Wormhole Detection and Prevention Authentication based Delay Per Hop Technique for Wireless Ad-hoc Network

Siddhesh Khanvilkar
PG Student
Pillai HOC College of
Engineering and Technology

Sandeep B. Raskar
Pillai HOC College of
Engineering and Technology

ABSTRACT
In wormhole attack, an attacker node keeps data packets at one location in the network and forward to another attacker node far away by tunneling, which again broadcast them into the network locally. The proposed technique is an efficient detection and prevention method called Wormhole Attack Prevention and Detection Using Authentication Based Delay per Hop Technique for Wireless Network. Detection of wormhole attack is done using number of hops and delay of each node in different paths available in network. The sender node is capable to identify both types of wormhole attacks. Proposed technique detects the legitimate path and path under the wormhole attack. From quantitative viewpoint, relevant network simulations were conducted to validate the proposed scheme using a NS2 network simulator.

General Terms
Security, Wormhole attack, Authentication, Caeser Cipher, Inband Channel, Out of Band Channel.

Keywords
Wireless ad-hoc network, Wormhole attack, Tunnel, Wormhole detection technique, wormhole affected path avoidance.

1. INTRODUCTION
Wireless ad-hoc network is an assembly of nodes facilitate with wireless communication and networking capabilities, nodes can be wireless devices, computers, and mobile phones etc [1] [2]. In network each node works as router. The comfort of communication extremely depends on coordination of other nodes. Most of the protocol assumes that nodes which are available in the network are trust able, so they do not assume the security problems. Wireless network is the most vulnerable to wide range of security attacks [3] [4], because of lack of infrastructure, open medium and dynamically changing network topology. In time varying network topology node are acts as host and router, due to this hard to identify the malicious node or attacker node or infected node [2]. In wormhole attack attacker stores packet at one location in the network, tunnels packet to another location and retransmit them into the network [5] [6]. A wormhole attack can be done using In-band and Out-of band channel as shown in figure 1. In In-band channel, attacker node uses the normal nodes as an intermediate node to forward the route request packets from one attacker node to another attacker node. In out-of band channel, by using wired link or long range of wireless link one malicious node is directly connected to another malicious node [7][8].

Gathering the sensitive information from network or packet is the main aim of the wormhole attack.

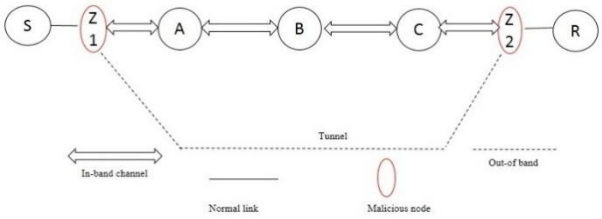

Figure 1. Wormhole Attack

In Figure 1, the receiver node R notice that sender node S is directly neighbor of it, but actually packet is delivered via node S-Z1-A-B-C-Z2-R in In-band wormhole attack and S-Z1-Z2-R in out-of band wormhole attack.

2. LITERATURE SURVEY
Introduced an End-to-end Detection method of wormhole attack [9], is worked on the smallest hop count estimated between source node and destination node. The source node starts the wormhole detection procedure. Source node selects an appropriate shortest path from a set of legal routes for data transmission.

Detection of wormhole attack without using any hardware is done by Wormhole attack detection Protocol using Hound Packet [WHOP] [10]. In this method Source node counts hop difference by using hound packet to detect the wormhole attack. WHOP required extra processing time to process the hound packets for detection of wormhole attack.

To protect against wormhole attacks technique was proposed [11], the main intention of this technique is to limit the extreme allowed transmission distance. Authentication is necessary to receive the packets. In Geographical leashes, loosely clock synchronization and accurate location information of each node is required. In temporal leashes, loosely location information and exact clock synchronization of every node is required.

AllHop count and delay per hop are supervised for wormhole detection in DELPHI called as Hop Count Delay per hop indication technique [12].This technique requires extra resources to differentiate different trials in data collection procedure from source to destination.

