Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet

Priyank Nayak, Akshay Sahay, Yogadhar Pandey

Abstract- In MANET, data transmission is performed within an un-trusted wireless environment. Various kinds of attack have been identified and corresponding solutions have been proposed. In wormhole attack, an attacker record packets at one location into the network, tunnel them to another location and retransmits them there into the network. Previous works on wormhole attacks have focused only on detection and used specialized hardware such as directional antennas or extremely accurate clocks. More recent work has difference of hop distance at node, create packet with two fields processing bit, count to reach next hop and AODV for route establishment, public key encryption method are also used. In this paper, we present a general mechanism, without use of hardware, location information and clock synchronization called detection packet for detecting malicious node in network. Detection Packet has three fields: processing bit, count to reach next hop and time stamp. Timestamp is used for strongly detection with conformance at wormhole attack. Here detection packet can easily be included in the wide range of ad hoc routing protocol with only significant change in the existing protocol to defend against wormhole attack. Here DSR protocol is use for route establishment and NS-2 for simulations.

Keywords- Network Security, Wormhole Attack, Tunnel, Wireless Ad-Hoc Network, Routing Protocol, Selective Forwarding, NS- 2

---

1 INTRODUCTION

In an ad-hoc wireless network [7], the routing and resource management are done in a distributed manner in which all node coordinate to enable communication among themselves. This requires each node to be more intelligent so that it can function both as a network host for transmitting and receiving data and as a network router for routing packets from other nodes. Ad-hoc network has infrastructure-less, multi-hop wireless links, quick and cost-effective deployment, application domain include battlefields, emergency search and rescue operation, self-organization and maintenance properties are built into the network, collaborative computing, main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths.

Wormhole attack is one of the most threatening and hazardous attacks. A wormhole attack is usually performed by pair of malicious node. Two malicious nodes at different location sending- receiving routing message to each-other via a tunnel. Wormhole nodes can successfully execute such attacks without compromising any host and are unavoidable. Then MANETs [7] provide authenticity and confidentiality protection.

- *Priyank Nayak is currently pursuing masters degree program in Software engineering in SIRT, Bhopal (MP), India, E-mail: priyank_nayak@yahoo.in*
- *Akshay Sahay is A.P. in CSE Dept. in SIRT, Bhopal (MP), India, E-mail: sahayakshay@yahoo.com*
- *Yogadhar Pandey is A.P. in CSE Dept. in SIRT, Bhopal (MP), India, E-mail: p_yogadhar@yahoo.co.in*

Two type of wormhole attacks have been discussed in the literature: hidden wormhole attack and exposed wormhole attack. In hidden wormhole attack, this attack can be easily mounted and without compromising any host in the network [5], [11-16] and in exposed wormhole attack, in which two end points are two compromised hosts [8-10]. But our attention will focus on hidden wormhole attack.

In Fig 1, the destination D notice that a packet from the source S is transferred under hidden wormhole attack, while it believes that the packet is delivered via node S, A1, W1, W2, B1, D under hidden wormhole attack.

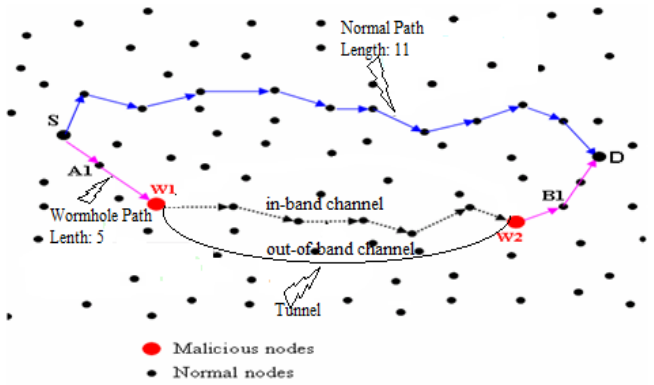

Fig.1: Wormhole Attack

2 WORMHOLE CREATION

In any ad-hoc network, a wormhole can be created through the following three ways:

- Tunneling of above the network layer.
- Tunnel creation via internal hidden infrastructure.
- Tunnel creation via external wired infrastructure.

