International Journal of Scientific Research & Engineering Trends
Volume 2, Issue 2, March-2016, ISSN (Online): 2395-566X

Hop Count Based Conjunction Control Wormhole Detection Approach for MANET

Mithilesh Kumar
Department of Computer Science and Engineering,
ASCT Bhopal, India
Email: er.mithilesh.30@gmail.com

Prof. Praveen Kataria
Department of Computer Science and Engineering,
ASCT Bhopal, India
Email: er.mithilesh.30@gmail.com

***Abstract* – Mobile ad hoc networks are comprised of nodes that must cooperate to dynamically establish routes using wireless links. Routes may involve multiple hops with each node acting as a host and router. Since ad hoc networks typically work in an open entrusted environment with little physical security, they are subject to a number of unique security attacks like wormhole attack. The wormhole attack is considered to be a serious security attack in multi-hop ad hoc networks. In wormhole attack, attacker makes tunnel from one end of the network to the other, nodes stay in different location on two ends of tunnel believe that they are true neighbors and makes conversation through the wormhole link. Unlike many other attacks on ad-hoc routing, a wormhole attack cannot be prevented with cryptographic solutions because intruders neither generate new, nor modify existing, packets, but rather forward existing ones. In this paper a simple technique to effectively detect wormhole attacks without the need for special hardware and/or strict location or synchronization requirements is proposed. The proposed technique makes use of variance in routing information between neighbors to detect wormholes.**

***Keywords* – Mobile Ad Hoc Network, Selfish, Malicious, ICMP, AODV, Hop Count.**

I. INTRODUCTION

Mobile ad hoc network [3] is a form of centralized management involuntarily self-configuration of a plurality of mobile nodes without the need for a fixed infrastructure or network. Each node is prepared with a transmitter and a wireless receiver that lets you communicate with other nodes in its range. For a node to send a packet to a node which is outside the range of the radio supported by other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must behave as both a router and a host at the same time. The network topology changes usually due to the mobility of mobile nodes in the network.

MANET was primarily developed for military works, as nodes are spread across a battlefield and there is no infrastructure to help them form a network. MANETs have been increasing quickly and are steadily more being used in many applications, ranging from military to civilian and commercial uses, since building up such networks can be done without the assist of any infrastructure or interaction with a human. Some examples are search-and rescue missions, data collection, and virtual classrooms and conferences where laptops, PDA or other mobile devices share wireless medium and communicate to each other. As MANETs become widely used, the security issue has become one of the principal concerns. For example, most of the routing protocols proposed for MANETs believe that every node in the network is supportive and not wicked. Therefore, only one compromised node can cause the failure of the entire network.

MANET is vulnerable to various types of attacks. Some attacks affect to general network, some affect to wireless network, and some are particular to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in MANET and all other networks can be generally classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

The wormhole attack is a serious threat to Sensor Network as it cannot be detected easily. In a wormhole attack (figure 1), two attacker nodes join together. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. In the reactive routing protocols such as AODV, the attackers can tunnel each route request packets to another attacker that is near to destination node. When the neighbours of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process. This type of attack prevents other routes instead of the wormhole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed [14].

International Journal of Scientific Research & Engineering Trends
Volume 2, Issue 2, March-2016, ISSN (Online): 2395-566X

