Impact of Wormhole Attacks on MANETs

Saurabh Upadhyay [1] and Brijesh Kumar Chaurasia[2]

[1]SATI, Vidisha, INDIA,
[2] MIR Labs, Gwalior, INDIA,
Corresponding Adresses
[1]saurabh.cse.cs@gmail.com, [2]bkchaurasia.itm@gmail.com

***Abstract*:** A mobile ad hoc networks (MANETs) consists of a collection of wireless mobile nodes that are capable of communicating with each other. MANETs is infrastructure-less, lack of centralized monitoring and dynamic changing network topology. So, this network is highly vulnerable to attacks due to the open medium. In this paper, we discuss the impact of wormhole attack in MANETs. The wormhole attack is difficult to detect by using any cryptographic measures because they do not create any separate packets. In this work, several techniques of wormhole detection like watchdog, nodes with directional antenna and cluster based approach etc. Some prevention techniques such as packet leashes, time-of-flight, delphi protocol, pathrater technique etc. are also presented. The result analysis shows the impact of wormhole attack on MANETs in terms of throughput variations.

***Keywords*:** MANETs, Wormhole attack, Wormhole detection technique, Wormhole prevention, Attack model**.**

1. Introduction

A MANET is also known as a mobile mesh networks that consists of wireless mobile nodes that dynamically self organized connected by wireless links. Vehicular ad hoc networks and Sensor ad hoc networks are the varieties of MANETs.

In general, attacks are two types; active attacks and passive attacks. Wormhole attack [1] comes under active attack category is depicted in Fig. 1.

Passive attack: These types of attacks are not disrupting the network. For example eavesdropping attacks and traffic analysis and monitoring etc.

Active attacks: These types of attacks are disrupted the network, to alter or destroy data being exchanged in the network. These attacks can be internal or external.

Wormhole attack:

In wormhole attack [1], an attacker connects two distant points in the network, and then replays them into the network from that point. An example is shown in Fig. 2. Here *S* and *D* are the two end-points of the wormhole link (called as wormholes). In Fig. 2, wormhole attack is assumed between the node *A* and node *H* and their neighbor nodes, vice versa. The wormhole link can be established by many types such as by using ethernet cables, long-range wireless transmissions and an optical link in wired medium. Wormhole attack records packets at one end-point in the network and tunnels them to other end-point [2]. These attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as AODV/ DSR, the attack could prevent the discovery of any routes other than through the wormhole.