3 RELATED WORKS

Saurabh gupta , Subrat Kar and S. Dharamraj [5] introduced "WHOP: Wormhole Attack Detection Protocol using Hound Packet". WHOP is take the help of others nodes (nodes who were not involved in path) after the path has been discovered to found worm hole in the network. For path discovery, the AODV protocol is used. AODV [1] RREQ packet to find the path from source to destination, After the source node receive RREP packet, it creates packet called Hound Packet, before forwarding this packet has public key encryption method. Different hound packets received at destination node. Here destination node performs calculation on the received values of hound packet to detect wormhole in the pre-formed path between itself and sender. Destination node create table for each entry of hound packet. If difference value for all row is equal or greater than all node in the path, then the node and its previous node in the path may forming wormhole and will be malicious node.

Sakthivel and Chandrasekaran [6] introduced "Detection and Prevention wormhole Attack in MANET using Path Tracing Approach". For route discovery, DSR [2] protocol is used. In order to detect the wormhole, Prior per hop distance field, per hop distance field and timestamp fields are added to the header of each packet. We consider both prior per hop distance and per hop distance so as to compare the difference between the two distances. If the difference is too large that exceeds the maximum threshold value, then wormhole is detected. These wormhole node are then isolated from the network.

Maulik and Chaki [4] introduced "A Study on Wormhole Attacks in MANET" Here analyzed the performance of mobile ad hoc network under wormhole attack in different routing protocol. and here source node set the wormhole prevention timer (WPC) with sending packet.

4 PROBLEM STATEMENT

When wormhole attack is occurring in wireless ad-hoc networks then processing delay of the data packet, pair of malicious node is established on the path. Conformance and Prevention problem is occur.

5 PROPOSED METHOD

The Principal of our proposed method is to take the help of others nodes (nodes who were not involved in path) after the path has been discovered to found worm hole in the network. In path discovery, the protocol uses DSR RREQ [2] packet to find the path from source to destination, RREQ packet is broadcasted by some other node except the destination node. Each node replying back RREP to source node must store its identity into RREP packet. The path details are stored in the DSR routing cache [2]. After the source node receives RREP packet, it creates packet called Detection Packet. In order to detect the wormhole, we optimize the general DSR header [2] by adding extra fields. Total Hop Count [5], Processing Bit [5], Count to Reach Next Hop [5] and Timestamp [6] fields are added to the header of Detection packet.

Type	Flags	Reserved	Total Hop Count
Destination IP Address			
Destination Sequence Number			
Source IP Address			
Source Sequence Number			
Addr [1]	Processing Bit	Count to Reach Next Hop	Time Stamp
Addr [2]	Processing Bit	Count to Reach Next Hop	Time Stamp
……	……..	……..	……
Addr [n]	Processing Bit	Count to Reach Next Hop	Time Stamp
Last Hop			

Fig.2: Detection Packet

5.1. Detection Packet

The "processing bit" (P.B) [5] can either be 0 or 1, initially all are 0, represents neighbour node of the entry has been visited or not, its value will only be set by the neighbour node of that entry. "Total hop count" [5] field in the packet is used to prevent the packet looping in the network. "Count to reach next hop" (CRNH) [5] represents the hop difference between neighbours of one hop separated node, its value will be increment by each node for the first node entry whose processing bit is zero in the packet. The "Timestamp" [6] field is initialized to the time of the first bit of RREQ is sent. timestamp field cannot be altered by any other nodes.

Fig 3. shows an example where source node S send the Detection packet to each of its neighbour where node A will drop the packet because its identity included in the packet. When node J receives the Detection packet founds it is the neighbor of node A, so it increments the CRNH field by 1 and set the P.B for the node entry A in the packet and forward the packet to node K. Node K founds it is also neighbour of node A but P.B for node A is already set then

it increments the CRNH of entry B. Similarly when node L gets the detection packet founds it does not have any node listed in the Detection packet as its neighbour, it then increments the CRNH of the first entry in the packet whose P.B is zero i.e Node entry A. and broadcast the Detection packet. Now node M receives the packet, founds it is the neighbour of entry A and B then it increments the CRNH field of entry A and set all P.B in the packet till the node entry to which it is a neighbour i.e B.

Every detection packet has Time-stamp for initialized to the time and calculate of bit transfer of neighbour node.

