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. 3, Issue 3, March 2015

Performance Evaluation of Advanced OLSR against Black Hole Attack and Wormhole Attack in MANET

K.Sivagurunathan[1], K.Manojkumar[2], D.Sounder[3], Midhun Sebastian[4]

Assistant Professor, Dept. of ECE, Dr.S.J.S Paul Memorial College of Engineering and Technology, Puducherry, India[1].

B.Tech, Dept. of ECE, Dr.S.J.S Paul Memorial College of Engineering and Technology, Puducherry, India[2,3,4].

ABSTRACT: Mobile Ad hoc Network (MANET) is an autonomous system which consists of a collection of self-configurable mobile node connected through wireless links. This kind of network is also known as infrastructure less networks. These networks have no centralized administration. Security is a major issue in MANET. Black hole attack and wormhole attack are the most severe attacks those occur in MANET. It is difficult to detect those attacks. In this paper, we analyze the nature of black hole attack and wormhole attack in mobile ad hoc network. Analyzing the attacks, we propose a mechanism called Advanced OLSR (AOLSR) protocol is acts as the proactive routing protocol as its nature. The experiment results show that our protocol achieve routing security with 22% increase in packet delivery ratio, 27% reduction in packet loss rate, 42% increase in throughput and 69% reduction in packet end to end delay than standard OLSR.

KEYWORDS: Mobile Ad Hoc Network, Black Hole Attack, Wormhole Attack, Optimized link State Routing (OLSR), MPR.

I. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is an autonomous network system of routers and hosts connected by wireless links. They can be setup anywhere without any need for external infrastructure like wires or base stations. The routers are free to move randomly and organize themselves. The network can be set up anywhere without any geographical restrictions. Mobile Ad-hoc network is suitable for areas where fixed infrastructure is not possible. Because this network have no fixed infrastructure or centralized administration. Hence they are also known as infrastructure less network. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, and no clear defense mechanism. The nodes communicate with each other on the basis of mutual trust. This characteristic makes it easier for the attacker to go inside the network and get access to the ongoing communication.

Routing protocols in MANET can be classified into two categories: reactive protocol and proactive protocol. In proactive routing protocols, all nodes need to maintain a consistent view of the network topology. When a network topology changes, respective updates must be propagated throughout the network to notify the change. In reactive routing protocols for mobile ad-hoc networks, which are also called “on-demand” routing protocols, routing paths are searched for, when needed. Nowadays, the most promising protocol in the field of MANET tends to be the Optimized Link State Routing (OLSR) protocol. Because the overall results show that the OLSR protocol provides connectivity and routing with a good performance in terms of bandwidth and traffic overhead. It has valuable features such as no route discovery delay and ease of integration into existing systems, which makes it well-suited for time critical and emergency rescue applications. But OLSR does not incorporate any security issues. OLSR is vulnerable to various kinds of attacks.

In this Paper, we analyze the two spreading attacks called Black Hole attack and Wormhole attack. After monitoring the activity of network, Black Hole attack and Wormhole attack can be easily launched in OLSR. We propose a solution called Advanced OLSR (AOLSR) for detecting and preventing the Black Hole attack and Wormhole attack.

II. RELATED WORK

Most of the previous works on security attacks have mainly addressed in reactive routing protocol such as AODV and DSR protocol. In [5], a cryptographic based approach has been proposed for protecting the network. This technique classifies the OLSR nodes into either trusted or un-trusted nodes with an assumption that trusted nodes are not compromised. The signature is used to authenticate messages from trusted nodes, and timestamps are used to prevent replay attacks. The main drawback of this approach is that it does not deal with defense against compromised trusted nodes.

. In [11] & [12] Hu et al & Kurosawa et al introduced a rushing attack which results in DOS attack on MANET and black hole attack on AODV protocol

[7], [8], [5], [13] A number of articles has analyzed security properties and vulnerabilities of routing protocols in MANETs. These papers identify resources of MANET routing protocols that are potentially vulnerable to attacks, and propose several attacks against these resources, as well as counter-measures against such attacks. [6] Present a more detailed security analysis of the OLSR routing protocol and analyze the Dos attack and present a simple technique to detect and avoid the attack. [9] Proposed an intrusion detection technique that observes TC message from its MPR node regularly to detect Malicious MPR nodes.

