Wormhole Attack Isolation Access from Mobile Ad hoc Network with Delay Prediction Method

Shruti Thapar, Sudhir Kumar Sharma

***Abstract:** The moveable ad hoc networks are untrustworthy and inclined to any intrusion due to their wireless interaction approach. Therefore the information from these networks can be stolen very easily just by introducing the attacker nodes in the system. The straight route extent is calculated with the help of hop count metric. For this purpose, routing protocols are designed. The wormhole attack is considered to be the hazardous one among several attacks. This intrusion is commenced with the help of couple attacker nodes. These nodes make a channel by placing some sensor nodes between transmitter and receiver. The accessible system observes the wormhole intrusions in the absence of intermediary sensor nodes towards the target. This mechanism is significant for the areas where the route distance amid transmitter and receiver is two hops merely. This mechanism is not suitable for those scenarios where multi hops remain amid transmitter and receiver. In the projected study, a new technique is implemented for the recognition and separation of attacker sensor nodes from the network. The wormhole intrusions are triggered by these attacker nodes in the environment. The projected scheme is utilized in NS2 and it is depicted by the reproduction outcomes that the projected scheme shows better results in comparison with existing approaches.*

***Keywords:** MANET, AODV, WORMHOLE, THRESHOLD TECHNIQUE*

I. INTRODUCTION

In today's world of digitalization, technology is mainly concerned on the efficient controlling and governing power of the system. For this, suitable routing protocols and secure communication environment are must to maintain some wireless sensing applications like Military area, Commercial Sector, Personal use, Bluetooth and local level [4][9][25][33]. MANET has shown tremendous growth in emerging wireless sensing networks because of the highly increasing demands and numerous expectations in this area [5]. It has several characteristics such as lack of infrastructure, channel sharing for wireless communication, lesser number of nodes, dynamic topology and moderate sources. There is no central infrastructural setup in between the network to verify the data transmission between the nodes [13] [31]. Any node in the network can act as sender, receiver and router as well. There is no information to any node in the environment about its intermediate nodes. Routing protocols play a vital role in MANET. Initializing new routes, conserving and adjusting new routes within the network topology are the key roles to it [10] [14][20][24].

Due to lack of infrastructural setup and mobile nodes, security and maintaining efficient routing of nodes, is becoming the major challenge in MANET [29]. The major harms which affect the network setup are instant changing topology, no centralized control, restrained resources and lack of information about intermediate nodes[18][22][40]. Hence, MANET is very much prone to the cyber-attacks because of its self-organizing and configuration property. This attack directly harms the major quality of service factor in the network setup like battery backup, performance measurement, sustainability and the most important security of the network[35][43].

In MANET, two different kinds of attacks are there which can cause the causality in the network setup i.e. external and internal attacks [19] [30] [38] [41].

1.1 ***External Attack**:* These attacking nodes are not present in the environment setup and can cause harm to the network from outside. Congestion, sending wrong routing information and causing unavailability of network services are the major effects of this attack [2].

1.2 ***Internal Attack:*** In this attack, attacking node remains present as genuine node of the environment setup. This false node in the setup will gain unauthorized access and can harm the network in many ways [7]. This internal attack is again classified into two categories i.e.

1.2.1 ***Passive attacks:*** In this attack, the data is only fetched from the user site and not altered anyhow. Generally hacker launches this attack to fetch the data and use outcomes [6] [12].

1.2.2 ***Active attacks:*** In this attack, attacker fetches the data and does some alteration in it to gain the access and break the privacy of the network [11]. This kind of attack is adaptable and productive in quality as they keep on changing their topology very frequently.

MANET is becoming less secure and less effective because of dynamic changing structure and open medium access control. Some of the attack forms in MANET are Wormhole attack, black hole attack, grayhole attack, flooding, replay attack, DoS (Denial of Service) attack, Man-in-middle attack and eavesdropping attack etc.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author

Shruti Thapar*, Department of Electronics & Communication, Jaipur National University, Jaipur, India, E-mail: shrutithapar5@gmail.com

Sudhir Kumar Sharma, Department of Electronics & Communication, Jaipur National University, Jaipur, India. hodece_ E-mail: sadtm@jnujaipur.ac.in

Retrieval Number: F8230038620/2020©BEIESP
DOI:10.35940/ijrte.F8230.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

These attacks are able to harm the network topology and upper layer Applications [3] 8][21][32][36][37]. In this paper, we will try to evaluate the MANET's performance under wormhole attack. Detection and prevention mechanism will be discussed and analyzed under suitable network environment.

II. WORMHOLE ATTACK IN MANET

The most harsh and serious form of attack in MANET environment is wormhole attack [17]. Wormhole is a Denial of Service type of attack which is effective on network layer. It is a passive type of attack so; it creates a shortcut to the destination by gaining data packets from initial stage of the network and broadcast it to another end. It can easily disturb the whole network, due to strong malicious intentions attack and the alliance of two false nodes with proper information about the network topology. It is begun by hook up nodes [9] [26] [39] [42]. In wormhole attack, a tunnel is formed between the false nodes to drop the traffic and perform nasty functions in the network. It takes lesser amount of time to deliver the data packets on destination then the normal time interval. This is due to fewer amounts of nodes in between the path in comparison with multiple path routes [25] [31].