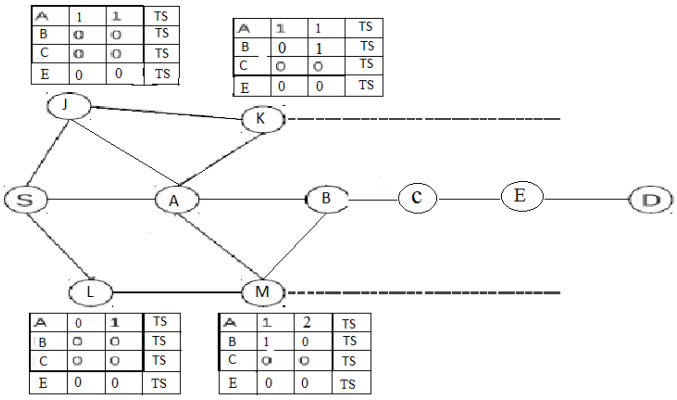

Fig.3: Detection Packet Processing

Similarly, Detection packet entry will be updated by each nodes in the network and destination node will receive multiple Detection packet with different values and different Timestamp in μs.

TABLE 1
Detection Packet at Destination Node

Address	Processing Bit	Count to reach next Hop	Time Stamp
A	1	2	5.6
B	1	3	28.8
C	1	2	18.3
E	1	1	54.4

Address	Processing Bit	Count to reach next Hop	Time Stamp
A	1	2	12.2
B	1	4	5.8
C	1	0	44.9
E	1	1	63.7

Address	Processing Bit	Count to reach next Hop	Time Stamp
A	1	2	9.7
B	1	5	33.8
C	1	0	36.3
E	1	0	25.5

5.2. Processing of Detection Packet at Destination Node

Table-1 shows the different Detection Packets received at destination node. Here destination node performs calculation on the received values of Detection Packet to detect wormhole in the pre-formed path between itself and sender. Destination node create table for each entry of Detection Packet, as it receives new Detection Packet, receiver adds one new row in each table.

5.3. Detection table at Nodes of Actual Path

Table-2 showing table for node A, B, C and E created by destination node. First column [5] indicates the number of hop and Second column [5] indicates the next entry in the Detection Packet whose neighbour node has been found after table node neighbour, this entry got filled after examined next entry in the detection packet which has non zero hop count. Third column indicates [5] the hop difference for example see second row in Fig-5 where node E neighbour was found after node B neighbour and the difference of hop between B and E is 1 which is subtracted from column 1 value, similarly for row 1 and 3 and so on. and fourth column [6] indicates time-stamp for strongly wormhole detection with confirmation.

TABLE 2
Detection Table of Node A, B, C and E

Node A			
Hops	Next Node Whose Neighbour Found	Actual Difference	Time Stamp
2	B	2	5.6
2	B	2	12.2
2	B	2	9.7

Node B			
Hops	Next Node Whose Neighbour Found	Actual Difference	Time Stamp
3	C	3	28.8
4	E	4-1=3	5.8
5	dest.	5-2=3	33.8

Node C			
Hops	Next Node Whose Neighbour Found	Actual Difference	Time Stamp
2	E	2	18.3
0	E	0	44.9
0	dest.	0-1=-1	36.3

Node E			
Hops	Next Node Whose Neighbour Found	Actual Difference	Time Stamp
1	dest.	1	54.4
1	dest.	1	63.7
0	dest.	0	25.5

5.4. Malicious Node Detection at Actual Path

If difference value for all rows is equal or greater than 4 [5], [6], then that node will be malicious node. and path will be forming wormhole attack.

5.5. Confirmation of Wormhole Attack

To detect the wormhole attack, we can find the average transmission time at per node of the actual path by using the formula,

$$\textbf{Detection Packet Transmission Time at per Node} = \frac{\text{Total of Timestamp}}{\text{Total of Hop-Count}}$$

If difference value for all rows is equal or greater than 4 and general method transmission time > detection packet transmission time, then wormhole attack is available on the actual path.

5.6. Prevention

Malicious node is available in the detection table and table is available in the cache memory. if data is transfer on any route, then data is use detection table and ignore the malicious node by detection table whose available in the cache memory. Thus wormhole attack is strongly detected with conformance and prevent.