3. WORKING METHODOLOGY

The proposed system is Wormhole Attack Prevention and Detection Using Authentication Based Delay Per Hop Technique for Wireless Network. In proposed system, an idea to detect wormhole attacks in the wireless network by gathering number of hop count and delay per hop information from different paths from source to destination and destination to source, which offers a solution to detect both types of wormhole attack. The scenario under the legal situation , the delay for each packet is same along each hop in the path, but under wormhole attack, for each packet delay should be high , the reason behind is there can be many nodes available between them or can be attached through a long wireless link. The path which is under the wormhole attack is having large delay then the normal path. Therefore, path is under the wormhole attack if it has large delay per hop.

To keep away from the necessity of special types of hardware and clock synchronization techniques like directional antenna, positioning system and IDS, proposed technique collects both number of hop count and delay information in same routine to AODV route discovery process and perform detection process at sender node. Sender node broadcast a route REQ message to receiver and receiver gives reply by broadcasting route REP message to the sender. By comparing the delay between hop and hop count information of different paths a wormhole can detected.

For prevention of wormhole attack, every transmitting and receiving node has its own node id. Node id is initiated and verified using lightweight cryptography algorithm known as ceaser cipher in which input is converted into cipher text by applying some arithmetical operation and at the receiver end reverse operation is carried out to get back the original text. All authorized nodes are aware of the common key. Hence only authorized nodes can generate valid signature and it will not produce any error at the receiver side. Attacker's signature will be identified as invalid at receiver side.

There are three steps for detection and Prevention of wormhole attack. First step offers data collection of information like delay and number of hop count. Detection starts by sender node in second step by using collected data in first step. In Third Step authentication is provided to prevent the wormhole attack.

3.1 Information Gathering in Wireless Network

This step will enable sender to gathers information of each route from source to destination and vice versa. In this process as shown in figure 2 when the sender starts route discovery process, it broadcasts an RREQ packet to the destination node. RREQ packet includes previous hop field, hop count field and time-stamp field. Destination node gives reply to Sender node by broadcasting RREP packet which includes same fields as in RREQ packet.

3.2 Broadcasting of RREQ Packet and RREP Packet

RREQ packet is processed by many intermediate nodes before reaching the destination node. RREP packet is processed by many intermediate nodes before reaching the Sender node. Intermediate node change the previous hop field and hop count field after receiving the RREQ packet or RREP packet.

When an intermediate node receives RREP packet or RREQ packet, it reads the previous hop field and makes a reverse route to the sender node (neighbour node) and the replaces its node ID into the previous hop field and increase the hop count field by 1 and RREP packet forward or RREQ packet to its neighbor node.