The working of wormhole attack is best understood with the help of diagram [1] [10]. Figure 1 represents normal nodes and normal links with malicious nodes (S2, S9) will grab the data and elaborate the route lengths by using private channel known as wormhole tunnel in between. Malicious node will attract the data packet towards itself by showing lesser number of hops and less delivery time. In this tunnel, the false node occupies the data envelope and transfers it to the next intermediate node on the last point of the tunnel through private channel, which will retransmit the data packet provincially. Because of having better surroundings for nodes in the wormhole network i.e., few hops or less time, in comparison with data forwarded on normal routes, that's why the route between source and destination is selected through the private channel. It normally initiates in two parts [28]. Firstly, the attacker node involves themselves in many paths and secondly, these false nodes kickoff start their mischievous activity on the packets they receive. Due to this, the functionality of the network will be harmed in many ways like, creating confusion between the nodes, increases the traffic rate, overhead issues and the most important it will exhaust the battery consumption of the system [19]. It forwards the data through off channel links, so it is difficult to find out the false node in the system. One line definition for Wormhole will be that it can delay, drop, edit and transfer packet to unknown node with false intentions.

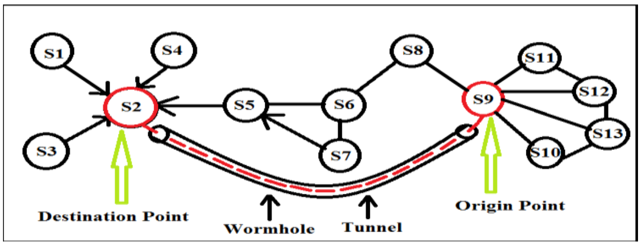

Figure 1: Wormhole Attack.

Wormhole can be classified as:-

Out-of-band wormhole: In this, attack comes from outer nodes. False nodes can easily make a connection in the network. Special infrastructural setup is required for communication between the nodes [27]. It provides faster delivery rate then in-band wormhole attack.

In-band wormhole: In this, no external connection is required in the system nodes. Also, there is no need of any hardware setup and routing protocols to deliver data packets from one node to another [16]. In both forms of attacks, the attacking nodes do not present at very near to each other but seem to be the neighbors.

III. LITERATURE REVIEW

In this research paper [1], author focused on multi rate Delphi process for wormhole detection, as normal Delphi scheme does not work good on variable bit rate traffic in wireless network environment and also attacks are not fully detected by it. So, multi rate Delphi is used for safety enhancement with three different cases i.e. multi rate transmission, processing delay and neighboring process. Author suggested that if these three conditions are detected carefully then 90% of the detection part is managed and updated in the network. Author came on to the point that none of the method can allow detection and prevention from attack simultaneously for safety and security. Author also suggested that detection rate of any malicious node can be increased using such version of schemes which will directly increase the PDR and good put factor in the system by reducing the delay rates. In this [15], survey and comparison over various methods for detecting and preventing wormhole attack is been done. Researcher implemented a hop count authentication scheme for the detection and to do cryptography for the prevention mechanism. The suggested method does not require any kind of hardware in it. In this method malicious nodes can be finding out by using number of hops and delay of each node present in the system. Transmitting nodes can easily able to track wormhole attack. Using this detection method on multipath routing protocol, if hop count is more than the normal threshold limit, then the path is malicious and it will be removed and a vice versa. After detecting false node, cryptographic patterns are implemented on the nodes in the network for safety purpose. Author has concluded that PDR and throughput factor can be increased and overhead issues can be controlled wisely without any attacking node in the network. In [16], author worked on detection and prevention policies of wormhole attack. Tunneling method is been used for the detection while hash function and digital signatures are used to prevent attacks in the network caused by the false nodes. Here, detection method will give the exact location and current status of the malicious nodes. The suggested method uses tunneling time calculation used by tunnel to observe the nature of wormhole. Firstly, it will analyze the time consumed by the tunnel to find the attack and according to that threshold, level will be analyzed. After that, prevention mechanism will be applied on it.

Author concluded that using such techniques, delay will be decreased, whereas lifetime and throughput will be increased in the system. Paper [17], presents a detail description about trust established methods to find and solve the attacks in MANET.

Here, author used trustworthy and honor based method to find out the trustworthy path and trustful nodes in the presence of wormhole attacks in the network. Author used base stations and majority mining technique to generate the trust in the network and also to find the appropriate location of nodes in the network. They provide the foundations for estimating the data trustworthiness so that wormhole attack may not harm the network anymore. Finally, results proved that this technique will able to calculate the received packets, drop rate of the packets and forwarded packets on a trustworthy location efficiently. The outcomes of the proposed work show that the suggested scheme is better than the current one. Like above mentioned research papers, here author [28] deals with multi path routing protocol with trust based scheme and cryptographic patterns for the detection and prevention of wormhole attack in the network. This scheme works on multiple routes to find out the best route or path in the network. After constant monitoring on routes, the path which will cross the threshold limit will be having a malicious node on it. If the multipath routing in the network possess time greater than 0.5 threshold limits, then system is trustworthy and vice versa. After that, a cryptographic scheme is applied on the network for preventing the attack. Researcher concludes that the network environment totally depends on the threshold value. This means that the greater threshold value will increase the quality of service and vice a versa. Outcomes of the scenario show that Packet drop rate and delay can be minimized, whereas throughput can be maximized using such multipath routing schemes. In [34], specification based scheme is used for the black hole attack detection while hop count is used for the wormhole attack detection. As it does not use any area awareness, time sync and hardware setup for any analysis. The research paper also gives a brief overview on hop count detection method to find false nodes in the networks. Researcher worked on different steps including five routing protocols i.e. AODV, black hole AODV, IDS-AODV, wormhole AODV and modified AODV. According to these steps, all the methods have shown higher PDR and throughput rates but as count of nodes raises, delay also increases in the system. Finally, author comes on the results that IDS –AODV has shown tremendous results with lesser delay rates as compared to modified AODV because in AODV, as the count of node will increase, it will automatically raise the packet delivery ratio and throughput in the network. But it will raise the rate of delay with increasing number of nodes. The reason is this, if node count increases, traffic will increase which is the main cause of collision in the environment for route generation process obtaining higher delay but using IDS method with it gives outstanding results. The paper [35], worked on a new technique to find the wormhole attack in the system using improved clustering method. Firstly, it deals with hop count and time sync method which will check the presence and location of the malicious nodes in the environment. The whole network is sectioned into clusters which will be having individual Cluster Head, and can able to control all the nodes in the area for controlling action in MANET. Researcher observes that the proposed technique is able to give a lot of improvement in PDR and throughput factors due to harmless environment setup as clustering technique will provide the best prevention policies for a safe network setup. In paper [41], author deals with AOMDV routing protocol with hop count and RTT (Round Trip Time) calculation for finding the false nodes in the system. AOMDV routing protocol will help to establish a new route in the network, if any intermediate node moves in between the routing process. It will help the network to maintain and calculate the proper hop count and RTT around the network. The results show that if RTT becomes greater than the normal route establishment, than malicious nodes will occur in the network and vice a versa. That’s how, false node will be detected on a large scale and system can be made error free. Finally, author announces that an increased throughput factor will be shown using this modified AOMDV.

