Detection and Avoidance of Wormhole Attack in MANET

Dhruva Patel, Parth Trivedi, Dr. M.B Potdar

Abstract— The wireless mobile Ad-hoc network (MANET) is self-configuring mobile nodes connected through the wireless links with the decentralized networks where the nodes communicate with each other on the basis of mutual trust. For the network design, nature of the MANETs brings a new security challenges. Due to the dynamic infrastructure less nature and decentralized networks, wireless Ad-hoc networks are unprotected and vulnerable to the attack. This paper focuses on the study of the wormhole attack and avoidance of it. In this paper detection and avoidance techniques of wormhole attack are implemented in MANET routing protocol namely TORA as reactive routing protocol. The performance of TORA is compared without wormhole attack, with wormhole attack and after avoidance of wormhole attack. Performance metrics used for evaluation are throughput, delay and packet delivery ratio. The technique is based on the nodes quality index value. Simulation done with 16 nodes and in these two nodes considered as malicious node in Network Simulator2 (NS2).

Index Terms— MANET; TORA; Wormhole Attack

1 INTRODUCTION

HIS document is a Mobile ad-hoc network is a temporary network without using any centralised administration and with no pre-defined infrastructure. MANET network is defined by collection of mobile nodes that can communicate with each other using dynamic links. Mobile ad-hoc networks are uniquely characterized by some factors that differentiate them for conventional wired or wireless networks in terms of absence of a fixed infrastructure, mobility and limited bandwidth[1]. MANET must have a secure transmission and communication and this is the challenging and important issue as there is increasing threats of attacks on MANET. The securities of MANET are threatened due to its dynamic topology and mobility of nodes. In MANET nodes can freely join or leave the network because there is no central administration. In MANET there are many security attacks are possible like black hole attack, wormhole attack, grey hole attack, jellyfish attack etc. For our research purpose we consider wormhole attack and apply proposed algorithm in it

2 PROTOCOLS USED IN MOBILE AD HOC NETWORK [1]

Mobile ad hoc networks are basically classified into three categories based on how routing information is acquired and maintained while nodes freely roam and organize themselves in arbitrary fashion. These are:

2.1 Proactive protocol

Proactive routing protocols or table driven routing protocols maintain consistent and up-to-date routing information about each node in the network. Information is maintained in the form of routing table and when there is a change in network topology update has to be made throughout the network. Ex. DSDV (Destination-Sequenced Distance Vector Routing) protocol and OLSR (Optimized Link State Routing) protocol.
.

2.2 Reactive protocol

Reactive or on demand routing protocols, nodes only maintain the routes to active destinations. A route is established only on demand for every new destination. Therefore, the communication overhead is reduced at the cost of delay due to route search. Furthermore, the rapidly changing topology may break an active route and cause subsequent route search. Examples of reactive protocols are AODV (Ad hoc Distance Vector Routing) protocol and DSR (Dynamic Source Routing) protocol.

2.3 Hybrid protocol

All A hybrid protocol combines the characteristics of both the proactive and reactive routing protocols. An illustration of such a protocol is the Zone Routing Protocol (ZRP). In ZRP, topology is divided into zones and looked for to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols.

3 TEMPORARY ORDERED ROUTING ALGORITHM (TORA)

Operation: The TORA attempts to achieve a high degree of scalability using a "flat", non-hierarchical routing algorithm. In its operation the algorithm attempts to suppress, to the greatest extent possible, the generation of far-reaching control message propagation. In order to achieve this, the TORA does not use the shortest path solution, an approach which is unusual for routing algorithms of this type.
TORA builds and maintains a Directed Acyclic Graph (DAG) rooted at the destination. No two nodes may have the same

————————————————

- *Dhruva Patel is currently pursuing M.E in gtu pg School, Ahmedabad . E-mail: dhruva385@gmail.com*
-
- *Parth Trivedi is project Scientist at BISAG Gandhinagar. E-mail: prem30488@gmail.com*
- Dr.M.B. Potdar is Project Director at BISAG, Gandhinagar:
- E-mail:mbpotdar11@gmail.com

height.

