Evaluating Impact of Wormhole on Distance Error and Connectivity of Network

Shalki Naresh
M. Tech, CSE Dept.
MVEC, Jagadhri
Yamuna Nagar, India

Navjot Singh
Assistant Professor, CSE Dept.
MVEC, Jagadhri
Yamuna Nagar, India

ABSTRACT
Wireless mesh networks are the emerging wireless networks which are self organizing, maintaining, healing and configuring. The main trait of WMN is its dynamic and multi-hop nature. These networks provide the internet services to its users on low costs and with high bandwidth. These are made up of mesh routers and mesh clients. They can be easily deployed and are highly scalable. But the security of WMNs is the area of concern due to their vulnerable features they are open to many attacks of which wormhole attack is the worst. A wormhole attack is the one in which two or more conspired nodes forms a tunnel between them via which they sends the network traffic to one another and replays it. In our paper, we study the wormhole attack and then find its impact on distance error and connectivity of nodes. The distance error is found by knowing the ratio of trusted links and that of connectivity is found by knowing the unaffected, disconnected and partially affected nodes.

Keywords
WMN (Wireless mesh networks), wormhole attack, impact on distance error, impact on connectivity.

1. INTRODUCTION

1.1 Wireless Mesh Networks
A self configured, organized, self healed and self maintained network which utilizes the method of packet switching in multi-hops is called as Wireless Mesh Network (WMN). A wireless mesh network is composed of number of nodes that are linked to each other via wireless medium and assembles them in the form of mesh topology. These nodes are free to leave or join the network at any time. WMN is capable of providing services to its users even if there is absence of fixed infrastructure. The features of both fixed and ad-hoc network are possessed by a WMN. It configures its nodes as ad-hoc networks and then mesh connectivity is formed in the nodes. The nodes of WMNs can behave as host or router, but mostly they are classified as: Mesh Routers (MR) or Mesh Clients (MC). The infrastructure backbone of the network is made by fixed nodes which are MRs and the nodes which moves around MRs and are mobile are MCs. The gateway to internet access is MRs and MCs are able to connect to other MCs and MRs. In the network, the access services to the internet in a multi-hop way are provided by fixed backbone infrastructure (MRs) to MCs. The routing protocols are used to select the route for packet communication [8]. But there are some vulnerabilities in these networks like wireless medium, Cooperative MAC, Multi-Hop environment, etc due to which they are open to many security attacks one of which is the wormhole or tunneling attack. The figure 1 below represents a WMN.

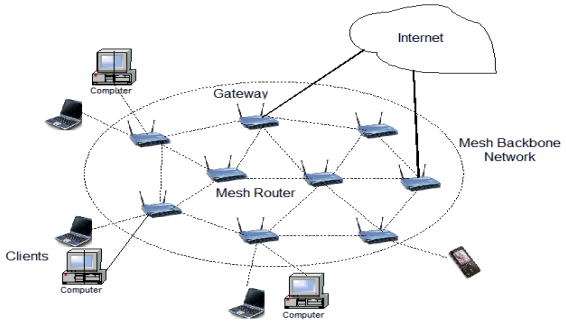

Figure 1: Representing Wireless Mesh Network

1.2 Wormhole Attack
An internal attack in which the malevolent nodes of the network plan to form a virtual channel among them is known as wormhole attack. The channel can be formed by employing in-band tunneling scheme or by the use of high-speed communication which is out-of-band, so that the in-between nodes can be bypassed. This virtual link is known as wormhole which is formed by two or more far away colluding or conspired nodes of the network. In wormhole attack, one of these nodes captures or overhears the data packets and tunnels them to far away conspired node which then replays those packets in the network. The wormhole is capable of capturing a bulk of network traffic because it shows the better metrics than other paths or routes. This attack when succeed can cause many types of DoS attacks which are done to disrupt the routing of network. This attack is hard to detect as these conspired nodes appear to be the part of the network and by using only cryptographic methods it can't be detected [10].

