International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

A Modified AODV based Wormhole Detection Using Hop Count and Packet Sent and Receiving Ratio in MANETs

M.Ramya[1], P.Nagarjuna Reddy[2], M.Triveni[3], M.Ratheesh[4], Y.Adi Lakshmi[5]

[1,2,3,4]UG Scholar, Dept. of Computer Science Engineering, Gudlavalleru Engineering College, Andhra Pradesh, India
[5]Associate Professor, Dept. of Computer Science Engineering, Gudlavalleru Engineering College, Andhra Pradesh, India

---

Abstract - *The remote correspondence is well known these days .The remote advances gives quick organization and the remote gadgets are anything but difficult to haul around and needs less support.MANETs are turning out to be increasingly basic using because of their simplicity of organization. Manets have dynamic framework on account of this security is an extremely challenging issue in MANET, there is a high chance that the middle nodes can be vindictive and they may be a danger to the security. Wormhole is one of the most every now and again happening attacks in adhoc systems. In wormhole attack, the attacker gets packets at one point in the system and passages them to another piece of the system and replays them into the system starting there forward.The proposed framework is a proficient identification and anticipation strategy of wormhole attack with AODV convention. Recognition of wormhole attack is finished utilizing number of hops ,delay per hop and number of packets sent and got at every node. Prevention of wormhole attack is finished utilizing verification of nodes. Simulations are finished utilizing NS2 arrange test system.*

***Key Words*: Wormhole Attack, MANET, AODV protocol, Network Security, HopCount, Packets sent and received.**

1. INTRODUCTION

Portable Ad-hoc Network (MANET) is a gathering of remote versatile hosts without fixed system framework and brought together organization. Multi-hop packets are utilized to set up correspondence in MANET. A portable adhoc arrange is a gathering of versatile nodes, which shapes a temporary and these nodes regularly have a fractional communicated go and, thus, every node seeks after the assistance of its contiguous nodes in quickening packets and from this time forward the nodes in an impromptu system can turn as together switches and has. Subsequently a node may forward packets among different nodes as fine as track client applications. Naturally these kinds of systems are reasonable for circumstances where either no unmoving structure exists or situating system isn't conceivable. In our everyday life the need of the buyer is expanding as far as speed and quick conveyance of information. A remote system shows a huge job in current period for imparting information with irrelevant overhead and incomparable conceivable speed. These frameworks have grown efficient with the layout of portability thought of nodes.

But MANET is a difficult field: MANET comprises of various assets; the line of defence is extremely questionable;Nodes work in shared remote medium; Topology changes unpredictably and powerfully; Reliability in the radio connection is an issue; association breaks are frequent. Additionally, the density of nodes, number of hosts and portability of these hosts may fluctuate in various applications.

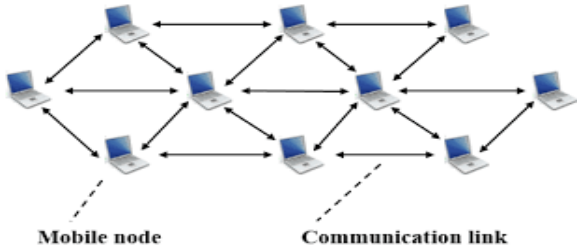

Fig -1: Mobile Ad-hoc Network

MANET has a few vulnerabilities, for example, Resource accessibility, Scalability, Bandwidth requirement, Limited power supply, Cooperativeness and Dynamic Topology. In MANET, all frameworks organization limits, for instance, coordinating and pack sending, are performed by centers themselves in a self-sifting through way. Therefore, making sure about a portable promotion ad-hoc arrange is a challenging task. The objectives to assess if versatile specially appointed system is secure or not are Availability, Confidentiality, Integrity, Authentication, Non denial and Authorization.

The expanding prevalence and use of remote innovation is making a requirement for progressively secure remote systems. Remote systems are especially defenseless against a Powerful attack known as the wormhole attack, which is one of the risky attacks. Wormhole attack is a grave attack where in two attackers find themselves deliberately in the system. At that point the assailants continue tuning in to the system, and record the remote data. The underneath figure shows the two attackers are situated in a solid vital situation in the system.