6 IMPLEMENTATION DETAILS

6.1. Simulation Model

The NS2 (version 2.34) network simulator has been used for simulation work. The mobility scenarios are generated by a Random waypoint model and Reference Point Group Mobility Model (RPGM). The numbers of nodes tested in a terrain area of 600m x 600m are 50. The simulation parameters are summarized in Table 3. A new routing agent called wormhole, DSR is added to include the wormhole attack. Here, 45, 46, 47, 48 and 49 are posed as malicious nodes and the required coding is done so that they together form a wormhole link. Random Way Point mobility model is the most commonly used model for research purpose. Here all the nodes are randomly distributed with uniform speed. and We created maximum of 20 CBR connections.

TABLE 3
Simulation Parameters

FEATURE	DESCRIPTION
Simulator	NS-2 Version 2.34
Mobility model	Random Waypoint (RWP)
Routing Protocol	DSR
Tunnel Length	5 node
Number of node	50
Simulation Area (m x m)	600 x 600
Simulation time	120 seconds
Transmission Range	250 m
Packet Sending Rate	100 pkt/sec
Nodes in all scenarios	10, 20, 30, 40, 50
Traffic Type	CBR
MAC	802.11
Packet size	512 byte
Performance Parameters	PDR, Throughput and Delay
Examined approaches	Normal, Attack and Defense

6.2. Performance Discussion

6.2.1. Packet Delivery Ratio

PDR is the proportion of the total amount of packets reached the receiver and amount of packet sent by the source. If the amount of malicious node increases, PDR also decreases gradually. The higher mobility of nodes causes PDR to decrease.

$$PDR = \frac{\text{Total amount of data packet received (Receiver)}}{\text{Total amount of packet sent (Source)}}$$

Attack reduces the average Packet delivery Ratio (shown in Red) from normal condition (shown in Blue) and the proposed method significantly regains the Packet delivery Ratio by avoiding the attacker (shown in green)

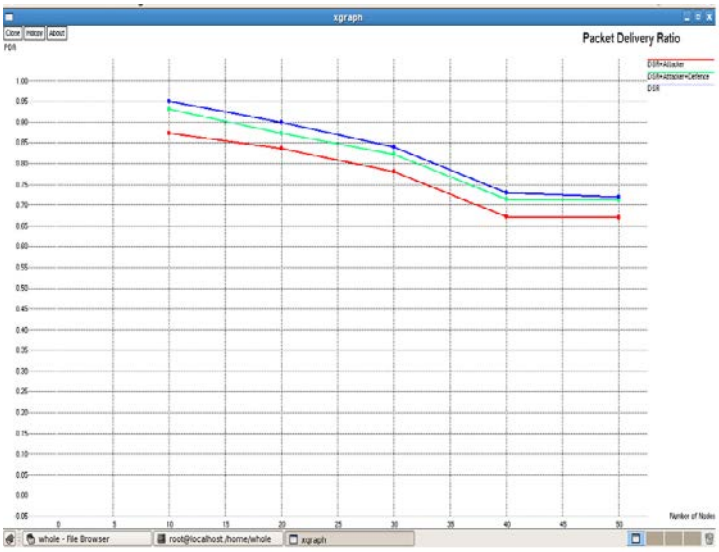

Fig 4: Packet Delivery Ratio per Route Comparison

Fig-4 describes the dependence of the packet delivery ratio on the number of nodes in action. All path decreases with increasing the number of nodes in the network. but defense path are increase compare than attacker path.

TABLE 4
Values of selected Node on per Route in Packet delivery Ratio

Node	*DSR*	*DSR + Attacker*	*DSR + Attacker + Defense*
10	**0.95**	**0.902**	**0.941**
20	**0.90**	**0.837**	**0.891**
30	**0.84**	**0.756**	**0.823**
40	**0.73**	**0.686**	**0.723**
50	**0.72**	**0.648**	**0.713**

Here in table-4, some selected analysis node (10, 20, 30, 40 and 50) results are available from the simulation with three routes. First route is normal path (DSR) without malicious node in blue color. Second route is attacker path (DSR + Attacker) with malicious node in red color. Third route is defense path (DSR + Attacker + Defense) where malicious nodes are isolated in green color.

