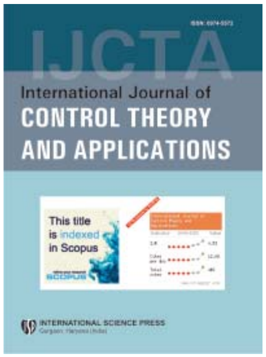


International Journal of Control Theory and Applications

ISSN : 0974–5572

© International Science Press

Volume 9 • Number 40 • 2016

Taxonomy of Worm Hole Attack Solutions in MANET

G. Usha[a] S. Kannimuthu[b] D. Bhanu[c] K.S. Bhuvaneshwari[d] and H. Karthikeyan[e]

[a]*Assistant Professor(Sr.G), Department of Software Engineering,SRM University, Kattankulathur, Kanchipuram Dt*

[b]*Associate Professor, CSE, Karpagam College of Engineering, Coimbatore*

[c]*Professor, Department of IT, Karpagam Institute of Technology, Coimbatore*

[d]*Associate Professor, Department of CSE, Karpagam College of Engineering, Coimbatore*

[e]*Assistant Professor(O.G), Department of Software Engineering, Kattankulathur, Kanchipuram Dt*

Abstract: Mobile Adhoc Network (MANET) does not have any fixed infrastructure. Self and easy deployment feature of MANET makes it easy to use anywhere and at any place. MANET consists of a collection of mobile nodes and does not rely on any wired resolution network. In MANET, security is one of the critical tasks because any nodes can join and leave the network at any time. Worm hole attack is the most critical and serious routing attack where it affects the communication path between the nodes. In this paper we focus about the problems caused due to worm hole attack and we provide a taxonomy solutions proposed to detect worm hole attack. We also analyzed various network parameters that are used to defend worm hole attack. Finally, we conclude our paper with future work.

Keywords: *Mobile adhoc networks; Worm hole attacks; tunnelin;, security; malicious nodes)*

1. INTRODUCTION

Communication is an important role in nowadays world. MANET communication is the most important concept because MANET's does not have any fixed infrastructure. MANET does not require any backbone network or wire connection. The advantage of MANET is any node can join and leave the network at any time. Infrastructure less nature of MANET makes vulnerable to many types of attacks. Hence securing MANET is one of the key area of research community. MANET networking environment suffers for various types of attacks. One of the most vulnerable attack is known as worm hole attack. The attacker node create tunnel between the nodes. Once the tunnel has been created the worm hole node pretends to be the normal node in the communication path and creates an illusion that it is normal neighbor node in the network. The worm hole nodes create the shortest path among them and this route is shorter compared to other communication path in the network. The working of worm hole attack is explained below. The worm hole node consists of two attacker nodes where each nodes are tunneled by a link. The attacker nodes in the network captures the packet from legitimate nodes and encapsulate the packets and transmits the packets in to the tunnel. The tunnel can be formed inband or outband. The following Figure 1 displays in band channel tunnel and Figure 2 displays outband channel tunnel.

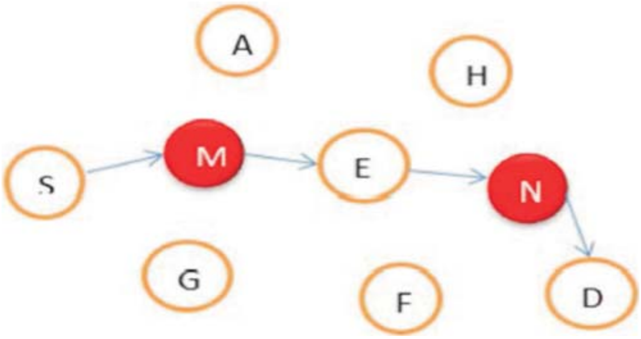


Figure 1: Inband Channel

In Fig1, initially the source node S broadcasts the RREQ packets, in return the malicious node M in the network replies that it has the shortest route towards the other nodes in the network. Hence the source node starts forwarding the packets through the malicious nodes. In that way, the malicious node become part of the network, distract the normal communication and drop the packets, reduces bandwidth of the MANET.