IV. RESEARCH METHODOLOGY

The proposed environment is set to track the Wormhole Attack and to remove it from the network using Trust Based Delay per Hop Technique in the Network. Using this methodology, we try to find out the fraudulence node in the wire free medium by collecting hop count and delay per hop data from different routes in the established network and vice a versa. We have taken a bidirectional communication with shared wire free environment and ad hoc network having N count of nodes. Where, M is a false node in the network. There is a condition for this false node M, that its count should be greater than 1 and less than $(N-1)$. All the nodes in the network should monitor neighboring nodes. Without any modification by MAC layer, all the packets are directly send to the higher layer i.e. network layer. At this layer, packets are checked and processed further.

Table 1: Notations

TN_{RREQR}	Request Packet receiving time
TN_{RREQF}	Request packet forwarding time
$RREQ_{SN}$	Request Packet size at node N
TN_{RREPR}	Reply Packet receiving time
TN_{RREPF}	Reply Packet forwarding time
$RREP_{SN}$	Reply Packet size at node N
$RTT_{N_x N_y}$	Round Trip Time between nodes
PT_{N_x}	Processing Time at node N_x

In our proposed system, we use multi rate forwarding network to calculate the RTT between the nodes. Source node S is subjected to calculate the RTT and processing time of all the nodes in the network between its initial and end stage.

The node is send to be in suspicious list if any of the neighboring nodes does not send its route request or replies packet sending and receiving time with RREP. Processing time is the main factor at each intermediate node to find the false node of the network and is evaluated by the source node.

This scheme follows the rule to send the RREQ from source node until it reaches the destination node. As it is mentioned above that all the nodes are equally responsible to check their intermediate nodes and save the time of RREQ and RREP packets.

After calculation of RTTs, the source will differentiate between the expected RTTs and the actual RTTs to find the false node of the network. Mainly, the difference between the two RTTs must be zero, but here it is defined a particular threshold value, which is equal to 0.3 ms to avoid the harmful activity in the system. This value will avoid the unexpected delays in the network.

4.1 Round Trip Time and Processing Time evaluation:

Calculation between RTT and PT at each and every node of the network is done. For this the network setup is shown in Fig.2

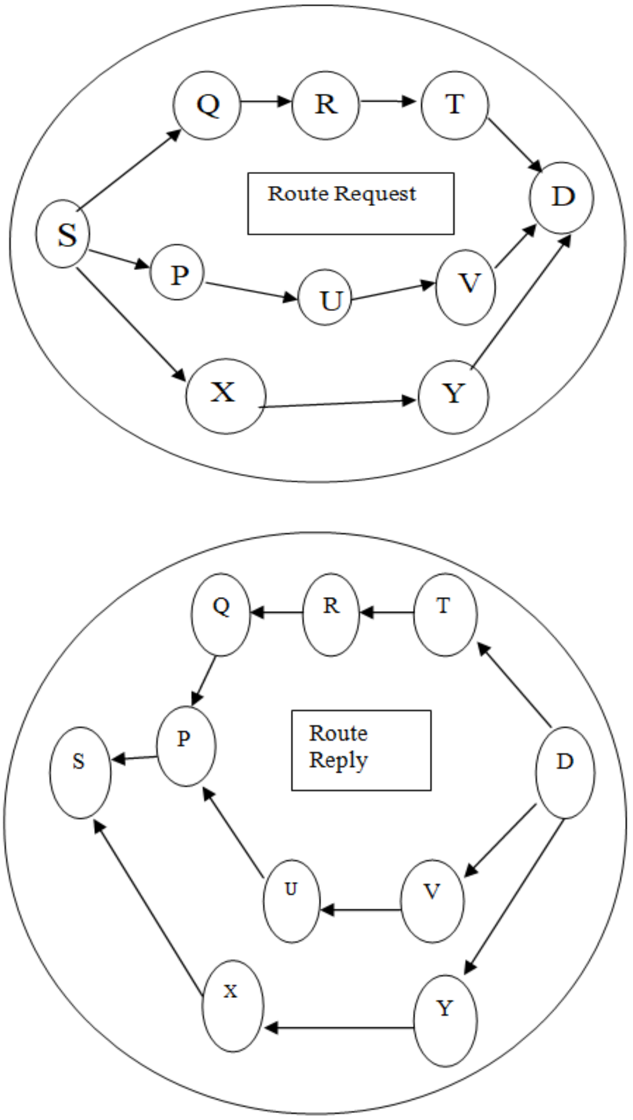

Figure 2: Route Request/ Reply from Source to Destination

A source node S will broadcast a route request RREQ to find the suitable path between sources to destination. According to Fig. 2, three way routes are present in the network. First is ($S \rightarrow P \rightarrow Q \rightarrow R \rightarrow T \rightarrow D$), second route is (S$\rightarrow P \rightarrow U \rightarrow V \rightarrow D$) and third route is (S$\rightarrow X \rightarrow Y \rightarrow D$). The request which comes first to the destination will be selected and else will be rejected. The node will be sent to the suspicious list for further verification, if it is unable to receive any RREQ packet from the intermediate node in a particular time interval. This suspicious list is maintained by the source node and the each neighboring node on that route. RTT between the nodes and destination is shown in Table 2 (Mentioned Below)

After the RTT calculation, the source node *S* evaluates the RTT in between neighboring nodes, shown in Table 3.

