A Novel Approach for Detection and Prevention of Wormhole Attack In Ad-hoc Networks

Monika[#1] , Jyoti Thalor[*2]

[1]Assistant Professor, Department of Computer Science & Applications, Kurukshetra University Kurukshetra, Haryana, India

[2]Department of Computer Science & Applications, Kurukshetra University Kurukshetra, Haryana, India

***Abstract*— MANET, due to the nature of wireless transmission, has more security issues compared to wired environments. In this paper we specifically considering Tunnelling attack which does not require exploiting any nodes in the network and can interfere with the route establishment process. Wormhole attack is a network layer attack observed in MANET, which completely disrupts the communication channel. Instead of detecting suspicious routes, we suggest a new method which detects the attacker nodes and works without modification of protocol, using a hop-count analysis from the viewpoint of users without any special environment assumptions. The tunnelling attack is simulated using OPNET and proposed work showing the detection and isolation algorithm.**

***Keywords*— Intrusion Detection, Mobile Ad hoc network security, Wormhole detection techniques, hop-count analysis, network security, Tunnelling attack.**

1. Introduction

A mobile Ad hoc network is a collection of two or more devices or nodes using wireless communication and networking capabilities [1][2]. Mobile Ad-hoc network (MANET) is composed of collection of independent mobile hosts connected by wireless links without any fixed administration. MANET is characterized by its dynamic topology, multi hop routing, energy limited operations and network scalability. Malicious nodes carry out both active and passive attacks [2] due to the open and ad hoc nature of MANET. In all possible methods of attacks in Mobile Ad hoc Networks (MANETs), the wormhole attack is one of the most threatening and hazardous attacks. A wormhole attack is usually performed by two or more malicious nodes in conspiracy. Two malicious nodes at different locations send received routing messages to each other via a secrete channel. In this way, although the two malicious nodes are located far from each other, they appear to be within one-hop communication range. Therefore, the route passing through the malicious nodes is very likely to be shorter than any other regular one. Wormhole nodes can easily grab the route from the source node to the destination node, and then sniff, drop, or selective-drop data packets passed by. The wormhole attack can be launched regardless of the MAC, routing, or cryptographic protocols used in the network and is thus difficult to defend against.

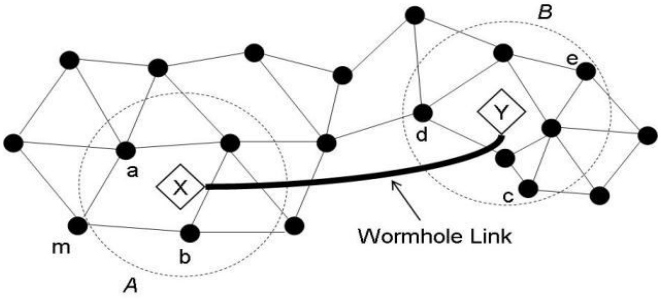


Fig 1 Wormhole attack

Here X and Y be two intruder connected by wormhole link. X replay in its neighbourhood (in area A) everything that Y hears in its own neighbourhood (area B) and vice versa . The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbours and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through them and use the large amount of collected information to break any network security. In a wormhole attack using wired links or a high quality wire-less out-of-band links, attackers are directly linked to each other, so they can communicate swiftly. However they need special hardware to support such communication. On the contrarily, a wormhole using packet encapsulation is relatively much slower, but it can be launched easily since it does not need any special hardware or special routing protocols [1] [2] .

2. WORMHOLE ATTACK

In this section we explain the wormhole attacks modes and classes while pointing to the impact of the wormhole attack and the efforts that have been done in the literature to detect and prevent this attack.