In wormhole attack, the attackers put themselves in ground-breaking key spot in the system. They use their area, that is, they have most limited course among the

nodes as. They advance their course to different nodes in the system to report them they have the most brief course for moving their data. So as to recording the continuous correspondence and traffic at one system position and channels them to another situation in the system the wormhole attackers make a passage.

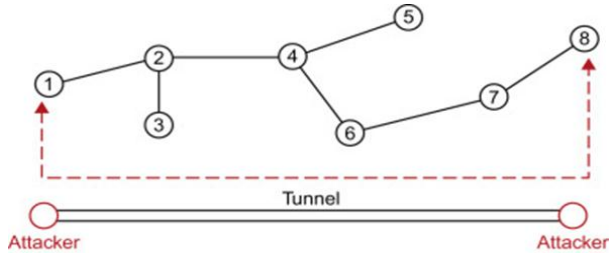

Fig -2: Wormhole Attack

There are two types of wormhole attack that occur in a network. They are In-band wormhole attack and out-of-band wormhole attack.

In-band wormhole attack: In this wormhole attack, the assailant assembles overlay burrow over the current remote medium. This attack is a lot of perilous and assailant most wants to pick this one.

Out-of-band wormhole attack: In this wormhole attack, the assailant nodes make an immediate connection between one another in the system, at that point the wormhole aggressor at one side gets bundles and moves them to the opposite side of the system.

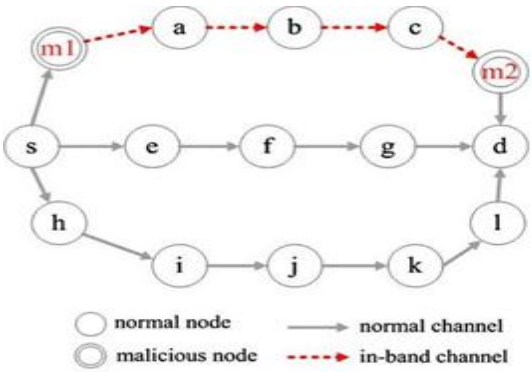

Fig -3: In-band Wormhole Attack

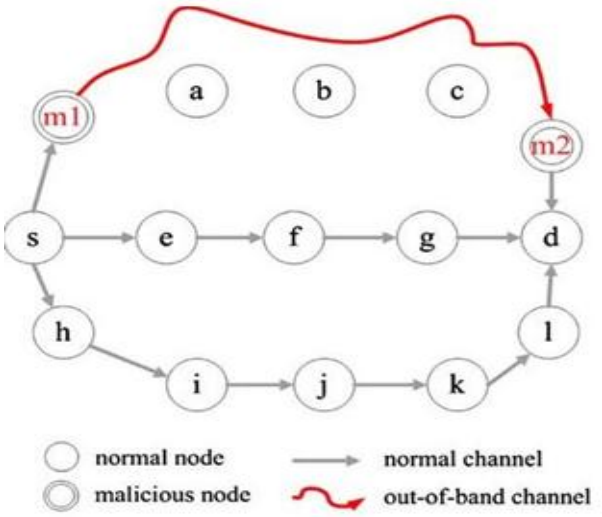

Fig -4: Out-of-band Wormhole Attack

2. RELATED WORK

Hu and Evans et al. developed a "protocol using directional antennas to prevent wormhole attacks". Directional receiving wires can in this convention, two nodes convey realizing that one node ought to get messages from one edge and the other ought to get it at the contrary point. This convention fails just if the attacker deliberately positioned wormholes living between two directional antennas[1].