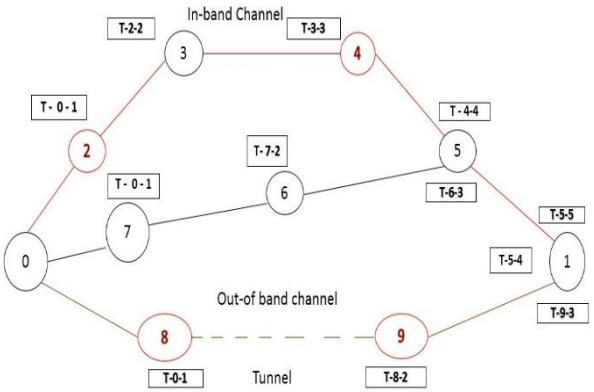

Figure 2: RREQ Road Map

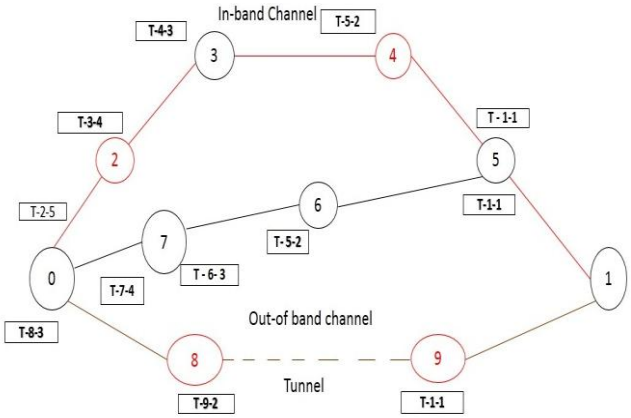

Figure 3: RREP Road Map

In figure 2 sender node '0' broadcast RREQ packet to Receiver node '1' from different paths which is available in network. When intermediate node receives RREQ packet update hop field with previous node id and increase its hop count by one and after that forward RREQ packet to its next neighbor. As shown in Figure 2and Figure 3 there are three different paths are available in network, so RREQ packets and RREP packets broadcast from path 0-2-3-4-5-1, path 0-7-6-5-1 and path 0-8-9-1. In path 0-2-3-4-5-1 node '2' and node '4' is attacker node (red colored) which forms wormhole attack through in-band channel (red colored path). In path 0-8-9-1 node '8' and node '9' is the attacker node (red colored) which is directly connected through long range of wireless link to forms wormhole attack through out-of band channel (brown colored path).Figure 2 shows the Road map for RREQ packet from sender to the receiver node and figure 3 the Road map for RREP packet from receiver to the sender node.

In Figure 3 receiver node '1' broadcast RREP packet to sender node '0' to the paths from request comes. When intermediate node receives RREP packet update hop field with previous node id and increase its hop count by one and after that forward RREP packet to its next neighbor.

3.3 Route Optimization Process in Wireless Network

In this step, after gathering all information from different path, detection process starts by the sender node. Suppose RREQ packet sent at time Ts by the sender node. RREQ

packet received from receiver node at time Tt. Ht is the hop count field, PT is propagation time given by

$$PT_{t} = T_{t} - T_{s} \quad (1)$$

Delay per hop value is calculated is as follows

$$DPH_{t} = PT_{t} / H_{t} \quad (2)$$

In normal situation a smaller h provides a smaller value of PTt. It can be explained by the fact that a shorter path should have a smaller round trip time. Hence the DPHs of normal paths should have similar values independent to h.

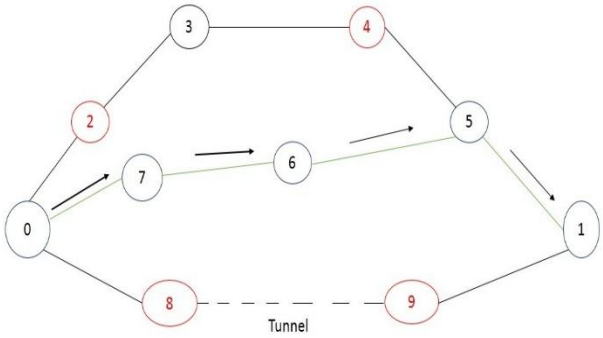

Figure 4: Path Selection

Sender node identifies the path under the wormhole attack and path which is not affected by wormhole attack. So basically gathers the information of disjoint path and arrange them based on number of hops and delay per hop in each path. In Figure 4 shows that sender select second route 0-7-6-5-1 (green color path) for transmission, because path 0-2-3-4-5-1 is under wormhole attack through in-band channel and path 0-8-9-1 is under the wormhole attack through out-of band channel.

3.4 Secure Route Authentication Process

Every node has its own node id. Nodes must be capable to validate that the data or packet has been sent by the authorized node. A node getting the RREQ validates that the sender is genuine user or not along with the checking of proposed technique and it sends the request to its neighbors only if it is received from genuine user otherwise it will not forward the RREQ.

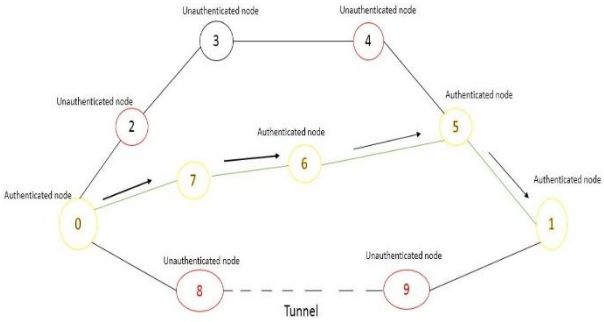

Figure 5: Node Authentication and Verification

Key is generated and verified using lightweight cryptography algorithm called as Ceasar cipher in which input is converted into cipher text by applying some arithmetical operation and at the receiver end reverse operation is carried out to get back original text. All the authorized nodes are aware of the common key. Attacker is unaware of the common key. Hence only the authorized nodes, can generate valid signature and it will not produce any error at the receiver side. Attacker's signature will be identified as invalid in the receiver side. As shows in figure 5 authentication is provided for path 0-7-6-5-1 (in green colored) and all yellow colored nodes are authenticated node.