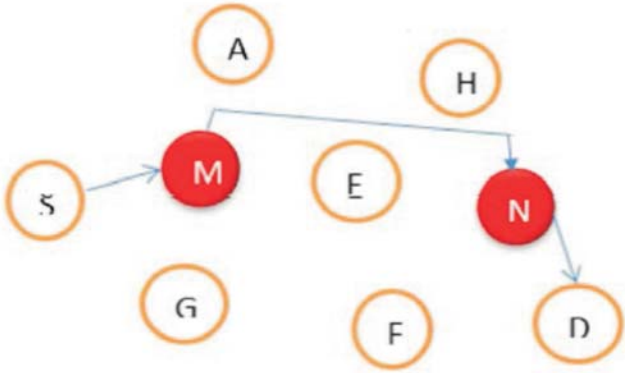


Figure 2: Outband Channel

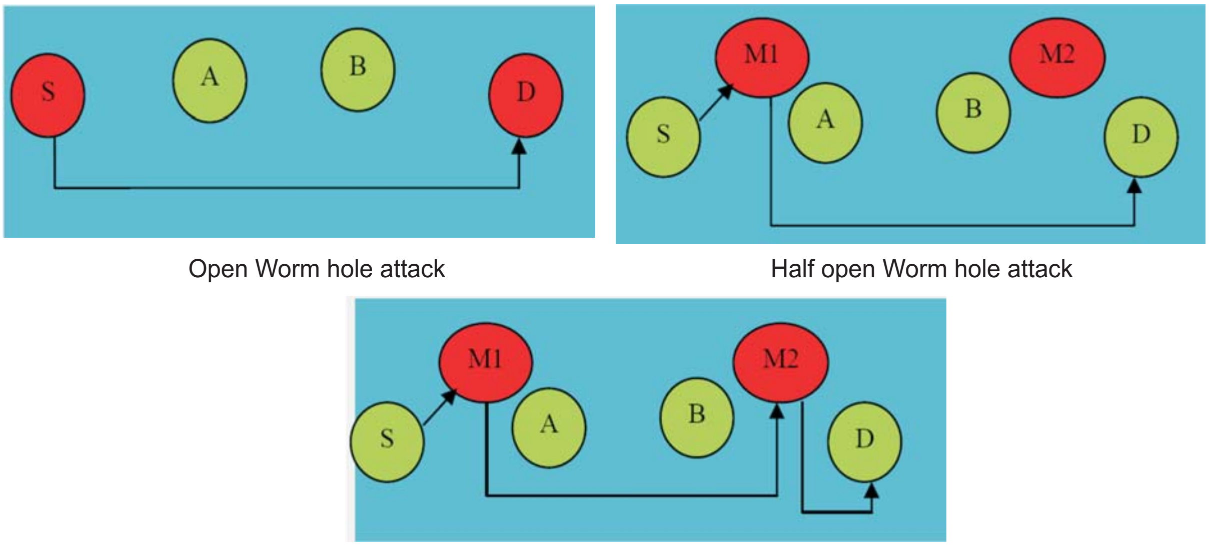
In Fig 2, the nodes M and N are worm hole nodes that form tunnel among them. Thus the packets from source node to destination node D are tunneled by the worm hole nodes M and N. In this way the worm hole node forms outband channel.

The organization of the paper is as follows: Section II we present types of worm hole attack, Section III we present security solutions suggested in literature against worm hole attack. Finally we conclude the section with concluding remarks and future work.

2. TYPES OF WORM HOLE ATTACKS

Based on the literature [1-5] it is observed that there are following types of worm hole attacks are there. They are

1. Open wormhole attack/Exposed
2. Half open wormhole attack
3. Closed wormhole attack/hidden
4. Worm hole using Encapsulation
5. Worm hole using high power transmission



Open Worm hole attack

Half open Worm hole attack

Closed Worm hole attack

Figure 3: Design of Open, Half open and Closed wormhole attack

The above diagram represents the design of open, half open and closed wormhole attacks.

1. **Open Wormhole attack :** The Source node S and Destination node D forms the tunnel and traverse the packet among themselves. These nodes include themselves in the packet header and follows the route discovery procedure.

2. **Half open wormhole attack:** The malicious node M1 overhears the network and forms a tunnel between nodes S-M1-D. The another malicious node M2 instead hides the network and tunnels the packet from one side of wormhole to another side of the network. In this way the packets are rebroadcasted to another side maliciously and may flood the network.