Another localization scheme known as the coordinate system involves the work done by Nagpal, Shrobe and Bachrach et al. at Massachusetts Institute of Technology (MIT). It utilizes a subset of GPS nodes to give nodes without GPS a feeling of relative area. This is accomplished utilizing two algorithms: The angle which gauges a GPS node's bounce include from a point in a system, and multilateration, which decides the manner in which GPS nodes spread data of its area to nodes without GPS. Hop counts tell how far a node is from a specific source. A flaw in utilizing this plan is that wormholes can upset hop counts inside a system. Hence, any framework following this plan is rendered helpless under wormhole attacks.

Rouba El Kaissi et al. obstacles impede the successful deployment of sensor networks. Notwithstanding the constrained assets issue, security is a significant concern particularly for applications, for example, home security checking, military, and combat zone applications. This paper presents a protection system against wormhole attacks in remote sensor networks[2].

Y. C. Hu et al. have considered "packet leashes – geographic and temporal". In geographic leashes, area data of node is utilized to bound the separation a packet can cross. Since restriction is influenced by wormhole attack, the area data must be acquired by means of an out-of-band system, for example, GPS. In temporal leashes, incredibly exact all inclusive synchronized tickers are

utilized to bound the proliferation time of bundles that could be difficult to get especially in ease sensor hardware. Even when accessible, such planning investigation will most likely be unable to distinguish sliced through or physical layer wormhole attacks[3].

Yudhvir Singh et al. utilizes DSR convention to discover malevolent nodes productively. The Dynamic Source Routing (DSR) explicitly intended for use in multi-hop remote specially appointed system. The DSR convention doesn't require any current system foundation or focal organization and is totally self sorting out and self-configuring. But, DSR convention builds the system load[4].

Zubair Ahmed Khanuses et al. an altered steering table that will help in the recognizable proof of malignant connections. Since we know routing tables are utilized to look after courses, we are proposing an answer wherein we will consider changes made to the courses and the full way from source to end. By doing this we can quickly distinguish a potential wormhole connect when it is made. By enabling the nodes to investigate/share each other's directing tables we can likewise recognize the potential wormholes. It assists with recognizing malevolent nodes rapidly since the hub which is generally utilized is considered. But, no counteraction procedure is mentioned[5].

A Vani et al. proposed an answer that joins the techniques for hop count, choice abnormality and neighbor list check strategies for AODV convention. The procedure relies on progressive handling of hubs and their neighbors. They utilized the hop count include present in the steering table of nodes, this will necessitate that we have to store two duplicates of directing table of every node so that to monitor past hop counts[6].

3. PROBLEM DEFINITION

A MANET is a portable impromptu system which is an collection of independent nodes that speak with one another by keeping up radio associations in a decentralize way. Security is a significant issue for MANET because of its qualities :-

Dispersed Operation: There is no foundation organize for the focal control of the system activities; the control of the system is circulated among the nodes. The nodes associated with a MANET ought to help out one another and convey among themselves and every node goes about as a transfer varying, to actualize explicit capacities, for example, routing and security.
Dynamic Topology: Nodes are permitted to move discretionarily with different paces; as such, the framework topology may change subjectively and at impulsive time.The nodes in the MANET progressively establishing their own network.

Common Physical Medium: The remote correspondence medium is open to any substance with the fitting hardware and sufficient assets. In like manner, access to the channel can't be limited.

So as to give security administrations, for example, Confidentiality, Integrity, Authorization we are attempting to give a protected framework by utilizing redesigned AODV Protocol.

A defected node working in the system gets packets at one area and passages them to another area in the system, where these packets are changed and resent into the system. The passage that is between two scheming attackers is alluded to as a wormhole. The principle extent of this undertaking is to identify nearness of a wormhole in the system and build up a procedure with the goal that different nodes acknowledge what the undermined divert in the system is, and subsequently dodge that way for sending information. Move of smart packet through the system will deceive the plotting vindictive nodes to send a reaction for that packet, and hence we can comprehend what the compromised path is. The project depends on ns2 as it were. Nowadays there is a colossal should be shielded from malignant attacks on the system, which are continually attempting to take client information. Since a great deal of correspondence happens through MANET, it is required to create systems to forestall these attacks.

