Deployment of coordinated worm-hole peer in MANETs

With the enhancement in technical field of communication, efforts are made by the researchers to provide security. Security is dispensing protection and privacy to the system for the channeled data against any unwarranted access and refinements. MANET is a variant of wireless network used essentially by the dynamic devices with high motility and vulnerability. The distinctions like dynamic layout and curbed resources make them susceptible to miscellaneous kinds of threats. One such attack is wormhole which sneak and peep data with malicious intensions and operates either in coordinated or uncoordinated fashion. In its coordinated version, the malicious nodes coordinate their operations whereas in the uncoordinated version; they operate solitarily with the aim to decline the network performance. In this work, we aim to propose an algorithm for deployment of wormhole attack communicating with its peer through a tunnel. Planting of this attack in the network lays the foundation for developing successful strategies to mitigate their effects on the system.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27516v1 | CC BY 4.0 Open Access | rec: 3 Feb 2019, publ: 3 Feb 2019

Deployment of coordinated Worm-hole peer in MANETs

Fahmina Taranum [1], Syeda Hajra Mahin [2], Khaleel Ur Rahman Khan[3]

[1,2] Computer Science and Engineering, Muffakham Jah College of Engineering and Technology,Hyderabad,Telangana,India[1,2]
[3]Computer Science and Engineering, Ace Engineering College[3]
Ghatkesar, Hyderabad

Corresponding Author:
Fahmina Taranum
16 2 35, Akbarbagh, Hyderabad, India 500036
Email address: ftaranum@mjcollege.ac.in

Abstract

With the enhancement in technical field of communication, efforts are made by the researchers to provide security. Security is dispensing protection and privacy to the system for the channeled data against any unwarranted access and refinements. MANET is a variant of wireless network used essentially by the dynamic devices with high motility and vulnerability. The distinctions like dynamic layout and curbed resources make them susceptible to miscellaneous kinds of threats. One such attack is wormhole which sneak and peep data with malicious intensions and operates either in coordinated or uncoordinated fashion. In its coordinated version, the malicious nodes coordinate their operations whereas in the uncoordinated version; they operate solitarily with the aim to decline the network performance. In this work, we aim to propose an algorithm for deployment of wormhole attack communicating with its peer through a tunnel. Planting of this attack in the network lays the foundation for developing successful strategies to mitigate their effects on the system.

Introduction

With refinements in communication, various kinds of networks have also evolved including MANETs. MANET is an impromptu network that routinely reconfigure, thereby increasing an option of providing extra surveillance. MANET holds varying aspects like [1]:

1. MANET manifests anonymity and can acquit oneself as host as well as router.
2. It follows Multi-hop intended dissemination with distributed nature.

3. Nodes are owned with fewer memory and battery resources.
4. It provides support for vast density and mobility.
5. Node to node association is sporadic.

MANETs are also vulnerable to certain challenges, which includes the following:

1. Finite range for channeling the data.
2. Regular network segregation.
3. Packet mislaying on account of erroneous channeling.
4. Route refinements attributed by mobility.

Since the need for communication has increased, there is also increase in need to protect this communicated data against varying threats and attacks. Attacks can be any of the following forms [2]: Either active or passive. In passive, the attacking node taps the channeled data with the endeavour to exploit confidentiality. Instances of passive attacks include eavesdropping, traffic and location disclosure. In active, the attacking node disturbs the channeled data by tempering the data packets in the route. Instances of active attacks include black hole, wormhole, Sybil, jellyfish, etc.

Wormhole attack is an attack where it exploits the vulnerabilities of open communication and diversifies the transmission by projecting itself as the most attentive node. It is classified into coordinated and uncoordinated wormhole attacks. In coordinated version, the two attacking nodes coordinate their actions and mediate by establishing a tunnel between them. Whereas, in the uncoordinated version; the attacker node functions individually.

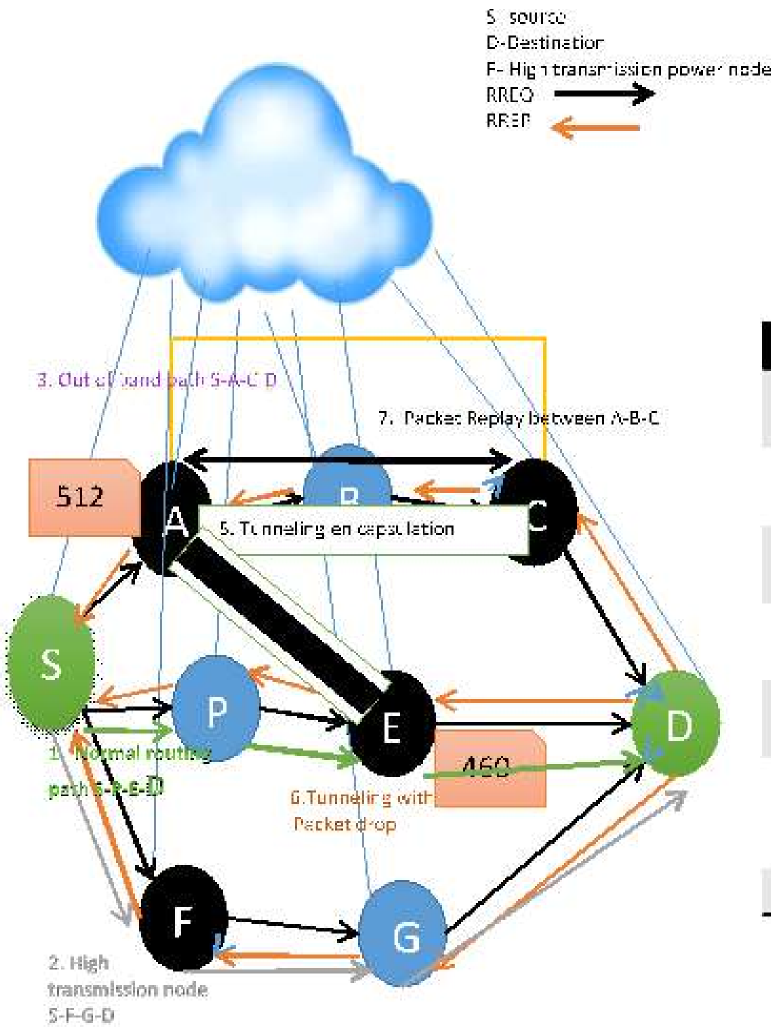
The variants of wormhole attacks are: High transmission power wormhole, out of band, tunneling with encapsulation and Packet replay. The parameters used to design the scenarios are listed out in table 1.