Table 2: Intermediate nodes RTT

RTT_{SP}	$= RTT_{SD} - RTT_{PD}$
RTT_{PU}	$= RTT_{PD} - RTT_{UD}$
RTT_{UV}	$= RTT_{UD} - RTT_{VD}$

Now, the source will analyze the processing time and the expected transmission time using packet size and transmission rate factors between the nodes. After analysis, the source node will compare it with actual RTTs. If the result is lesser or equal to threshold value then the route is meant to be safe or wormhole is detected in the network.

Calculation of expected transmission time:

$$TT = \frac{\text{Packet Size (bits)}}{\text{bandwidth (bps)}} \ldots \ldots \ldots \ldots \ldots (1)$$

Calculation of processing time between nodes in the network is shown in Table 4:

Table 3: Processing Time

$PT_{RREQ_{N_x}}$	$PT_{RREP_{N_x}}$
TN_{XRREQ_F} - TN_{XRREQ_R}	$TN_{XRREP_F} - TN_{XRREP_R}$

According to Eq.1, calculation of transmission time is:

$$TT_{N_i N_{i+1}} = \frac{\text{Packet Size (RREQ)}}{\text{bandwidth}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Table3: Participating nodes and Destination node's RTT

Node	TN_{RREQ_R}	TN_{RREQ_F}	$RREQ_{SN}$	TN_{RREP_R}	TN_{RREP_F}	$RREP_{SN}$	RTT_{ND}
S	TS_{RREQ_R}	TS_{RREQ_F}	$RREQ_{SS}$	TS_{RREP_R}	TS_{RREP_F}	$RREP_{SS}$	TS_{RREP_R} -TS_{RREQ_F}
P	TP_{RREQ_R}	TP_{RREQ_F}	$RREQ_{SP}$	TP_{RREP_R}	TP_{RREP_F}	$RREP_{SP}$	TP_{RREP_R} -TP_{RREQ_F}
U	TU_{RREQ_R}	TU_{RREQ_F}	$RREQ_{SU}$	TU_{RREP_R}	TU_{RREP_F}	$RREP_{SU}$	TU_{RREP_R} -TU_{RREQ_F}
V	TV_{RREQ_R}	TV_{RREQ_F}	$RREQ_{SV}$	TV_{RREP_R}	TV_{RREP_F}	$RREP_{SV}$	TV_{RREP_R} -TV_{RREQ_F}

Therefore,

$RTT_{N_i N_{i+1}} = TT_{N_i N_{i+1}} + TT_{N_{i+1} N_i}$ ……… ..(3)

As mentioned, the above equation does not have processing time of RREP packet, so it is added in Eq.4.

Now the source can evaluate both the RTTs as:

RTT=$\sum_i^{2N-1}(TT_i + PT_i)$……………….……. (4)

Hence,

RTT= $\sum_i^{2N-1}((\frac{Packet\ Size}{Bandwidth_i}) + PT_i)$ ………… (5)

After calculating RTTs, the source node is able to reject malicious intruder node and find the best suitable path in the network.

Table 4: Participating nodes and Destination node's RTT

Node	TN_{RREQ_R}	TN_{RREQ_F}	$RREQ_{SN}$	TN_{RREEP_R}	TN_{RRE_F}	$RREP_{SN}$	RTT_{ND}
S	0	0	30	26.5	26.5	80	26.5
X	3.5	4.6	34	21.5	22	71	16.9
Y	4.8	6.8	38	18	20.5	56	11.2

Table 5: Intermediate nodes RTT

RTT_{SX}	9.6
RTT_{XY}	5.7
RTT_{YD}	11.2

Table6: Processing Time at intermediate nodes

Node	PT_{RREQ}	PT_{RREP}
X	0	0
Y	1.1	0.5
D	2.0	2.5

Table 7: Expected and actual RTT's

Nodes	Expected RTT	Actual RTT
RTT_{SX}	2.28	9.6
RTT_{XY}	1.55	5.7
RTT_{YD}	4.45	11.2

As shown in Table 8, shows that the result of compared RTTs is greater than the fixed threshold value (0.3ms). So this network is unsafe to work as it will be having unexpected delays and congestion in the system.

Retrieval Number: F8230038620/2020©BEIESP
DOI:10.35940/ijrte.F8230.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