4. PROPOSED SYSTEM

The proposed system aims at finding a safe path for sending packets for information correspondence. This procedure focuses around the location of acting up nodes and attempts to forestall the wormhole attack on the system by preventing those nodes to utilize the current directing way and select an elective way by again following the course revelation strategy for the equivalent. In this strategy for wormhole evasion, existing AODV convention is altered with the usefulness of wormhole attack discovery and anticipation.

In proposed structure, an arrangement to recognize wormhole attack in the remote framework by get-together number of and deferral hop count and delay per hop information, number of packets sent and got at each node from different ways from source to goal and destination to source, which offers a response for perceive the two sorts of wormhole attack for instance In-band wormhole attack and Out-of-band wormhole attack.

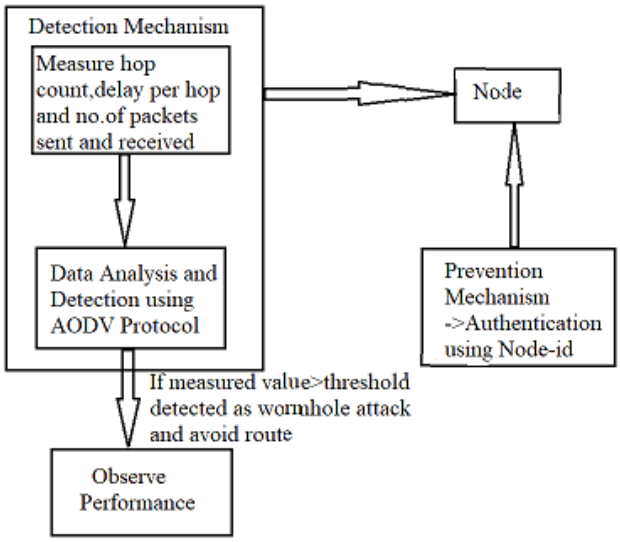

Fig -5: Architecture for Detection and Prevention of Wormhole Attack

Architecture for detection and prevention of wormhole attack contains mainly three steps. They are:-

1)Detection Mechanism

2)Prevention Mechanism

3)Observe Performance

In Detection Mechanism, wormhole attack is detected using AODV routing protocol. It is done by calculating hop count, delay per hop and packets sent and received at each node. After gathering the required information, detection process is done by using AODV protocol. If the measured value > threshold value then wormhole attack is detected i.e. the selected path contains malicious nodes so we need to select another path and repeat the above process to know whether the path is wormhole attacked path or wormhole free path.

In Prevention Mechanism, each transmitting and getting node has its own node id. Node-id is started and verified utilizing lightweight cryptography calculation known as ceaser cipher which info is changed over into cipher message by applying some arithmetical activity and at the recipient end invert activity is done to get back the first content. Every single approved node know about the normal key. Hence only approved nodes can create legitimate mark and it won't produce any blunder at the recipient side. Aggressors mark will be identified as invalid at collector side.

In Observe Performance, evaluation of the data is carried out on the basis of throughput, delay, packet delivery ratio, packet drop.

1)Detection Mechanism

In Detection Mechanism contains mainly two steps. They are:-

i) Measure hop count, delay per hop and packets sent and received at every node

ii)Data Analysis and Detection using AODV Protocol.

i)Measure hop count, delay per hop and packets sent and receives at every node

First step: We need to calculate the information like delay and number of hop count from the network. For information gathering, sender needs to send RREQ packet to the receiver which is shown in fig.6

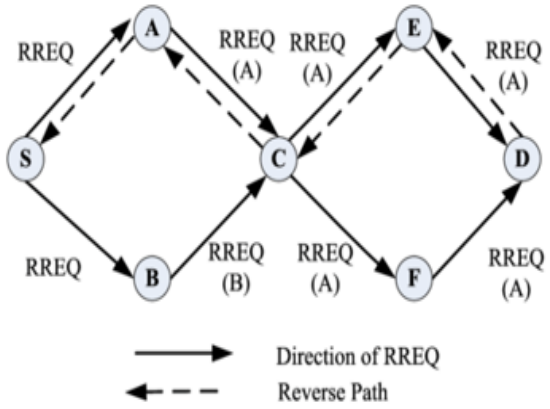

Fig -6: RREQ roadmap

Second step: After receiving the RREQ packet from the sender, receiver sends RREP packet to the sender.