Table 1: Parameter used to design the scenario

Parameter	**Value**
Channel type	Wireless Channel
Propagation model	TwoRayGround
MAC type	IEEE 802_11
Network interface type	DropTail/PriQueue
Antenna model	Omni directional
Max packet in ifq	50
Number of mobile nodes	10
Routing protocol	AODV
Terrain size	800,541 in X,Y axis
Simulation	100 seconds
Traffic	CBR

Variants of Wormhole Attacks

This section explains the variants of wormhole attack. Figure 1 reflects some possible scenarios that are probable to occur in the network. This pictorial representation depicts a network with 10 nodes, node S as source node and D as the destination node. Four nodes namely, A, C, E and F are taken as wormhole nodes. The black arrow shows the flow of RREQ packets forwarded from source to destination, likewise the red arrows depict the RREP packets forwarded back to the source from the destination. The cloud is an illustration of the wireless network. The blue dashed lines show the wireless network connectivity.



Scenarios	Path
Normal path	S-F-E-D
HTP	S-F-G-D
Out of band	S-A-C-D
Tunneling	S-A-E-D
Tunneling with encapsulation	S-A-B-C-D
Packet drop	At node E
Packet Replay	A-B-C

Fig. 1: Some possible worm_hole attacks in network

- The first scenario illustrates the routing path which would be selected based on hop count value. The path S-P-E-D is the normal and obvious routing path that would be selected.
- The second scenario depicts the presence of a high transmission power based wormhole attack. This kind of wormhole attack is triggered by a single malicious node which advertises itself with high transmission power (HTP). In this architecture the node F is taken as the HTP node. Once the source receives the RREP from a HTP node, the path via that node is prioritized and selected for communication.

- The third scenario illustrates out of band wormhole attack where the coordinating wormhole nodes communicate by establishing a special high quality out of band link between them. In figure 1, the nodes A and C communicate via out of band link.
- The fourth scenario depicts the general wormhole where the malicious coordinating nodes create a tunnel and forward the data packets through it. By doing so, they aim to modify the communication route. The path S-A-E-D gives a visual representation of this case.
- The fifth scenario shows tunneling with encapsulation. Concept of encapsulation is considered, when intermediate nodes are available in the tunneled path. Since the data packets are encapsulated between the wormhole nodes, the intermediate nodes are halted from incrementing the hop count value. This is shown in path S-A-B-C-D.
- The sixth scenario depicts tunneling with packet drop. One of the possible benefits of tunneling data to the attacker node is to send packets to wormhole peer. When the node A sends data to E via the tunnel following the routing path S-A-E-D, at E data loss is depicted.
- In the seventh scenario another possible advantage of tunneling is exploited where the two wormhole nodes A and C repeatedly exchange data packet among themselves with the aim to drain the battery resource of the intermediate node B.

Existing Related Work

Through this work [3], the authors have recommended a strategy to weaken high transmission power wormhole attack. This reforms the route location phase and route amending by instigating hardware capabilities check, prior to processing and appending of path record into routing table. Hello Packet verification approach also assists to justify the existing node potential and commit trusted circulation. If and only if any extra potential node is detected, this strategy will not process and append any record in the table. Thereafter, it boycotts the doubted node to regulate from coming interaction. Put forth strategy scrutinizes all the default nodes with the aim to lessen the impact of a wormhole attack.

In this suggested mechanism [4], the initiator welcomes RREP control packets from numerous nodes, the initiator stows all RREPs along with their sequence number entries. Then initiator reckons the average of all the sequence number entries:

S-Avg= (sequence 0+ sequence 1+ sequence 2+…..+ sequence m)/m

{Sequence i is sequence number entry of distinct RREP; m is aggregate of RREPs}

The initiator dismisses RREPs having sequence number beyond S-Avg. It opts for the route possessing value equal or beneath S-Avg. The odds of opting attacker's RREP are reduced for the reason that, the intruder principally aims high number to persuade that its respective RREP is settled on for relaying.

In this submitted scheme [5], the AODV routing protocol is lodged to the trust function. The conveyance in the MANET network is pivot on the cooperation and trust on its bordering nodes. In the course of path searching of AODV, the trust value is quantified for all bordering nodes. Grounded on this, apt threshold values are defined as follows:

Unreliable: this is when the value lies in the range of 0 to 0.5.

Reliable: this is when the value lies in the range of 0.4 to 0.7.

Most Reliable: this is when the value lies in the range of 0.7 to 1.

The outcome of this gives the status of trust of bordering nodes, which is either of the above three. Based on these status results an appropriate route is selected for relaying.

Through this work [6], authors have recommended an inventive approach against wormhole based attack. In this scheme the routing track evolution is done by wielding the conventional AODV. In the course of packet conveying, the PDR is quantified for one and all of the nodes. Rechanneling of Hello packets to target node is carried out together with the quantification of RTT for all the following nodes. Given that, for whichever node RTT is found to be inferior to the pre-settled threshold along with its PDR less than 1; then this respective node is pondered to be a malicious node.

In this put forward approach [7], the authors have proposed merging of TRB with 3PAT with the main consideration to mitigate wormhole kind of attacks. At the outset 3PAT is appended for relaying the data. Supposing the existence of any irregular activity in the route, the 3PAT works good enough to detect such Black hole node. This node could be the under way of a more trivial tunnel instigating a wormhole attack. To identify this behavior TRB i.e., transmission radius based scheme is sought to diagnose the presence of the tunneled wormhole.

The TRB is vaguely refined for this need. In the course, when the single attacking node is observed; this node's table entries are examined. This scrutinizing is carried out to observe if the receiving nodes of the doubted node are genuine nodes. Assuming that, the cardinality of it is low; the odds of discovering a tunnel becomes high. By following this approach, it is agreed that the detection of such kind of attack can be made successful provided they exist in the network.