The fig. 2 below shows the wormhole attack where X and Y are its end points. Y replays every data packet in its neighborhood (area of node B) which is overheard by X from its neighborhood (area of node A) and vice versa. By the analysis of this fact it is clear that, nodes of area A assumes B as its neighbors and that of B assumes A as its neighbor which results in affected routing of the network. As new paths via X and Y are formed by the use of XY shortcut, the data packets are now started to be dropped which cause network disruption [7].

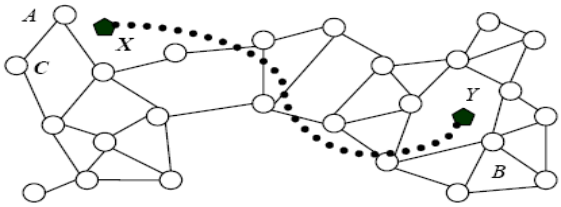

Figure 2: Wormhole Attack

2. LITERATURE SURVEY

Lingxuan Hu et.al [1] Wormhole attack is an attack in which an attacker with no cryptographic material and limited resources is able to cause calamity on wireless networks. There is no general protection against such attack. In this paper, wormhole attacks had been analyzed and its cure by the use of directional antennas has been given. In this paper, a cooperative protocol in which nodes share directional information so that wormhole endpoints may not present themselves as false neighbor is given by them. This protocol greatly decreases the threat of wormhole attacks and there is no need of clock synchronization or location information.

Stephen Glass et.al [3] Wireless networks have many applications in health care, public-safety, military and industrial environments. All these environments are security dependent and security is very important in these environments as successful attack on these networks may cause a threat to organisms and their environment. Both protective and unmasking steps are needed to secure such wireless networks from hostile attacks. To identify wormhole attacks and man-in-the–middle attack in wireless mesh networks, a novel intrusion detection mechanism is proposed in this paper. Wireless MAC protocol is modified so that malicious nodes which conduct frame-relaying attacks are exposed. The MAC protocol is modified experimentally and the evaluation shows that the detection mechanism has no false positives, high detection rate, and has a small communication and computational overhead.

Divya Bansal et.al [4] Wireless mesh networks (WMNs) has emerged recently to provide better knowledge and key technology. Among many deployment issues of WMNs the security is the grave one. The network security is achieved by authentication of users and devices present in the network. IEEE 802.11s mesh networks do not possess any well specified or well defined architecture of security due to which it can be used for many applications. As WMNs is based on multi-hops so use of 802.11i as security standard is insufficient for security purpose in Wireless Mesh Networks because 802.11i uses the central security mechanism. In this paper, an approach which uses the Clustered Certificate Authority with threshold authorization model is given which uses both distributed and centralized architecture.

Aggeliki Sgora et.al [6] For accessing broadband and internet services at less cost, Wireless Mesh Networks (WMNs) are a promising solution. However, the main and important challenge in these networks is that they are open to many security attacks. In this paper, the primary security challenges and restrains of WMNs are analyzed. Also the classification of possible attacks and their detection mechanisms with their response is done.

Kaifeng Wen et.al [9] There are lot of issues related to the security in MESH networks. In this paper a research based on intrusion detection in wireless mesh networks security is presented. The system architecture and related algorithms are rearranged by the combination of intrusion detection characteristics. The feasibility of the system is tested by using the delay and error rate. The result of experiments proves that the given system keeps the accurate data and reduces the delay.

3. PROPOSED WORK AND IMPLEMENTATION

This paper is about the wormhole attack affect or impact on some of the parameters of network: distance error and connectivity of nodes. The impact on distance error is found by knowing the trust link ratio and that on connectivity is found by knowing the partially affected, unaffected and disconnected nodes. The work is done by taking the parameters which are given in table 1.

