ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Mitigation of DOS Attack in Wireless Mesh Network

Anju Singh [1], Nisha Pandey[2]

M. Tech. Student, Department of CSE, Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India [1]

Asst. Prof, Department of CSE, Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India [2]

ABSTRACT: Wireless Mesh Networks (WMNs) have secured an important position in the technological world because of their unique features. These networks are self-healing, dynamic and self-organizing in which the nodes reflexively established and manage mesh connectivity with one another. For detecting the DoS attack (Denial-of-Service attack) when wireless mesh networks follow AODV routing protocol of Ad Hoc networks. These technologies as an end-to-end authorization, usage rate of cache memory, two pre-considered threshold value and disseminated voting are utilized in this paper to determine DoS attacker, which is based on hierarchical configuration structure in wireless mesh networks. Through performance analysis in simulations and theory experiment, the technique would enhance the accuracy and flexibility of DoS attack detection, and would obviously enhance its security in wireless mesh networks.

KEYWORDS: wireless mesh network; intrusion detection, denial of service attack; distributed voting

I. INTRODUCTION

As a novel wireless network technology, WMN (wireless mesh network) that is based on its high usage ratio of frequency spectrum, wide coverage region, good reliability and expandability can get rid of some limitations of Ad Hoc network, WPAN (wireless personal area network), WLAN (wireless local area networks), and WWAN (wireless wide area network). At present WMN has been paid great care to by more and more researchers from academic to commercial circles, particularly security problems in WMN.

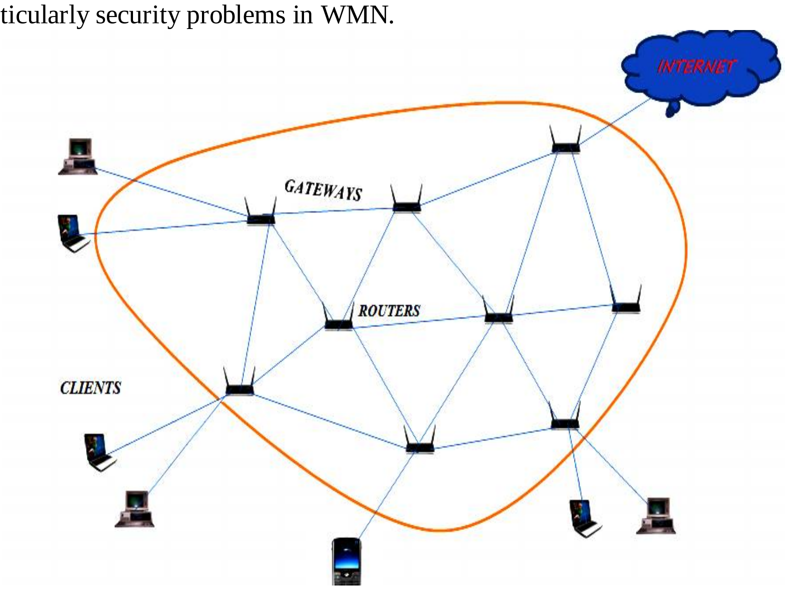

Figure 1: Wireless Mesh Network

DOI: 10.15680/IJIRCCE.2016. 0406098

DoS attack means that a node couldn't offer normal needed facilities to other legitimate nodes or terminals, and can be conducted on each layer in network[1]. There are a lot of evaluations to establish DoS attack from the physical layer to the application layer in WMN due to its own features. Since, most DoS attacks are conducted in the network layer, whose manifestation are explained as follows[1-2]:

(1) Signal interference. The intruders fetches the frequencies of message signal forwarded and obtained by network nodes, and then continuously forward the DoS signals.

(2) Changing of routing nodes sequence. Attackers alter the sequence and hop in AODV (Ad hoc On-demand Distance Vector) to generate a wrong route, which importantly decrease the performance of the entire network[2].

(3) Faked legitimate nodes. However, message address isn't determined in routing protocols, intruders may fake specific legitimate nodes for accessing the network, and even mask legitimate nodes to obtain their messages rather than them [3].