III. EXISTING SYSTEM

The Optimized Link State Routing (OLSR) protocol is the proactive routing protocol. It is also called table driven protocol. These protocols maintain the updated topology of the network. Every node in the network knows about the other node. All the routing information is usually kept in routing tables. Whenever there is a change takes place in the network topology, these tables are updated according to the change. The nodes exchange topology information with each other and they can have route information any time when they needed. OLSR is one of the best protocol which suitable for large and dense network.

The basic concept of MPR is to reduce the number of transmissions. In OLSR, two types of routing message are used. They are HELLO message and Topology Control (TC) message. Each node broadcast HELLO message periodically to all the neighbor nodes. HELLO message contains its own address and list of addresses of its neighbors. It is used for neighbor discovery and MPR selection. Every MPR node floods TC message periodically using multipoint relaying mechanism. TC message contains the list of addresses of senders MPR selector. A TC message is used for the route calculation.

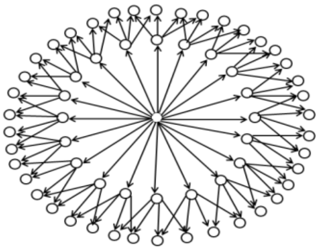

Fig. 1 Normal Flooding

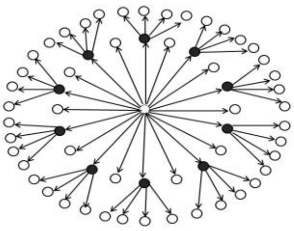

Fig. 2 MPR Flooding

To perform the task of routing OLSR protocol carries out different functions follows:

A. Neighbor Discovery

In neighbor discovery process, each node senses the nearest neighboring node which are in direct link range of itself and detects with which of these it can establish bi-directional link [2].Each node periodically sends its HELLO messages, containing the information about its neighbors and the status of their link. These are received by all the one-hop neighbors.

B. Multipoint relay flooding

In multipoint relay (MPR) flooding process, each node selects its own set of multipoint relay independently [1]. Each node selects a set of its neighboring nodes as MPR nodes and selecting nodes must be with symmetric links. Only MPR nodes are responsible for broadcasting as well as forwarding topology information into the network.MPR set is calculated in a manner to contain a subset of 1-hop neighbor which covers all the 2-hop neighbors. Node which expresses their willingness by HELLO messages is taken into consideration for MPR calculation. Each node selects its MPR set from among its 1-hop neighbor. Each node periodically updates information about its MPR set from HELLO messages. Each MPR node must forward the data and routing message receiving from any of its MPR selectors.

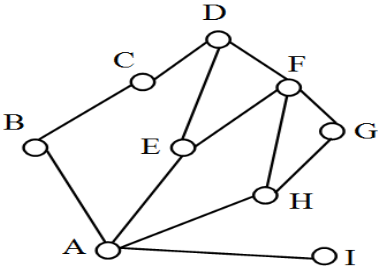

Fig. 3 MPR selection

Node	1-hop neighbors	2-hop neighbors	MPRs
A	B,E,H,I	C,D,F,G	E

Table.1 MPR selection

From the perspective of node A, both E and H cover all of node A’s 2-hop neighbors. However, E is selected as B’s MPR node as shown in Table 1.

C. Link state Broadcasting

In link state broadcasting, nodes are determines the link state information to broadcast through the network [1]. The link state broadcasts are carried in Topology Control (TC) messages, broadcast through the network using the MPR flooding process. The link advertised in TC message are bi-directional path because a node selected the MPRs only from among its bi-directional neighbors. TC messages are sent periodically for routing paths calculation.

IV. BLACK HOLE ATTACK

Black hole attack is kind of DOS attack which is launched by malicious node against [3]. An attacker sends fake routing information to the neighbor node that it is having the shortest path between source and destination. So, the other nodes send information through the malicious nodes and the attacker will capture all the data. An attacker drops the data packets or modifies the data packets coming from the source node and sends it to the destination. Only with the help of HELLO & TC message the information is exchanged between the nodes in OLSR protocol [3]. The node acting as a black hole sends a fake HELLO to the nodes and shows that it is having the multiple neighbor nodes for retransmitting the data. In these HELLO messages an attacker node claims to have links to more neighbors than it actually has. So the source node selects that node as a Multipoint Relay (MPR) node. When black hole node is selected as a MPR node then all the data which is sent through the neighbor nodes of the MPR will pass through them and the entire data packet will be captured.