Table 1: Various parameters and their value on which work is done

S. No.	Parameter	Value
1.	Terrain Range	500, 500
2.	No. of nodes	50, 100, 150
3.	No. of wormholes	1, 2, 3
4.	Antennas	Omni-directional, Directional
5.	Radio ranges	50, 55
6.	Directional Ranges	80, 85
7.	Antenna No.	6

After knowing the impact on these two factors the value of radio and directional ranges are altered to know its impact on the connectivity of the nodes. The work can be discussed as:

3.1 Impact on distance error:

The impact of wormhole attack on the distance error is found by knowing the ratio of trust links in case of 50, 100 and 150 nodes. The trust link ratio can be given as:

Ratio of trusted link= Trust link num/ Link num

This impact is studied for directional range=80 and radio range=50. This ratio gives us the trust level of the link i.e. how much a link can be trusted for the delivery of packets. By knowing this value we came to know the trust level of the links and then we can set a threshold value of this and the links that have that value can be used to transfer the data and data packets.

3.2 Impact on connectivity

The impact of wormhole on the connectivity of the network is studied by knowing the unaffected, partially affected and disconnected nodes in the network. The unaffected nodes are those which have no affect or impact of wormhole on them, partial affected nodes are the one that has partial affect of wormhole on them and disconnected nodes are those that are separated from the network due to wormhole attack. These nodes are calculated for 50, 100 and 150 nodes on radio and directional ranges equal to 50 and 80 respectively.

3.3 Mitigation by varying radio and directional ranges

Finally, in the end the radio range and the directional ranges are varied to study its impact on the connectivity of the nodes.

This is done for two cases on 50, 100 and 150 nodes. The values that are taken are:

1. Radio range = 50, Directional Range = 80

2. Radio range = 55, Directional Range = 85

On both these cases, the connectivity of the nodes is checked and the results that are obtained by us are discussed in next section.

4. RESULTS AND DISCUSSION

4.1 Impact on the distance error

The impact on the distance error is found for 50, 100 and 150 nodes and the ratio of the trusted links are found for each 50, 100 and 150 nodes. The figure 3 shows the results that are obtained.

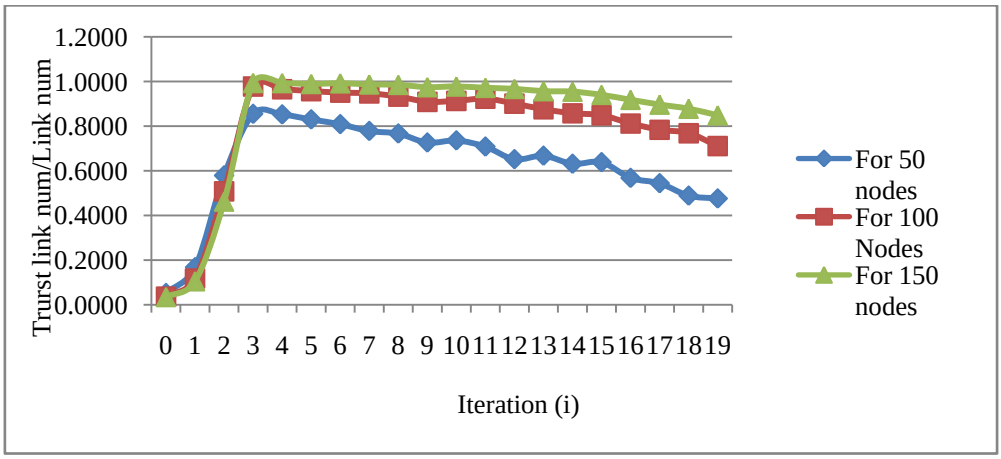

Figure 3: Trust link ratio for 50, 100 and 150 nodes

The results that are shown above contain iterations and the trust link ratio of the nodes. By seeing the graph above it is clear that when the number of nodes in the network increases the impact of wormhole on the distance error decreases as the ratio trust link increases with the increase in the number of nodes. In our results, the ratio of trust link is maximum for 150 nodes and is least for 50 nodes.

4.2 Impact on connectivity

The impact of wormhole on the connectivity of the nodes is found for 50, 100 and 150 nodes and the number of unaffected, disconnected and partially affected nodes is checked for them at radio range equals 50 and directional equals 80. Figure 4, 5 and 6 shows the affect of wormhole on the connectivity for 50, 100 and 150 nodes respectively.