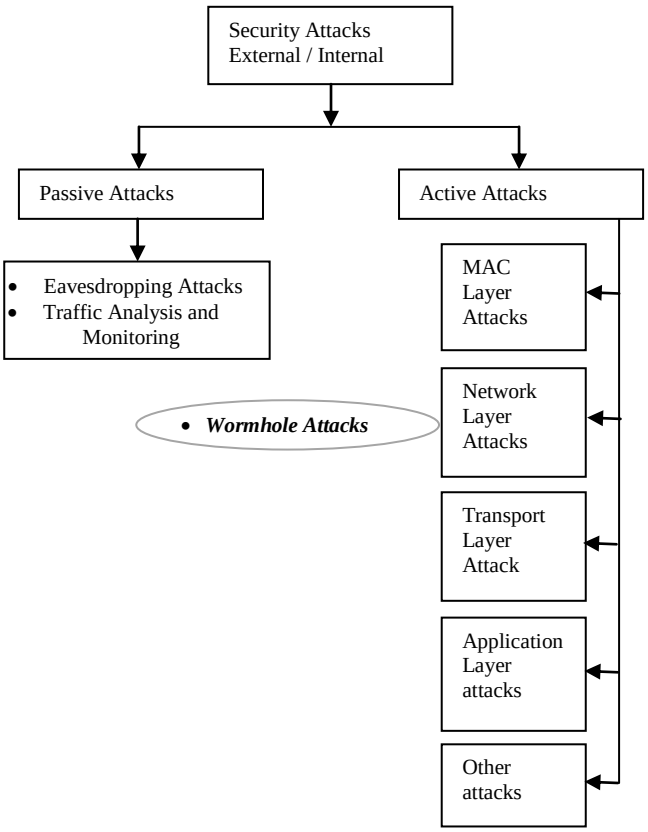

Figure 1. Categories of attacks in MANETs

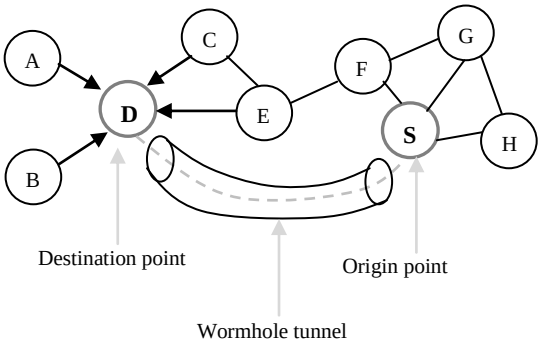

Figure 2. Wormhole attack in a network

The rest of the paper is organized as follows. Section 2 describes the problem. Section 3 of this paper presents the model and types of wormhole attack. In Section 4, we present the wormhole detection and prevention technique. Section 5 provides impact on MANETs. Section 6 concludes the work.

2. Problem Description

Wormhole attacks put severe threats to MANETs. This attack is very much dangerous because it can also still be performed even if the network communication provides authentication and confidentiality. Wormhole attack can also affect the network even if the attacker has no cryptographic keys. The wormhole attack is especially harmful against many ad-hoc routing protocols for example, ad hoc on-demand distance vector (AODV) [3], dynamic source routing (DSR) [4], the hop count of a path effects the choice of routes, clusterhead gateway switch routing protocol (CGSR) [5], hierarchical state routing protocol (HSR) [6] and adaptive routing using clusters (ARC) [7]. The wormhole attack is able to confuse the clustering procedure and lead to a wrong topology and it can partition the network through control links between two cluster heads of the routing hierarchy.

3. Wormhole Attack Model

A wormhole attack is consisting of two attackers and a tunnel through which the data is transmitted. For creating the wormhole attack the attacker creates a direct link referred as wormhole tunnel. The network which is caused by wormhole attack is depicted in Fig. 3.

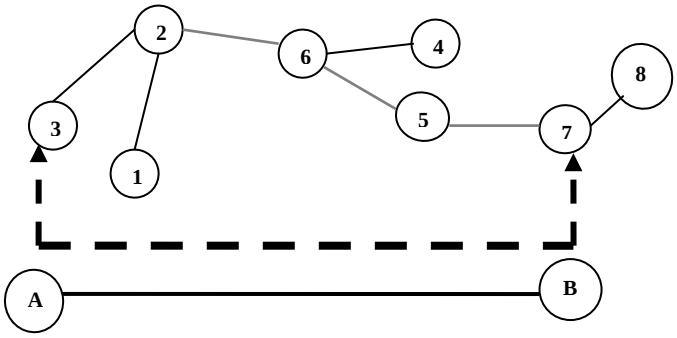

Figure 3. A netwok affected by wormhole

In Fig. 3, the tunnel represented by wired link, wireless out-of-bank link and logical link where the routing packet being encapsulated. When a wormhole tunnel has been created, attacker will receive packets from its neighbors and copies them and forwards them to the other attacker by using wormhole tunnel. Receiving node receive these tunneled packets. In a wormhole attack that uses wired links, high quality wireless out-of-band links, the attackers are directly connected to each other, so they can communicate very easily. However they require some special hardware to support such types of communication. A wormhole designed by using packet encapsulation is relatively much slower, but it can be launched very easily because it does not need any special hardware or special routing protocols.

Intruders A and B are connected by a wireless link, wireless link will be used to tunnel network data from the one end of the network to the other end of the network. Without presence of wormhole, node 7 and node 3 are apart from the cluster and their messages will forward to each node via nodes 2, 6 and 5. When wormhole attack is activated by intruders A and B, the node7 and node 3 are able to directly communicate to each others' messages and they will response that they are immediate neighbors.