Information may flow from nodes with higher heights to nodes with lower heights. Information can therefore be thought of as a fluid that may only flow downhill. By maintaining a set of totally ordered heights at all times, TORA achieves loop-free multipath routing, as information cannot 'flow uphill' and so cross back on itself.

Key design concepts of TORA is localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain the routing information about adjacent (one hop) nodes. The protocol performs three basic functions:

- Route creation
- Route maintenance
- Route erasure

During the route creation and maintenance phases, nodes use a height metric to establish a directed acyclic graph (DAG) rooted at destination. Thereafter links are assigned based on the relative height metric of neighbouring nodes. During the times of mobility the DAG is broken and the route maintenance unit comes into picture to re-establish a DAG routed at the destination. Timing is an important factor for TORA because the height metric is dependent on the logical time of the link failure.

TORA's route erasure phase is essentially involving flooding a broadcast clear packet (CLR) throughout the network to erase invalid routes.

4 WORMHOLE ATTACK

The wormhole attack is one of the most efficient attacks, which can be executed within MANET. There are two collaborating attackers should establish the wormhole link (using private high speed network e.g. over Ethernet cable or optical link): connection via a direct low-latency communication link between two separated distant points within MANET. When this wormhole link is built up one of the attackers captures data exchange packets, sends them via the wormhole link to the second one and he replays them.

In wormhole attack, a tunnel is created between two nodes which are used to secretly transmit data packets. In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network and then replays them into the network from that point. For tunnelled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunnelled packet arrive sooner than other packets transmitted over a normal multi hop route. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbour of) that node.[9]

Classification of Wormhole Attack:

In MANET it is difficult to detect such dangerous attacks and no one can predict what the wormhole nodes can do and where and when. At the higher layer wormhole attack is invisible; therefore two end points of the wormhole are not visible in the route in which detection becomes much more complex. Wormhole attack can be classified into five categories:

- Wormhole using Encapsulation.
- Wormhole using out of band channel.
- Open wormhole attack.
- Closed wormhole attack.
- Half open wormhole attack.
- Wormhole with high power transmission.

4.1 Wormhole Using Encapsulation In this mode of worm hole; a malicious node at one part of the network and hears the RREQ packet. It channels that packet to a second party at a distant location near the destination. The second party then rebroadcasts the RREQ packet; neighbours of the second party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multi hop paths.

4.2 Open wormhole attack In this attack malicious node keep examine the wireless medium to process the discovering RREQ packets, in the presence of malicious node in the network other node on the network suppose that malicious node are present on path and they are their direct neighbours.

4.3 Closed wormhole attack In this the attacker does not modify the capture packet nor did it modify the packet field head. The attacker takes the advantage when the packets are in the process to find a route known as route discovery. At route discovery process attack tunnel the packet from one side of the network to another side of the network and re-broadcast packets.

4.4 Half open wormhole attack In this attack only one side of the packet is modified from the malicious node and the other side of the malicious node do not modify the packet subsequently route discovery procedure.

4.5 Wormhole with high power transmission In this attack malicious node use maximum level of energy transmission to broadcast a packet, When malicious node received a Route Request (RREQ) by using route discovery process, it broadcast the Route Request (RREQ) at a maximum level of energy of it power so the other node on the network which are on the normal power transmission and lack of high power capability hears the maximum energy power broadcast they rebroadcast the packet towards the destination. By doing this malicious node get more chances to create a route between source and destination without using colluding [2].