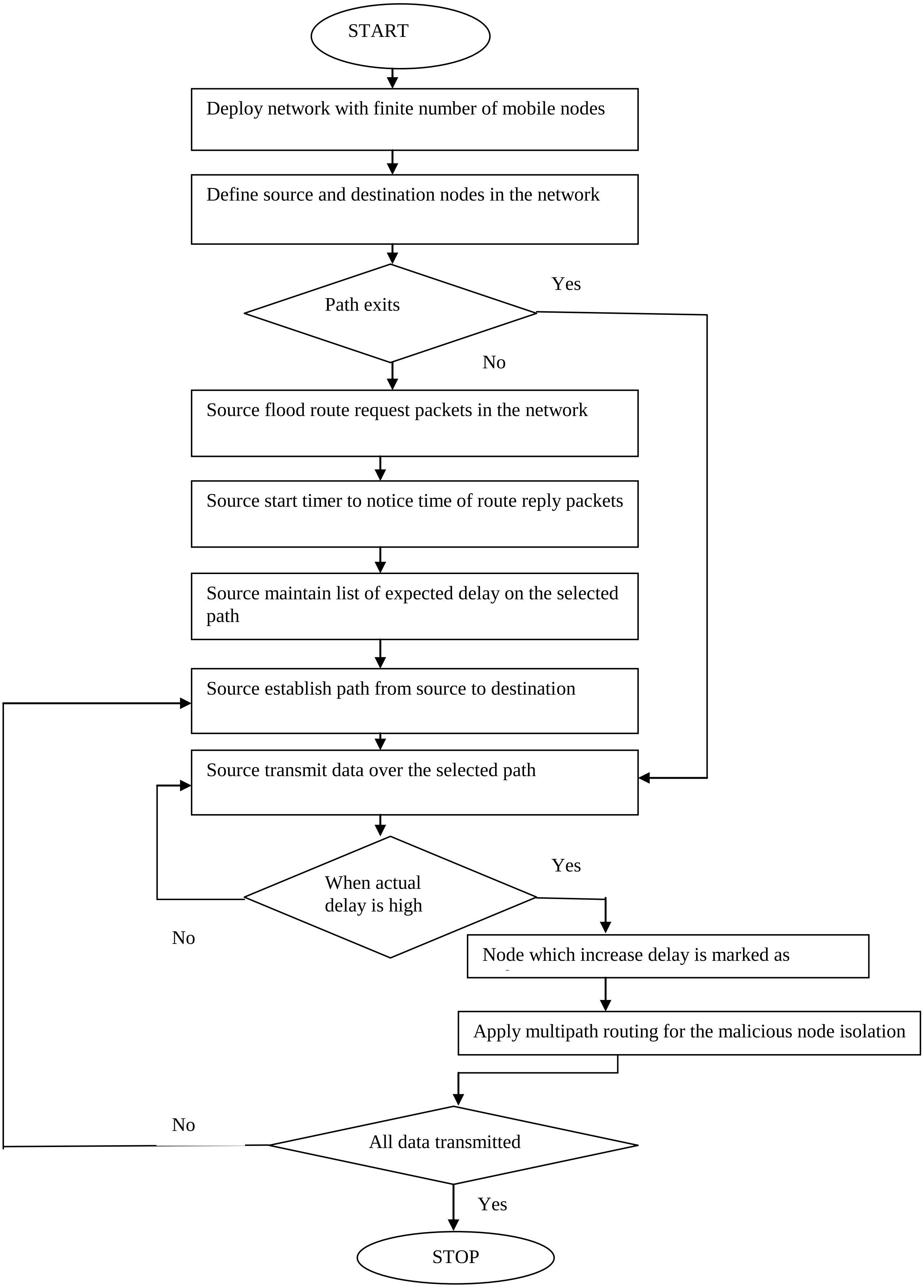
START
Deploy network with finite number of mobile nodes
Define source and destination nodes in the network
Path exits
Yes
No
Source flood route request packets in the network
Source start timer to notice time of route reply packets
Source maintain list of expected delay on the selected path
Source establish path from source to destination
Source transmit data over the selected path
When actual delay is high
Yes
No
Node which increase delay is marked as
Apply multipath routing for the malicious node isolation
No
All data transmitted
Yes
STOP

Figure 3: Proposed Methodology

V. RESULT AND DISCUSSION

The wormhole attack is delay conscious it will increases delay in the network. The shortest path between sources to destination is based on hop count and sequence number. Route which has less hop count and maximum sequence number is best suitable for data transmission from source to destination. The malicious node exits in the selected path which can increase delay in the environment. The false node create tunnel from one end to another which leads to increase delay over the network. The threshold based method is designed in this research work for the detection of false nodes from the network. The expected delay is calculated before data transmission in the network. The predicted delay is calculated from the network and node which has more delay than the expected delay is marked as malicious. The proposed model is executed in network simulator version 2. The results are analyzed on parameters like throughput and packets loss corresponds to different set of mobile nodes. It is been noticed that the suggested methodology will find the malicious node efficiently and compared to other techniques. The various simulation framework are explained in the table 9

Table 8: Simulation Parameters

Parameters	Values
Simulator	NS2-2.35
Area	8zsx* 800
Number of nodes	24
Antenna type	Omi-directional
Queue type	Priority queue
Queue length	50
Propagation model	Two ray

As shown in figure 4, the overall performance of intrusion state, foundation document set-up and projected set-up is evaluated for the presentation scrutiny. It is investigated that overall performance of projected set-up is utmost in comparison with other setups.

Table 9: Throughput Analysis

Time	Attack Scenario	Existing Technique	Proposed Technique
20 second	50 packets	120 packets	350 packets
60 second	60 packets	350 packets	370 packets
100 seconds	150 packets	470 packets	550 packets

Table 10Packet loss Analysis

Time	Attack Scenario	Existing Technique	Proposed Technique
20 second	50 packets	32 packets	15 packets
60 second	52 packets	40 packets	20 packets
100 seconds	140 packets	110 packets	22 packets