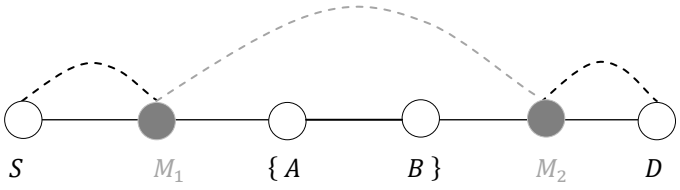

Figure 4a. Open wormhole

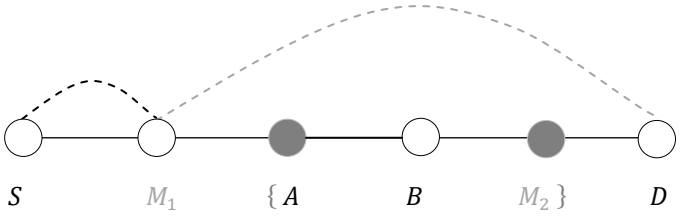

Figure 4b. Half open wormhole

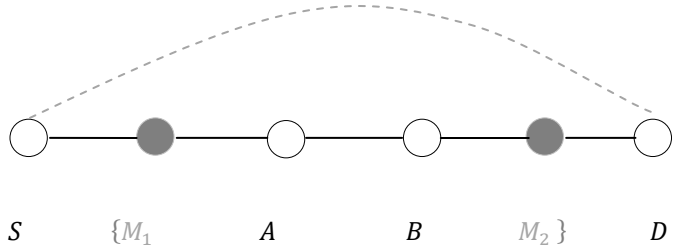

Figure 4b. Closed wormhole

If this happens, all communications between nodes 3 and 7 will be done by using the wormhole link introduced by A and B between node 3 and 7. The wormhole attack can be divided in three categories [8]; Open wormhole, half open wormhole and close wormhole.

In the given Fig. 4a, Fig. 4b and Fig. 4c M_1 and M_2 are presented the malicious nodes. S and D are the good nodes that are representing source and destination respectively. A and B are the good nodes between source and destination. The nodes in the curly-braces { } are the nodes that are on the path but are invisible due to presence wormhole and the curly-braces is presented here as false route in Fig. 4. Hence node S and D are connected by using a wormhole, so source and destination nodes think that they are immediate neighbors and all data between them will be transmitted by using this wormhole link. Both the nodes M_1 and M_2 are in the wormhole. In Fig. 4.b, M_1 node is the neighbor of source node S and it tunnels to destination through node M_2 and only one node can be seen by S and D due to wormhole attack. In the open wormhole attack both nodes M_1 and M_2 are visible to source node and destination node as shown in Fig. 4.a.

There is another classification of wormhole is discussed in [8], [10]. This classification is also categorized in three types;

i. Threshold based wormhole attack: In this category, wormhole will drop the packets of size greater than or equal to the threshold value.
ii. All pass based wormhole attack: In this type, wormhole will passes all packets irrespective of their size.
iii. All drop based wormhole attack: In this category, wormhole will drop all packets irrespective of their size.

4. Wormhole Detection and Prevention Techniques

In this section, we introduce the mechanism for detecting the wormhole attacks. To identifies misbehaving nodes and avoids routing through theses nodes, watchdog and pathrater is proposed in [11]. In this technique, watchdog identifies misbehavior of nodes by copying packets and maintained a buffer for recently sent packets. The overheard packet is compared with the sent packet, if there is a match then discards that packet. If the packet is timeout, increment the failure tally for the node. And if the tally exceeds the thresholds, then node will misbehave. The implementation of watchdog technique is shown in Fig. 5.

