order to identify and avoid two key attacks on the AODV, namely the black hole and the worm hole assault.

Many writers have already addressed numerous ways for detecting network black holes. A technique for identifying the presence of black holes in the system may be identified based on the verification of the token serial number.
An extra parameter, such as "timer," can be included with each RREQ and RREP packet to keep track of each visit of these packets to each node, in addition to the detection parameter. The timing table will be very

valuable in finding nodes that are consuming packets or not delivering packets to other nodes, as well as detecting network black holes.

Future Works describes an easily deployable black hole attack for the MANET and an effective technique for isolating the multiple black hole attack. In Future work, we may focus on the proposed method, which can be compared with some other intrusion detection methods for mobile peer-to-peer networks. Malicious nodes that increase network latency. We are also doing the wormhole attack for higher topologies such that our approach can be used by some higher users.
We are evaluating the impact of a black hole attack on MANETs and WSNs. Further work is needed to study how to mitigate the effects of black hole attacks. We are also trying to improve the technique with many more attacks which are growing concern now a days. We are trying to extend the attacks and mitigation from black hole and wormhole to other attacks also.

11. REFERENCES

[1] Sherif, Bismin V., and P. Salini. "Effective and Prominent Approaches for Malicious Node Detection in MANET." In 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA), pp. 1-6. IEEE, 2021.

[2] Yasin, Adwan, and Mahmoud Abu Zant. "Detecting and isolating black-hole attacks in MANET using timer based baited technique." Wireless Communications and Mobile Computing 2018 (2018).

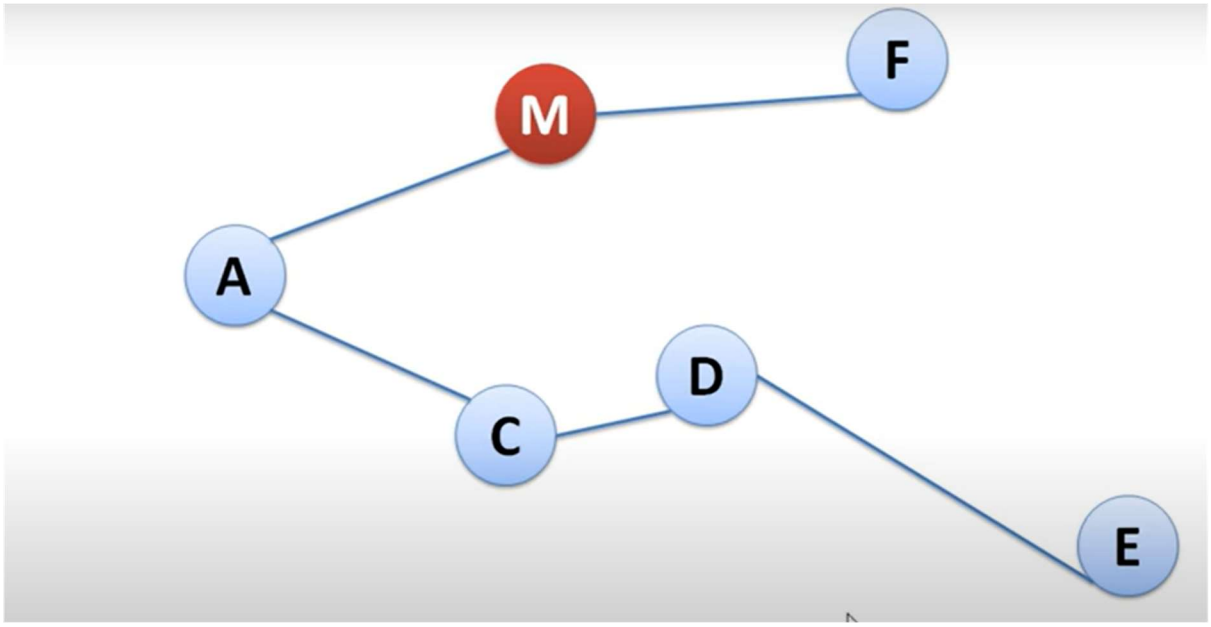
[3] Islabudeen, M., and M. K. Kavitha Devi. "A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks." Wireless Personal Communications 112, no. 1 (2020): 193-224.

[4] Patel, Kajal S., and J. S. Shah. "Detection and avoidance of malicious node in MANET." In 2015 International Conference on Computer, Communication and Control (IC4), pp. 1-4. IEEE, 2015.

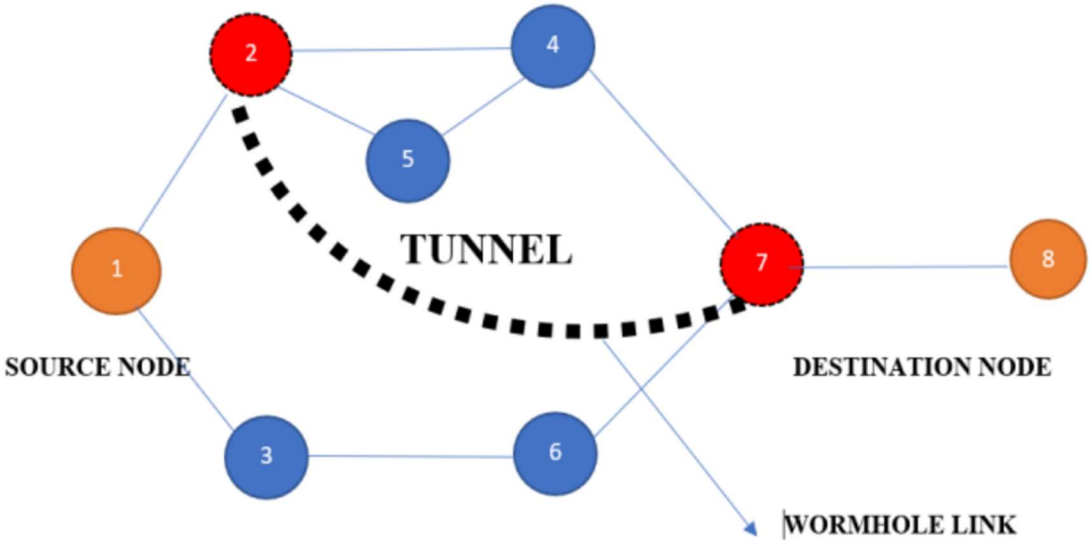
[5] Parvinder, Dalveer Kaur, and Rajiv Mahajan. "Wormhole attack detection technique in mobile ad hoc networks." Wireless Personal Communications 97, no. 2 (2017): 2939-2950

[6] Rahman, Mohsin Ur, Sohail Abbas, and Seemab Latif. "Lightweight detection of malicious nodes in mobile ad hoc networks." In 2017 International Conference on Communication Technologies (ComTech), pp. 191-194. IEEE, 2017.

12. APPENDICES



Blackhole attack



Wormhole attack