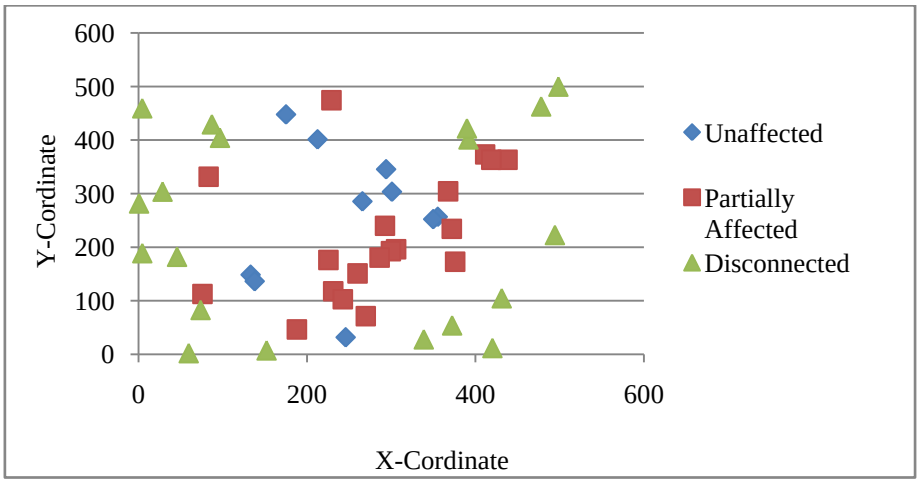

Figure 4: Connectivity at radio range=50, directional range=80 for 50 nodes

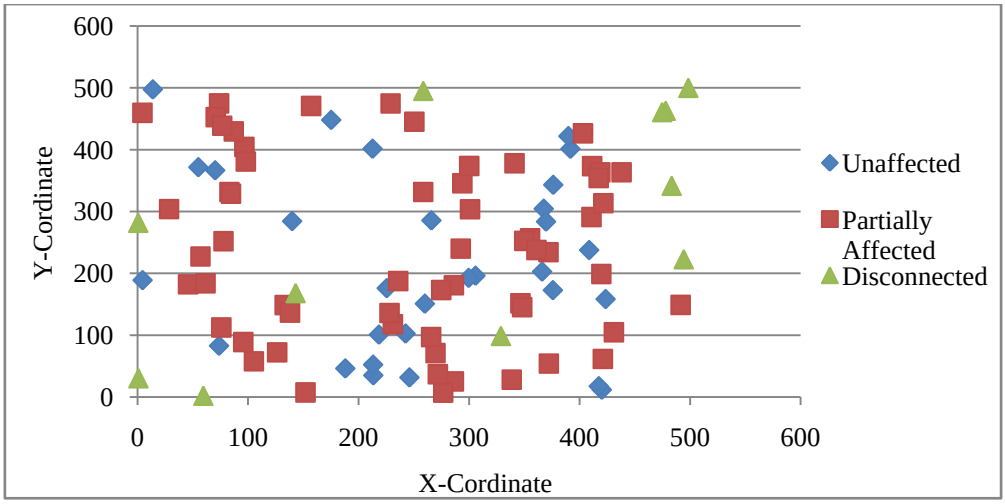

Figure 5: Connectivity at radio range=50, directional range=80 for 100 nodes

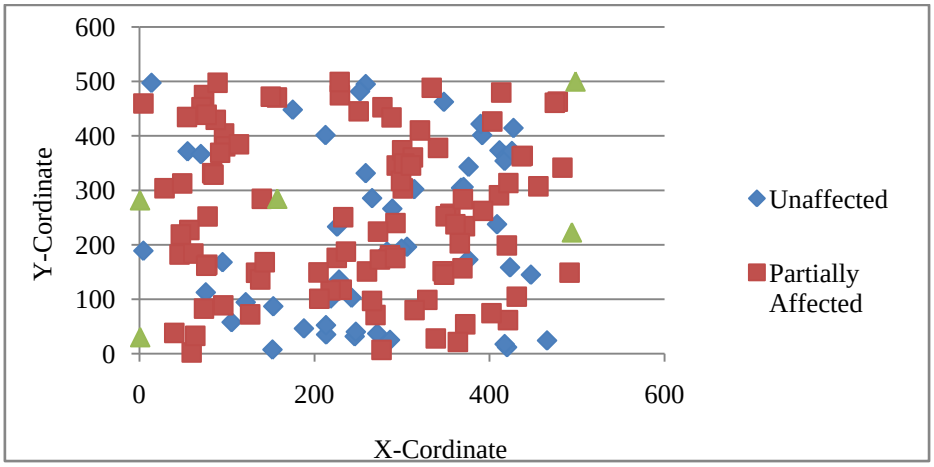

Figure 6: Connectivity at radio range=50, directional range=80 for 150 nodes

From the results that are obtained above, we came to know that as the number of nodes in the network increases the impact of wormhole on the connectivity decreases as the count of disconnected nodes decreases. In our result the count of disconnected nodes is maximum for 50 nodes and is minimum for 150 nodes. So, the network with 150 nodes is maximum connected.

4.3 Mitigation by varying the radio and directional ranges

Finally, we vary the radio and directional ranges to see its impact on the connectivity of the network. The cases we study are:

(i) Radio Range = 50, Directional Range = 80