In this suggested work [8], to begin with; the network is believed to have the form of a circle. This is then considered to be segregated in sectors. After which the trust values of the nodes are individually assessed based on their conduct while transmission, reception, dissemination and mis-relaying of data packets. This quantified result is taken as input for Dempster Shafer D-S, just to categorize the nodes with regard to their conduct into reliable or unreliable. By following this procedure the status of nodes are assessed.

This proposed approach [9], depends upon the connectivity length between the initiator and the target nodes. It mainly believes that the wormhole incorporates the logic of having the shortest route with minimal links. A node is titled suspect node, if it strives to give the best shortest route to the target, marked as sp. T is taken as the time span taken by all the route request packets to make it to the target. Giving the chance that, the target can now identify the sp and monitor its routing entries made in the table for its surrounding nodes V (sp). The target computes $V(t) \cap V(sp)$, which is the set of surrounding nodes of the target with that of sp. The routes are identified. A distinguishing value is to be agreed to inspect the presence of wormhole.

In this proposal [10], the solidity and movability of nodes are examined. All the component nodes attempts to gain information regarding its bordering nodes along with successive hop or for coming hops. While the initiator circulates the Request packet to the bordering nodes for forming some route to target, the opening attacker node conveys data and advertises to possess a new track leading to target; after which the initiator investigates the bordering nodes subsequently to gain proficiency and it later adjoins this collected data to its information table and channels the data. Waiting for some span of time if the initiator fails to acquire acknowledgement from target, it then retransmits the data and waits for some fixed time for receiving acknowledgment and if it again fails in acquiring then a query is relayed to the node's border nodes questioning their consequent hop neighbors. This is done to spot the presence of wormhole node. Blacklisting and relaying of this is done to prevent against this attack.

Materials and Methods proposed

Our work mainly proposes the logic for deploying the wormhole attack in the network. The network considered is a mobile network i.e. MANET. This network is ad-hoc and security is a major concern here. In our proposal, the nodes in MANET disseminate using an On-demand routing protocol i.e., AODV.

AODV proposes two phases: Route discovery together with route maintenance. It uses control packets for deriving a route for communicating the data. For a sender to channel data to target, it first needs to check for an existing route to the target. If no such route exists, then the first stage of discovering the possible route is initiated by circulating RREQ to all the surrounding nodes. Once a node acquires this request packet it checks its table for existing route to the target, if found a RREP is sent back or else this RREQ is subsequently passed on until it makes it to the target. Once the target node receives it, it then disseminates a RREP right back to the sender. Subsequently, each of the nodes passing these control packets appends these route entries into their routing tables. Each node maintains a routing table including details of the path reaching the target. This route would be further used for data imparting. Whereas, during the second stage i.e., Route maintenance stage the already existing route data are maintained. This protocol also uses sequence number to inspect the freshness of the route. Due to frequent layout changes, if any existing link between nodes are broken; then this information is communicated to all the nodes using RERR packet. Any node acquiring this packet will delete that node's data from its routing table. For deploying the wormhole node certain refinements are incorporated to the AODV routing protocol. AODV is modified such that if a wormhole node is encountered the data is dropped at that node. The algorithm for deployment of wormhole attack is stated below for the mac.cc, aodv,cc, aodv.h and mac.h files.

Algorithm 1

Mac.cc

Step 1: Initiation of the head of the list for coordinated wormhole node peer

Step 2: Examining for coordinated wormhole node for locating worm-peer

For a coordinated node, pointer is assigned to the allocated memory

If there is no pointer assigned to the coordinated node, then an error is displayed.

Entries are pushed to the list at the head.

Step 3: Examining the subsequent hops of the coordinated node for peer or broadcast

Step 4: Channeling of query and inspecting against a certain resolving point for detection of Wormhole.
Decisions are made if the data is passed past the attacking node.
Packets are sent to all the coordinated nodes.
Channels this to the interface and generation of statistical index is done.
Each receiving coordinated nodes checks if the data is for that concerned coordinated node only. If it is for only that coordinated node then no further channeling is done.
Step 5: Pushing of this coordinated node to the anterior part of list

Algorithm 2

Mac ll.cc

Step 1: Set node 4,6 as wormhole peer

$n4 set ll_(0)] wormhole-peer [$n6 set ll_(0)]
[$n6 set ll_(0)] wormhole-peer [$n4 set ll_(0)]

Step 2: Agents Definition
#Setup a UDP connection, attach-agent, set sink [new Agent/LossMonitor]
Connect udp agent and sink, set packetSize_ 1000

Step 3: Applications Definition-Initialization

I. Setup a CBR Application over UDP connection
Set cbr rate_ 0.1Mb, cbr start at 1.0 and stop at 100, holdrate1 0, Sampling Time to 0.9 Sec, bw0 to bytes, bw1 to nlost, bw2 to lastPktTime, bw3 to npkts

II. Assignment- # Record Bit Rate in Trace Files
now = (bw0+holdrate1*8)/(2*time*1000000)
# Record Packet Loss Rate in File
now = (bw1/time)+0.5869

III. Test if (bw3 > holdseq)
now= (bw2 - holdtime)/(bw3 - holdseq)
else
now= (bw3 – holdseq)

Step 4: Exit Mac layer file

Algorithm 3

AODV.CC

Step1: if (wormhole == true) then
Drop (p, DROP_RTR_ROUTE_LOOP);
// DROP_RTR_ROUTE_LOOP is added for no reason.
Step2: else exit aodv.cc

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27516v1 | CC BY 4.0 Open Access | rec: 3 Feb 2019, publ: 3 Feb 2019

Algorithm 4

MAC ll.h

Step 1: Initialize TRACE_DROP 0, hdr_ll::offset_ to integer.

Step2: Modify the class PacketHeaderClass

LLHeaderClass(): PacketHeaderClass("PacketHeader/LL", sizeof(hdr_ll))

Begin bind_offset(&hdr_ll::offset_);end

Step 3: Exit the mac.cc file

Results

Below is the architecture onto which the deployment scheme is applied and the results are assessed. The no. of nodes taken is 10. The routing protocol applied is AODV. Node 0 is the source and node 3 is the destination. Nodes 4 and 6 are the deployed wormhole nodes. The simulations are carried out using NS-2 simulator. The traffic generator taken is CBR. Table 1 gives the details for carrying out the simulations.