3. **Closed wormhole attack:** The worm hole nodes M1 and M2 occupies between source node ,destination node and intermediate nodes. Thus the normal nodes think that they are one-hop away from each other. Thus the malicious fake nodes are formulated in the network.

4. **Wormhole using Encapsulation:** In this method, the malicious node overhears the RREQ packet where it forwards the malicious packet to some other location. Then another malicious wormhole node rebroadcasts the RREQ packet and drops the further legitimate packet on legitimate multihop path.

5. **Wormhole using High power Transmission:** In this type a malicious wormhole node exploits the energy of the normal nodes in the network by requesting a Route Request(RREQ) packet by using at a maximum level of energy. Hence the other nodes in the network lack of power capacity to broadcasts the packet towards the destination.

3. SECURITY SOLUTIONS AGAINST WORMHOLE ATTACK

In this section we will discuss about various types of security solutions provided by various authors in literature. We will provide a taxonomy to understand the attacks and its solutions in details. Figure 4 explains the mind map technique about the proposed taxonomy for worm hole attack detection technique.

The techniques which are proposed in literature are discussed one by one in following paragraph. Each technique has its own advantage and disadvantage.

1. **Packet Leash Technique:** This technique uses reactive routing[11] protocols to detect worm hole attacks in MANET. Leash is defined as an information added to a packet which restrict the transmission distance of a given packet. They proposed two kinds of leashes which are known as