Wormholes using Out-of-band attack- This mode of the wormhole attack is launched by having an out-of-band high-bandwidth channel between the malicious nodes. This channel can be achieved, for example, by using a long-range directional wireless link or a direct wired link. This mode of

attack is more difficult to launch than the previous one since it needs specialized hardware capability. Consider the scenario depicted in Figure 2[10]. Node *A* sends a route request to node *B*, and nodes *X* and *Y* are malicious nodes having an out-of-band channel between them. Node *X* tunnels the route request to *Y*, which is a legitimate neighbour of *B*. Node *Y* broadcasts the packet to its neighbours, including *B*. *B* gets two route requests—*A-X-Y-B* and *A-C-D-E-F-B*. The first is both shorter and faster than the second, and is thus chosen by *B*.

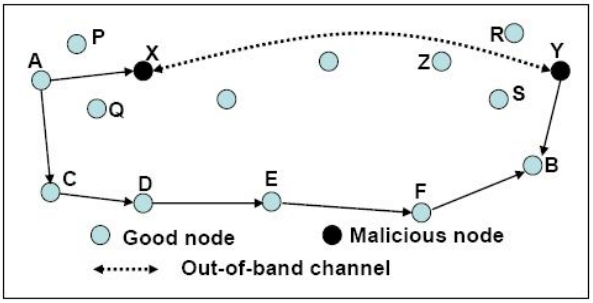


Fig 2 Wormholes through out of band channels [10]

Wormholes using Packet Encapsulation- Consider Figure 3 [10] in which nodes *A* and *B* try to discover the shortest path between them, in the presence of the two malicious nodes *X* and *Y*. Node *A* broadcasts a route request (*REQ*), *X* gets the *REQ* and encapsulates it in a packet destined to *Y* through the path that exists between *X* and *Y* (*U-V-W-Z*). Node *Y* get the packet, and rebroadcasts it again, which reaches *B*. Note that due to the packet encapsulation, the hop count does not increase during the traversal through *U-V-W-Z*. Concurrently, the *REQ* travels from *A* to *B* through *C-D-E*. Node *B* now has two routes, the first is four hops long (*A-C-D-E-B*), and the second is apparently three hops long (*A-X-Y-B*). Node *B* will choose the second route since it appears to be the shortest while in reality it is seven hops long.

Any routing protocol that uses the metric of shortest path to choose the best route is vulnerable to this mode of wormhole attack. This mode of the wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic information, nor do they need any special capabilities, such as a high speed wire line link or a high power source. A simple way of countering this mode of attack is a by-product of the secure routing protocol ARAN [10], which chooses the fastest route reply rather than the one which claims the shortest number of hops.

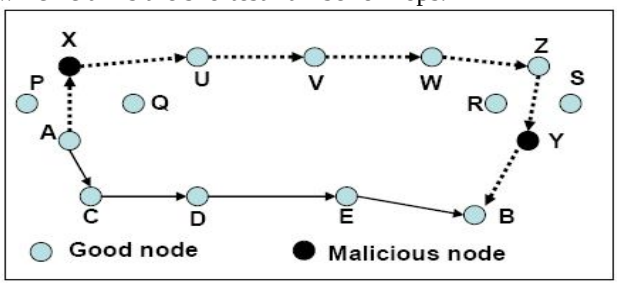


Fig 3 Wormhole Attack using packet encapsulation [10]

Wormholes with High Power Transmission- In this mode, when a single malicious node gets a RREQ, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high-power broadcast rebroadcasts it towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a colluding node.

Wormholes using Packet Relay - In this mode of the wormhole attack, a malicious node relays packets between two distant nodes to convince them that they are neighbours. It can be launched by even one malicious node. Cooperation by a greater number of malicious nodes serves to expand the neighbour list of a victim node to several hops. For example, assume that node. *A* and node *B* are two non-neighbour nodes with a malicious neighbour node *X*. Node *X* can relay packets between nodes *A* and *B* to give them the illusion that they are neighbours.

3. RELATED WORK

In this section we review works related for the wormhole attack defences.

Packet leash[3] in is a mechanism to detect wormhole attack. The mechanism proposes two types of leash for this purpose. Geographic leash and Temporal leash. In Geographic Leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through wormhole or not. In Temporal Leashes, the sender appends the sending time to the packet and the receiving node computes a travelling distance of that packet assuming propagation at the speed of the light and using the difference between packet sending time and packet receiving time. This solution requires a fine grained synchronization among all nodes.