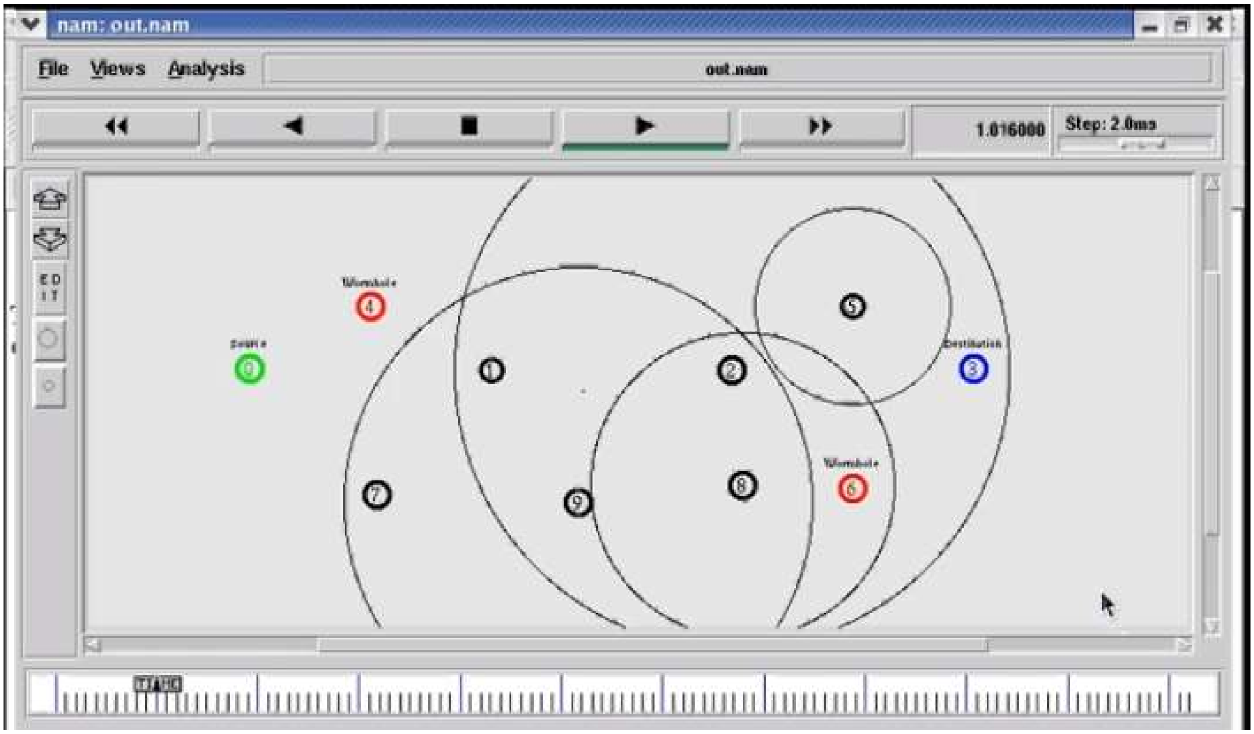


Fig. 2a: Nam file –With node 4 and node 6 deployed as worm_hole peers

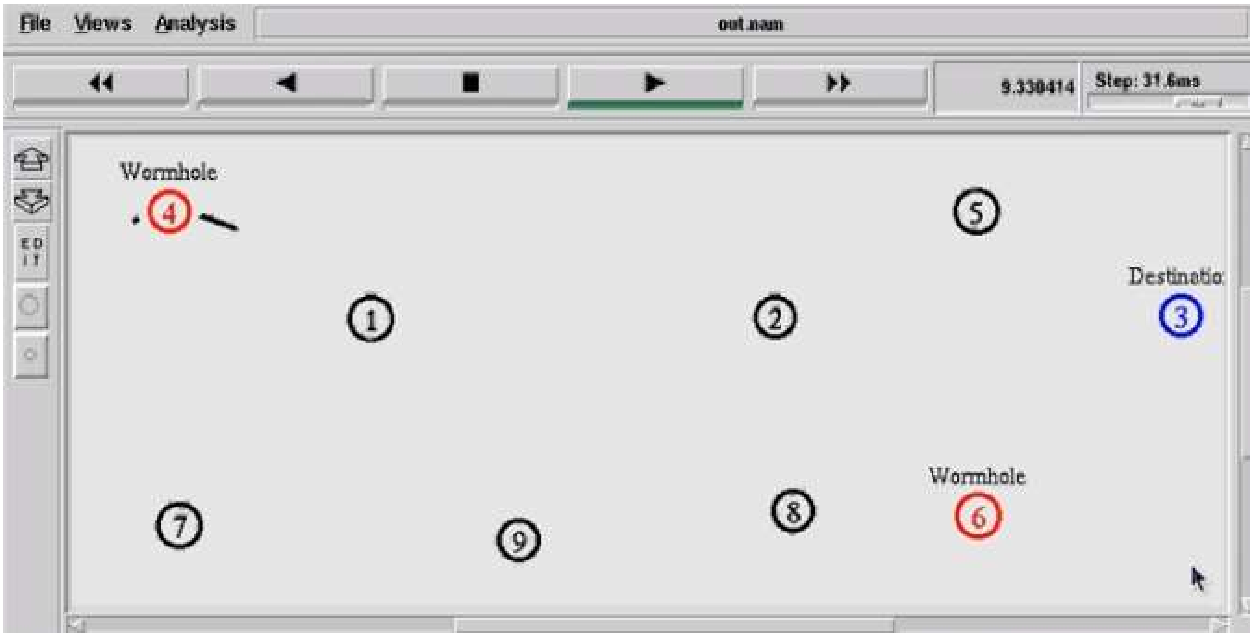


Fig. 2b: Data transmitted to Worm-peer, with destination kept deprived of packets