3.5 Signature Generation and Verification of the Genuine Node

Common key is 35. Encrypted id of node 0 (sender) is 35 in which id 0 is added with key 35. In the receiver side, encrypted id is decrypted by subtracting key value that results in sender id.

Key = 35

The encrypted id of node 0 is 35 and decrypted id of node 0 is 0.

Encrypt(0) = key + node id

= 35 + 0

encrypt(0) = 35

decrypt(0) =0

Decrypt(0) = encrypt(0) - key

= 35 - 35

Decrypt(0) = 0

The node id is equal to the decrypted id.

3.6 Signature Generation and Verification of the Attacker Node

Encrypted id of node 2 (attacker) is 16 here because, node 2 is unaware of key value and hence it generates its signature by adding the random key (14) value which results in 16. When the receiver decrypts the encrypted value with key (35), it results in -19 [16-35]. Node with id -19 is not existed in the network. Hence node 3 is identified as attacker here.

encrypt(2) = 16

decrypt(2) =-19

The node id is not equal to decrypted id.

Node 2 is not an authenticated user.

4. PERFORMANCE EVOLUTION

Node 0 is sender and Node1 is receiver. 50 nodes are deployed randomly in the area of 1000 X 1000. Node 2 &3 are wormhole attacker1 and wormhole attacker2 respectively. RREQ packets broadcasted from sender to receiver and receiver reply to sender through RREP packets from different roots which is available in network. Sender node calculates hop count and delay per hop of each root from sender to receiver. Based on hop count and delay per hop information sender is able to detect legitimate path and wormhole path which is under wormhole attack for In-band channel and Out-of band channel. After detecting the wormhole attack authentication is provided for secure transmission. Here consider two scenarios for analysis. In first scenario here consider two path, one is normal path and second is wormhole path. Genuine path and wormhole path which is form through in-band channel is identified. After identification of genuine path authentication is provide for secure transmission and compare the authenticated path with wormhole affected path for different attributes. Same procedure is applied in second scenario to detect wormhole attack which is form through out-of band channel.

4.1 Analysis Attributes

4.1.1 Delay

When number of node is increased delay is decreased. Delay in wormhole detection path is higher than the delay in worm hole detection path authentication, shows in Figure5 and Figure10.

4.1.2 Dropped Packets:

Dropped packet ratio is increased because of number of node is increased. Dropped packet in wormhole detection is higher than dropped packet in wormhole detection authentication, shows in Figure 6 and Figure 11.

4.1.3 Packet Delivery Ratio

Packet delivery ratio in wormhole detection authentication path is higher than the packet delivery path in worm hole detection path, shows inFigure 7 and Figure 12.

4.1.4 Throughput

Throughput in wormhole detection authentication path is higher than the throughput in worm hole detection path, shows in Figure 8 and Figure 13.

4.1.5 Overhead

Overhead ratio is increased because of number of node is increased.Overhead in wormhole detection is higher than overhead in worm hole detection authentication, shows in Figure 9 and Figure 14.