(4) Resources consumption. Intruders forward a lot of waste messages, i.e. routing query messages, to use resources of the nodes and network, i.e. memory, bandwidth, CPU and batteries power.

II. RELATED WORK

At present AODV routing protocol in ad hoc networks is also utilized in some WMNs, in which setting up of route is conducted entirely on the needs. When a source node requires to forward messages to another node which current routes cannot arrive, it flood RREQ (route request), which are broadcasting in the network to investigate a reachable route. When obtaining RREQ, a node will firstly examine whether there is a stored route to arrive the target node in its routing table or not. If not, it will locally record DNA (destination node address), SNA (source node address), UNA (upstream node address) and destination sequence no. to establish a reverse route, and then flood RREQ again. If there is a latest reachable route, or local node is the target one, it will forward RREP (route reply) back to the source node along with the route RREQ reaches. When the source node obtains RREP, a route from the source node to the destination node is established. Link status is scanned by periodically flooding "hello" message in AODV. If a node detects a utilized connection is broken off, it will remove all routes with the broken connection from its routing table, and forward RRER (route error) to starting nodes of the routes to report them that correlative routes should be removed from their routing tables. And those nodes sending RRER along the way will also alter their tables. When RRER reaches at the source node, it will remove the false routes, and query a new route if required. In conventional defence models, the node generates a single table for every neighbour. It will initiate the timer when obtaining a neighbour's message at the first time, and increase the correlative counter value by 1 with every new obtained message before timeout. If the value exceeds a threshold designed, an attack alarm will be conducted. And if no attacks are determined before timeout, the value will set zero as its initial, until the timer begins again.

In this paper [1] . proposed a novel technique to detect and isolate DoS attack in AODAV protocol. In his work authors uses hop count and sequence number as parameters and used ICMP packet as monitoring node to detect malicious node which further does not send ICMP packet to the destination, and then isolate the malicious node from the network.

In this paper [2]. discuss the DoS attack in broadband wireless network along with possible defence and future directions. The authors discuss the various broadband wireless network and relative effect of DoS attack in these networks and in different layers of OSI model.

In this paper [3],. discuss the impact of Distributed Denial of service attack in wireless mesh network. His work is based on Optimized link state protocol (OLSR). The authors introduced the concept of learning automata thereby optimizing the packet sampling mechanism. The author suggested two new frame format and evaluate the performance of system using the NS3 simulator.

III. A NEW DOS ATTACK DETECTION SCHEME

3.1 CTS/RTS defence mechanism

The Request to Send/Clear to Send (RTS/CTS) mechanism is a handshaking process when hidden nodes are operating on the network that minimizes the occurrence of collisions.

When mobile node A want to send a packet to mobile node AP it initially send a small packet called RTS (Request-To-Send) and replies to it with small packet CTS (Clear-To-Send). After receiving CTS , node *A* sends the *DATA* packet to node *AP*. In-between mobile node B receives the CTS packet since the Mobile Node A is sending data and the mechanism Informs the mobile Node B that the AP is transmitting or receiving data at that time frame and Mobile Node B to wait for a particular time. Fake RTS frames are sent to the AP mobile node When a DoS attack is launched on the network, that keeps the medium busy or introduces packet collisions causing forced and prevents other nodes from being able to begin with legitimate MAC operations, and repeated back offs.