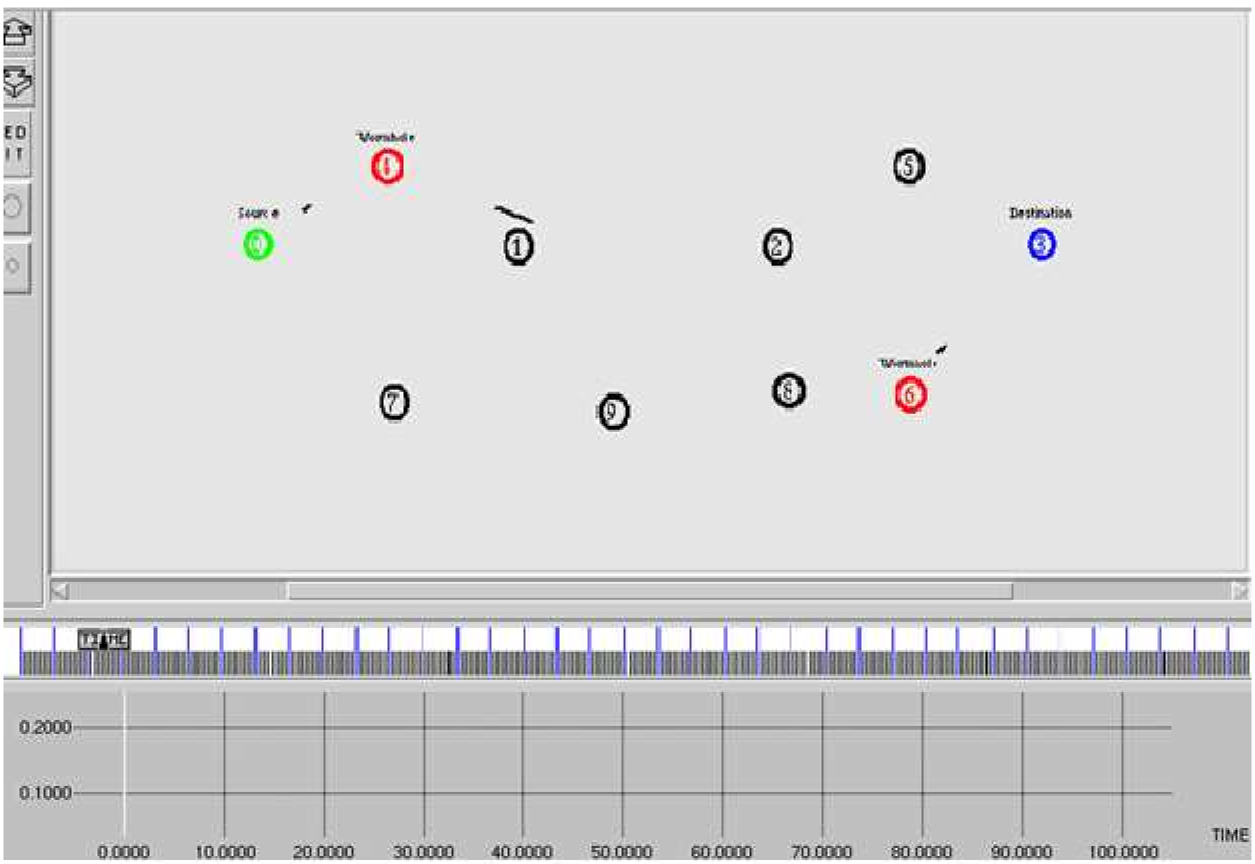


Fig. 2c: Data transmitted to Destination through tunnel created in between worm-peer

The normal transmission is shown in figure 2a.The figure 2b visualizes the created network for running the deployment algorithm using NS2 for communication to wormhole peer through tunnel and then the packets are dropped at the peer, keeping destination deprived of packets
Figure 2c depicts a scenario to show that loss less communication in between wormhole peer and. then the data is sent to destination node.

The performance of this proposal is assessed based on the following evaluation metrics:

- Packet delivery ratio
- Delay
- Throughput

1. Packet delivery ratio: PDR is considered as an inspection metric to evaluate the proposal.

$$\boxed{Packet\ delivery\ ratio = \frac{\text{quantity of data packets acquired at the targeted node}}{\text{quantity of the data packets dispatched by the initiator node}}}$$

Figure 3a, conveys that the normal PDR of the network i.e., in the absence of wormhole attack the PDR is high. Whereas the PDR is observed to drop when the proposed deployment technique is implemented. The maximum PDR obtained after the deployment is much less due to packet drop by the wormhole nodes.

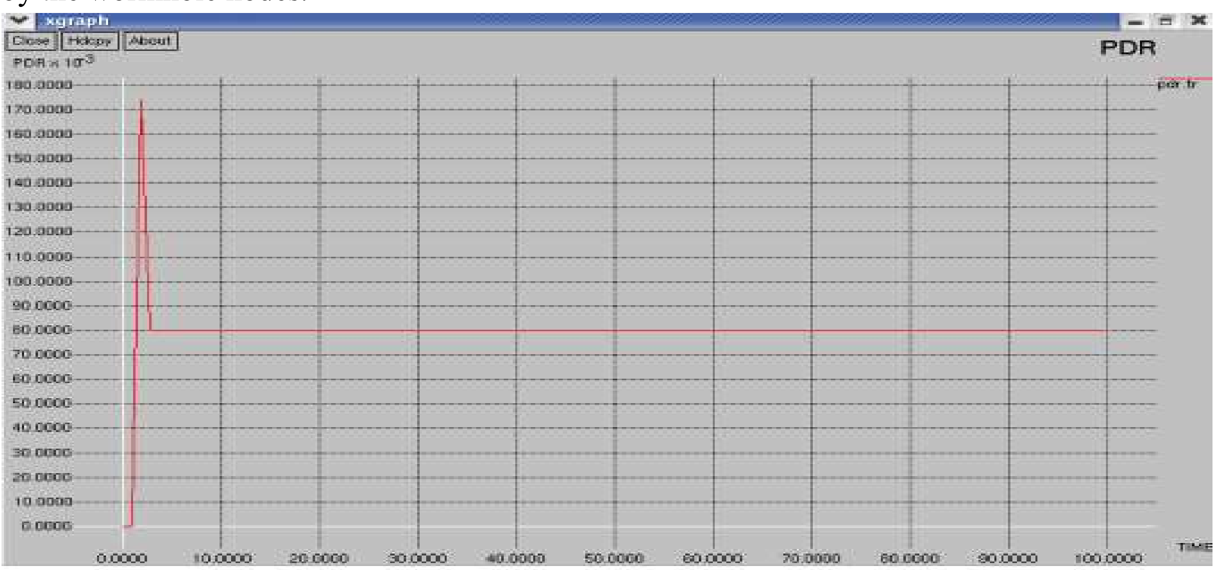


Figure 3a: The normal Packet delivery rate of the network

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27516v1 | CC BY 4.0 Open Access | rec: 3 Feb 2019, publ: 3 Feb 2019