5 LITERATURE SURVEY

Paper	**Protocol**	**Simulator**	**Technique**	**Result**	**Conference & Publication year**
A Lightweight Technique to Prevent Wormhole Attacks in AODV [3]	AODV	Network Simulator2 (NS2)	A light weight technique, a mobile backbone network is constructed from regular MANET nodes based on the nodes trust value. The backbone network is used to detect and remove malicious nodes based on monitoring other nodes in the MANET.	highly detect and remove the wormhole attack and gives the lowest total packet loss rate compared with AODV under attack and the other techniques.	International Journal of Computer Applications , October 2014
An Efficient Approach for Detection of Wormhole Attack in Mobile Ad-hoc Network [4]	AODV	Network Simulator2 (NS2)	In this, work divide into two phases in phase 1 describe the generation of wormhole attack and in phase 2 describe an efficient approach for analyzing and prevention of wormhole attack. In phase 2 the author used Neighbor list Detection Approach for Wormhole Attack:	wormhole attack in Mobile ad hoc network analyzed and prevented by using neighbor list based detection algorithm for wormhole attack in Manet.	International Journal of Computer Applications , October 2014
Multipath Algorithm For Prevention Of Wormhole Attack In Manet [5]	AODV	OPNET simulator	enhancing multipath algorithm resulting in regaining of the average no. of hops as well to get normal delay by excluding the attacker nodes and these factors will be implemented using existing multipath algorithm with relevant changes which can prevent Wormhole attacks in MANET networks	Module use to evoke the multipath properly of AODV process and hence eliminate the nodes by introducing the query messages to the neighbours and find the exact malicious nodes. Elimination of nodes takes place on Network layer by broadcasting the information of malicious nodes.	Journal of Advanced Studies and Communication Research, March 2014
Trust based solutions using counter strategies for Routing attacks in MANET [6]	AODV	NS2	The proposed routing algorithm adds a field which stores trust value or node's trust on its neighbours. Based on the trust value, the routing information will be transmitted to highest trust valued node. This method pertaining to mobile ad-hoc networks can provide secured routing and can also improve the network throughput.	computation overhead can be minimized and also trustworthiness of routing procedures can be guaranteed. Based on this trust factor, routing takes place. This saves nodes transmission power by avoiding unnecessary transmission and also its bandwidth.	International Journal of Innovative Science, Engineering & Technology, June 2014

6 Proposed Work

Because TORA is reactive routing protocol. For security of MANET we applied our proposed algorithm in to TORA routing protocol. It is a time based routing protocol. In this paper we propose detection and avoidance technique against wormhole attack for TORA. These techniques are based on following algorithm.

```
Step 1: select one transmitting node and one receiving node
Step 2: select route from transmitting node to receiving node
Step 3: give the quality index to each node in the network
Step 4: take one threshold value for quality index
Step 5: now start timer to count hop and delay
Step 6: if hop count increase than at least one malicious node in the network.
        If not
Step 7: check delay
Step 8: if delay increase than at least one malicious node in it
Step 9: now to find exact malicious node check the node frequency to sending packets
Step 10: if node frequency high> average frequency
Step 11: than decrease the quality index of selected node
Step 12: repeat the whole process to find exact malicious node
Step 13: if quality index <= threshold value than that node is the malicious
Step 14: for prevention blacklists the all malicious node and do not use in future
Step 15: for avoidance use another path for routing.
```

To avoid the wormhole attack, proposed algorithm has been implemented in scenario affected by wormhole attack and this tried to normalize the scenario to its original state. Proposed algorithm, randomly generate a number in between 0 to maximum number of nodes and make the node with same number as transmitter node as wormhole attack is done by transmitter and receiver so have to decide the transmitter and receiver. After that give the quality index to each node in the network and select one threshold value to count quality index. Then generate the route from selected transmitting node to any destination node with specified average route length. After this it will send packet according to selected destination and start timer to count hops and delay. By repeating the whole process up to this point will be required as to store routes and their hops and delay. Now for detection of malicious node; if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker. Algorithm checked the delay of all previous routes which involve any on node of the suspicious route. If delay of the route is increased than also at least one malicious node in the network. Now to find exact malicious node check the node transmission frequency. If node transmission frequency is greater than average node frequency than decrease the quality index of that node. Find all nodes frequencies which are involved in that route. If quality index goes to the threshold value than that node is the malicious node. for avoidance use another path for routing. In future for prevention, blacklist of all malicious nodes are checked and do not use that nodes in future routing process.