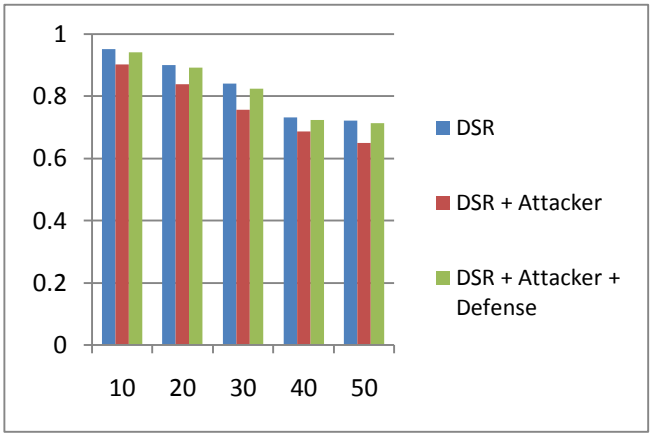

Fig 5: Packet Delivery Ratio per Route Comparison in Column Chart

Fig-5 shows the packet delivery ratio of three different routes as DSR, Attacker on DSR and Defense mechanism on Attack based DSR. In that X-axis specifies the node and Y-axis specifies the packet delivery ratio. Here we compare three routes for Packet Delivery Ratio with the proposed method. When malicious node occurrence is 0 then this method give a good packet delivery ratio. Normal path (in the blue) is providing 72% packet delivery ratio at node 50 in decrement order. When malicious node are occur in this normal path then it is called attacker path (in the red) is providing 64.5% packet delivery ratio at node 50 in decrement order. and when malicious node are isolated then it is called defense path (in the green) is providing 71.5% packet delivery ratio at node 50 in decrement order. but defense path are increase and provide better packet delivery ratio compare than attacker path.

6.2.2. Throughput

Attack reduces the average Throughput (shown in Red) from normal condition (shown in Blue) and the proposed method significantly regains the Throughput by avoiding the attacker (shown in green)

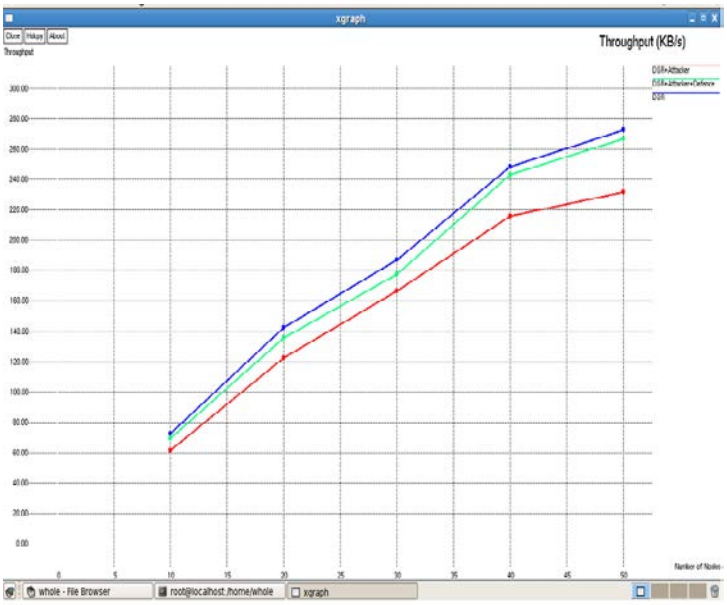

Fig 6: Throughput per Route Comparison

Fig-6 describes the dependence of the Throughput on the number of nodes in action. All path increases with increasing the number of nodes in the network. and defense path are also increase compare than attacker path.

Here per node communication is increase, hence route is available in increasing order. if we are make constant traffic then all route is available in decreasing order.

TABLE 5
Values of selected Node on per Route in Throughput

Node	*DSR*	*DSR + Attacker*	*DSR + Attacker + Defense*
10	72.38	62.971	70.932
20	142.54	122.584	138.264
30	186.95	162.647	177.602
40	248.25	223.425	235.838
50	272.25	239.580	261.360

Here in table-5, some selected analysis node (10, 20, 30, 40 and 50) results are available from the simulation with three routes. First route is normal path (DSR) without malicious node in blue color. Second route is attacker path (DSR + Attacker) with malicious node in red color. Third route is defense path (DSR + Attacker + Defense) where malicious nodes are isolated in green color.