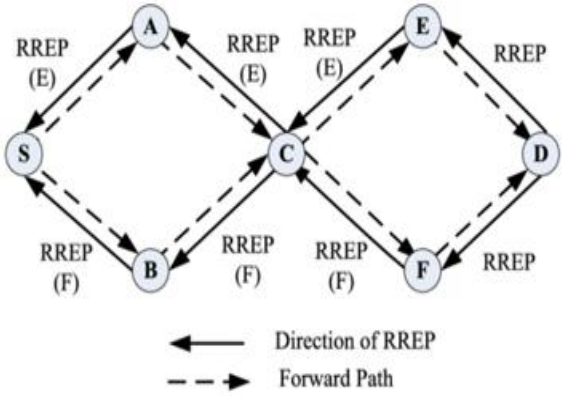

Fig -7: RREP roadmap

Third step: After gathering all the information, detection process starts by the sender node. Suppose RREQ packet sent at time Ts by the sender node and received RREQ packet at time Tt. Ht is the hop count field, PT is propagation time given by

$$PT = Tt - T$$

Delay per hop value is calculated as follows, if the hop count field in the RREP from node is Ht then the delay per hop value of the path to the destination through node is given by

$$DPH = Tt - Ts/Ht$$

By using Poisson process, no. of packets sent and received at every node is calculated.

No . of packets sent = p / (1-p)

No . of packets received = p2 / (1-p)

Where p = λ / μ , here p is Traffic Rate

λ is Arrival Rate

On an average, WSλ packets sent at a node and the average time WS spent at the node.WQ (average number of packet arrivals during the time spent in the queue is λWQ and the average time WQ spent in the queue.

ii)Data Analysis and Detection using AODV Protocol

On the basis of Delay per Hop value from the Measurement of delay and hop value, the detection of wormhole attack is analyzed and the proper decision is taken in that situation. The scenario under the legal situation, the delay for each packet is same along each hop in the path. But under the wormhole attack, for every packet lagging time should be huge. The reason behind is there can be many nodes available between them or can be attached through a long wireless link. The path which is under the wormhole attack is having large delay than the normal path. On the basis of packets sent and received at node, when the no. of packets sent at a node is more and no. of packets received at another node is more then those two nodes are malicious nodes which transmit data packets through tunneling.

Detection of wormhole attack is done using AODV protocol. The steps that are done using AODV protocol is shown in fig. 8.