(ii) Radio Range = 55, Directional Range = 85

And then we calculate the connectivity of the nodes on these cases which is discussed below:

(i) Radio Range = 50, Directional Range = 80

Table 2 and figure 7 gives the connectivity of nodes for 50, 100 and 150 nodes at radio range=50 and directional range=80.

Table 2: Connectivity at 50, 80 for 50, 100 and 150 nodes

No. of Nodes	Unaffected	Partially Affected	Disconnected
50	10	20	20
100	30	59	11
150	50	95	5

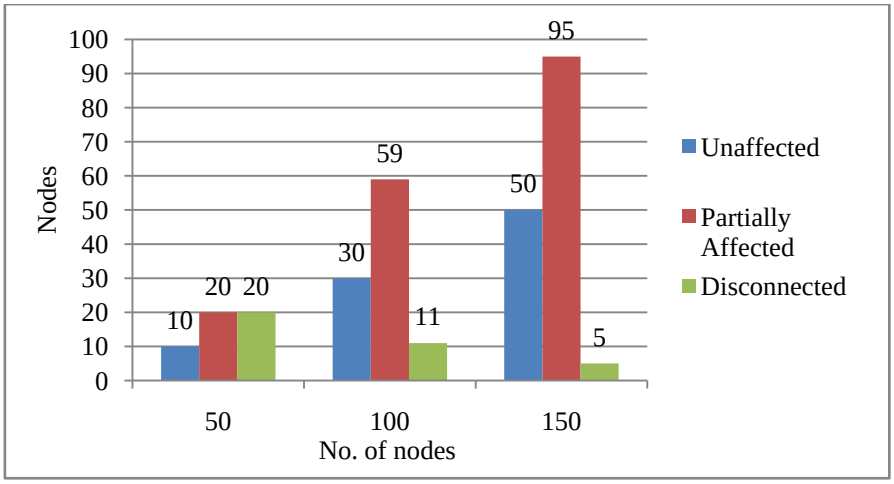

Figure 7: Connectivity at 50, 80 for 50, 100 and 150 nodes

The table and graph above shows the connectivity of the network for 50, 100 and 150 nodes on radio range=50 and directional range=80. The number of disconnected nodes in 50, 100 and 150 nodes is 20, 11 and 5 respectively.

(ii) Radio Range = 55, Directional Range = 85

Table 3 and figure 8 gives the values of connectivity for 50, 100 and 150 nodes at radio range=55 and directional range=85.