3.2 PROPOSED METHODOLOGY

The attacker nodes in the wireless network keep the channel busy for an additional time by changing the duration field value of the RTS packets. Since legitimate nodes will obviously respond to RTS request with CTS frame, an attacker could exploit legitimate nodes to disseminate CTS with manipulated duration field, which causes the attack automatically. These types of attacks on RTS /CTS frame can be identified and removed in order to improve performance efficiency, throughput of network. The packet synchronization mechanism can be applied to do so. The algorithm is as follows:

```
1. Start
2. Create MANET Scenario with 100,200 Mobile Nodes.
3. Apply Simulation Statistics.
4. Set Threshold = Value;
5. Packet Sent = Value;
6. Run and analyze Results
7. If (Packet Sent > Packet Threshold && Packet Sent < Packet Threshold)
8 Then
9 Declare the Node as a Attacker Node and go to step 12.
10 Else
11 End
12 Apply Modified CTS/RTS Mechanism.
    13  f ( Packet Sent  > Packet Threshold && Packet Sent < Packet Threshold )
{
14. Then Block that Node and go to Step 12.
15 else
{
16 end
17 Display the list of all Blocked Nodes in the MANET that Blocked Node will not be able to participate in further communication.
```

3.3 NETWORK MODEL FOR WMN

The detection technique shown in this paper depends on a zone-based hierarchical network model for WMN [6], as illustrated in Figure1. The entire network contains one backbone network and one or more local area networks known as zones. The backbone network contains backbone routers, an off-line CA which only links to the network under the situation that it is realized of the availability of an intruder, being it a zone router, a terminal user or a backbone router, and a database of authenticated certificates that are shared only between the backbone routers. There are also minimum two backbone routers linked to the Internet. Every zone network has two zone routers linked to the backbone network and to the subscribers. There is also a database that records subscriber information, i.e. zone ID, user ID, authenticated key, etc., which is shared between the two zone routers.

In the network model, it is considered that communication among subscribers has the following features:

(1) One zone router may link to one or more terminal users.

(2) Subscribers in a zone network interact with one another within a comparatively shorter range and those in a backbone network interact with one another within a comparatively longer range.

(3) Terminal users link to the Internet via backbone routers and any one of the two zone routers. Those in the same zone network may interact directly. And those in adjacent zone networks may interact with one another via their zone routers.

(4) Authentication among subscribers would utilize authenticated certificates. And cryptographic communication among subscribers follows the identity-based cryptosystem.

(5) The communication cost through the backbone network is higher as compared to zone networks.

3.4 Detection Mechanism

Paper [8] follows priority technique to decrease malicious nodes' forwarding priority, since, nodes resources being attacked is still expended, particularly cache memory. Attackers can alter their IP to control its forwarding frequency less than the threshold and its total packets more than cache memory.
For preserving restricted node resources, an enhancement upon priority technique is proposed in this paper. An end-to-end authentication is utilized to prevent subscribers altering its IP for faked identity; and usage rate of cache memory, two-threshold value, and distributed DoS intruder or not.
(1) Before communication, mutual authorization of two sides of communication is obtained utilizing their issued authority certificate.
(2) A table of priority is established by the node for its every neighbour, which is associated to the neighbour's former forwarding frequency. When dealing with message, high priority is firstly assumed. Each's initial value is set to 1.
(3) When a node has forwarded *m* message in the earlier 1 second, its priority will be changed to *1/m* by its neighbouring nodes.
(4) A specific size of buffer is assigned to every neighbour by the node, whose threshold is set to *Pn*. The neighbour with greater priority is assigned more buffers, which means its *Pn* is greater. When a neighbour's packets have arrived the threshold, then its excessive packets will be directly abandoned rather than processed, and its excessive assigned buffer will be taken back.
(5) Every node set a threshold *P* for its total buffer size, which is the sum of *Pn*. When some nodes combine to launch a cooperated DOS attack, and if the total utilized buffer exceeds the threshold *P*, specific packets will be dropped and their assigned buffer would be taken back. Packets with least priority will be dropped more.
(6) Packets with greatest priority in the buffer are processed at the first turn.
(7) If a node determines a terminal user, i.e., its neighbouring node, being a DoS intruder, it would observe its zone router.
(8) If a zone router finds a terminal user being an intruder, the zone router would disconnect the terminal user with the zone network. Then, the zone router would use its authenticated key and update the key pair of the zone network. At last, the zone router would declare that the terminal user is an ineligible subscriber to the zone members in the same zone and to its neighbour backbone router. The backbone router will start any t-1 out of the n-1 backbone routers to use the terminal user's identity-based private key and authenticated certificate along with itself. Simultaneously, the backbone router would forward the result to the off-line CA so that the off-line CA would use the key pair and the public certificate of the terminal user [7].