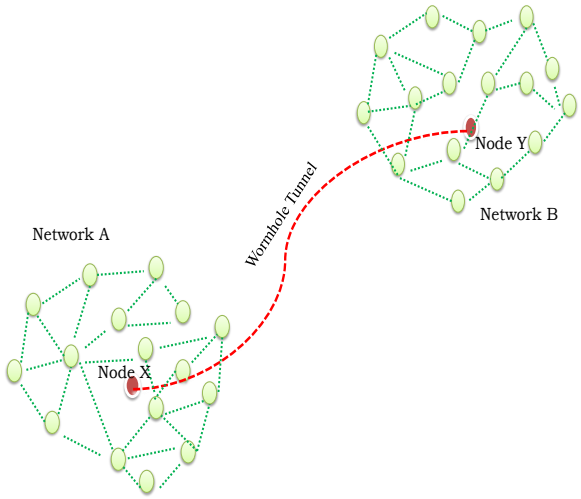

Fig.1. Worm hole

Organization of wormhole depend upon visibility of attacker on the route, wormholes can be classified into three types: closed, half open, and open. As show in figure 1 consider two nodes behave like worm hole stating point (WHS) and worm hole ending point (WHE), represent the malicious nodes and all other node entitle with NNi treated as good node .The nodes between the pipe are the nodes which are on the path but invisible to Source and Destination because they are in a wormhole. In closed wormhole attack tunnel start from source and include the entire intermediate node and where as in open wormhole tunnel start from source but not include the entire intermediate node. In figure 2 , WHS and WHE tunnel the neighbour discovery beacons from Source to Destination and vice versa, for this reason Source and Destination assume that they are direct neighbours to each other. In figure 3, WHS is a neighbour of Source node and it tunnels its beacons through WHN to Destination, Only one malicious node is visible to Source and Destination node. In an open wormhole, both attackers are visible to Source and Destination node as shown in figure 4 [15].

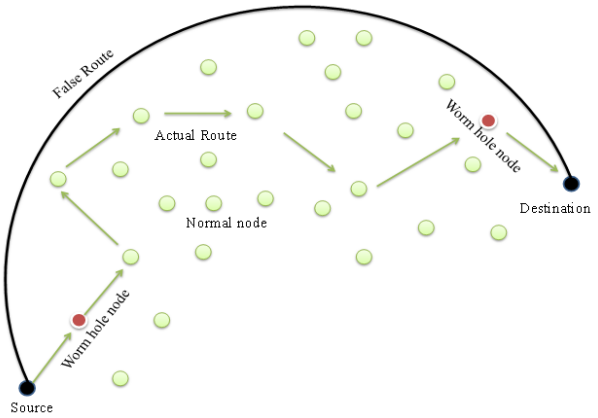

Fig.2. Closed Warm Hole

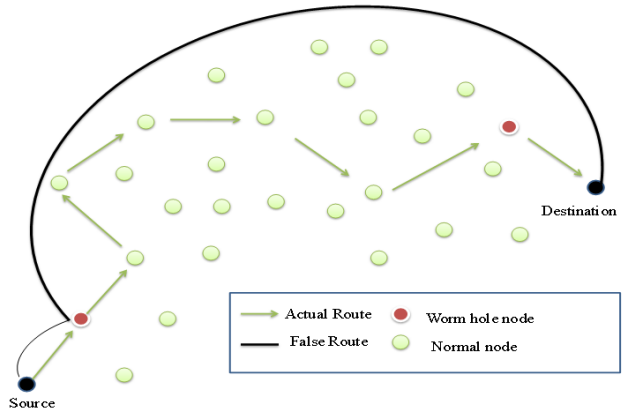

Fig.3. Half Open Warm Hole

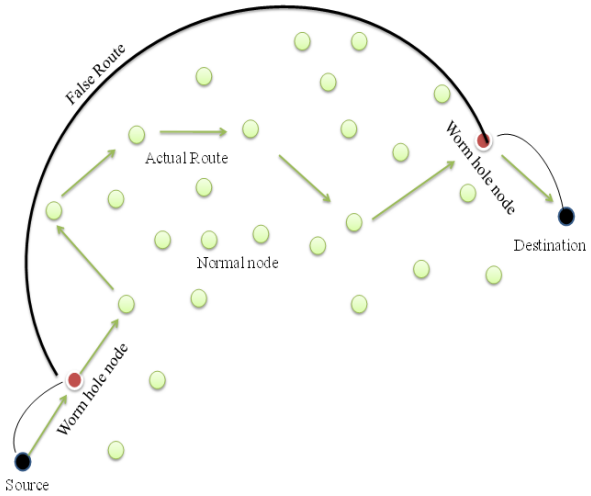

Fig.4. Open Warm Hole

II. Related Work

Marti et al. proposed two techniques that improve throughput in an ad hoc network in the presence of selfish and malicious nodes [1]. The watchdog method is used for each node to detect misbehaving nodes in the network. When a node sends a packet to next hop, it tries to overhear the packet forwarded by next hop. If it hears that the packet is forwarded by next hop and the packet matches the previous packet that it has sent itself, it considers the next hop node behaves well. Otherwise it considers the next hop node is misbehaving. The pathrater uses the knowledge about misbehaving nodes acquired from watchdog to pick the route that is most likely to be reliable. Each node maintains a trust rating for every other node. When watchdog detects a node is misbehaving, the trust rating of the node is updated in negative way. When a node wants to choose a safe route to send packets, pathrater calculates a path metric by averaging the node ratings in the path.