7 Exprementations

Basic parameters used for experimentation. Some of the experimentation done for checking the behaviour of AODV protocol under wormhole attacks are given below:

Examined protocols	TORA
Simulation time	1000 seconds
Number of Nodes	16
Number of malicious no	2
Traffic Type	TCP
Performance Parameter	Throughput, delay, Network load
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Tim	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

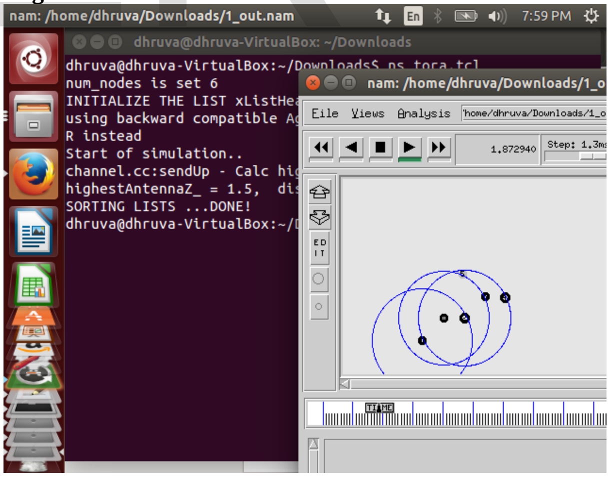
Results obtained for normal performance of TORA, Performance of TORA under wormhole attack and performance behaviour of TORA with avoidance of wormhole attack in term of throughput, delay and packet delivery ratio in TORA network is discussed in the following sections.

1.1 Implementation

As per our proposed work we start our implementation into two phases.

Phase 1: Patching TORA- Temporary Ordered Routing Algorithm in to ns2 and creating wormhole attack in it.
Phase 2: Apply the proposed algorithm in that.

Patching TORA


nam: /home/dhruva/Downloads/1_out.nam
En
7:59 PM
dhruva@dhruva-VirtualBox: ~/Downloads
nam: /home/dhruva/Downloads/1_o
File Views Analysis
'home/dhruva/Downloads/1_o
1.872940
Step: 1.3ms
EDIT

```
dhruva@dhruva-VirtualBox:~/Downloads$ ns tora.tcl
num_nodes is set 6
INITIALIZE THE LIST xListHea
using backward compatible Ag
R instead
Start of simulation..
channel.cc:sendUp - Calc hig
highestAntennaZ_ = 1.5,  dis
SORTING LISTS ...DONE!
dhruva@dhruva-VirtualBox:~/D
```

Fig 1: Patching TORA

Creating Wormhole Attack in TORA: For creating wormhole attack in to TORA we use 16 nodes. Here node 12 is the source node and node 13 is the destination node. In this network node 14 is the wormhole node. It forwards the packets to another node. As shown in the bellow figure

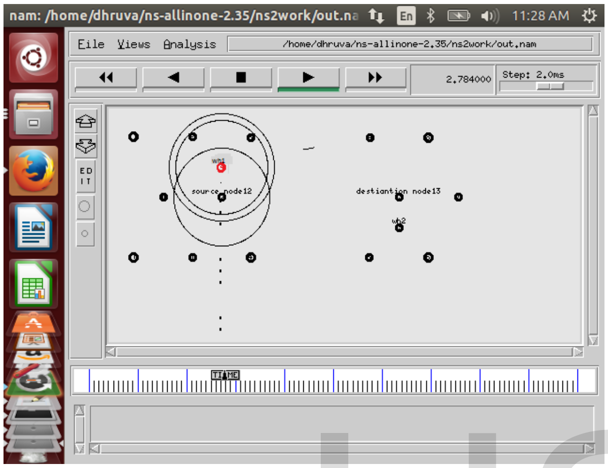

nam: /home/dhruva/ns-allinone-2.35/ns2work/out.na
11:28 AM
File Views Analysis
/home/dhruva/ns-allinone-2.35/ns2work/out.nam
2.784000
Step: 2.0ms
source node12
destiantion node13
wh1
wh2
TIME

Fig 2: Creating wormhole

Detecting Wormhole Attack: For detection of wormhole attack we applied our algorithm. In this we set Quality index value for each node and take one threshold value for compare the Q.I. for each node we set Q.I = 10 and we take 7 as threshold value. Now for detection we start our algorithm. As per algorithm we detect node 14 as wormhole node. So we decrease the Q.I for that node. Now Q.I for node 14 is 9. This is shown as following figure.