Similar packet leash, In references [3], SECTOR which does not require any clock timing synchronization and location information by using mutual authentication. Node A estimates the distance to another node B in its Transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of Flight, A detects whether or not B is a neighbour or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash is in references [18] presented a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. With the help of extensive simulations, demonstrate that scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network

establishment and operation phase. In reference [6], both hop-count and delay per hop indication (DELPHI) are monitored for wormhole detection. The fundamental assumption is [6] is once again that the delay a packet experiences under normal circumstances for propagating one hop will become very high under wormhole attack as the actual path between the nodes is longer than the advertised path. Like [6], the proposed methodology in [6] for wormhole detection is also a two step process. In the first phase the route path information are collected from a set of disjoint paths from sender to receiver. Each sender will include a timestamp on a special DREQ packet and sign it before sending it to the receiver. Each node upon receiving the packet for first time will include its node ID and increase the hop count by 1 and discards the packet next time onwards. The DREP packets will be sent by the receiver for each disjoint path received by it. This procedure is carried out for three times and the shortest delay as well as hop count information will be selected for wormhole detection. In the second phase, the round trip time (RTT) is taken by calculating the time difference between the packet it had sent to its neighbour and the reply received by it. The delay per hop value (DPH) is calculated as RTT/2h, where h is the hop count to the particular neighbour. Under normal circumstances, a smaller h will also have smaller RTT. However, under wormhole attack, even a smaller hop count would have a larger RTT. If one DPH value for node X exceeds the successive one by some threshold, then the path through node X to all other paths with DPH values larger than it is treated as under wormhole attack.

4. Wormhole Detection and Prevention Algorithms

1. Hop Count Based Detection

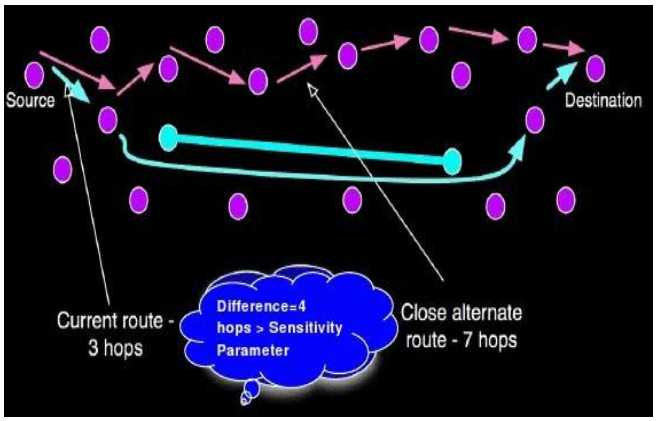


Fig 4 Wormhole example

Wormhole attack generally refers to the network layer but it also effect to the physical layer as well. This method is used to detect wormhole attack and isolate it.The source node S as shown in figure will initially established route to destination and now want to check wormhole attack or not. Source node has to start with each one hope neighbour and discover attacker node. After receiving replies source node create routing table of all one hop neighbours that excludes the next hop along the route. The source will check the routes that are used by these one-hop neighbours to the second hop along the route to the destination. Node S compares the length of a selected route with the one he has to the target node. The selected route is chosen from the routes reported from the neighbours. If the difference between the numbers of hops of the two routes is greater than a certain value called the "VERGE VALUE", the source will consider that a wormhole presents. If not, this process is repeated by each node that lies on the route (such nodes also exclude the previous hop from the list).

2. Inconsistency node detection

The principle of Wormhole Route Reply Decision Packet [18] is to allow neighbouring nodes of a wormhole node to notice that the attacker node has great capability of competition in path discovery. In the path discovery , an intermediate node will attempt to create a route that does not go through a current neighbour node, which has a route-building rate higher than the threshold. Thus, not only are wormhole nodes gradually identified and isolated by their normal neighbouring nodes.