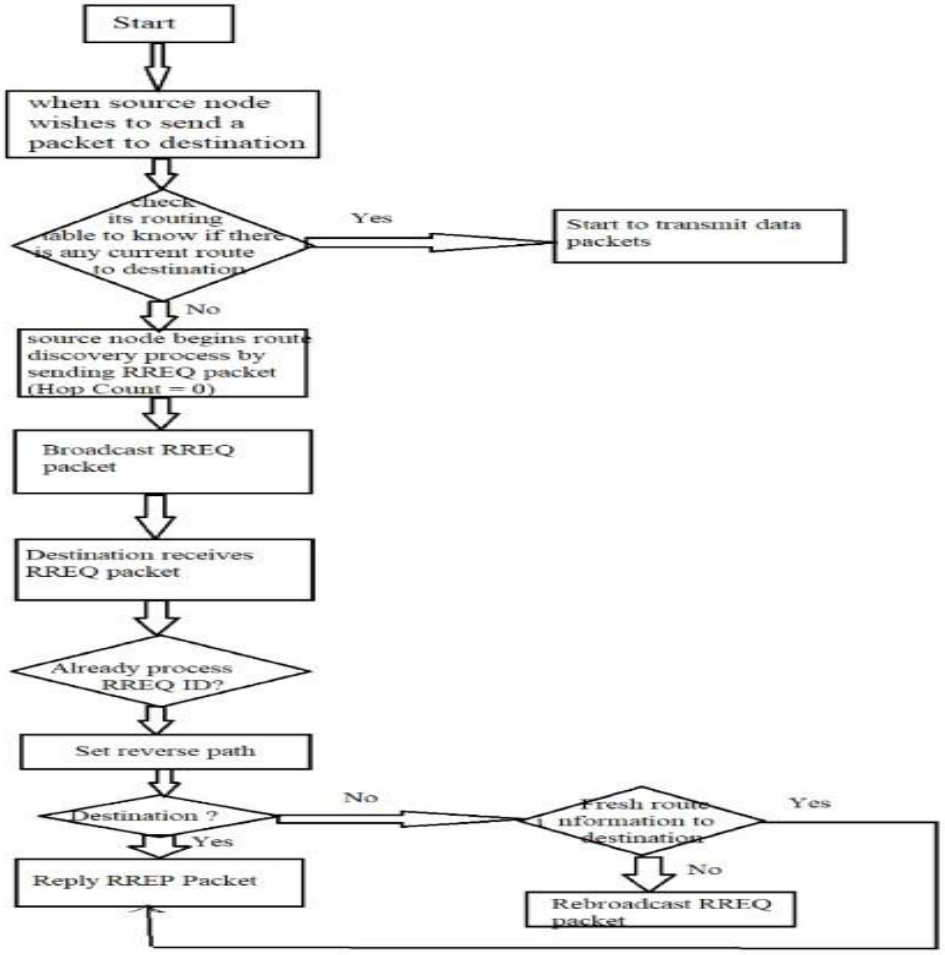

Fig -8: Flowchart for AODV Routing Protocol

In AODV route discovery, there are two important control messages namely Route Request (RREQ) and Route Reply (RREP).Source sends RREQ packet to destination in the process of route discovery. At the point when a node establishes that it has a present course to react to RREQ i.e. has a path to destination .It creates RREP (Route Reply) packet and it can be sent either by any intermediate node or by the destination.

After the selection of path, every node in the path calculates Round Trip Time values based on the time HELLO messages sent and received. And also every node in a path executes per hop distance with its neighbour.

If the per hop distance exceeds the maximum threshold range then check for the maximum count a link takes part in the path. If the count of a link takes part in a path is more than the defined value (FAcount > FATh), then the link is wormhole i.e. Wormhole Attack is detected. The

neighboring node gives feedback to other nodes in a network to know about the attack in a network.

After detecting wormhole attack, we need to detect the malicious nodes on the basis of no. of nodes sent and received that are calculated. The node at which no. of packets sent are more is one of the malicious nodes and the node at which no. of packets received are more can be identified as another malicious node. And also we can detect malicious nodes, on the basis of above calculated data, we are trying to avoid single hop nodes which are connected to malicious nodes in a network. By the use of distance formula we can measure the X and Y co-ordinates of the nodes in a network. With this information about nodes single hop distance node near wormhole node will be found out.

2) Prevention Mechanism

a) Blacklist of Malicious Node: When the source node gets the encoded answer and the wormhole presence is affirmed, we have to remove the malevolent nodes so no further correspondence happens with them and henceforth they are blacklisted.

b) Alert Generation and Communication: Upon the affirmation of wormhole, both end nodes communicates a blacklisting message. This message contains rundown of malignant nodes to be avoided from correspondence and not to engage any way update or any future solicitation from them.

Keep up a table of blacklisted nodes. At the point when the source node gets the smart packet and the wormhole presence is affirmed, we have to confine the noxious nodes from the system so no further correspondence happens with them and henceforth are blacklisted.