   a) Geographical Leashes

   b) Temporal Leashes

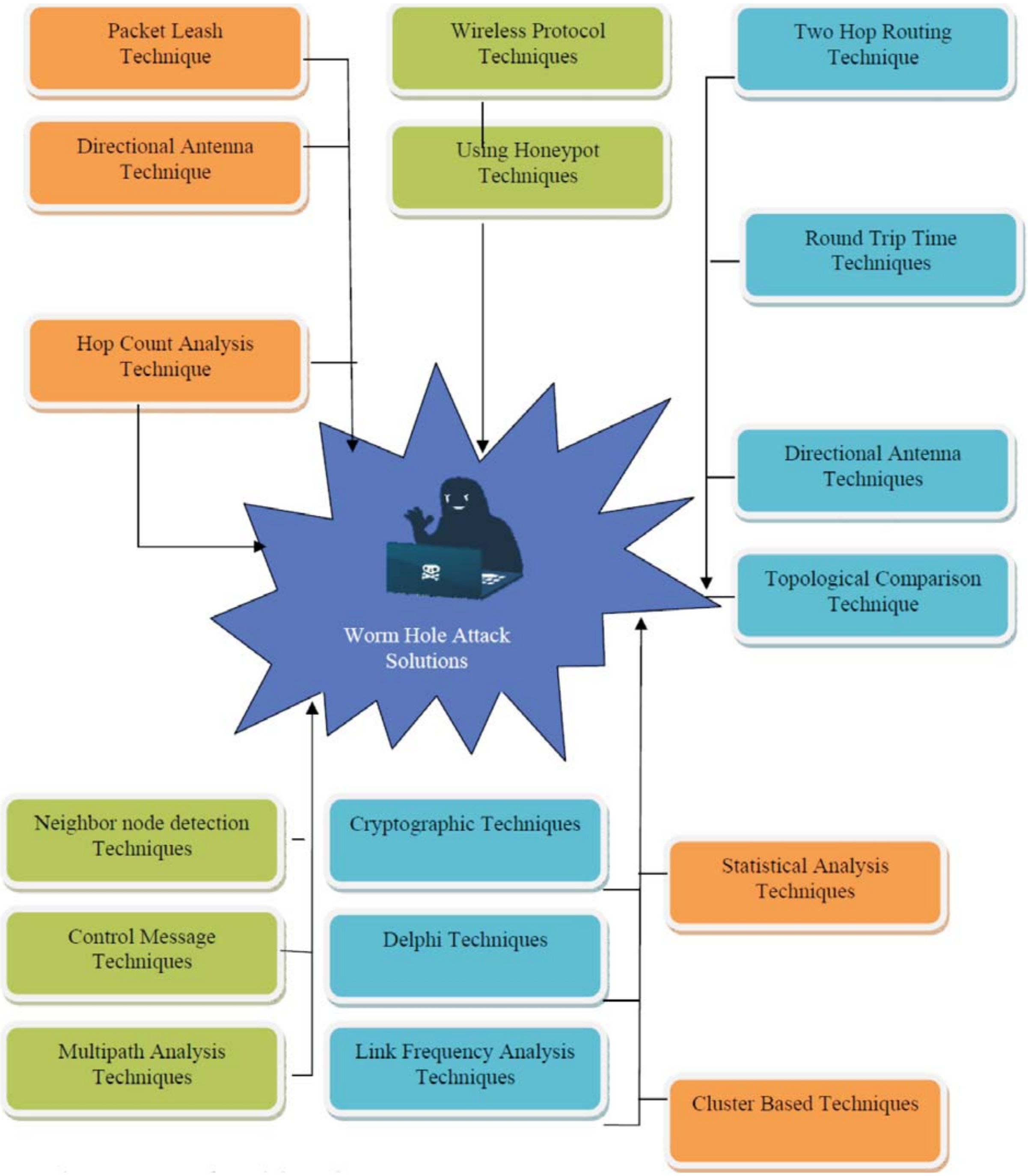

Packet Leash Technique
Wireless Protocol Techniques
Two Hop Routing Technique
Directional Antenna Technique
Using Honeypot Techniques
Round Trip Time Techniques
Hop Count Analysis Technique
Directional Antenna Techniques
Topological Comparison Technique
Worm Hole Attack Solutions
Neighbor node detection Techniques
Cryptographic Techniques
Statistical Analysis Techniques
Control Message Techniques
Delphi Techniques
Multipath Analysis Techniques
Link Frequency Analysis Techniques
Cluster Based Techniques

Figure 4: Taxonomy of worm hole Attacks

Geographical Leashes sends the location and the time of sending a packet. The receiver node calculates the upper bound of the distance for the sender. But this technique needs the location information and synchronization of all the nodes in the MANT.

Next, the temporal leash technique appends the sending time of the packet. The receiving node calculates the distance of the packet using the propagation speed using the sending and receiving time. The proposed solution suggests the synchronization among all the nodes in the MANET.

2. **Directional Antenna Technique:** This technique uses the GPS[12] based technique to prevent worm hole attacks from MANET. The nodes in MANET uses the particular region which uses the antennas that communicate with each node. The nodes are examining the received signals from the neighbor nodes. The neighbor relation of each node are set only if the pairs of each nodes met each other. Hence the nodes have to maintain the additional detail of extra bit information which causes the network to made additional inconsistencies in the MANET. The directional antennas have to maintain the information about the mobile devices which creates the problems for introducing the security level. In order to discover the neighbor nodes each node has to broadcast the HELLO messages in each direction. In their network, each node listens the neighbor nodes using the HELLO messages which contains the encrypted message that contains the random challenge nonce. The announcer node announces the responder nodes about the neighbor list. But this technique partially mitigates the worm hole attack problem. The directional antennas are used to identify the worm hole attacks in MANET. The detection of authentic node is identified by sending the data packets in one direction and receiver node receives the data packets in another direction. Thus the nodes are validated each other by examining the sending and receiving packets. This technique requires two end points one is sender node and another node is destination node. Thus the nodes validate each other in opposite direction. This technique works only when the intruder nodes consist of two end points. This technique requires additional hardware functionalities to detect worm hole attacks in MANET.

3. **Hop Count Analysis Technique :** This technique detects the worm hole attacks by introducing the routes and avoids the network overhead in the MANET. They used hop-count analysis technique which uses multi-path routing protocol. This technique does not support any special type of hardware's. Since this protocol uses multi path routing protocol it splits the routing technique into multiple paths. Hence the attacker cannot intercept the contents. This technique is designed to provide high efficiency and low overhead.

4. **Neighbor Node Detection Technique :** Many authors proposed various types of solution to detect worm hole attacks. The nodes in MANET maintains the complete two-hop information from the neighbor nodes in the network. But this technique can be implemented in static networks. In normal routing scenarios of MANET, each node maintains the details of next one hop neighbors. But this proposed technique maintains the two-hop information of neighbors which is exploited to detect about worm hole attacks in MANET. Thus each nodes in MANET which uses this technique observes the neighbor nodes behavior in the MANET.