3. Neighbour List Based Detection

In this method secure neighbour discovery from source to destination obtained by neighbour list and detect the inconsistency if attack is present.

- Each node sends a HELLO message for the neighbour discovery immediately after the deployment of the mobile nodes. Each node that receives a HELLO message sends a RREP.
- Each node builds its neighbour list which could include remote neighbours connected by a wormhole. The neighbouring nodes interchange their neighbour lists.
- Each node will compare its neighbour list with its neighbours' neighbour list. If they are similar, either these nodes are close enough or are connected by a wormhole.
- Next, both of these nodes and their neighbours will rebuild their neighbour lists which will remove these two nodes and their neighbours.

Algorithms steps-

1. Source to destination route establishment- Source send RREQ to all its neighbour nodes.

Destination Address	SEQ. NO	Source address

RREQ

2. When RREQ received by neighbour nodes they match destination address if match then stop otherwise repeat till destination not found.
3. RREQ is broadcast RREP is unicast by destination node.
4. RREP Contains

Rrep_count	Neighbour_list(destination)

Where neighbour_list (destination)= Destination's neighbour list

5. Route from source to destination established. Each intermediate node increase rrep_count.
6. Source save neighbour_list(destination) and hop_count. (between source to destination).Hop_count (HC) is defined as no. of nodes between source to destination.
7. To check neighbour list verification go to step 12.
8. Now source send route_reply_dec to destination and confirm to the destination about their participation in route.
9. Destination conatins neighbour_list(source) through route_reply_dec

Route_reply_dec_count	Neighbour_list(source)

10. Each intermediate node increase route_reply_dec_conut by 1 and forward towards source to destination. Each node select second node as a target node.
11. To check hop_count verification go to step 17.

#Neighbour list detection method

12. neighbour_list(source) and neighbour_list(destination)
Compare both of them and calculate matching node between them.
13. For(i=0;i<no_source_neighbour;i++)
For(j=0;i<no_destination_neighbour;j++)

If(neighbour_list(source)(i)=neighbour_list(destination)(j))
Common_node++;
14. Depend on HC value set neighbour_verge.
15. If common_node>neighbour_verge
Wormhole may be present
16. Go to step 32.

#Hop Count detection method

17. Each node send hop_catch to all its neighbour node .It contains the target node ID.
18. Hop count between sources to next selected target is 2. Selected node show target_HC between their neighbour node to the target node.
19. Each one hop neighbour find target_HC entry in routing table.
20. If target ID not present in the table we send RREQ to find target_HC.
21. In general cases one hop neighbour of source can reach destination node by 3 hops (maximum hop) and by 1 hop (minimum hop).

If target_HC >3
Then Last node is wormhole node.
Fix target_HC as HC_verge.
Verge value between 3 to 6.
By fixing minimum verge value we can identify all wormhole nodes. But sometimes it can be false positive. To avoid this we set verge value of hop count according to the environment variable.

22. If target_HC >HC_verge
That confirms previous node and target node is wormhole nodes.
23. Go to step 32.
23. Go to step 24.

#Inconsistency presence of node

24. Each Node sends Hello message to its entire neighbor periodically to check the presence of neighbors. We create an additional field Inconsist_value.
25. Inconsist_value is defined as unexpected behaviour or presence of nodes if an node present in different routes.
26.
$$\text{Inconsist\_Value} = \frac{\text{route\_reply\_dec\_count}}{\text{Route\_reply\_count} + 1}$$
27. Each node who receive HELLO message check it's value.
28. for all nodes Inconsist_Value should be less than 1(always). But on starting it's value is set to 0. It varies from ½,2/3,3/4,4/5……. So on.
29. Inconsist_verge_value=1;
30. if neighbour node have high Inconsistancy value then surly that node is wormhole nodes
31. Go to step 32.