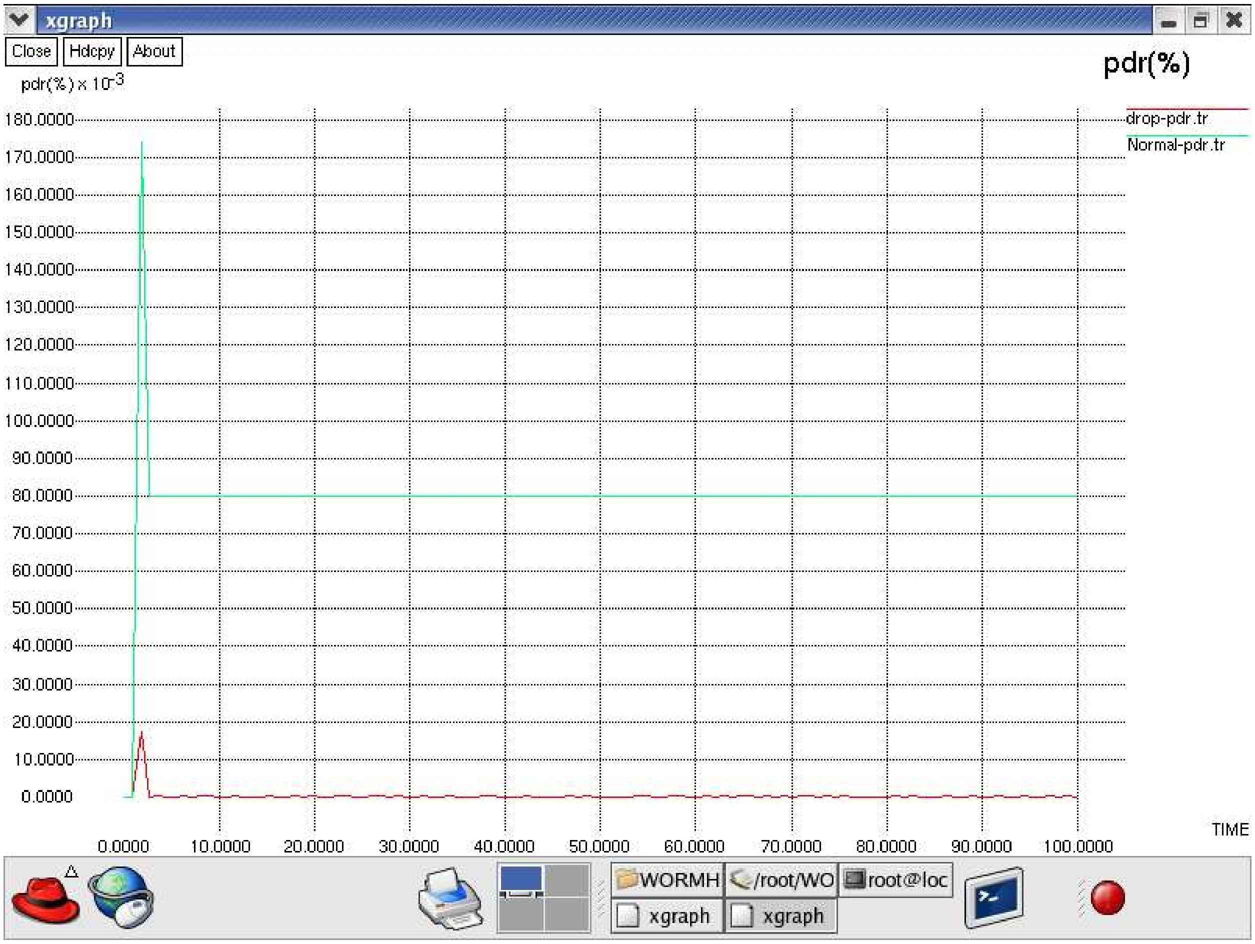


Figure 3b: Comparative analysis of packet delivery rate of the network

The comparison of PDR with normal and dropped scenario is depicted in Figure 3b, for transmission of packets to destination while a tunneled wormhole peer is in activation.

2. Delay: Delay is taken as another inspection metric.

Delay = aggregate time consumed by a data packet to mediate from initiator end to the targeted end.

Figure 4a, conveys that the delay is noticed to be less in the case of normal trusted transmission i.e., noted to be 240ms. But After the deployment of the wormhole nodes the delay has escalated to 580ms.This is for the packet drop scenario at peer

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27516v1 | CC BY 4.0 Open Access | rec: 3 Feb 2019, publ: 3 Feb 2019