5. **Wireless Protocol Technique:** In this technique, a new wireless protocol was developed to prevent worm hole attacks in MANET. This technique is also based on the symmetric and asymmetric cryptographic technique. They used GPS based nodes to detect attacks. The GPS nodes identifies the location of the nodes directly. The non-GPS nodes in this technique provide information about relative location by getting information from GPS nodes. The asymmetric key cryptography technique provides information from integrity and trust from GPS nodes.

6. **Using Honeypot Techniques:** Recently many authors proposed various techniques to detect and prevent worm hole attacks in MANET. The honeypot concepts on MANET is used to the honeypot technique to understand the behavior of the worm hole attacks in MANET. The honeypot concepts are used to detect, capture and misguide the attackers. Honeypot technique is used to understand the vulnerabilities of the attacker and is used to distract the attacker which gives early warning about the attackers in MANET.

7. **Cryptographic Techniques:** Various authors proposed many cryptographic solutions to detect worm hole attacks. The symmetric cryptography technique uses Ariadne technique. In this technique, the destination node authenticates the source node. The source node authenticates each intermediate node. The Route Request packet removes or adds the nodes in the network. The cryptographic[13] technique uses the key administration protocol which is known as TESLA that uses the concept of clock synchronization technique which authenticates the routing messages. Each node authentication depends on the RREQ packet which contains the authentication information about the previous node. Ariadne prevents the attacker from flooding the network by using the shared secret key among the nodes. This is achieved by adding the authentication code to each of the RREQ packet in the network.

8. **Delphi Technique:** The Delay Per Hop Count technique[14] is used to monitor the worm hole attacks in MANET. The assumption about this technique is it propagates the one hop distance is longer than the actual path. It is a two-step process. In the first phase, the routing information is collected from the set of various paths between the source node to the destination node. Each sender node includes a timestamp with the DREQ packet. This packet is send to receiver before each packet. The node which receives the packet initially, receives the packet for the first time includes the node ID and the hop count is increased by 1 and discards the packet from the next time. This technique is repeated for 3 times and the smallest delay is computed and the delay information is calculated for detecting worm hole attacks. The next phase consists of calculation of round trip time(RTT) is calculated based on the packet send and packet received. Thus the delay per hop value is computed as RTT/2h. The h is known as the hop count from the neighbor node. In normal circumstances the hop count will be smaller, but whenever the MANET suffers for worm hole attack, the hop count is increased. Thus the worm hole detection is achieved in this technique.

9. **Link frequency Analysis Technique:** In order to detect the presence[15][16] of worm hole attack, the source node sends the RREQ messages and waits for the RREP packet. The source node receives the RREP packets coming from the various different routes. The high link frequency is checked with the help of the following formula:

$$\begin{aligned} Pi &= ni/ N, \text{ fof all } Ii \\ Pmax &= \max (Pi), \end{aligned}$$

Where R is the route obtained from various routes. Ii is the i^{th} link ,ni is the number of times Ii appears in the network in R, N is the total number of links presented in R, Pi is the relative frequency. Pmax> P threshold value is checked for the trust information which is available in the RREP packet on the route. The pre-set threshold value determines whether the node is malicious or not. If t is more than the pre-set threshold, then the node is marked as malicious and this information is broadcasted to the neighbor nodes in the network.

10. **Two Hop Routing Technique:** The two hop routing[17] method consists of measuring round-trip-time (RTT) between the source node and the destination node. The next method consists of the one-hop and the two-hop neighbors which forms the neighbor set. If the destination node is not the neighbor node from the source node, the link is considered as malicious. The next phase of this technique consists of using the RTS/CTS packets to confirm the suspicious activity of worm hole attacks.

11. **Round Trip Time(RTT) Technique:** In this RTT mechanism, the worm hole nodes are identified by the network by identifying the neighbor nodes in MANET by understanding network and MAC layer. The active worm hole attacks change the packet header in order to reach wrong destination. In order to solve the problem, a flag is set. The flag contains the information about the reception of the data packet, which is involved in transmission of data packets. The RTT of the packet is calculated based on the actual routers and the nodes which are there in the neighbors. Initially, the neighbor list is constructed which is involved in the routing process. Next, in second phase the routing is constructed from source node to the destination node. The final phase consists of detecting the existence of the worm hole link in the network. The source node broadcasts the RREQ packets initially. While travelling the RREQ packet, the other nodes save the TREQ packet. Once this node reaches the destination node, the destination node replies with RREP message. The destination node forwards the reply with the TREP packet which it receives with the RREP message. The routers save the TREP time when it receives the RREP message.