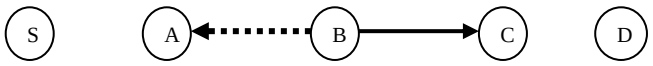

Figure 5. Watchdog implementation

In this figure, it is assumed that bidirectional communication symmetry on every link between nodes that want to communicate. If a node B can receive a message from a node A at time t, then node A could instead have received a message from node B at the time t will implement the watchdog. It maintain a buffer of recently sent packets and compares each overheard packet with the packet in the buffer, when B forwards a packet from S to D with the help of C, A can overhear $B's$ transmission and capable of verifying that B has attempted to pass the packet towards C. But this approach has some limitations and it is not detect the misbehaving node during ambiguous collisions, receiver collisions, false misbehavior and collusion.

The approach is used directional antenna to detect and prevent the wormhole attack [12]. The technique is assumed that nodes maintain accurate sets of their neighbors. So, an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbor and its messages are ignored. To estimate the direction of received signal and angle of arrival of a signal it uses directional antennas. This scheme works only if two nodes are communicating with each other, they receive signal at opposite angle. But this scheme is failed only if the attacker placed wormholes residing between two directional antennas.

Statistical analysis scheme [13] is based on relative frequency of each link which is part of the wormhole tunnel and that is appears in the set of all obtained routes. In this techniques, it is possible to detect unusual route selection frequency by using statistical analysis detected and will be used in identifying wormhole links. This method do not requires any special hardware or any changes in existing routing protocols. It does not require even the aggregation of any special information, since it uses routing data that is already available to a node the main idea behind this approach resides in the fact that the relative frequency of any link that is part of the wormhole tunnel, will be much higher than other normal links.

In [14] is discussed graph theoretic model that can characterize the wormhole attack and can ascertain the necessary and sufficient conditions for the candidate solution to prevent wormhole attack. This scheme is also discussed a cryptographic based solution through local broadcast key and to set up a secure wireless ad hoc network against wormhole attacks. In this scheme, there are two types of nodes in the network named as: guards and regular nodes. Guards access uses GPS to access the location information or other localization method like secure range independent localization for wireless sensor network is presented in [15] and rebroadcast location data. Regular nodes need to calculate their location relative to the guards' beacons, thus they are able to distinguish abnormal transmission due to beacon retransmission done through the wormhole attackers. In this scheme, sender is encrypted all transmissions from local broadcast key and these information must be decrypted at the receiver end. But this scheme will be suffer the time delay to accumulate per node traveled and special localization equipment is needed to guard nodes for detecting positions.
To mitigate the wormhole attack in mobile ad hoc network, cluster based technique is proposed in [16]. In this approach clusters are formed to detect the wormhole attack. The whole network is divided into clusters. These clusters can either be overlapped or disjoint. Member nodes of cluster pass the information to the cluster head and cluster head is elected dynamically. This cluster heads maintains the routing information and sends aggregated information to all members within cluster. In this scheme, there is a node at the intersection of two clusters named as guard node. The guard node has equipped with power to monitor the activity of any node and guard the cluster from possible attack. The network is also divided into outer layer and inner layer. The cluster head of outer layer is having the responsibility of informing all nodes of the inner layer about the presence of the malicious node.

To prevent and detect the wormhole attack most common approach is discussed in [1] and [17], known as packet leashes mechanism. In this paper, they are presented two types of leashes: geographic leashes and temporal leashes also presented an authentication protocol. The authentication protocol is named as TESLA [18] with instant key disclosure and this protocol, for use with temporal leashes. In, geographic leashes each node access GPS information and based on loose clock synchronization. Whereas temporal leashes require much tighter clock synchronization (in the order of nanoseconds), but do not tightly depend on GPS information and temporal leashes that are implemented with a packet expiration time. The observation of this scheme is geographic leashes are less efficient than temporal leashes, due to broadcast authentication, where precise time synchronization is not easily achievable.

Other temporal leashes wormhole prevention technique is discussed in [19] based on time of flight of individual packets. This scheme is to measure round-trip travel time with its acknowledgment. This technique is used merkle hash tree and hash chains as explained in TESLA.