10.15680/ijircce.2015.0303063

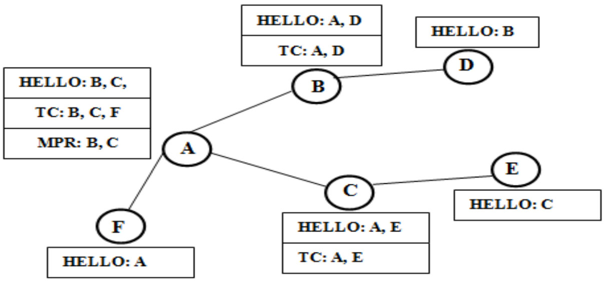

Fig. 4(a) OLSR without Black hole

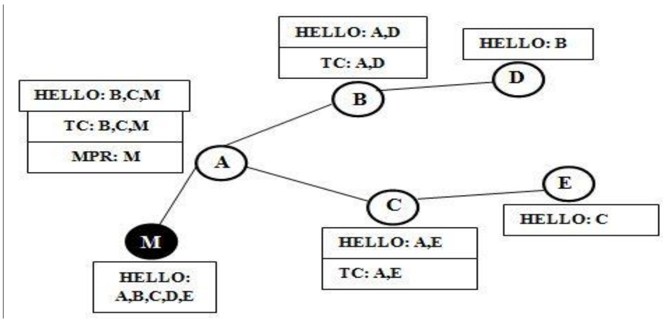

Fig. 4(b) OLSR with Black hole attack

The more neighbors the attacking node claims to have, the larger the potential impact of the attack. Due to the fake messages of the attacker, in its neighborhood falsified TC messages with too few entries or no TC messages due to an empty MPR selector set are propagated. Thus, the attacker is able to capture the routes. This time node F has been taken over and acts as black hole node. This leads to some changes in the network. In this figure, the lines just show Node A's view of the network. Change Nr.1 is the fake Hello message of the black hole node. It contains nodes A, B, C, D and E. This leads to Node A selecting only the black hole node as MPR node. Since Node A does not select nodes B, C as MPR nodes, these send TC messages not containing Node A. Additionally, instead of sending data packets to nodes D, E through nodes B respectively C, node A tries to send these data packets through the black hole node. Therefore, the black hole has gained control over the connections from A to D and E.

V. WORMHOLE ATTACK

A wormhole attack is a severe attack on MANET. In this attack two attackers connected by a high speed off-channel link called the wormhole link [4]. The wormhole link can be established by using a network cable which may be any form of wired link technology or a wireless transmission in a different band. Once the wormhole link is established, it record the wireless data they overhear, forward it to each other and also replays the packets through the wormhole link at the other end of the network. Wormhole attackers can make far apart nodes believe they are immediate neighbors and force all communications between wormhole nodes to go though them. A wormhole attack is equally dangerous for both table driven protocol and reactive protocols.

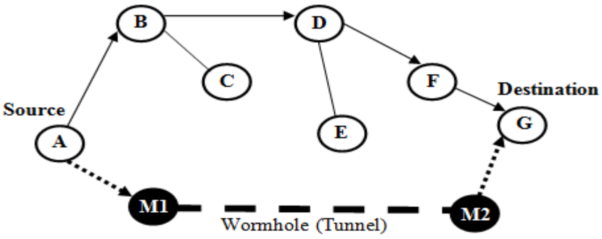

Fig. 5 OLSR with Wormhole attack

In Figure 5, when node A sends a HELLO message, intruder M1 forwards it to the other end of the network, and node H hears this HELLO message. Since G can hear a HELLO message from A, it assumes itself and node A to be direct neighbors. Thus, if G wants to forward anything to A, it may do so unknowingly through the wormhole link. This effectively allows the wormhole attackers full control of the communication link.

VI. PROPOSEDWORK

The proposed solution called AOLSR is an enhancement of the basic standard OLSR routing protocol, which will be able to detect the presence of malicious nodes in the network. In this solution, the AOLSR protocol senses the nodes in the network by broadcasting periodically regarding the behavior of the nodes. It monitors the number of broadcasts, inactive time period of nodes, data handover and log. If any suspicious activity is done by the malicious nodes during the transmission of data, those malicious nodes will be detected and alert will be sent by broadcasting to source and destination. After alerting the source and destination it limits the input with respect to routing table. It reduces the number of routing table entry and the transmitting node shrinks the number of inbounds to only the active link.