12. **Topological Comparison Technique:** The next technique known as topological comparison technique that is based on the round trip time topological comparison mechanism. The suspected list is maintained by the nodes in the network. In case of worm hole attack, two malicious neighbors will have the longest RTT. But the normal nodes have smaller RTT. The topological comparison is done based on the RTT measurement with the neighbors. The relay of nodes is done based on the measurement which is used to identify the worm hole attacks that uses topological comparison of the nodes. This comparison includes genuine neighbor nodes and suspected nodes.

13. **Statistical Analysis Technique:** In the Statistical Analysis Multipath (SAM) technique it uses the Pmax and Φ value. These two values are higher means it indicates the presence of the attacks. Φ is known as the link which is most frequently appear. Next, the most frequent approach is obtaining the set of all obtained routes for route discovery process. In their technique, a Probability Mass Function (PMF) is used to identify the highest relative frequency for more than a single system under the worm hole attack. In this technique the performance of On-Demand Multipath Routing (MR) and DSR routing protocol are compared.

14. **Cluster Technique:** A cluster based technique is used to detect worm hole attacks in MANET. The WHID technique is proposed to detect worm hole attacks in MANET. These techniques get success when there is minimal number of worm hole attacks in MANET. But these techniques fail under the presence of multiple worm hole attacks in MANET.

4. CONCLUSION

In this paper we have surveyed several techniques such as algorithms that are proposed by various researchers. This paper describes about various types of solutions against worm hole attacks proposed in literature. This paper also provides the road map for the researcher who wants to do research work in MANET against worm hole attacks. Further, the taxonomy provides the deep understanding of this attack.

REFERENCES

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

[2] Aarti: “Study of MANET: Characteristics, Challenges, Application and Securiy Attacks” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013. R. Nicole, “The Last Word on Decision Theory,” J. Computer Vision, submitted for publication.

[3] P.Chandra Sekhar: “A SURVEY ON MANET SECURITY CHALLENGES AND ROUTING PROTOCOLS” Int.J.Computer Technology & Applications(IJCTA), Vol 4, Mar-Apr 2013.

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

[5] Farman Ahmed, Ankit Jha ,Neeraj Kumar: "Efficient Approach for the Detection of Wormhole Attack Using Dynamic Source Routing Protocol in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, August 2014

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

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

[8] Yih-Chun Hu, Adrian Perig, David B. Johnson: "Wormhole Attack on Wireless Network" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol. 24-No 2,2006.

[9] K. Sivakumar, Dr. G. Selvaraj: "Analysis of Worm Hole Attack In MANET And Avoidance Using Robust Secure Routing Method" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013.

[10] K A Arun Kumar,"Worm hole-black hole attack detection and avoidance in Manet with random PTT using FPGA",IEEE International Conference on Communication Systems and Network, 2016.

[11] Yih-Chun Hu, Adrian Perrig, David B. Johnson. "Packet leashes: A Defense against Wormhole Attacks iWireless Ad Hoc Networks". In 22nd Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM) , 3, pp. 1976-1986, 2003

[12] L.Hu and D.Evans.Using directional antennas to prevent wormhole attacks. In Proceedings of the Network and Distributed System Security Symposium. 2004

[13] D. Vivian, E.A.P. Alchieri, C.B. Westphall. "Evaluation of QoS Metrics in Ad Hoc Networks with the use of Secure Routing Protocols". In Network Operations and Management Symposium, pp. 1-14, 2006.

[14] H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, (2006).

[15] M.S. Sankaran, S. Poddar, P.S. Das, S. Selvakumar. "A Novel Security model SaW: Security against Wormhole attack in Wireless Sensor Networks". In Proceedings of International Conference on PDCN, 2009.

[16] Khin Sandar Win. "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology, 48, pp. 422-428, 2008.

[17] Khalil, S. Bagchi, and N. B. Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. In Dependable Systems and Networks (DSN), pages 612–621, Jun 2005.