An efficient detection method known as delay per hop indication (DelPHI) for wormhole attack prevention is discussed in [20]. The protocol is developed for hidden wormhole attack and exposed wormhole attack. In this scheme, sender will check whether there are any types of malicious nodes presented in the routing path by that they will receive and implement the wormhole attacks. This scheme

will not require clock synchronization, position information of nodes and any special types of hardwares.

Pathrater technique [11] calculates path metric for every path. By keeping the ratings of each node in the network, the path metric is calculated by using the node rating and connection reliability which is obtained from previous experience. Once the path metric has been calculated for all accessible paths, Pathrater will select the path with the highest metric. The path metrics would enable the Pathrater to select the shortest path. Thus it avoids routes that may have misbehaving nodes.

5. Impact of Wormhole Attack on MANETs

The wormhole attack is dangerous against the security in MANETs in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. It is one of the most the powerful attack that are faced by many ad hoc network routing protocols. Since The wormhole attack does not require exploiting the feature of nodes in the network and it can interfere while executing the routing process. Attacker uses these attacks to gain unauthorized access to compromise systems or perform denial-of-service (DoS) attacks. In wormhole, the attacker at one end records the incoming traffic and tunnels packets to the other end. If routing control messages like RREQ are tunneled, this will result in distorted routing tables in the network. If there exist fast transmission path between the two ends of the wormhole that may tunnel the data at higher speed than the normal mode of wireless multi-hop communication. Thus, they will attract more traffic from their neighbors. This will results in rushing attack. In Rushing attack, due to the presence of fast transmission path all the packet will start following that path and this will increase the Average Attack Success Rate. Wormhole attack can also act as the first stage attackers where they can lead to the denial-of-service attacks. In the second stage, this may compromise the security of the global network as that breaks confidentiality and integrity. The wormhole attack is very harmful to the security of network. Due to the placement of the wormhole in the network there will be significant breakdown in communication across a wireless network. A successful wormhole attack may be the reason of disruption and breakdown of a network. Proper balance between these two is necessary to prevent much consumption of resources.

6. Simulation and Results

In this section, the impact of wormhole attack on MANETs is presented through simulation using QualNet [21]. The setup is shown in Fig. 6. The throughput is estimated by running the simulation experiment for 50 nodes in 1500x1500 m^2 area. increased and on increasing the data rate then packet drop is also increased. Fig. 7. and Fig. 8. represents the total packet sent and received at 2 Mbps constant bit rate (CBR). Fig. 9 depict the total packet sent and received at 11 Mbps CBR. Fig. 10. show the packet drop at nodes before or after the wormhole attack implementation. The result presents the packet drop is increased when attack is implemented in between the source and destination nodes. The observation and analysis shows that when wormhole is deployed on a route than packet drop is increased while maximizing the data rate, then packet drop is also swells.

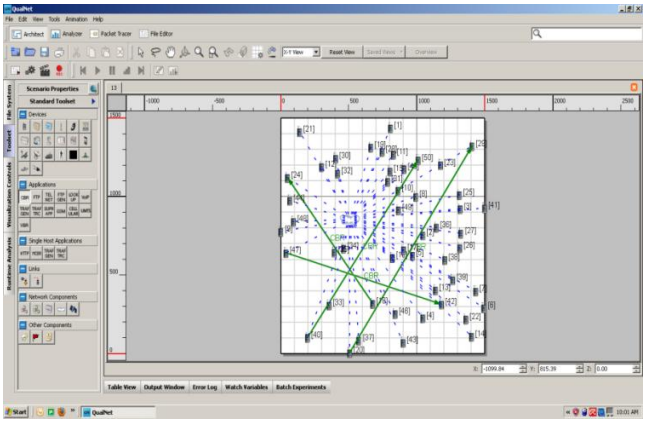

Figure 6. The simulation framework for wormhole attack

The simulation parameters are shown in Table1.