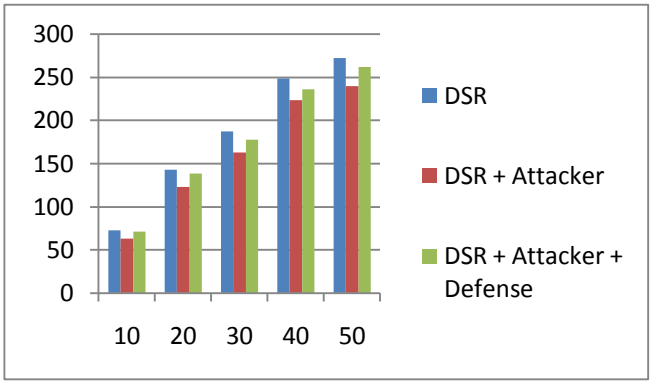

Fig 7: Throughput per Route Comparison in Column Chart

Fig-7 shows the Throughput of three different routes as DSR, Attacker on DSR and Defense mechanism on Attack based DSR. In that X-axis specifies the node and Y-axis specifies the Throughput. Here we compare three routes for Throughput with the proposed method. When malicious node occurrence is 0 then this method give improve Throughput. Normal path (in the blue) is providing 272 kbps Throughput at node 50 in increment order. When malicious node are occur in this normal path then it is called attacker path (in the red) is providing 239.5 kbps Throughput at node 50 in increment order. and when malicious node are isolated then it is called defense path (in the green) is providing 261.5 kbps Throughput at node 50 in increment order. but defense path are increase and providing improve Throughput compare than attacker path.

6.2.3. End to End Delay

The average delay is the elapsed time between the packet sent and received. Attack increase the End to End delay (shown in Red) from normal condition (shown in Blue) and the proposed method significantly reduce the End to End delay by avoiding the attacker (shown in green)

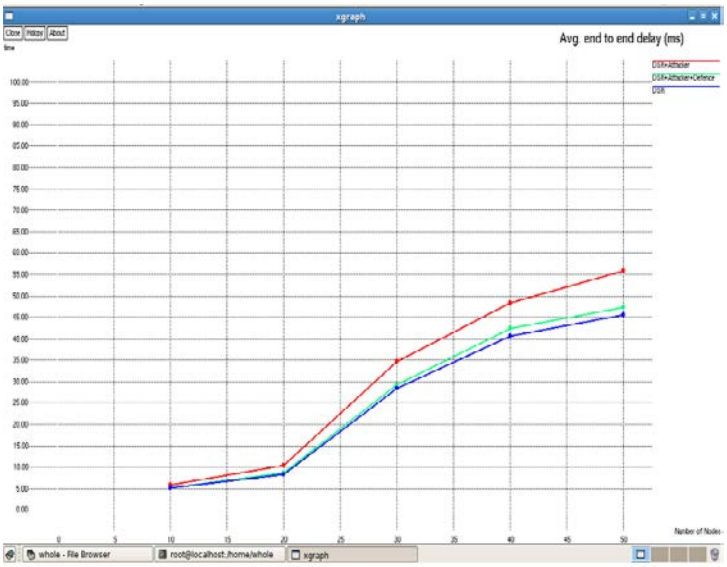

Fig 8: End to End Delay per Route Comparison

Fig-8 describes the dependence of the End to End Delay on the number of nodes in action. All path increases with increasing the number of nodes in the network. but defense path are decrease compare than attacker path for reduce the delay.

TABLE 6
Values of selected Node on per Route in End to End delay

Node	*DSR*	*DSR + Attacker*	*DSR + Attacker + Defense*
10	5.075	6.090	5.329
20	8.324	10.405	8.740
30	28.4509	34.141	29.873
40	40.6786	50.441	41.899
50	45.4786	56.848	46.843

Here in table-6, some selected analysis node (10, 20, 30, 40 and 50) results are available from the simulation with three routes. First route is normal path (DSR) without malicious node in blue color. Second route is attacker path (DSR + Attacker) with malicious node in red color. Third route is defense path (DSR + Attacker + Defense) where malicious nodes are isolated in green color.