Marti et al. implemented the solutions on DSR protocol using ns2 as simulation environment. The simulation result shows the throughput of the network could be increased by up to 27% in a network where packet drop

attack happens. However routing overhead is also increased by up to 24%.

In [2], authors study the impact of wormhole attacks on a real wireless mesh network test bed. Through theoretical analysis and comprehensive experiments, and find that when a path is under the control of wormhole links, standard deviation of RTT (steed (RTT)) is a more efficient metric than per-hop RTT to identify wormhole attacks. Based on the observation, authors propose a neighbour-probe-acknowledge algorithm (NPA) to detect wormhole attacks by identifying the occurrence of large steed (RTT). The evaluation results on test bed show that the proposed algorithm can achieve near 100% wormhole detection rate and zero false alarm rate both in light and heavy background traffic load scenarios. But, the parameters in NPA are static and not adaptive. So, in the future work on dynamic adjustment of algorithm parameters and routing algorithm that is resilient to wormhole attacks will be done. Furthermore, there will a possibility of adopt the observation to design a new routing protocol which can resilient to inside attacks without triggering the detection frequently to further decrease the overhead.

In [3] authors used the scheme called multi hop count analysis (MHA) with verification of legitimate nodes in network through its digital signature. Destination on node analyses the number of hop count of every path and selects the best path for replying. For checking the authentication of selected path, proposed methodology used verification of digital signature of all sending node by receiving node. If there is no malicious node between the paths from source to destination, then source node creates a path for secure data transfer.

In [4] authors proposed E2SIW, a routing protocol immune to wormhole attacks. E2SIW uses a simple location information and alternate route finding techniques to detect and prevent wormhole attack in ad hoc networks. E2SIW has a high detection rate and less energy requirements compared to the De Worm protocol And also contributed in reducing the overhead associated with the control packets. Most of the work done so far in this topic assumes that the wormhole nodes are not capable of maliciously changing the data passing through them. But this may not always be the case. The design of the mitigation solutions keeping in mind that intelligent malicious nodes may exists is the need of the hour.

In [5] wormhole attack defence strategy of WSN based on neighbour nodes verification. Under this strategy, when each normal node received control packet, it will monitor the packet to determine whether it comes from its normal neighbour nodes to avoid Wormhole attack effectively. Modelling and simulation of WSN based on OMNeT++ shows that the AODV added neighbour nodes verification successfully implement effective defence.

A Defence against Wormhole Attacks in Wireless Networks: As mobile ad hoc network applications are structured, security appears as a central requirement. The author introduces the wormhole attack, a severe attack in ad hoc networks that is mostly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. Author presented the design and performance analysis of a novel, efficient protocol, called TIK, In particular, a node needs to perform only between 3 and 6 hash function evaluations per time interval to maintain up-to-date key information for itself, and roughly 30 hash functions for each received packet. When used in conjunction with precise timestamps and tight clock synchronization, TIK can prevent wormhole attacks that cause the signal to travel a distance longer than the nominal range of the radio [9]. and wireless MAN technology could be sufficiently time-synchronized using either GPS or LORAN-C radio signals.

The wormhole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the wormhole attack in MANET a technique has been proposed. In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network. The wormhole keeps the attacker nodes in a very dominant position as compared to additional nodes in the network. In the immediate routing protocols such as AODV, the attackers can tunnel each route request packets to a different attacker that is close to to destination node. When the neighbors of the destination listen to this RREQ, they will rebroadcast this RREQ and then dispose of all other received RREQs in the same route finding process. This type of attack prevents other routes instead of the wormhole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed [16].

III. PROPOSED SOLUTION

The system model considered for the detection of wormhole using proposed approach includes following: An ad hoc network consisting of n number of nodes. Where P_{ij} denote the set of nodes on the path from node i to node j. The length of the path from node i to j is denoted by l_{ij} hops. We represent the m^{th} node on the path as $P^{m}_{ij,}$ So P^{1}_{ij} will be the one hop neighbor on the path P_{ij} from node i. Let the set of one-hop neighbors of a node i be Ni.