4.2 In-band Channel

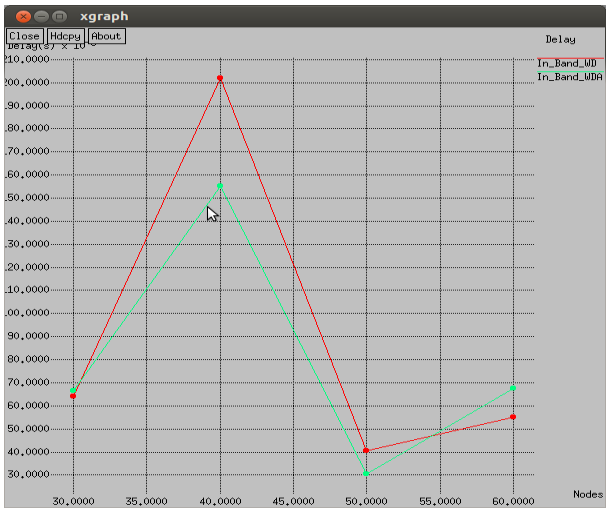

Figure 5: Delay

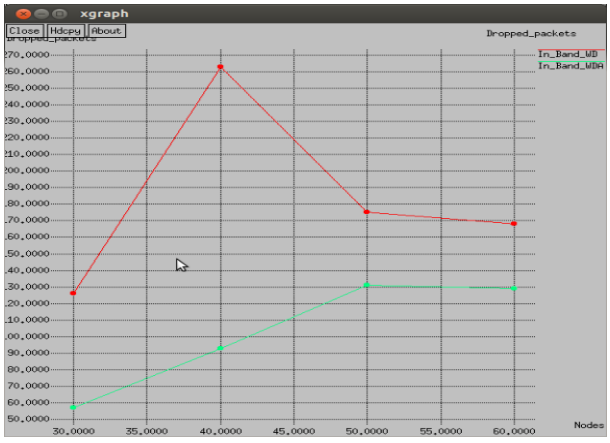

Figure 6: Dropped Packets

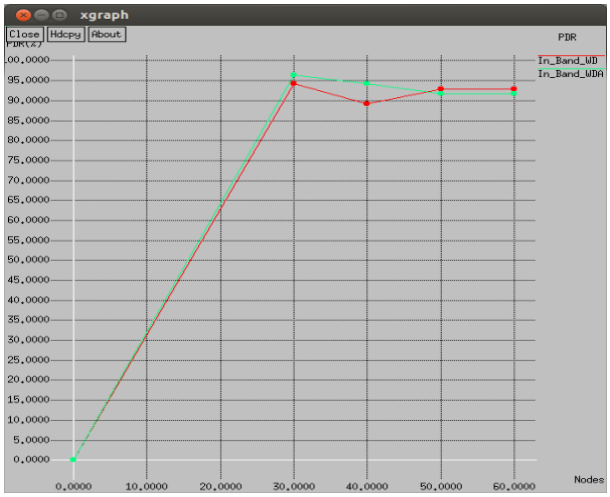

Figure 7: Packet Delivery Ratio

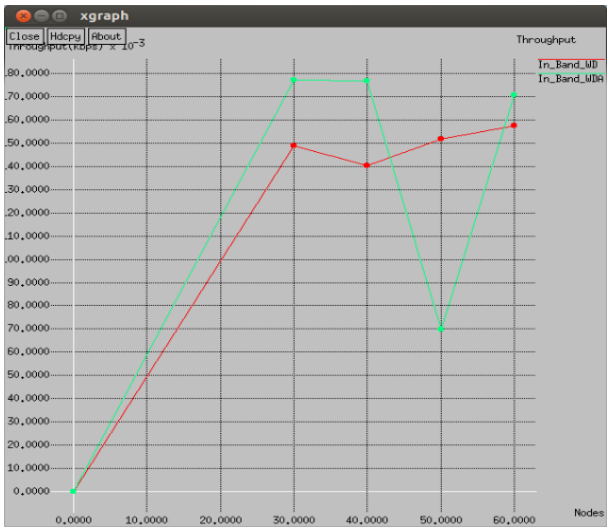

Figure 8: Throughput

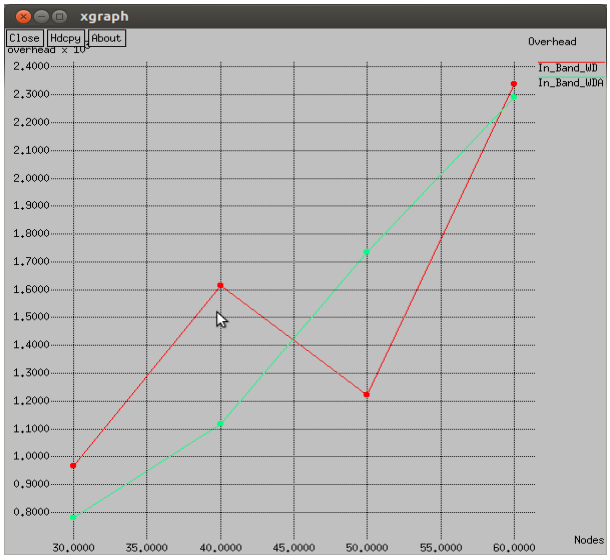

Figure9: Overhead

4.3 Out-Of Band Channel

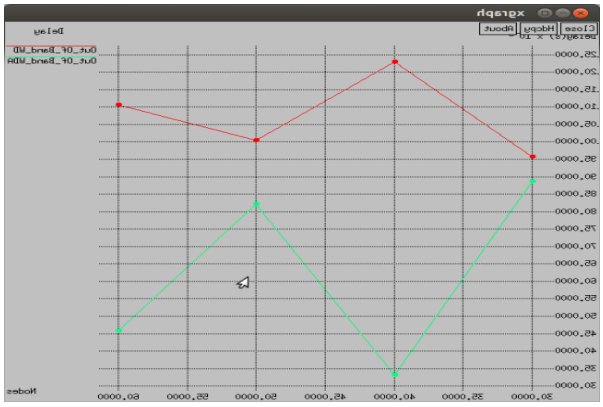

Figure 10: Delay

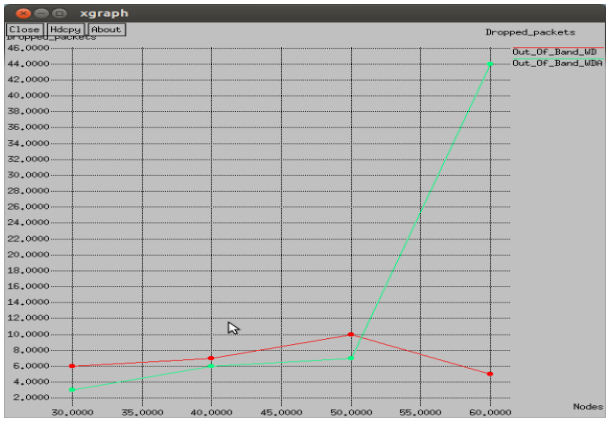

Figure 11: Dropped Packets

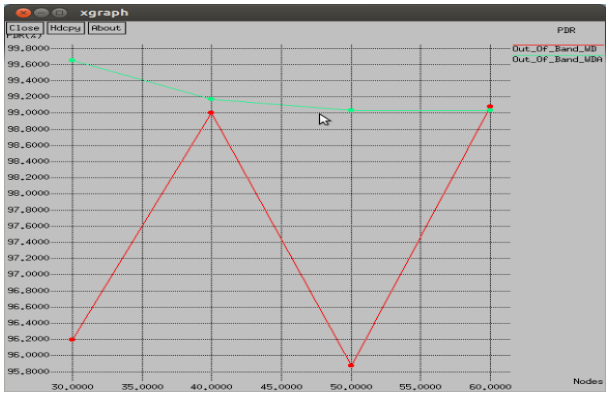

Figure 12: Packet Delivery Ratio

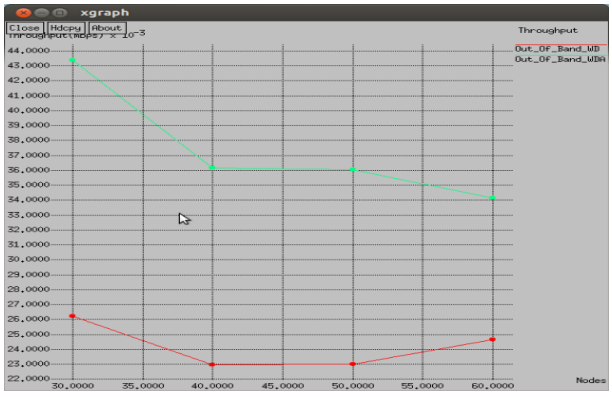

Figure 13: Throughput

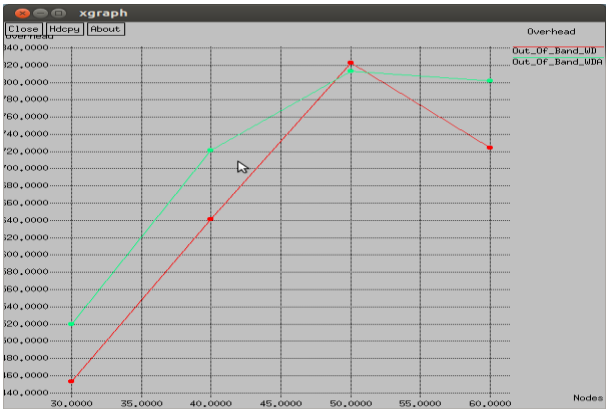

Figure 14: Overhead

5. CONCLUSION AND FUTURE SCOPE

5.1 Work Conclusion

Wormhole attacks are the powerful attacks that can be easily set up in wireless networks. Proposed technique does not required special hardware like antenna to get accurate node position and information, clock synchronization and special types of packets. Detection technique is focused on delay per hop values between normal path and wormhole path. Authentication is provided for secure transmission and for prevention of wormhole attack. Authentication of nodes in path is provided for secure transmission and prevention of wormhole attack in future.

5.2 Future Scope of Work