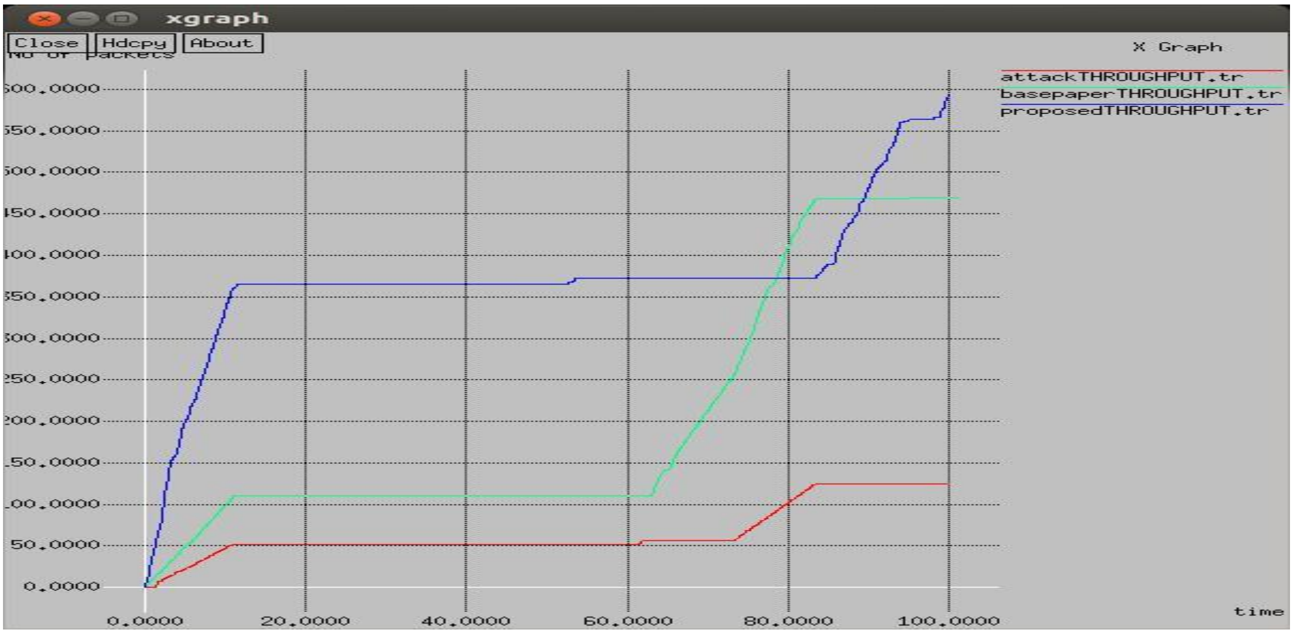

Fig 4: Throughput Comparison

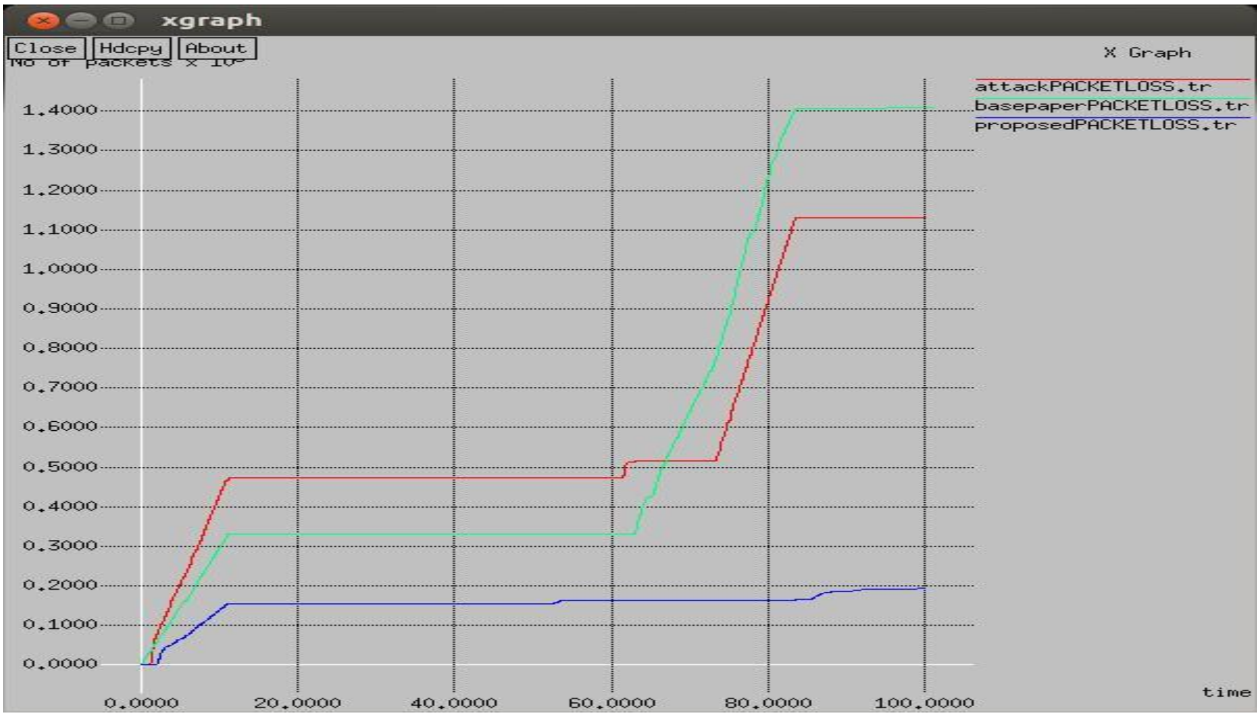

Fig 5: Packet loss Comparison

VI. CONCLUSION

It is identified that the wireless ad hoc systems are disseminated kind of networks in which sensor nodes can join or depart the system according to them. No middle regulator is presented in the wireless ad hoc systems. Because of the self-reliance character of the system; safety, direction finding and service quality are the main problems associated with this system. An active kind of attack named wormhole intrusion may be the reason of the entering of attacker nodes in the system and because of this, delay increases. In the presented research, Delphi scheme is utilized. For the recognition of attacker sensor nodes, this scheme shows lesser precision and large implementation time. In the presented study, for the recognition of attacker sensor nodes, threshold relied approach is implemented. The projected and accessible approaches are applied in NS2 and the reproduction outcomes depict development in power utilization, overall performance, and package thrashing.