3.1 Main Steps for Detection of Wormhole

In the technique for detecting the wormhole in the path the technique works through the nodes in $P_{S,D}$ by examine the length of alternate routes between nodes that are a short distance apart that is two hop. Consider a source node S that wants to communicate with destination node D and want to test for a wormhole. Let a, b, c belongs to $P_{S,D}$. – they are nodes on the path from S to D that was

International Journal of Scientific Research & Engineering Trends
Volume 2, Issue 2, March-2016, ISSN (Online): 2395-566X

take by using some standard routing protocol. Let the wormhole x1 ↔ x2 connect nodes a and b where a belongs to Nx1 and b belongs to Nx2. Let c be the next hop from b on the route from S to D. Note that a and b are typically separated by several hops, but now will believe that they are neighbors.

The stepwise description of all the process is considers bellow.

1) In the first step the sender node S will set a target node T that is two nodes away from the sender i.e., $T = P^2_{S,D}$.

2) Sender node S will find all its one-hop neighbors NS by sending a "hello" message. The nodes in NS will listen the hello message and will reply to sender S.

3) Sender build a list of the nodes in NS and pointed node $P^1_{S,D}$.

4) Sender will send the list (NS, T) and request every node r excepted the node from which actual path is made to find a route to T. Each node r will run the network routing algorithm and reply to S with l_{rt} the length (in number of hops) of its route to T. If l_{rt} does not exist then r will inform S and S discards r from the list.

1) S will take an alternate route and find its length. The length of the highest route is used. The sender tests for the existence of a wormhole by comparing the length of the "selected route" to T with the direct route. If length L > threshold then the wormhole is detected.

2) If the no wormhole present, then increment the method to the next hop along the route.

3) In the next step run this process for the entire path from source to destination.

IV. PROPOSED ALGORITHM FOR THRESHOLD

Threshold is an important part of the proposed technique. In the technique a wormhole tunnel present in the network or not, is decided by the threshold. If the value of alternate path is greater than the threshold, the wormhole is detected. For deciding the threshold considers a network with n number of nodes. In the network, each and every node finds the alternate route to its two hop neighbor that is called target node. The shortest path of minimum number of hop count of each and every alternate path is taken by the algorithm [1]. After that the algorithm consider the highest number of hop count which is comes from these various alternate paths in the whole network and consider highest hop count as a threshold.

Assumptions:

(a) Total number of node in desire network is TN.
(b) Si represent any node among TN, where i = 1,2,3,…….,< TN.
(c) (RSi)j represent the node that's come in the range of Si.
(d) ((RSi)j)k represent the node that's come in the range of (RSi)j and assume as a target node Tjk for Si.
(e) PST represent path between S and T.
(f) NSi represent the neighbor node of S_i.
(g) ($l_{NSi,Tjk}$) represent number of node in the path $P_{NSi,Tjk}$.

Algorithm:

Step 1
If (i <= TN)
Goto step 2
Else
Threshold (T) = max (nH (PS_i,T_{jk}))

Step 2
If (j <= n(RS_i))
Goto step 3
Else
i++, goto step 1

Step 3
Set S_i as a source node and determine $(RS_i)_j$

Step 4
If (k <= (n$(RS_i)_j$))
Goto step 5
Else
J++, goto step 2

Step 5
Determine $((RS_i)_j)_k$ and set $T_{jk} = ((RS_i)_j)_k$ as a target node for S_i.

Step 6
Set (PS_i, T_{jk}) as a path

Step 7
Determine NS_i node and find route to their respective node T_{jk}
(NS_i, T_{jk}) = $l_{NSi,Tjk}$
And reply in term of number of nodes to S_i

Step 8
Source S_i select max $l_{NSi,Tjk}$ among all (NS_i, T_{jk}) and set
nH(PS_i, T_{jk}) = max ($l_{NSi,Tjk}$)
k++, goto step 4.

V. IMPLEMENTATION DETAIL & RESULT SCENARIO

In order to validate the proposed approach a number of simulation experiments have been performed by using network simulator version 2.32. Table 6.2 shows the parameters used in the simulation experiments. The proposed approach is tested with wormhole using a rectangular scenario of 1000 × 1000 m square area; The network topology consists of different number of nodes. There are two types of communication traffic are used in the NS-2(CBR and FTP), CBR(Constant Bit Rate) traffic is used to generate UDP packets for the simulation. In the simulation, start on 0ms and end on the 100ms. The attack will start on 25ms in the simulation and recheck on 50ms. There are different packet sizes are used in the NS-2, for this simulation 1024KB packet are used. In the simulation the carrier sensing power is defined as 200m.The wormhole is arbitrarily produced somewhere between the sender and the receiver with a arbitrary length that is uniformly distributed between the nodes. The algorithm is implemented by modifying the original AODV source code in NS-2.