Fig 3: wormhole node detected at 2.78400sec (Q.I=9)

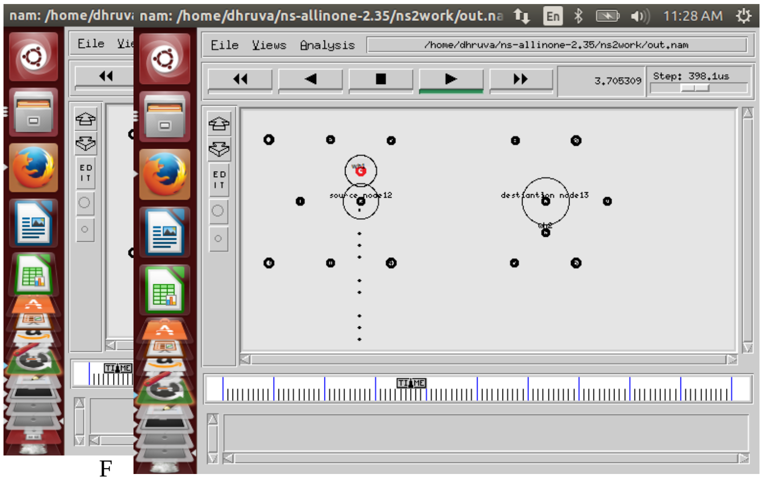

nam: /home/dhruva/ns-allinone-2.35/ns2work/out.na
11:28 AM
File Views Analysis
/home/dhruva/ns-allinone-2.35/ns2work/out.nam
3.705309
Step: 398.1us
source node12
destiantion node13
wh1
wh2
TIME

Fig 4: wormhole node detected at 3.705309sec (Q.I=8)

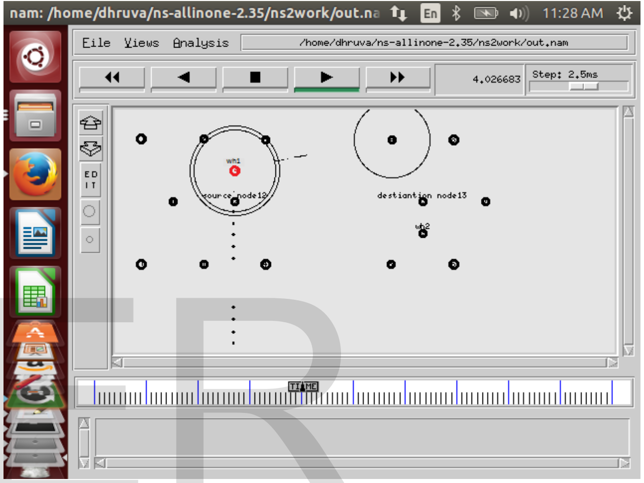

nam: /home/dhruva/ns-allinone-2.35/ns2work/out.na
11:28 AM
File Views Analysis
/home/dhruva/ns-allinone-2.35/ns2work/out.nam
4.026683
Step: 2.5ms
source node12
destiantion node13
wh1
wh2
TIME

Fig 5: wormhole node detected at 4.026683sec (Q.I=7)

The Q.I value goes at threshold value so the node 14 is detected as wormhole node and it is blacklisted and it will never use in future routes.

Avoidance of wormhole Attack: Now for avoidance the packets were sending from another route as shown below.