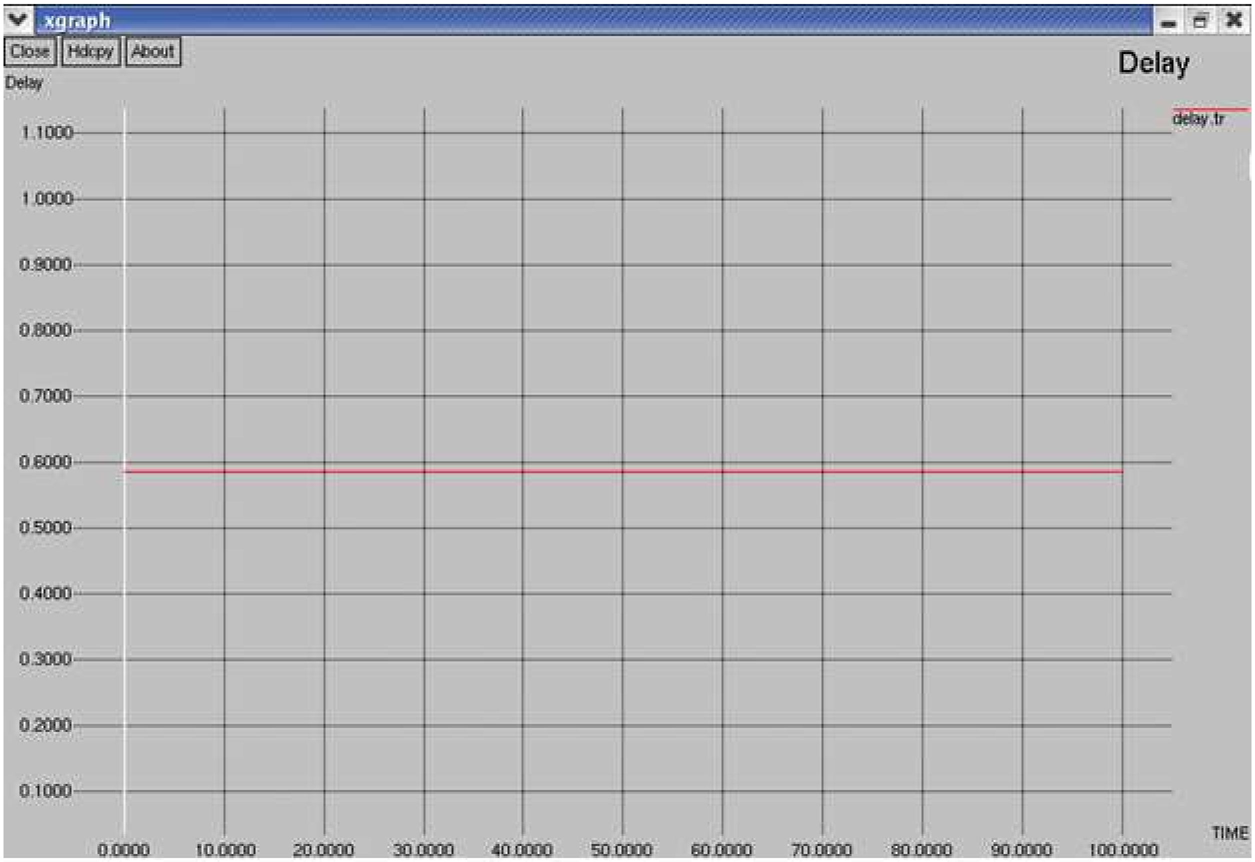


Fig. 4a: the delay in normal trusted transmission

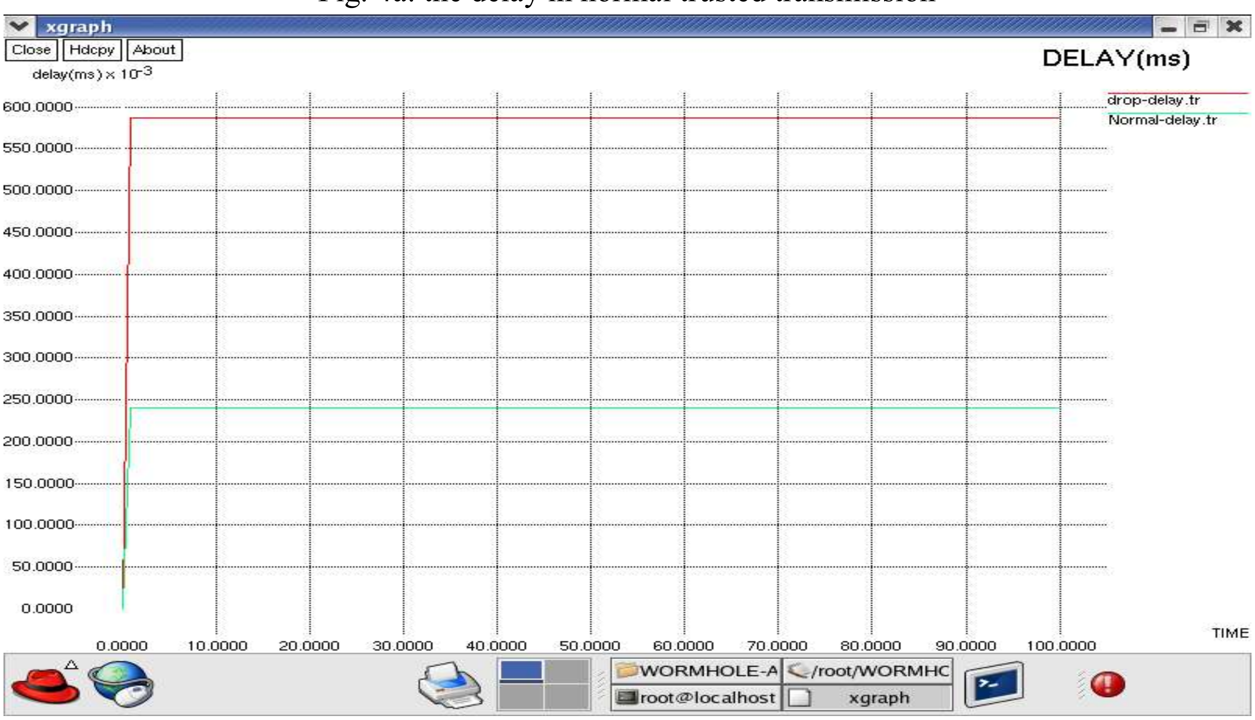


Fig. 4b: the delay with worm-peer and normal transmission

The Figure 4b depicts the delay in transmission through wormhole peer to destination node.

3. Throughput: Throughput is also taken as an inspection metric in our work.

> Throughput is the rate of victorious delivery of the data packets at the target end per unit time. We compute how many bytes were transmitted during time interval specified

Figure 5, conveys that prior to deployment of wormhole nodes the throughput of the network is observed to be very high. But post deployment of the wormhole nodes there is a considerable fall in the throughput of the network. The Red line represents throughput when the tunnel is used to transmit data to the destination node without dropping packets at wormhole node .The formulae used for performance metrics are listed below