Table 1. Simulation elements

Simulation area	1500m x 1500m
Number of nodes	50
Physical Layer	802.11
MAC Layer	802.11b

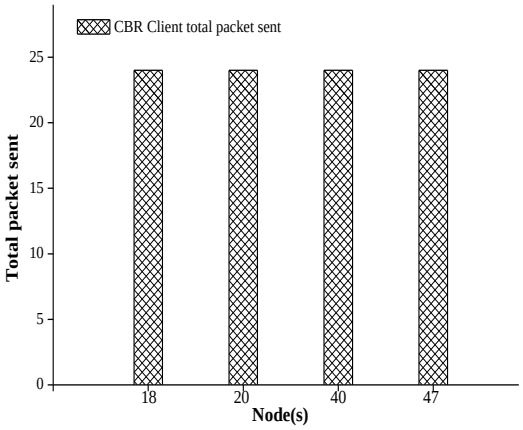

Figure 7. Total packet sent at 2 Mbps through client (CBR)

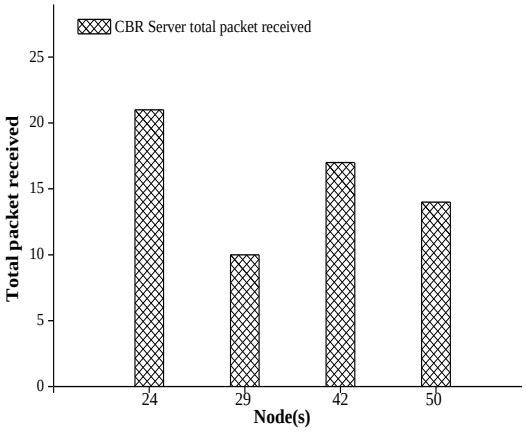

Figure 8. Total packet received at 2 Mbps

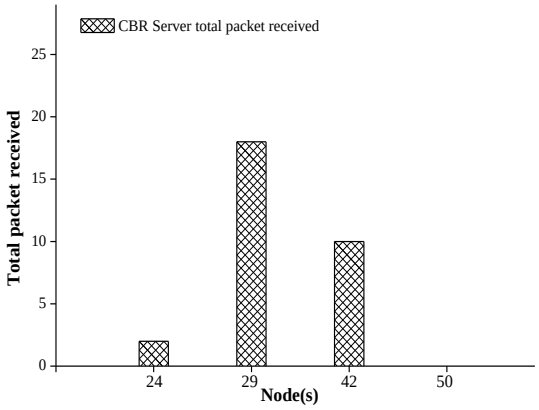

Figure 9. Total packet received at 11 Mbps

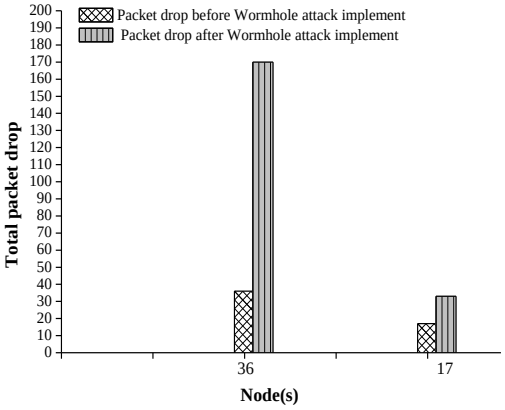

Figure 10. Packet drop at nodes

7. Conclusion

Wormhole attack is a very powerful attack that is created by malicious colluding nodes. It does not require any cryptographic breaks. The wormhole attack is a powerful attack that can have serious consequences on many proposed ad hoc network routing protocols. An attacker who can conducts a successful wormhole attack can disrupt routing, deny service to large segments of a network, creation of unconnected component within a network. In this paper we have discussed the several ways by which the wormhole can be handled. Results indicates that impact of wormhole attack is affected the throughput of packet ratio in terms of packet received, packet sent and packet drop at the nodes in ad-hoc networks as mobile ad hoc networks and sensor ad hoc networks. Future work on this topic will include developing any protocol that will prove much better security than existing against the wormhole attack.