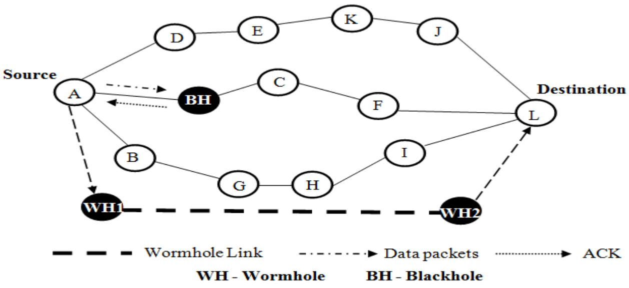

Fig. 6(a) MANET with Black hole attack & Wormhole attack

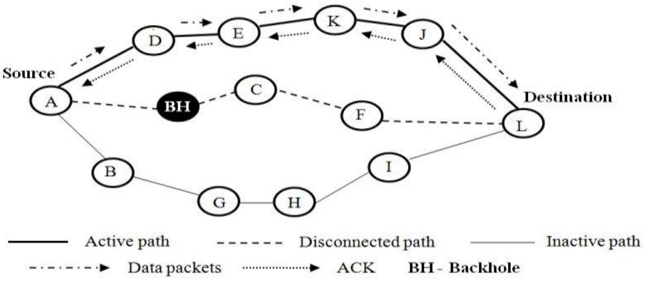

Fig. 6(b) MANET after the attackers are removed

In the routing discovery, black hole node (BH) sends a fake HELLO message to the source node A and shows that it is having the multiple neighbor nodes for retransmitting the data. In these HELLO messages an attacker node claims to have links to more neighbors than it actually has. So the source node A selects BH as a Multipoint Relay node (MPR). After node BH is selected as a MPR node, node A transmits the data to destination node L through BH. BH captures all the received packets and drops the data packets without forwarding to destination node L. meanwhile, wormhole attacker WH1 and WH2 overhears the data from A, modifies and forward to the L as shown in fig. 6(a). After monitoring the network, our proposed technique detects the malicious nodes BH and WH1 & WH2 (Black hole node & Wormhole node) and disconnects the attacked path A-C-F-BH-L between source node A and destination node L. Then source A selects the second shortest path A-D-E-K-J-Land transmits the data. It maintains only transmitting path as active path and other connected path as inactive path as shown in fig. 6(b).

VII. SIMULATION RESULTS

In this section, we present the performance evaluation on our technique using extensive simulations conducted with the network simulator 2 (Ns allinone-2.35). We generated random topologies with a maximum of 50 nodes over a rectangular field. The terrain dimension is fixed as 200 × 100 m. The maximum transmission range of each node is 550 m. The duration of the simulation is 15 s. Random waypoint model is used as the mobility model for each node. Node speed is varied from 2 m/s to 25 m/s. The node pause time is varied from 0 second to 300 seconds. The default settings as in the specifications of OLSR [2] were used for HELLO and TC messages. In our simulation, we used 35% of malicious nodes out of the normal nodes to launch the attack. The traffic load is simulated using 15 user datagram protocol-case based reasoning (UDP-CBR) connections generating traffic of 5 kb UDP packets (data payload 512 Bytes) with an inter departure time of 1 s. The average value is taken for the result.

A. Performance Evaluation

We used the following metrics to evaluate the performance of our proposed solution AOLSR against OLSR under attacks and the results obtained are shown in Figs. 7–9