IV. SECURITY ANALYSES

Comparing with recent DoS attack detection techniques, the scheme shown in this paper depends on a zone-based hierarchical distributed WMN has some benefits as follows:
(1) Zone-based hierarchical configuration can be increased easily to deal with WMNs of any sizes and combined easily with several networks.
(2) Assuming some uncertain attacks, disseminated voting is utilized in this technique, which can improve its reliability and flexibility.
(3) For defending against DoS attack, mutual authorization of terminal nodes is conducted before communication, and usage rate of cache memory is always scanned during communication. Its detection rate is greater than those who just scan neighbours' forwarding frequency.
(4) Two-threshold value shown in this paper is capable to resist collaborated DoS attack established by multi-nodes.
(5) When collaborated DoS attack take place, packets with least priority will be dropped first, which can enhance the accuracy to discard packets, and assure stable transmission of legitimate nodes.

V. SIMULATION RESULTS

After showing the all simulations results conducted in both scenarios, in this chapter, we examine and explain all these results. The performance metrics gathered and shown in our results are either depends on the global statistics or object

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

statistics of the MANET model such as the whole network. In presenting these data, we showed the results average or time average values in this report. We begin our analysis and discussion with the two significant scenarios in which the first scenario consists of 100 mobile nodes and the 2nd scenario contains 200 mobile nodes. In every scenario, we did two simulations of a continuous network operation in MANET and in MANET, a DoS attack to be accurate. All simulations such as both scenarios were operated for a specific time period of 30 minutes, which ranged from 0 to 1800 seconds as presented in the result graphs. After that, we examine and compare within every scenario and also both scenarios depend on their end to end delay and throughput. Basic parameters utilized for experimentation with OPNET modeller. Communication area is 55 x 55 km with 100 and 200 mobile nodes. The performance comparison of three scenarios with respect to throughput is described in fig 2 and 3.

6.1Throughput

Throughput can be described as the ratio of the total amount of data arrives a destination node from the source node. The time it consumes by the destination node to obtain the last message is known as throughput. It can represent as bytes or bits per seconds (byte/sec or bit/sec). There are some factors that influence the throughput i.e. existence of restricted bandwidth, changes in configuration, unreliable communication between nodes and restricted energy. A high throughput is absolute choice in each network. In fig the graph shows the throughput in bits per seconds. The x-axis presents the simulation time in minutes and the y-axis represents throughput in bits/sec. Scenario 1, shows the scenario with no malicious event and normal network state, scenario 2 shows the network that is under the DoS attack and scenario 3 shows the mobile jammers and implementation of the introduced technique. It can be clearly viewed, that the DoS attack reduces the total network throughput as compared to the normal network state. Since, the entire throughput of network is increased once the introduced unified technique is implemented. Additionally, the throughput state has increased more than the no attack scenario after implementing the unified security technique.