In future, this technology can be implemented with other protocols to get different result. One can apply different algorithms and methodologies for authentication to compare with current methodology to get better results in authentication. This methodology also can be useful for detection and prevention of other attacks like grey-hole attack and black-hole attack.

6. ACKNOWLEDGMENTS

During the entire period of this survey, my survey paper would not have been materialized without the help of many people, who made my work so easier. It gives me proud privilege to complete this survey paper working under valuable guidance of Prof. Sandeep Raskar. He has been very supportive and patient throughout the process. I am also thankful to all staff members for providing all facilities and every help for smooth progress of paper work. I thank all others, and especially, friends and our family members who in one way or another helped me in the successful completion of this work.

7. REFERENCES

[1] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing protocol Performance issues and Evaluation Considerations January 1999," RFC2501.

[2] SaurabhUpadhaya and ArunaBajpai, Avoiding Wormhole Attack in MANET using Statistical Approach, IEEE March 2012

[3] Y Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," MobiCom'2000, Boston, Massachusetts, Aug. 6-11, 2000, PP. 275 - 283

[4] Ming-Yang Su. Warp: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. Computer Security, Vol.29, March 2010

[5] RushaNandy and Debdutta Berman Roy, Study if Various Attack in MANET and Elaborative Discussion of Rushing Attack on DSR with clustering scheme, IEEE 13 March 2011

[6] ReshmiMaulik and NabenduChaki, A Study of Wormhole Attacks in MANET. International journal of computer information systems and industrial management application 2011 PP. 271-279.

[7] Khalil S. Bagchi and N.B. Shro_. LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. International Conference on Dependable Systems and Networks, PP 612-621,2005.

[8] W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Interscience, ―Defending agains Wormhole Attacks in Mobile Ad Hoc Networks,‖ Wireless Communication and Mobile Computing, January 2006.

[9] X. Wang and J. Wong. An end-to-end detection of wormhole attack in wireless ad-hoc networks. In the proceedings of the 31st annual international computer software and applications conference, PP 39-48, 2007.

[10] S. Gupta, S. Kar and S. Dharmaraja, "WHOP: wormhole Attack Detection protocol using hound packet". In the international conference on innovations Technology, IEEE 2011.

[11] Y Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless networks," Proc. Of INFOCOM',April 2003, PP. 1976-1986.

[12] H.S. Chiu and K.S. Lui. DELPHI: wormhole detection mechanism for ad hoc wireless networks. 1st International Symposium on Wireless Pervasive Computing, PP 6-11, January 2006