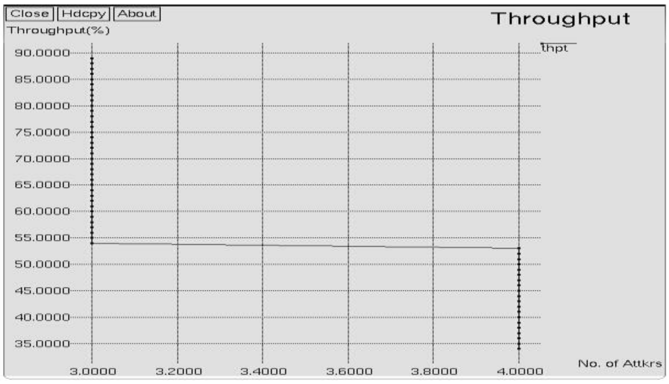

Fig.7 (a).Throughput of OLSR

Fig. 7(a) shows the throughput in existing approach where X-axis represents Number of attackers (%) and Y-axis represents Throughput (%). Gradually the throughput is decreased from 90 % to 55% in the presence of 2 attackers and again straightly decreased from 53% to 35% approximately. Finally after analyzing the above graph, the throughput achieved by OLSR in existing approach is approximately 55% as shown in fig. 7(a).

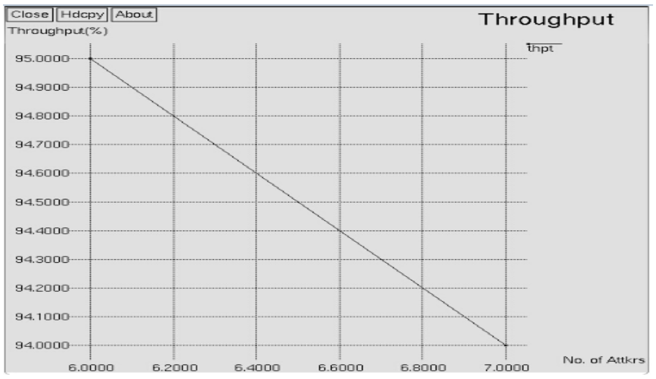

Fig. 7(b).Throughput of AOLSR

Fig. 7(b) shows the throughput in proposed approach where X-axis represents Number of attackers (%) and Y-axis represents Throughput (%). The throughput is 95% in the presence of 6 attackers and slowly decreased to 94% in presence of 7 attackers. Clearly throughput has been increased to the maximum. The throughput achieved by our proposed solution AOLSR in proposed approach is approximately 97%. Compared to existing approach, the proposed approach AOLSR increased the throughput by 42% as shown in fig. 7(a).

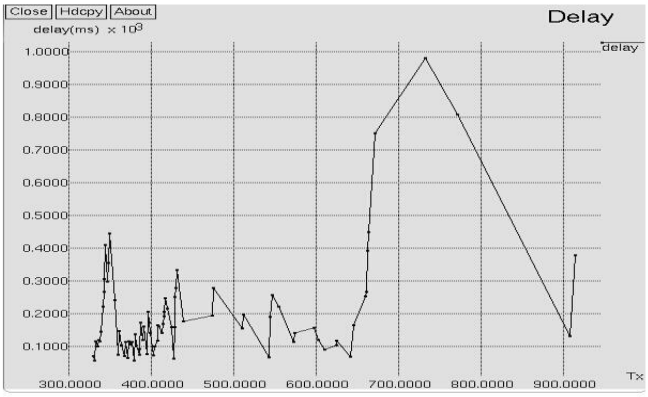

Fig. 8(a) Delay for OLSR

Fig. 8(a) shows the packet end to end delay for OLSR where X-axis represents Number of transmission and Y-axis represents Delay (ms). Packet end to end delay is below 500 ms between 300 and 650 transmission. The peak value is attained up to 1000 ms at 700 transmissions. After analyzing the above graph, the packet end to end delay in existing approach OLSR is approximately 78%.

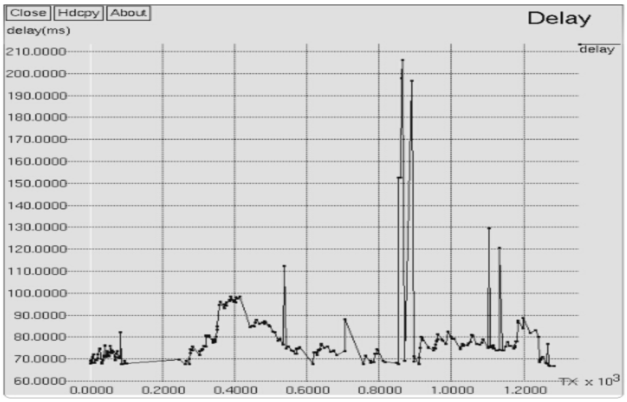

Fig. 8(b).Delay for AOLSR

Fig. 8(b) shows the packet end to end delay in AOLSR where X-axis represents Number of transmission and Y-axis represents Delay (ms). Packet end to end delay is below 110 ms until 800 transmissions and it attained is peak value as 205 ms approximately. The packet end to end delay in our proposed approach AOLSR is approximately 8%. Compared to existing approach, the proposed approach AOLSR reduced the packet end to end delay by approximately 69%.