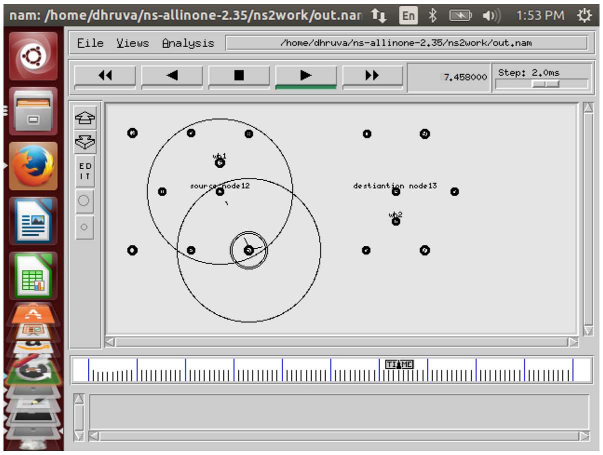

nam: /home/dhruva/ns-allinone-2.35/ns2work/out.nar
1:53 PM
File Views Analysis
/home/dhruva/ns-allinone-2.35/ns2work/out.nam
7.458000
Step: 2.0ms
source node12
destiantion node13
wh1
wh2
TIME

Fig 6: Route change for avoidance of wormhole attack

8 Results

Results obtained for Performance of normal TORA protocol, TORA under wormhole attack and performance behaviour of TORA with avoidance of wormhole attack in terms of packet delivery ratio, throughput and delay in TORA network is discussed in the following sections.

Performance of TORA with Throughput in three scenarios

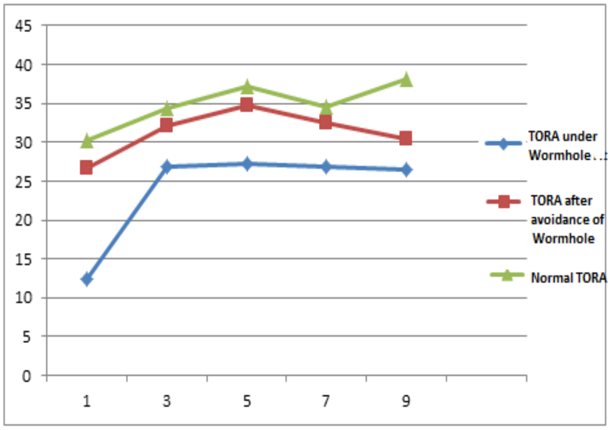


Fig 7: Throughput (Bits/sec) comparison with three scenarios

The performance of the network is compared in above figure and it shows that the green line of the throughput for normal TORA scenario. Blue line shows the decrease in the throughput in case of wormhole attack scenario. Red line shows the throughput of TORA after avoidance of wormhole attack which is gradually increase than with wormhole attack. It is clear from the graph that after avoidance of wormhole attack it provides great result than with wormhole attack.

Performance of TORA with Delay in three scenarios

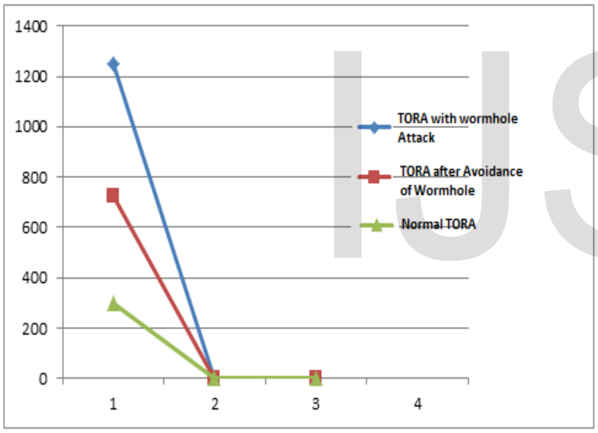


Fig 8: Delay (sec) comparison with three scenarios

The performance of the network is compared in above figure and it shows that the green line of the delay is for normal TORA scenario. Blue line shows the increase in the delay in case of wormhole attack scenario. Red line shows the delay of TORA after avoidance of wormhole attack which is gradually decrease than with wormhole attack. It is clear from the graph that after avoidance of wormhole delay of TORA protocol is decreased than delay of TORA with wormhole attack.