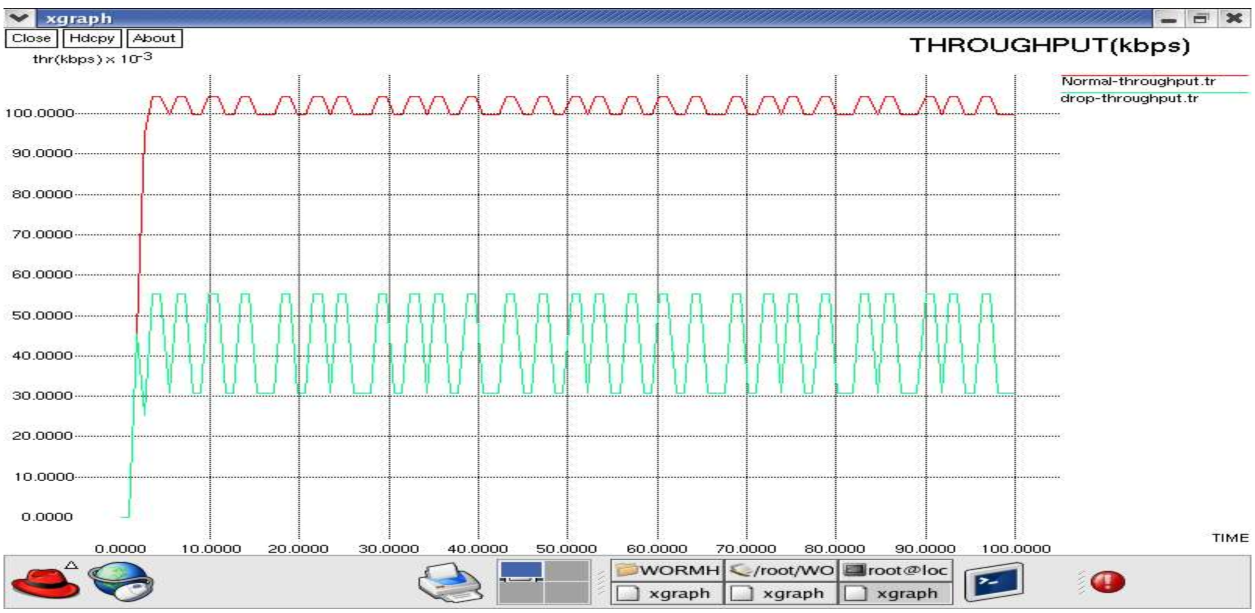


Fig. 5: Comparative analysis of throughput for normal and dropped scenario of worm-hole

The analysis of Drop rate and PDR is collected from the trace file using values generated in table 2 and the formulae.

Formulae

Drop_ratio = (dataRecv / dataSent) / 100;
Throughput = ((dataRecv / 100) * (8 / 1000));
PDR = dataRecv / dataSent;
Delay = (150-5) / dataRecv;
Overhead = ((aodvSent+dataSent)/ dataRecv) + 4.0;

Table 2: Results of simulation

Parameter	Value
Messages Sent	132
Messages Received	394
Messages Dropped	262
Drop Rate	0.03152

Discussion

In our findings, it is observed that the uncoordinated version of wormhole attack involving single malicious node is less disastrous as the malicious activities are carried out at only one node i.e., there could be packet drop at only one end. On the contrary, in the coordinated version of this attack; the effects are more disastrous as these nodes coordinate their actions and communicate via a tunnel to plan and perform malicious activities like packet dropping, delaying the transmission, etc. with the aim to degrade the performance of the subjected network.

In this proposed deployment scheme we were successful in deploying a coordinated version of wormhole attack. It is also discovered that the wormhole nodes can also be deployed by modifying the capabilities of the individual nodes which includes the antenna height, transmission range and transmission power of subjected nodes in the network.

The strength of our proposal is that by deploying an attack, we gain an insight on the conditions that could be responsible for the launch of the attack.

Conclusions

For data to communicate reliably over a network of intermediate nodes, imparting security becomes a vital concern. Wormhole is investigated to be an active attack that could conduct malicious activities, if found; to be in the network. In our work, we presented the algorithm for deploying of wormhole nodes in the network. The conduct of the network prior and subsequent to the deployment of the wormhole nodes is assessed using the NS2 simulator, with PDR, delay and throughput taken as the investigating metrics. This work is pondered to be crucial mainly because, to mitigate any kind of attack we need to first understand under what circumstances these attacks are planted in the network. Hence, with the supporting results; we prove to have succeeded in deploying a wormhole peer in the network.

For future, we aim to propose a mitigation strategy to recognize and intercept against the coordinated and the uncoordinated wormhole peer in the network.

Acknowledgements

We would like to acknowledgment and thank our college management for providing us enough resources for carrying out our work.

References

[1] Sagarika Kar Chowdhury. 2017. Attacks and mitigation techniques on mobile ad hoc network- A survey. International Conference on Trends in Electronics and Informatics ICEI.

[2] Sonia Verma, Jigyasa Sharma, Dr. Sima. 2016. A Study of Active and Passive Attacks In Manet. IJSRD-International Journal for Scientific Research & Development, Vol. 4, Issue 09.

[3] Mayank Kumar Sharma, Brijendra Kumar Joshi. 2016. A mitigation technique for high transmission power based wormhole attack in Wireless Sensor Networks. International Conference on ICT in Business Industry & Government (ICTBIG).

[4] Taranpreet Kaur , Rajeev Kumar . 2018. Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol. IEEE International Conference on Smart Energy Grid Engineering (SEGE).

[5] Piyush Kaneria , 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).

[6] Roshani verma, prof. Roopesh Sharma, Upendra singh. 2017. New Approach through Detection and Prevention of Wormhole Attack in MANET. International Conference on Electronics, Communication and Aerospace Technology ICECA.

[7] R. Thanuja , E. Sri Ram , A. Umamakeswari . 2018. A linear time approach to detect wormhole tunnels in mobile adhoc networks using 3PAT and transmission radius (3PATw). 2nd International Conference on Inventive Systems and Control (ICISC)

[8] Divya Goyal , Amrita Parashar . 2016. Trust computation using D-S in sector based area to detect or preventing worm hole in MANET. International Conference on Inventive Computation Technologies (ICICT).

[9] M. Rmayti , Y. Begriche , R. Khatoun , L. Khoukhi , A. Mammeri . 2018. Graph-based wormhole attack detection in mobile ad hoc networks (MANETs). Fourth International Conference on Mobile and Secure Services (MobiSecServ).

[10] Chitra Gupta , Priya Pathak. 2016. Movement based or neighbor based technique for preventing wormhole attack in MANET. Symposium on Colossal Data Analysis and Networking (CDAN).