10.15680/ijircce.2015.0303063

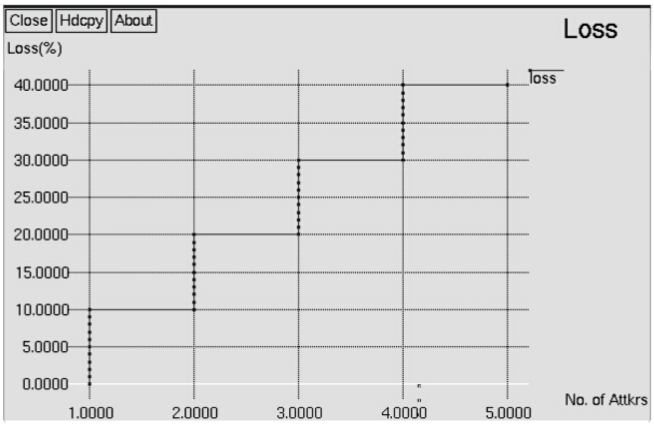

Fig. 9(a) Packet loss rate of OLSR

Fig. 9(a) shows the packets loss in existing approach OLSR where X-axis represents Number of attackers (%) and Y-axis represents Loss (%). In presence of 1 attacker, the packet loss is gradually increased from 0% to 10%. Similarly, the loss is increased with respect to increase in attacker as shown in fig. 9(a). The packet loss increased to 50% in presence of 6 attackers. The packet loss rate of OLSR in existing approach under the attacks is approximately 50%.

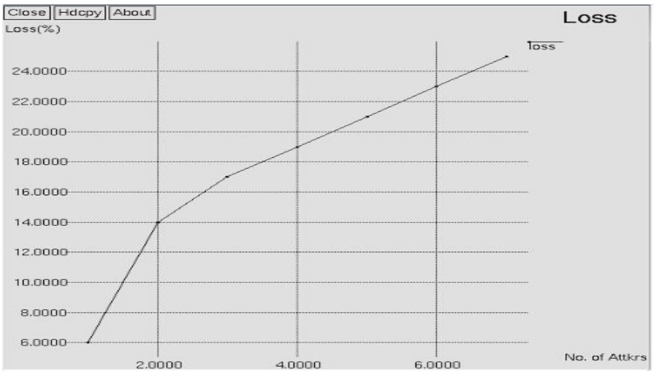

Fig.9 (b) Packet loss rate of AOLSR

Fig. 9(b) shows the packets loss in our proposed approach AOLSR where X-axis represents Number of attackers (%) and Y-axis represents Loss (%). In presence of 2 attackers, the packet loss is 14% and at 6 attackers packet loss is increased to 23%. The packet loss rate of AOLSR under the attacks was approximately 23%. Compared to the existing approach, our proposed approach AOLSR reduced the packet loss rate by 27%.

VIII. CONCLUSION AND FUTURE WORK

This paper proposes a solution for Black Hole attack and Wormhole attack launched against OLSR routing protocol. Here, we have discussed through an attack model, that it is easy for a malicious node to launch the Black Hole attack and Wormhole attack. The proposed solution called AOLSR, which is based on OLSR, uses intrusion detection system to detect the malicious nodes in the network. The experiment results show that the percentage of packets received through our proposed work is better than OLSR in presence of multiple attacker nodes. The simulation is done using Network Simulator 2 (Ns allinone-2.35) and our scheme is found to achieve routing security with 22% increase in packet delivery ratio, 27% reduction in packet loss rate, 42% increase in throughput and 69% reduction in packet end to end delay than OLSR. Compared to other related works, the proposed protocol has more merits.

IX. ACKNOWLEDGMENTS

We thank our HOD **Dr.T.Thirumurugan**, Ph.D. (Department of Electronics and Communication Engineering) to help us for creating this paper with his sincere guidance and Technical Expertise in the field of communication. The help of our guide **Mr.K.Sivagurunathan**, M.Tech, Department of ECE, Dr, SJS Paul College of Engineering and Technology is really immense and once again I thank her for her great motivation. I thank Dr. SJS Paul College of Engineering and Technology to provide me such a standard educational environment so that I am able to understand the minute concepts in the field of Engineering and Technology.