Performance of TORA with Packet Delivery Ratio in three scenarios

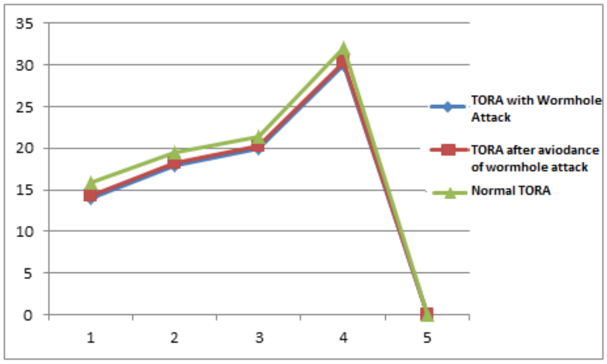


Fig 9: Packet Delivery Ratio(%) comparison with two scenarios

The performance of the network is compared in above figure and it show the green line of the packet delivery ratio for normal TORA scenario. Blue line shows the decrease in the packet delivery ratio in case of wormhole attack scenario. Red line shows the packet delivery ratio of TORA after avoidance of wormhole attack which is gradually increase than with wormhole attack. It is clear from the graph that after avoidance of wormhole packet delivery ratio of TORA protocol is increased than packet delivery ratio of TORA with wormhole attack.

So from the overall simulation performance, we can tell that the avoidance of wormhole attack scenario provides better results than with wormhole attack. And we try to normalise wormhole affected network to its normal state as close as possible.

8 Conclusion

In this work, the performance of the Temporary Ordered Routing Algorithm has been summarized. The main focus was to show the performance of TORA under normal environment, under wormhole attack and performance after avoidance of wormhole attack in term of throughput, delay and Packet delivery ratio. In doing so, a wormhole scenario has been created and two wormhole attacker nodes have been generated. These malicious nodes provide false information to the network and TORA consider the path defined by malicious nodes as best routing path available and start communication through it. Performance of network decreases after wormhole attack and to avoid of this attack, another approach of TORA protocol has been implemented by introducing quality index value. After implementation of this module, it finds the malicious nodes because the Q.I values of malicious nodes are very less as compare to threshold value used by network while communication. Elimination of nodes takes place on Network layer by broadcasting the information of malicious nodes. Avoidance of wormhole attack can be done so that adhoc communication can be normalized as normal communication

9 Future Work

For future enhancement you can detect and avoid wormhole attack in MANET very efficiently. In our research we use two malicious nodes so you can try with more malicious nodes and evaluate the performance of MANET using another routing protocols. There is a need to do research on other security attacks like jellyfish attack, grey hole attack etc.

ACKNOWLEDGMENT

We are sincerely thankful to Bhaskaracharya Institute of Space Applications and Geo-Informatics (BISAG) for the infrastructure, administrative and Qualitative support extended for the timely completion of this research.

References

[1] Kriti Gupta, Maansi Gujral and Nidhi "Secure Detection Technique Against Blackhole Attack For Zone Routing Protocol in MANETS" International Journal of Application or Innovation in Engineering & Management (IJAI-EM), Volume 2, Issue 6, June 2013

[2] Dhruva Patel, Parth Trivedi, Dr. M.B Potdar "A brief analysis on detection and avoidance techniques for wormhole attack in MANET" International Journal of Computer Applications (IJCA) , May 2015

[3] Assiut, Egypt, Hosny M. Ibrahim, Nagwa M. Omar, Ebram K. William: "A Lightweight Technique to Prevent Wormhole Attacks in AODV" International Journal of Computer Applications ,Volume 104 – No.6, October 2014

[4] Shivangi Dwivedi, Priyanka Tripathi: "An Efficient Approach for Detection of Wormhole Attack in Mobile Ad-hoc Network" International Journal of Computer Applications, Volume 104 – No.7, October 2014

[5] Ajit Singh, Lehra Gaga, O.S.Khanna: "Multipath Algorithm For Prevention Of Wormhole Attack In Manet", Journal of Advanced Studies and Communication Research, Volume.1, Issue.3, March 2014

[6] Prof. Ramya S Pure, Prof. Gouri Patil, Prof. Mohammad Manzoor Hussain: "Trust based solutions using counter strategies for Routing attacks in MANET" International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue4,June2014