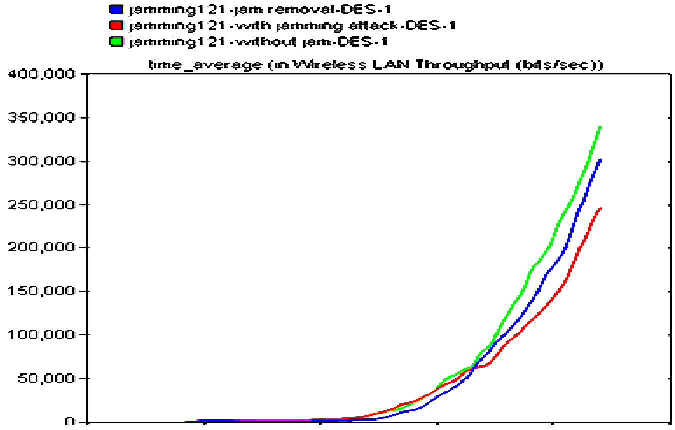

Figure: 2 Throughput of all three scenarios at 100 nodes

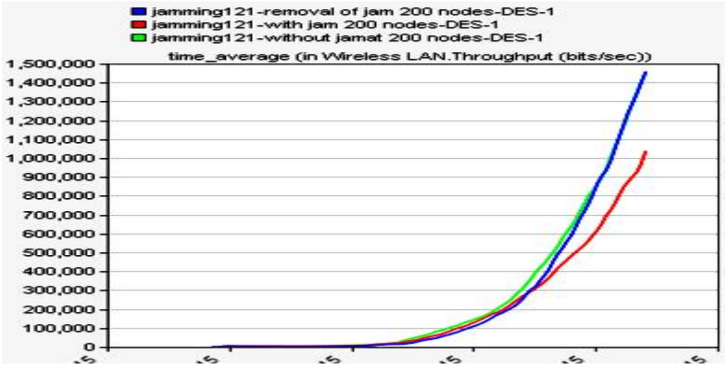

Figure: 3 Throughput of all three scenarios at 200 nodes

In first scenario of 100 nodes of our experimentation, packets travels are presented as throughput with maximum value of about 350064 bits/sec and it is expressed as bits per second. In second scenario which is under DoS attack, packets drops which are expressed as throughput, reduces to value of about 300435 bits/sec. In first scenario of 200 nodes of our experimentation, packets travels are represented as throughput with maximum value of about 14563478 bits/sec and it is expressed as bits per second. In second scenario which is under DoS attack, packets drops which are expressed as throughput, reduces to value of about 10435675 bits per second. This packet drop in form of throughput is because of the DoS attack. The throughput recovery occurs with introduced technique by removal of the DoS attack as throughput comes to same as the normal scenario.

6.2 END TO END DELAY

The packet end to end delay is the average time that packets consume to traverse in the network. This is the time from the packet creation by the sender node up to their reception at the destination node and is represented in seconds. Thus all the delays in the network are known as packet end-to-end delay. It involves all the delays in the network i.e. processing delay (PD), propagation delay (PD), queuing delay (QD), transmission delay (TD).

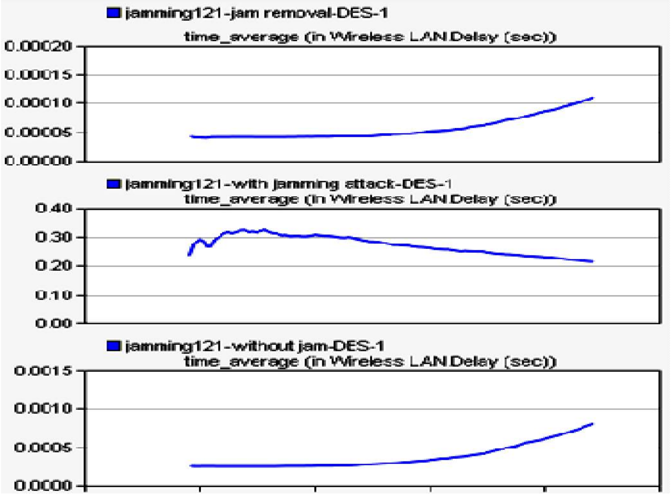

Figure: 4 Delay of all three scenarios at 100 nodes

In first scenario of 100 nodes of our experimentation, packets Delay are illustrated as fig 5.3 with maximum value of about 0.0010 seconds. In second scenario which is under DoS attack, packets delay Increases to value of about 0.35 seconds. In first scenario of 200 nodes of our experimentation, packets delay is about 0.0020 seconds. In second scenario which is under DoS attack, the value of packets delay increases to about 0.30 seconds. The end to end delay recovery reduces with our introduced technique by removal of the DoS attack as end to end delay comes to same as the value 0.000256 seconds. Hence our introduced technique removes network DoS attack.