#Wormhole Node Removal

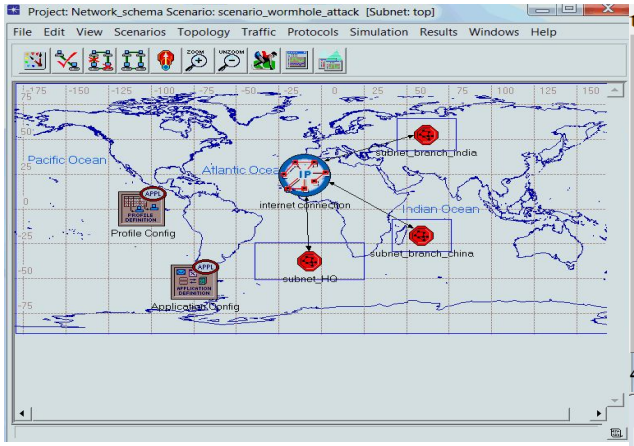
32. Send worm_annouce message to all nodes
33. Any node receives worm_annouce message it removes wormhole node id from its neighbor table and Routing Table.
34. If any forwarding node receives worm_announce message it will send RERR message to source. It will reinitiate route discovery process, and find the new path to the destination without wormhole node.

5. Simulation Result-

This simulation result shows the implementation of Ad Hoc network into opnet simulator . To explain the behaviour of network with or without wormhole attack we take 2 network scenarios. In one network perform normal and in another network show the wormhole attack. To simulate these we take servers (FTP,EMAIL, HTTP,DATABSE). Performance of these also changes as well as these characteristics related to packets.

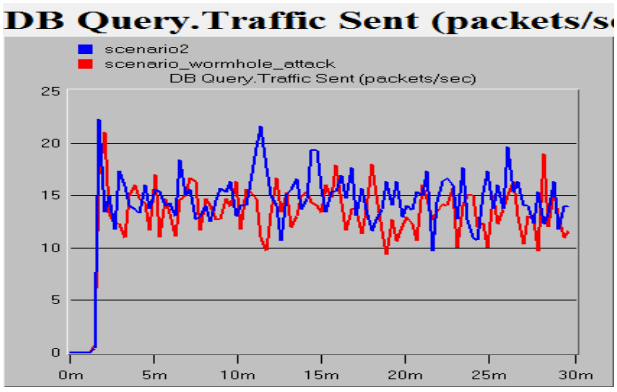
Topology of network- In each subnet branch we uses an star topology for connection, one firewall and routers also. Main subnet contain server to measure performances. For the simulation we have created some predefined node models from library. The details of models with their technical parameters are as follows (OPNET)-

Total Nodes = 10
Infected node=3
Packet size = 1024 bits constant
Applying protocol=AODV

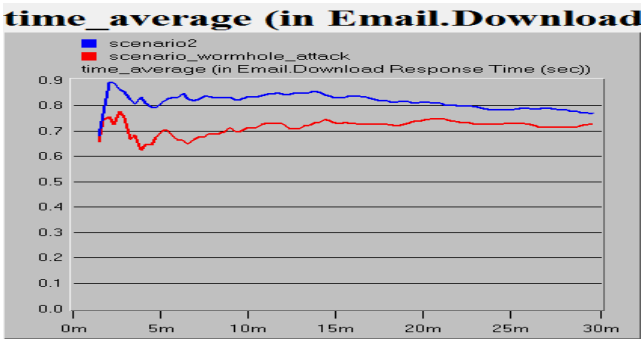


Network outer scenerio

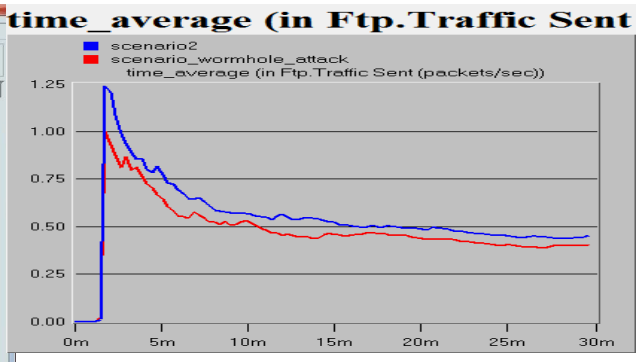
1) Database Query traffic sent(packets/sec)