International Journal of Scientific Research & Engineering Trends
Volume 2, Issue 2, March-2016, ISSN (Online): 2395-566X

Table 1: Simulation Parameter

Simulation Area	1000mx1000m
Number of Nodes	Vary from 40 to 100
Communication Traffic	CBR
Simulation Duration	100 Seconds
Packet Rate	1024 kbps
CSThreshold Used In Normal Nodes	200 Meter
RXThreshold Used In Normal Nodes	200 Meter

The performance of the algorithm is studied through a number of simulation test for network. Different numbers of nodes in each scenario and wormhole tunnels have been generated for the simulation. The simulation result shows that the detection technique depends on the network density. Threshold that is considered for wormhole detection also depends on the network density.

For the true detection of wormhole, proposed technique compares the hop count with the threshold. So the threshold is an important factor of simulation. If the value of threshold small than the hop count, it will give a higher value of false negative rate and if the value of threshold is higher than the hop count, it will give false positive rate.

In the simulation, first the value of threshold is set one and then the results of the proposed algorithm are calculated. After that, the value of threshold is set two, and the result is again calculated and so on. The simulation of these scenarios shows that increasing the value of threshold the detection ratio of wormhole shows good result. However, it is always not true because after increasing certain value of threshold, it gives false positive result

From the analysis we see that the overhead of our technique is more compared to the existing aodv. A graph of control packet is also shown, because the number of control packets in the proposed technique has increased. In the figure 5, it is shown that when the number of nodes increases the routing load is also increases.

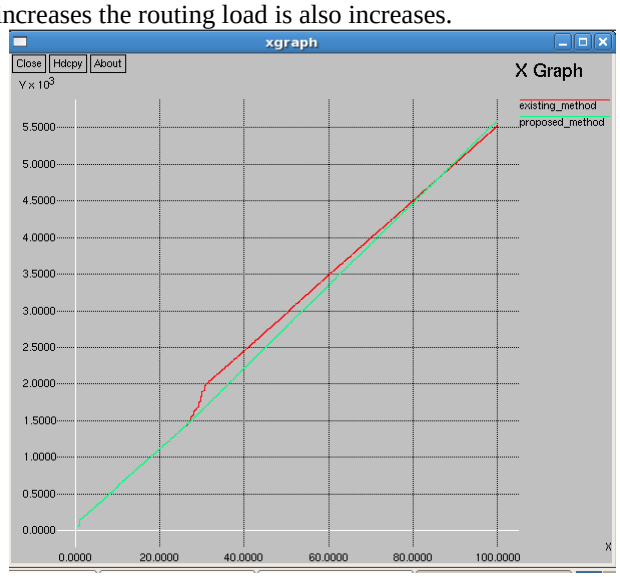

Fig.5. Shows routing load

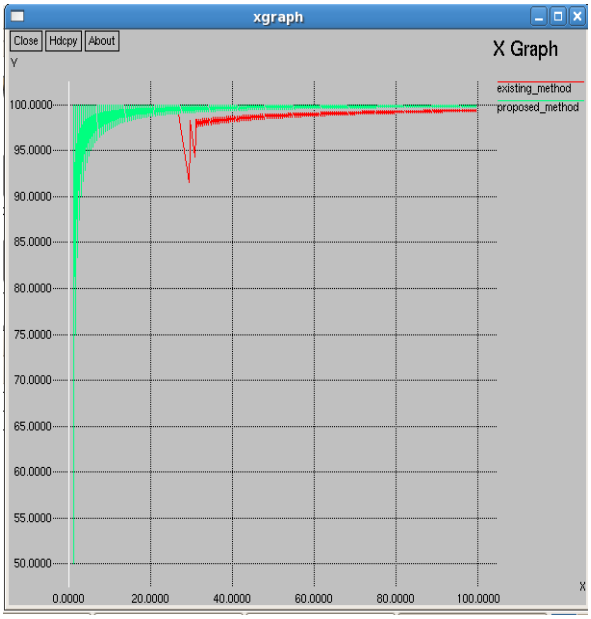

Fig.6. Shows the result of control packet and it shows that when the number of nodes increases the value of control packet also increases