References

[1] Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks, Selected Areas of Communications," in IEEE Journal on, vol. 24, no. 2, pp.370-380, 2006.

[2] P. M. Jawandhiya, M. M. Ghonge, M. S. Ali and J.S. Deshpande, "A Survey of Mobile Ad Hoc Network Attacks ," in International Journal of Engineering Science and Technology, vol. 2, no. 9, 4063-4071, 2010.

[3] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop on Mobile Comput. Syst. Appl., pp. 90–100, 1999.

[4] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in Proc. Conf. Commun. Architect., Protocols, Appl., pp. 234–244, 1994.

[5] Ching-Chuan Chiang, Hsiao-Kuang Wu, Winston Liu, and Mario Gerla, "Routing in clustered multihop, mobile wireless networks with fading channel," in Proceedings of IEEE Singapore International Conference on Networks (SICON '97), pp. 197–211, 1997.

[6] G. Pei, M. Gerla, X. Hong, and C.-C. Chiang, "A wireless hierarchical routing protocol with group mobility," in Proc. of IEEE on wireless communication and networking conference (WCNC), pp. 1538 - 1542, 1999.

[7] E. Royer, "Hierarchical routing in ad hoc mobile networks," Wireless Communication and Mobile Computing, vol. 2, no. 5, pp. 515-532, 2002.

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

[9] M. Jain and H. Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks," in procedding of International conference on advances in computing, control and telecommunication technologies, pp. 555-558, 2009.

[10] S. Suresh Kumar, T.V.P. Sundararajan and Dr. A. Shanmugam, "Performance Comparison of Three Types of Wormhole Attack in Mobile Adhoc Networks," in proceedings of the Int. Conf. on Information Science and Applications ICISA, pp. 443-447, 2010.

[11] O. Kachirski and R. Guha, "Effective Intrusion Detection using Multiple Sensors in Wireless Ad hoc Networks", in Proc. 36th Annual Hawaii Int'l. Conf. on System Sciences (HICSS'03), pp.57.1, 2003.

[12] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," in proceedings of the 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[13] N. Song, L. Qian and X. Li , "Wormhole Attack Detection in Wireless Ad Hoc Networks: a Statistical Analysis Approach," in proceeding of the 19th International Parallel and Distributed Processing Symposium (IPDPS'05), 2005.

[14] L. Lazos, R. Poovendran, C. Meadows, P. Syverson and L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach," in IEEE WCNC 2005, Seattle, WA, USA, pp. 1193–1199, 2005.

[15] L. Lazos, and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," in ACM WiSE'04, New York, NY, USA, pp. 73–100, October 2004.

[16] Debdutta Barman Roy, Rituparna Chaki and Nabendu Chaki, "New Cluster –based wormhole intrusion detection algorithm for mobile adhoc network," in International Journal of Network Security & Its Applications (IJNSA), vol. 1, no. 1, pp. 44-52, 2009.

[17] Y.-C. Hu, A. Perrig and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, vol. 3, pp. 1976-1986, 2003.

[18] Adrian Perrig, Ran Canetti, Doug Tygar, and Dawn Song, "Efficient Authentication and Signature of Multicast Streams over Lossy Channels,"in Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 56–73, 2000.

[19] S. Capkun, L. Buttyan and J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks," in processings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21-32, 2003.

[20] H.S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," in Proc. International Symposium on Wireless Pervasive computing, Phuket, Thailand, pp. 1-6, 2006.

[21] QualNet online available at: http://www.scalable-networks.com/products/system-requirements/qualnet/

Author Biographies

Brijesh Kumar Chaurasia is working in Privacy Preservation in Vehicular Ad hoc Networks. He is received his M. Tech. (Computer Science) degree from D.A.V.V., Indore, India. His research interest area is Security in Wireless Ad hoc Networks.

Saurabh Upadhyay is pursuing M. Tech. (Software System) degree from SATI, Vidisha, India. He is received his B. Tech. (Computer science) degree from GBTU (formally known as UPTU), India**.**
(saurabh.cse.cs@gmail.com)