REFERENCES

1. Shams Qazi, Raad Raad, Yi Mu and Willy Susilo (2018),"Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks", Journal of Information Security and Applications 39, pp. 31–40.
2. Mr.Shaubham N.Ghormare, Prof.Swati Sorte and Dr.S.S.Dorle (2018) "Detection and Prevention of Wormhole Attack inWiMAX Based Mobile Adhoc Network", International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), ISBN: 978-1-5386-0965-1
3. M. Anand and T. Sasikala (2018) "Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol", springer publications, doi.org/10.1007/s10586-018-1721-2.
4. Tu T. VO, Ngoc T. Luong and Doan Hoang (2018) "MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network", springer publication, doi.org/10.1007/s11276-018-1734-z.
5. Rubal Sagwal and A. K. Singh (2019) "A Power Efficient Solution to Counter Blackhole and Wormhole Attacks in MANET Multicast Routing", ICAICR, CCIS 956, doi.org/10.1007/978-981-13-3143-5_45
6. Kai Dong, Ding Zhu and A. Daniel Hill (2018) "Mechanism of wormholing and its optimal conditions: A fundamental explanation", Journal of Petroleum Science and Engineering 169-126–134,doi.org/10.1016/j.petrol.2018.05.060.
7. Jegan Govindasamy and Samundiswary Punniakody (2018) "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack", Journal of Electrical Systems and Information Technology, pp. 735–744
8. M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and A. Mammeri(2018)" Graph-Based Wormhole Attack Detection in Mobile Ad hoc Networks (MANETs)", International Conference on Mobile and Secure Services (MobiSecServ).doi:10.1109/mobisecserv.2018.8311439.
9. Sayan Majumder and Prof. Dr. Debika Bhattacharyya (2018) "Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach", 978-1-5386-4649-6/18/$31.00
10. Anusha K & Sathiyamoorthy E (2018) "A new trust-based mechanism for detecting intrusions in MANET",dx.doi.org/10.1080/19393555.2017.1328544
11. Roshani Verma, PROF. Roopesh Sharma and Upendra Singh (2017) "New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 978-1-5090-5686-6/17
12. Shahram Jamali and Reza Fotohi (2017)" DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system", DOI 10.1007/s11227-017-2075-x.
13. Parvinder Kaur, Dalveer Kaur and Rajiv Mahajan (2017) "Simulation Based Comparative Study of Routing Protocols under Wormhole Attack in Manet", DOI 10.1007/s11277-017-4150-2
14. D. Sasirekha and Dr. N. Radha (2017)Secure And Attack Aware Routing In Mobile Ad Hoc Networks Against Wormhole And Sinkhole Attacks" International Conference on Communication and Electronics Systems (ICCES 2017) ISBN: 978-1-5090-5013-0.
15. Miss. Supriya Khobragade and Prof. Puja Padiya (2016), "Detection and Prevention of Wormhole Attack Based on Delay per Hop Technique for Wireless Mobile Ad-hoc Network", International conference on Signal Processing, Communication
16. H.Ghayvat, S.Pandya, S.Shah, S.C.Mukhopadhyay, M.H.Yap and K.H.Wandra (2016), "Advanced AODV Approach for Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET", Tenth International Conference on Sensing Technology, 978-1-5090-0795-0/15