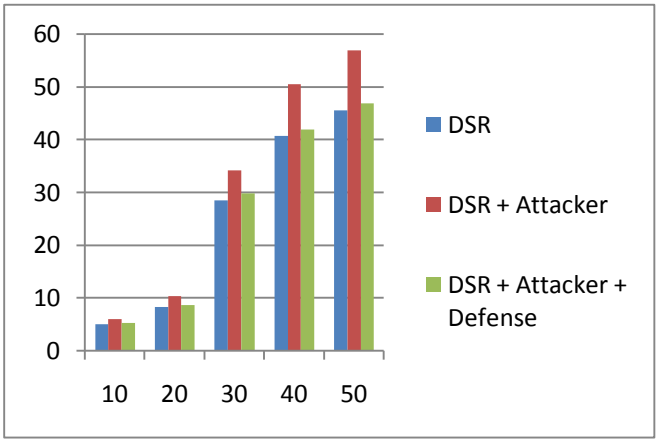

Fig 9: End to End Delay per Route Comparison in Column Chart

Fig-9 shows the End to End Delay of three different routes as DSR, Attacker on DSR and Defense mechanism on Attack based DSR. In that X-axis specifies the node and Y-axis specifies the End to End Delay. Here we compare three routes for End to End Delay with the proposed method. When malicious node occurrence is 0 then this method give reduce End to End Delay. Normal path (in the blue) is providing 45.5% End to End Delay at node 50 in increment order. When malicious node are occur in this normal path then it is called attacker path (in the red) is providing 56.8% End to End Delay at node 50 in increment order. and when malicious node are isolated then it is called defense path (in the green) is providing 46.8% packet delivery ratio at node 50 in increment order. but defense path are decrease and providing reduce delay compare than attacker path.

7 CONCLUSION

There have been many research efforts to overcome routing attacks in wireless ad hoc networks by security architecture, system or service such as authentication, encryption, extra hardware support etc. In this paper, we present a method by Detection Packet which is based on DSR [2] using simulations developed in Network Simulator 2 (NS-2) [3] to defend against wormhole attack in wireless ad hoc networks. and here wormhole attack is detect without use any hardware, location information and clock synchronization. Identify wormhole node and prevent them. Finally improve Throughput, Packet Delivery Ratio (PDR) and reduce End to End Delay compare than wormhole attack. These propose approach will help wireless ad-hoc networks to improve security.

REFERENCES

[1] Perkins CE, Royer EM, Das SR. Ad hoc on-demand distance vector (AODV) routing, IETF internet draft. MANET Working Group; Jan 2004.

[2] Johnson DB, Maltz DA, Hu YC. The dynamic source routing protocol for mobile ad-hoc network (DSR), IETF internet draft (work in progress); July 2004.

[3] The Network Simulator – ns-2, http://www.isi.edu/nsnam/ns/.

[4] Maulik and Chaki. A Study on Wormhole Attacks in MANET. 2011 In the proceedings of the IEEE conference on military communications; 2006.

[5] Saurabh Gupta, Subrat Kar and S Dharmaraja. WHOP: WormholeAttack Detection Protocol using Hound Packet. 2011.

[6] T. Sakthivel and R.M. Chandrasekaran. "Detection and Prevention wormhole Attack in MANET using Path Tracing Approach".2012

[7] S. Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF RFC 2501, January 1999.

[8] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, Jan. 2002.

[9] Y. Hu, D. Johnson, and A. Perrig. Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. In IEEE Workshop on Mobile Computing Systems and Applications, June 2002.

[10] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. In IEEE Security and Privacy, Special issue on Making Wireless Work, May 2004.

[11] Wassim Znaidi, Marine Minier and Jean-Philippe Babau. Detecting Wormhole Attacks in Wireless networks Using Local Neighborhood Information. 2008.

[12] Shang-Ming Jen, Chi-Sung Laih and Wen-Chung Kuo. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET.2009.

[13] Lee, and Heejo Lee. Transmission time-based mechanism to detect wormhole attacks. In the proceedings of the IEEE Asia- Pacific service computing conference; 2007. pp. 172–8

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

[15] Xia Wang and Johnny 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 (COMPSAC); 2007.

[16] Hon Sun Chiu, King-Shan Lui. DelPHI: wormhole detection mechanism for ad hoc wireless networks. In the proceedings of the 1st international symposium on wireless pervasive computing; 2006.