DOI: 10.15680/IJIRCCE.2016. 0406098

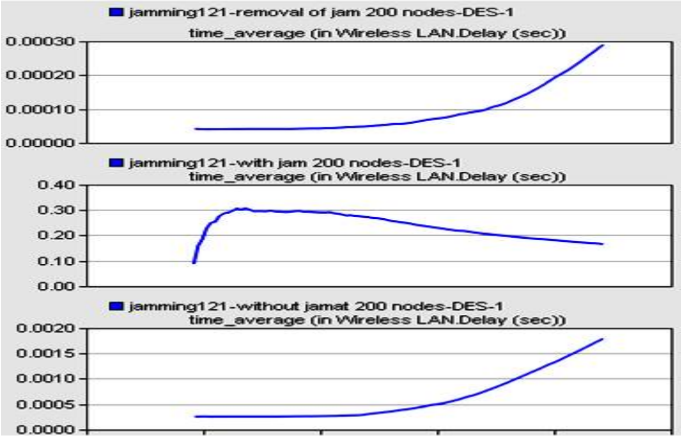

Figure: 5 Delay of all three scenarios at 200 nodes

VII. CONCLUSION

DoS attacks will have an impact on performance of networks as a result of the jammers disturbs with the conventional network operation. The impact of intruders studied in this paper was by increasing delay, data dropped traffic obtained and forwarded and reducing network packet drop ratio. In this research work, the performance of network under DoS attack is examining by applying integrated method. The objective of this simulation research study was to realize the effect of an integration of security techniques against DoS attacks. The unified technique is implemented on the chosen nodes on the network and deployed in the particular region. The discovery of the research clearly specifies that, the implementation of such unified techniques have an important effect on the total network through positively. On the other side, the implementation of such techniques does not only mitigate the DoS attack impacts, it also increases the total performance above the network normal state. The unified technique that consist an integration of PCF and RTS/CTS represents proper performance in MANET. However, 2 mobile jammers utilized in this simulation experiment, the introduced security technique satisfactorily mitigated the DoS attack impacts on the network and increased the total network performance while enhancing data drop rate. The data dropped rate reduces successfully. However, the DoS attack results packet drop rate and low throughput effect on the network, the rate of delay appears acceptable on the network. Future studies can be conducted to change the current model to reduce a total network delay.

REFERENCES

[1] Sabbar Insaif Jasim," Jamming Attacks Impact On the performance of Mobile Ad-Hoc Network and Improvement Using MANET Routing protocols," International Journal of Engineering and Advanced Technology(IJEAT), Volume 3, Issue 2, pp. 325-330, Dec. 2013.

[2] Ajana J., Helen K.J, "Mitigating Inside Jammers in MANET Using Localized Detection Scheme", International Journal of Engineering Science Invention, Volume 2, Issue 7, pp. 13-19, July 2013

[3] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar," Improving Reliability of Jamming Attack Detection in Ad-Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS) , Vol. 3, No.1, pp. 57-66, April 2011

[4] S. Raja Ratna, R. Ravi and Dr. Beulah Shekhar," Mitigating Denial of Service Attacks in Wireless Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, No.5, pp. 1716-1719, May 2013,

[5] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, pp. 45-51, December 2009

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, pp. 265-274, July 2010.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, pp.75-84, November 2006.

[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, pp. 331-335, May 2010.

[10] Dang Quan Nguyen and Louise Lamont, “A Simple and Efficient Detection of Wormhole Attacks”, New Technologies, Mobility and Security, pp. 1-5, November 2008

[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, “Analysis of Wormhole Intrusion Attacks in MANETs”, Military Communications Conference, pp.1-7, November 2008

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, ”Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis”, Military Communications Conference, pp. 1-7, October 2006

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, “Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks”, Second International Conference on Computer and Network Technology, pp. 102-104, 2010

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, pp. 370-380, February 2006.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, “Defending against Wormhole Attacks in Mobile Ad Hoc Networks”, Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[16] L. Qian, N. Song, and X. Li, “Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath,” IEEE Wireless Commuunication. and Networking Conference, 2005.