When the malicious node is detected which is the part of the attack then we need to update other nodes about the attack. For the avoidance of wormhole attack, each transmitting and accepting node has its own hub id.. Node-id is initiated and verified using lightweight cryptography algorithm known as ceaser cipher in which input is converted into cipher text by applying some arithmetical operation and at the receiver end reverse operation is carried out to get back the original text. Every single approved node know about the basic key Hence only authorized nodes can generate correct signature and it will not produce any error at the receiver side. Attackers signature will be identified as invalid at receiver side. Different nodes are educated about the noxious nodes and about the wormhole present between them. Safe way is examined by applying anticipation calculation and evasion system is applied.

5. RESULTS

```
set val(chan)          Channel/WirelessChannel;      # channel type
set val(prop)          Propagation/TwoRayGround;     # radio-propagation model
set val(netif)         Phy/WirelessPhy;              # network interface type
set val(mac)           Mac/802_11;                   # MAC type
set val(ifq)           Queue/DropTail/PriQueue;      # interface queue type
set val(ll)            LL;                           # link layer type
set val(ant)           Antenna/OmniAntenna;          # antenna model
set val(ifqlen)        50;                           # max packet in ifq
set val(nn)            16;                           # number of mobilenodes
set val(rp)            AODV;                         # routing protocol
set val(x)             1440;                         # X dimension of topography
set val(y)             100;                          # Y dimension of topography
set val(stop)          10.0;                         # time of simulation end
#set val(wormholes) 1;
```

Fig -9: Simulation Parameters

In the above figure, Simulation Parameters of the network that is implemented in NS2 are shown.

Fig -10: Command for executing the file in NS2

First, one need to redirect to the folder in the terminal where our file with .tcl extension is placed. Then execute the file by using 'ns filename' command.

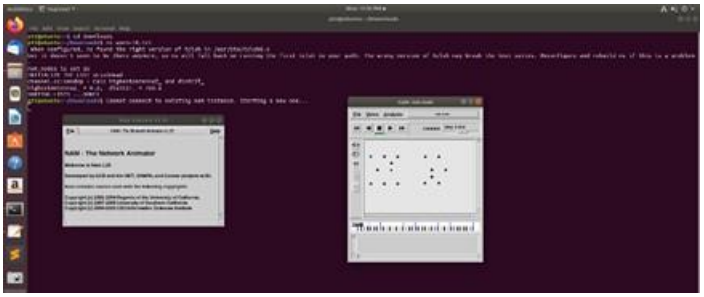

Fig -11: After executing the command, NAM file is generated

NAM document is a different program which is disseminated with NS2 test system to peruse an info record and draw the system occasions graphically. It is utilized to picture the movement of bundles through the Network.

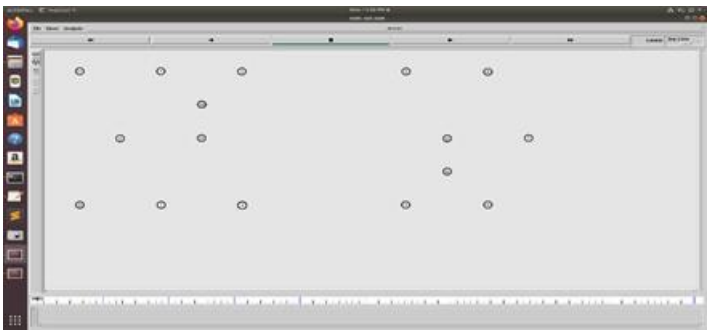

Fig -12: Simulation of 15 nodes in a network

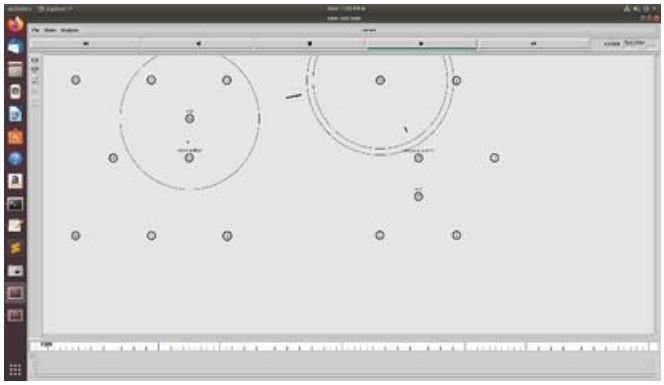

Fig -13: Simulation of AODV Routing Protocol

AODV Routing Protocol is simulated by sending RREQ packets from source to destination and by receiving RREP packets from destination to source.