REFERENCES

[1]. Mohanapriya Marimuthu and Ilango Krishnamurthi, “Enhanced OLSR for Defense against DOS Attack in Ad-Hoc Networks”, Journal of communications and networks, Vol. 15, no. 1, pp.31-37, Feb.2013.

[2].P. Jacquet, P. Muhlethalor, T. Clausen, A. Laouiti, A. Qayyam, L. Viennot, “Optimised Link State Routing Protocol for Ad Hoc Network”. Hipercom
project, INRIA Rocquencourt, BP105, 78153 Le chesnaycedex, France.

[3].Ankur Thakur and Anuj Gupta, “Black Hole Problem with OLSR Protocol in MANETs”, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 4. Pp, 1-4, Sept 2014.

[4].Ajay PrakashRai, VineetSrivastava and Rinkoo Bhatia, “Wormhole Attack Detection in Mobile Ad Hoc Networks”, International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, pp. 174-179, August 2012

[5].D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, “Securing the OLSR protocol,” Proc. Med-Hoc-Net, June 25-27, 2003.

[6] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, “An advanced signature system for OLSR,” Proc. ACM SASN, 2004.

[7] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, “Attacks against OLSR: Distributed key management for security”, Proc. OLSR Interop and Workshop, 2005.

[8] C. Adjih, T. Clausen, A. Laouiti, P. Muhlethaler, and D. Raffo, “Securing the OLSR routing protocol with or without compromised nodes in the network”, HIPERCOM Project, INRIA Rocquencourt, Tech. Rep. INRIA RR-5494, Feb. 2005.

[9] D. Dhillon, T. S. Randhawa, M. Wang, and L. Lamont, “Implementing a fully distributed certificate autorithy in an OLSR MANET,” Proc. IEEE WCNC, Vol.2, pp. 682 – 688, March 2004.

[10]. B. Kannhavong., “Analysis of the Node Isolation Attack against OLSR- Based Mobile Ad Hoc Network,” 7th International Symposium on Computer Networks, pp. 30 – 35, 2006.

[11]. Hu Y-C, Perrig A, Johnson D. “Rushing attacks and defense in wireless ad hoc network routing protocols”, ACM Workshop on Wireless Security (WiSe 2003), San Diego, California, U.S.A., 19 Sept 2003.

[12]. Kurosawa S, Nakayama H, Kato N, Nemoto Y, Jamalipour A. “Detecting black hole attack on AODV-based mobile ad hoc networks by dynamic learning method”, International Journal of Network Security 2007, Vol.5, No.3, pp. 338–346, Nov 2007.

[13]. T. Clausen, U.Herberg, “Security Issues in the Optimized Link State Routing Protocol Version 2 (OLSRv2)”, International Journal of Network Security and its Applications, Volume 2, No. 2, pp. 162-181, April 2010.

BIOGRAPHY

Mr.K.Sivagurunathan is working as an Assistant Professor (Department of ECE) in Dr. S.J.S PAUL MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY. He has done his UG degree in Electronics & Communication Engineering and PG degree in communication system. He has two years working experience as design engineer. He is interested in Ad-Hoc networks, Electro Magnetic wave theory, Digital circuits, wave guides and antennas, signals and system.

Mr.K.Manojkumar is a student who is pursuing B.Tech (Electronics and Communication Engineering) in Dr. S.J.S PAUL MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY. He is interested in Ad-Hoc networks, Electro Magnetic wave theory, wave guides and antennas and Data structure.

Mr.D.Sounder is a student who is pursuing B.Tech (Electronics and Communication Engineering) in Dr. S.J.S PAUL MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY. He is interested in Digital circuits, Digital signal processing, Electronic circuits, Ad-Hoc networks, Electro Magnetic wave theory, wave guides and antennas, signals and system, VLSI design and digital electronics.

Mr.Midhun Sebastian is a student who is pursuing B.Tech (Electronics and Communication Engineering) in Dr. S.J.S PAUL MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY. He is interested in Ad-Hoc networks, VLSI design, Digital signal processing, and digital electronics.