17. Shabina Parbin and Leeladhar Mahor (Asst. prof.) (2016), "Analysis and Prevention of Wormhole Attack Using Trust and Reputation Management Sc, "heme in MANET", 978-1-5090-2399-8/16
18. Parmar Amish and V.B.Vaghela (2016), "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science, pp. 700 – 707
19. Piyush Kaneria and Dr. Anand Rajavat (2016), "Detecting and Avoiding of Worm Hole Attack on MANET using Trusted AODV Routing Algorithm", Symposium on Colossal Data Analysis and Networking (CDAN), 978-1-5090-0669-4/16.
20. Sunil Kumar Jangir and Naveen Hemrajani (2016) "A Comprehensive Review on Detection Of Wormhole Attack In MANET", 978-1-5090-5515-9/16.
21. Nitika Gupta and Shailendra Narayan Singh (2016), "WORMHOLE ATTACKS IN MANET", 978-1-4673-8203-8/16
22. Shahram Jamali and Reza Fotohi (2016), "Defending against Wormhole Attack in MANET Using an Artificial Immune System", DOI: 10.1080/13614576.2016.1247741, Taylor & Francis.
23. Gautam M. Borkar and A. R. Mahajan (2016), "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", DOI 10.1007/s11276-016-1287-y, Springer
24. Ashka Shastri and Jignesh Joshi (2016), "A Wormhole Attack in Mobile Ad-hoc Network: Detection and Prevention", *ICTCS '16*, ACM. ISBN 978-1-4503-3962-9/16/03, ACM.
25. Xue-Wen WANG, Feng HU, Chun-Xue ZHA, Yuan ZHANG, Xing-Xing SU, Yan LI, Zhao-Ke WU, Ting-Ting LI and Zhou-Hu DENG (2016), "Research on Improved DV-HOP Algorithm against Wormhole Attacks in WSN", ITM Web of Conferences 477, 03007, DOI: 10.1051/itmconf/20160703007.
26. Miss. Supriya Khobragade and Prof. Puja Padiya (2016), "Detection and Prevention of Wormhole Attack Based on Delay per Hop Technique for Wireless Mobile Ad-hoc Network", International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016, 978-1-5090-4620-1/16, IEEE
27. Chitra Gupta and Priya Pathak (2016), "Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET", Symposium on Colossal Data Analysis and Networking (CDAN) 2016, 978-1-5090-0669-4/16, IEEE.
28. Manju Ojha and Rajendra Singh Kushwah (2015), "Improving Quality of Service of Trust Based System against Wormhole Attack by Multi-Path Routing Method", International Conference on Soft Computing Techniques and Implementations- (lCSCTI), 2015, 978-1-4673-6792-9/15
29. Saju P John and Philip Samuel (2015), "Self-organized key management with trusted certificate exchange in MANET" Ain Shams Engineering Journal 6, pp. 161–170
30. Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal and Muhammad Hanif Durad (2015), "Analysis of Detection Features for Wormhole Attacks in MANETs", International Workshop on Cyber Security and Digital Investigation (CSDI 2015), Procedia Computer Science 56 (2015), pp. 384 – 390
31. Anal Patel, Nimisha Patel and Rajan Patel (2015), "Defending Against Wormhole Attack in MANET", International Conference on Communication Systems and Network Technologies, 978-1-4799-1797-6/15, DOI 10.1109/CSNT.2015.253
32. Majid Meghdadi, Suat Ozdemir and Inan Güler (2015), "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", IETE Technical Review, doi.org/10.4103/0256-4602.78089
33. Nilesh N. Dangare and R.S. Mangrulkar (2015), "Desisgn and Implementation Of Trust Based Approach to Mitigate Various Attacks in Mobile Ad Hoc Networks", international conference on information security and privacy (ICISP 2015), Procedia Computer Science, pp. 342-349.
34. Kriti Patidar and Vandana Dubey (2014), "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks", 978-1-4799-3064-7/14
35. Anju J and Sminesh C N (2014), "An Improved Clustering based Approach for Wormhole Attack Detection in MANET", International Conference on Eco friendly Computing and Communication Systems, 978-1-4799-7002-5/14
36. Zolidah Kasiran and Juliza Mohamad (2014), "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV", ISBN: 978-1-4799-3724-0/14.
37. Fei Shi, Weijie Liu, Dongxu Jin and jooseok Song (2013), "A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology", Electron Commer Res (2013)13:329–345, DOI 10.1007/s10660-013-9122-3
38. T. V. P. Sundararajan , S. M. Ramesh , R. Maheswar and K. R. Deepak (2013), " Biologically inspired artificial intrusion detection system for detecting wormhole attack in MANET", DOI 10.1007/s11276-013-0623-8.
39. Ravinder Ahuja, Alisha Banga Ahuja and Pawan Ahuja (2013), "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack" International Conference on Image Information Processing (ICIIP-2013), 978-1-4673-6101-9/13.
40. Vandana C.P and Dr. A. Francis Saviour Devaraj (2013), "MLDW- a MultiLayered Detection mechanism for Wormhole attack in AODV based MANET", International Journal of Security, Privacy and Trust Management (IJSPTM), DOI: 10.5121/.2303.
41. V.Raju and K. Kumar (2012), "A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks", International Conference on Computing Sciences, 978-0-7695-4817-3/12
42. Subhashis Banerjee and Koushik Majumder (2012), "A Comparative Study on Wormhole Attack Prevention Schemes in Mobile Ad-Hoc Network", SNDS 2012, CCIS 335, pp. 372–384.
43. Jared Oluoch, Astrid Younang, Bao Tri-Tran, Huirong Fu and Ye Zhu (2012), "A Simulation Study of Impacts of Collaborative Worm Hole Attacks In Mobile Ad Hoc Networks (MANETs).", Information Security Curriculum Development Conference 2012, 978-1-4503-1538-8, ACM.
44. Jared Oluoch, Astrid Younang, Bao Tri-Tran, Huirong Fu and Ye Zhu (2012), "A Simulation Study of Impacts of Collaborative Worm Hole Attacks In Mobile Ad Hoc Networks (MANETs).", Information Security Curriculum Development Conference 2012, 978-1-4503-1538-8, ACM.

AUTHOR'S PROFILE:

Shruti Thapar, She is perusing her PhD in Electronics & Communication Department from Jaipur National University, Jaipur, and Rajasthan, India. She received his M.Tech in Electronics from Jaipur National University in 2014 and B.Tech from Rajasthan Technical University in 2011. She also has teaching experience of 8years in the same field. She has been carrying out research work in Mobile Ad hoc Networks, Network Sensors, Network Attacks, Detection & Prevention policies of Mobile Networks. She has published various research papers on national and international conferences from her area of interest topics. She handled many National and International Workshop, Seminar and Conferences as a core team member. She has awarded with scholarship award twice by her university for scoring excellence in academics.

Dr. Sudhir Kumar Sharma is Joint Director & Head (ECE), School of Engineering and Technology, Jaipur National University, Jaipur, Rajasthan, India. Professor Sharma received his Ph.D. in Electronics from Delhi University in 2000. Professor Sharma has an extensive teaching experience of 22 years. He has been keenly carrying out research activities in the field of Optical Communication, Antenna and Networking. He has taught various engineering courses at graduate as well as at post-graduate level in India and Overseas. His area of research includes Optical Communication & Antenna. He has authored and coauthored over 115 National and International publications along with one book in Opto-Electronics titled "Introduction to Opto-Electronics and Optical-Communication", Printice Hall, Malaysia. He has also served on the editorial board of six international journals. He has been part of many National and International conferences worldwide. Professor Sharma continues to serve on many academic, professional and governmental advisory committees. He has organized numerous National and International Workshop, Seminar and Conferences. He has visited *Spain, Holland, Malaysia, Ethiopia, Sudan and Syria* for academic and research related assignments. He has awarded Senior Research Fellowship by CSIR, New Delhi in 1997. He has also been honored with the prestigious ***Shiksha Rattan Puruskar*** by International Friendship Society, New Delhi for academic works in Feb. 2013. Dr. Sharma is Life time member of ISTE (Indian Society for Technical Education).