Table 3: Connectivity at 55, 85 for 50, 100 and 150 nodes

No. of Nodes	Unaffected	Partially Affected	Disconnected
50	12	21	17
100	32	62	6
150	55	91	4

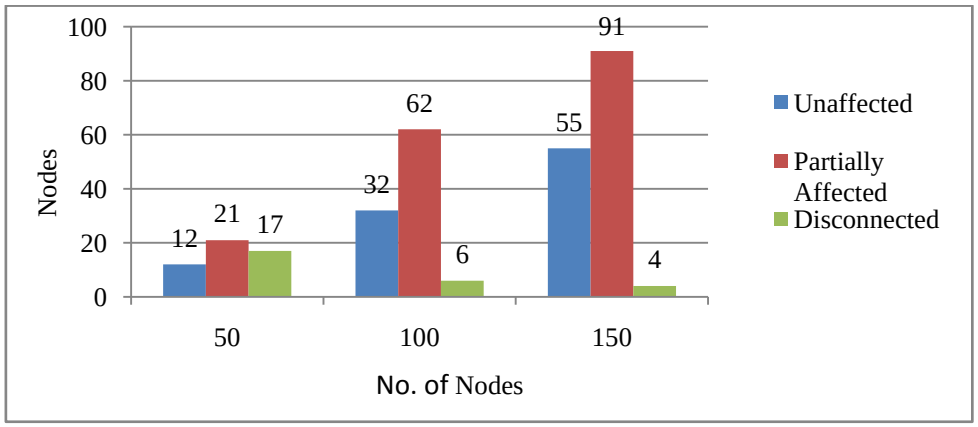

Figure 8: Connectivity at 55, 85 for 50, 100 and 150 nodes

The table and graph above shows the connectivity of the network for 50, 100 and 150 nodes on radio range=55 and directional range=85. The number of disconnected nodes for 50, 100 and 150 nodes is 17, 6 and 4 respectively.

(iii) Comparison of above two cases:

Then the comparison of these two cases is done to see its effect on connectivity of nodes. Table 4 and figure 9 shows the comparison:

Table 4: Comparison of connectivity at 50, 80 and 55, 85

Scenarios	50 nodes at 50, 80	50 nodes at 55,85	100 nodes at 50, 80	100 nodes at 55,85	150 nodes at 50, 80	150 nodes at 55, 85
Unaffected	10	12	30	32	50	55
Partially Affected	20	21	59	62	95	91
Disconnected	20	17	11	6	5	4

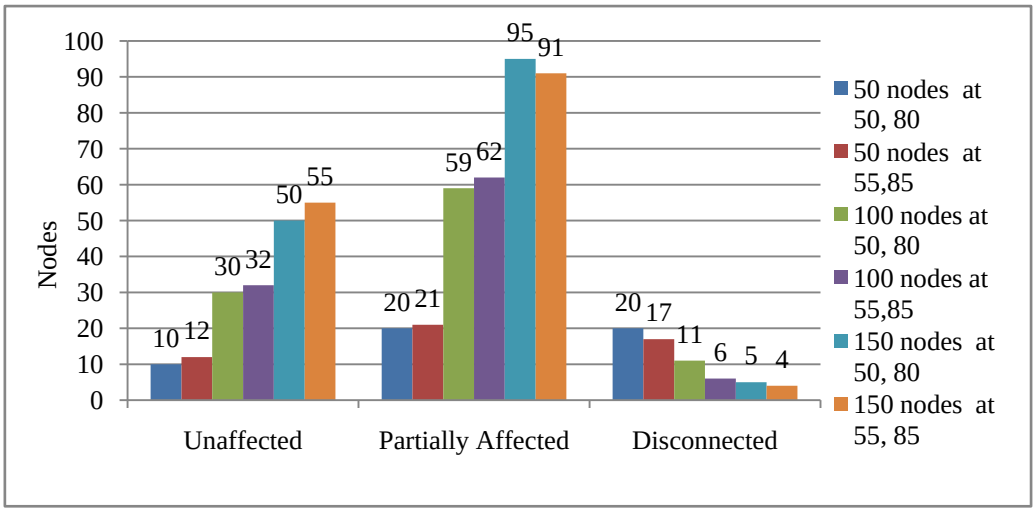

Figure 9: Comparison of connectivity at 50, 80 and 55, 85

The table and the graph above shows us the comparison of the connectivity of the nodes at radio range=50, directional range=80 and radio range=55 and directional range=85. With which the following points are concluded:

a. The number of disconnected nodes decreases with the increase in radio and directional ranges.
b. The number of partially affected nodes increases with the increase in radio and directional ranges.
c. The number of unaffected nodes increases with the increase in radio and directional ranges.