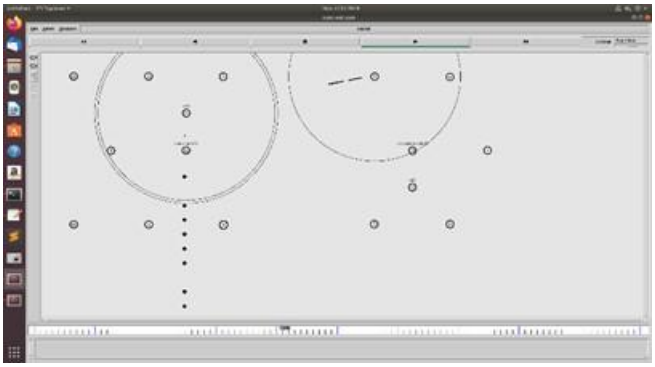

Fig -14: Wormhole Attack is Detected

Wormhole Attack is detected using hop count, delay per hop and no. of packets sent and received at every node.

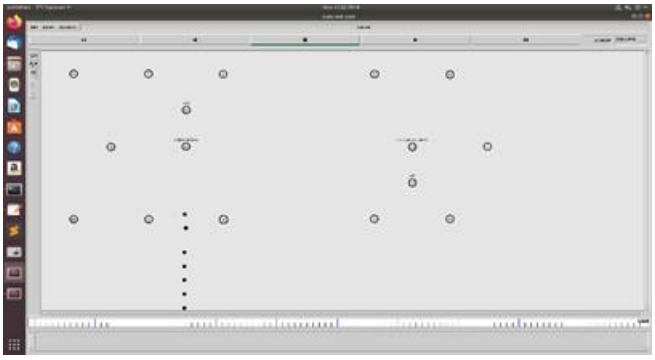

Fig -15: Wormhole nodes are detected so another wormhole free path is selected for data transmission

Once the wormhole attack is detected, that wormhole nodes are isolated from the network and another wormhole free path is selected for data transmission.

6. CONCLUSION

A wormhole is one of noticeable attack that is shaped by malignant colluding nodes. Wormhole attacks in MANET can fundamentally debase systems execution and undermine arrange security. The discovery and avoidance of such wormholes in a specially appointed system is as yet viewed as a difficult undertaking. Proposed strategy doesn't require extraordinary equipment like antenna to get exact node position and data, clock synchronization. Discovery strategies are finished utilizing hop count, delay per hop and packets sent and got at every node at various ways in the system. When the wormhole attack is recognized, maintain a strategic distance from that way and select new wormhole free way for transmission of information. Avoidance of wormhole attack is finished by authentication which is accommodated secure information transmission.

REFERENCES

[1] L. Hu and D. Evans, "Utilizing directional radio wires to forestall wormhole assaults," in Proceedings of the Network and Distributed System Security Symposium.
[2] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy,"Dawsen: a defense mechanism against wormhole attacks in wireless sensor networks", IN Second International Conference on Innovations in Information Technology (IIT'05).
[3] Y. C. Hu, A. Perrig, and D. Johnson, "Packet Leashes: a resistance against wormhole assaults in remote systems," in INFOCOM, 2003
[4] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, DheerDhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks" in 2012 Third International Conference on Advanced Computing & Communication Technologies.
[5] Zubair Ahmed Khan, M. Hasan Islam, "Wormhole Attack: another identification method", Electrical & Computer Engineering Department, Center for Advanced Studies in Engineering (CASE), Islamabad, Pakistan.
[6] A.Vani, D.Sreenivasa Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), 2011, Vol. 3 No. 6, pp. 2377-2384, June 2011