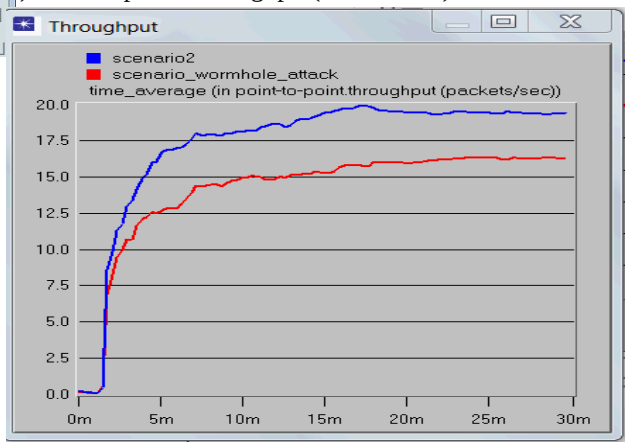
2) E-mail Server Time_average (response time(sec))- Download response time of scenario with wormhole attack in decrease with time.



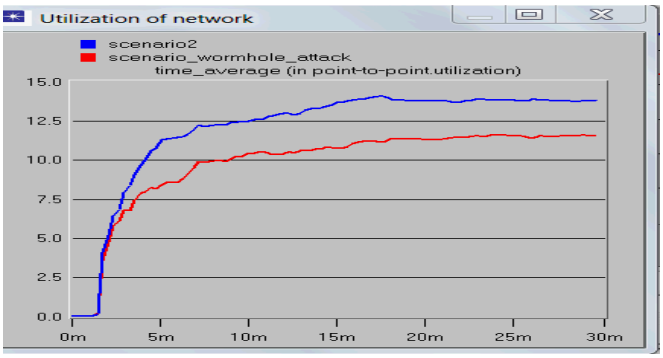
3) FTP Server (time _average) – File transfer protocol also effected by attacker nodes. Total time average of traffic sent diminished by attacker nodes, as shown in graph.



4)Point-to-point Throughput(Packets/sec)-



5) Utilization of network -



6. Conclusion-

In this study we analysed the effects of wormhole attack in ad hoc wireless networks. We implemented a network that simulates the behaviour of wormhole attack in OPNET and comparing features of services provided by the network . That shows that how attack effect whole network services. We have given an simple algorithms that detect and isolate wormhole attack. This algorithm has better performance comparing to three individual methods [Hop count, Inconsistency based, Neighbour list methods].The solution detects the malicious nodes and isolates it from the active data forwarding. As from the results we can easily infer that the performance of the normal AODV drops under the presence of worm hole attack .As a future work we can implement this algorithm to show the whole procedure of attacker node detection and isolation.