The above noted point conclude that as the value to radio and directional ranges increases the impact of wormhole on the connectivity of the network decreases. So, radio and directional ranges can be used to mitigate the wormhole affect on connectivity of nodes.

5. CONCLUSION

In this paper the wormhole attack is reviewed which is dangerous because it can drastically disrupt the network. In this paper the impact or affect of wormhole attack is found for distance error and connectivity of the nodes. The impact on distance error is found by knowing the trust link ratio for 50, 100 and 150 nodes and our work concludes that as the number of nodes increases the ratio of the trusted link also increases and is maximum for 150 nodes. The impact of wormhole on the connectivity of the network is also found out for 50, 100 and 150 nodes and it is concluded that as the number of nodes increases the count of disconnected nodes decreases. And finally, we conclude that by increasing the value of radio and directional ranges we can decrease the affect o wormhole attack on connectivity of nodes.

6. REFERENCES

[1] Lingxuan Hu, David Evans, "Using Directional Antennas to Prevent Wormhole Attacks", In Network and Distributed System Security Symposium (NDSS 2004), San Diego, California, USA. February 2004.

[2] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.

[3] Stephen Glass, Vallipuram Muthukkumurasamy, Marius Portmann, "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks", 2009 International Conference on Advanced Information Networking and Applications.

[4] Divya Bansal, Sanjeev Sofat, "Threshold based Authorization model for Authentication of a node in Wireless Mesh Networks", Int. J. of Advanced Networking and Applications Volume: 01, Issue: 06, Pages: 387-392 (2010).

[5] Nadher M. A. Al_Safwani, Suhaidi Hassan, Mohammed M. Kadhum, "Mobile Ad-hoc networks under wormhole attack: A simulation study", Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI 2011,8-9 June, 2011 Bandung, Indonesia.

[6] Aggeliki Sgora, Dimitrios D. Vergados and P. Chatzimisios, "A Survey on Security and Privacy Issues in Wireless Mesh Networks".

[7] Priti Gupta, Suveg Moudgil, "A Novel Scheme to Detect Wormhole Attacks in Wireless Mesh Network", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (3), 2014, 4798-4801.

[8] Binish Raza, Faiza Qaiser, Muhammad Ahsan Raza, "Study of Routing Protocols in Wireless Mesh Networks", IJASR International Journal of Academic Scientific Research ISSN: 2272-6446 Volume 2, Issue 2 (May-June 2014), PP 19-26.

[9] Kaifeng Wen, "Research on Wireless-Based Intrusion Detection in Mesh Network Security System", International Conference on Information Technology and Management Innovation (ICITMI 2015) © 2015. The authors - Published by Atlantis Press.

[10] Virendra Dani, Vijay Birchha, "An Improved Wormhole Attack Detection and Prevention Method for Wireless Mesh Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 12, December 2015.

[11] Jonny Karlsson, Laurence S. Dooley and Göran Pulkkis, "Identifying Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA) Wormhole Detection Algorithm", Sensors (Basel). 2013 May; 13(5): 6651–6668. Published online 2013 May 17.

[12] Monika, "Denial of Service Attacks in Wireless Mesh Networks", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012, 4516-4522.

[13] Dezun Dong, Mo Li, Yunhao Liu and Xiangke Liao, "WormCircle: Connectivity-based Wormhole Detection in Wireless Ad Hoc and Sensor Networks", 2009 15th International Conference on Parallel and Distributed Systems.

[14] Tahir Naeem, Kok-Keong Loo, "Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks", International Journal of Digital Content Technology and its Applications Volume 3, Number 1, March 2009.