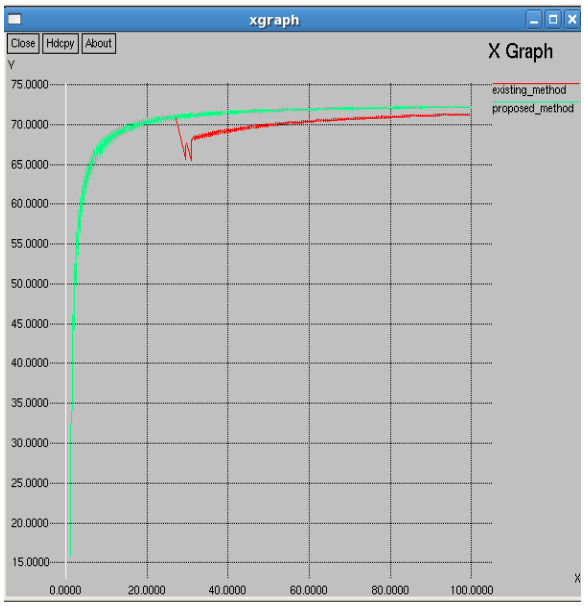

Fig.7. Shows the Result of packet delivery ratio

The above observation shows that the detection technique works efficiently but having some overhead, control packet is also increases in the graph, but the benefit of this technique is that it detects the wormhole, and will serve as an advantage when added to the existing AODV protocol.

VI. Conclusion and Future Work

A simple technique for detecting wormholes in ad hoc networks is presented in the paper. This method employs routing variation between neighbors to determine the

existence of a wormhole. The technique is localized, requires only a small overhead, and does not have special requirements such as location information, accurate synchronization between nodes, special hardware etc. The technique has been tested through simulations for different distributions of nodes for wormholes and different connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent detection probabilities with few false alarms that depend on the value of threshold.

MANET has properties that increase their vulnerability to attacks. We have presented and discussed various issues such as security attacks and threats that can cause vulnerability in Sensor Network. With authenticated assured, secure routing can be successful in MANET & the malicious nodes can be identified and excluded from routing. In future we plan to continue our work in field of securing MANET & present more security probabilistic routing techniques for MANET that avoid worm hole attack by applying special case of Bayesian probabilistic approach for node authentication as dumpster Shafer belief theory of probability.

REFERENCES

[1] Honglong Chena,b,Wei Louc,d, ZhiWang, JunfengWue, ZhiboWang , Aihua Xia "Securing DV-Hop localization against wormhole attacks in wireless sensor networks" in Volume 16, Part A, January 2015, Pages 22–35 , Volume 16, Part A, Elsevier 2015, Pages 22–35

[2] Jie Zhou1, Jiannong Cao, Jun Zhang1, Chisheng Zhang and Yao Yu, "Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Test bed" in 26th IEEE International Conference on Advanced Information Networking and Applications, 2012.

[3] Himani Bathla, Kanika Lakhani, "A Novel Method for Intrusion Detection System to Enhance Security in Ad hoc Network," journal of computing, volume 2, issue 5, may 2010.

[4] Tiranuch Anantvalee, Jie Wu, A Survey on Intrusion Detection in Mobile Ad Hoc Networks.

[5] Katrin Hoeper, Guang Gong, Pre-Authentication and Authentication Models in Ad Hoc Networks.

[6] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proc. of IEEE INFOCOM, 2003.

[7] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in Proc. of CNDS, 2002.

[8] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A secure routing protocol for ad hoc networks," in Proc. Of IEEE ICNP, 2002.

[9] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proc. of NDSS, 2004.

[10] S. Capkun, L. Buttya'n, and J.-P. Hubaux, "Sector: secure tracking of node encounters in multi-hop wireless networks," in Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003.

[11] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in Proc. of IEEE INFOCOM, 2007.

[12] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks," Comput. Netw., vol. 51, no. 13, pp. 3750–3772, 2007.

[13] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks: Research articles," Wirel. Commun. Mob. Comput., vol. 6, no. 4, pp. 483–503, 2006.

[14] X. Su and R. V. Boppana, "On mitigating in-band wormhole attacks in mobile ad hoc networks," in Proc. of IEEE ICC, 2007.

[15] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks.

[16] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Wormhole Attacks in Wireless Networks

[17] C. Perkins, E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," The Internet Society 2003.

[18] R. Barr. Ji, "Java in Simulation Time: User Guide and Tutorial", Sept. 2003.