REFERENCES

1. Perkins,Charles E, "Ad- Hoc Networking", Addision-Wesley,2001.
2. Perkins C. and Royer E. "Ad hoc on-demand distance vector routing ," *In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications*, pp.90-100
3. Srdjan Capkun, L.evente Buttyan, and Jean-Pierre Hubaux, 2003 "SECTOR: Secure Tracking of Node Encouters in Multi-hop Wireless Networks,"*In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS)*, pp. 21-32.
4. Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 "Packet Leashes : A Defence against Wormhole Attacks in Wireless Networks", *Twenty-Second ANNUAL Joint Conference of IEEE Computer and Communication*s , pp. 267-279.
5. Lingxuan Hu and David Evans, Feb. 2004 "Using Directional Antennas to Prevent Wormhole Attack ",In *Proceedings of the Network and Distributed System Security Symposium*, pp. 131-141.
6. Chiu, HS; Wong Lui KS, 2006 "DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks",*In Proceeding of International Symposium on Wireless Pervasive Computing*, pp. 6-11.
7. Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, Nov. 2008 "Analysis of wormhole Intrusion Attacks In MANETS",IEEE Military Communications Conference,MILCOM 2008.
8. Y.-C. Hu, A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, Security and Privacy Magazine IEEE V2I3 ,2004
9. R. S. Khainwar, A. Jain , J. P. Tyagi , Dec 2011 ,"Elimination of Wormhole Attacker Node in MANET Using Performance Evaluation Multipath Algorithm " *International Journal of Egineering Technology and Advanced Engineering*, Volume 1, Issue 2, pp. 40-47.
10. Issa Khalil, Saurabh Bagchi, Ness B. Shroff." LITEWORP: a Lightweight countermeasure for the wormhole attack in multihop wirelessnetworks". *In the proceedings of the international conference on dependable systems and networks* (DSN'05); 2005.
11. Issa Khalil, Saurabh Bagchi, and Ness B. Shroff. MOBIWORP: mitigation of the wormhole attack in mobile multihop , wireless networks. In the IEEE securecomm and workshops; 2006.
12. Xia Wang, Intrusion detection techniques in wireless ad hoc networks. *In the proceedings of the IEEE international computer software and applications conference; 2006*
13. Xia Wang and Johnny Wong, An end-to-end detection of wormhole attack in wireless ad-hoc networks. *In the proceedings of the 31st annual international computer* software and applications conference (COMPSAC); 2007.
14. Hu Yih-Chnu, Perrig Adrian, Jonhson David B. Wormhole attacks in wireless networks." *IEEE Journal on Selected Areas in Communication2006"*.
15. Lazos L, Poovendran R, Meadows C, Syverson P, Chang LW. Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach. "*In the proceedings of the IEEE conference on wireless communications and networking*; 2005", vol. 2. pp. 1193–9.
16. F. Natt-Abdesselam, B. Bensaou, T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Network", *IEEE Communications Magazine*, 46(4), pp. 127-133, 2008.
17. M.A. Gorlatva, P. C. Mason, M. Wang, L. Lamont, R. Liscano, "Detecting Wormhole attacks in Mobile A d Hoc Networks through Protocol Breaking and Packet Timing Analysis", In IEEE Military Communications Conference, pp. 1-7 ,2000
18. Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks" , *In Proceedings of the International Journal of Computer Theory and Engineering, Vol. 2, No. 1* February, 2010, pp.78-86.
19. Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. pp. 2-17.
20. M.S.Sankaran, S.Poddar, P.S. Das, S.Selvakumar "A Novel Security Model SaW: Security against Wormhole attack in Wireless Sensor Networks", *In Proceeding of International Conference on PDCN*, 2009.
21. Khin Sandar Win "Analysis of Detecting Wormhole Attack in Wireless Sensor Networks",World Academyof Science, Engineering and Technology, 2008,pp.422-428.
22. I.Khalil, S.Bagchi, N.B.Shroff, "A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", *In Proceedings of the 2005 International Conference on Dependable Systems and Networks (*DSN'05).
23. Maria Alexandrovna Gorlatova "Review of Existing Wormhole Attack Discovery Techniques" *A Contractor report at DRDC Ottawa*, pp. 1-23, August , 2006.
24. S.Choi, D.Kim , D. Lee, J. Jung " WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Network ", *In Proceeding International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*, 2008, pp. 343-348.
25. Guoxing Zhan, Weisong Shi, and Julia Deng, 2012 "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" *IEEE Transactions on Dependable and Secure Computing*, Volume 9, Issue 2, pp.184-197.
26. H. Vu, A. Kulkarni, K. Sarac, N. Mittal. "WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks". In *Proceedings of International Confernce on Wireless Algorithms Systems and Applications*, LNCS 5258, pp. 491-502, 2008.
27. On the Survivability of Routing Protocols in Ad Hoc Wireless Networks, A. Baruch, R. Curmola, C. Nita-Rotaru, D. Holmer, H. Rubens, Convergence on Security and Privacy for Emerging Areas Communications, Secure Comm 2005, September 2005.
28. Ritesh Maheshwari, Jie Gao and Samir R Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity In-formation", *Department of Computer Science, Stony Brook University Stony Brook, NY 11794-4400, USA.*