ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 10, October 2016

ANALYSING THE IMPACT OF SECURITY ATTACKS ON REACTIVE AND PROACTIVE ROUTING PROTOCOLS IN MANETS

Eshani[1] and Savina Bansal[2]
[1]Research scholar and [2]Professor
Department of Electronics & Communication Engineering,
Giani Zail Singh PTU Campus, Bathinda (Punjab), India, 151001

ABSTRACT **- Mobile ad-hoc networks are dynamic & decentralized wireless systems in which nodes (mobiles, laptops, and computers and so on) have self-configuration ability. Nodes can act as hosts/routers or both at the same time. When any node wants to communicate with any another node in the network, it sends packets to that using various routing protocols but the routing protocols in MANETs are not secure and hence ad-hoc networks are left unprotected from various malicious attacks i.e. there are various security issues in MANETs due to lack of central monitoring and management. The network consists of 20, 60 and 100 nodes (mobile nodes) which make usage of random model in flat area of 100m×100m. The main objective of this research is to analyze the impact of Sybil attack on proactive (OLSR) and reactive (AODV) routing protocols in terms of throughput, delay & load which are chosen as the performance metrics.**

Index Terms **- MANETs, OLSR, AODV, Black hole attack, Wormhole attack, Sybil attack.**

I. INTRODUCTION

Wireless networks are the networks which connect various nodes with one another for communication by transmitting and receiving data. Various types of wireless networks are wireless sensor networks, mobile ad-hoc networks, vehicular ad-hoc networks etc. In wireless sensor networks, various nodes processes, gathers the information obtained from sensor node for communicating it with other connected nodes [1].

MANETs play an important role in today's world. They are collection of nodes which are free to move anywhere during communication resulting in dynamic topology [2]. Nodes which are in range of each other can communicate with each other directly whereas other nodes communicate via intermediate nodes. Thus nodes in MANETs can act as hosts as well as routers. These networks find wide application in military, vehicular ad-hoc networks, civilian environment, disaster area etc. Out of these applications, military applications require a high level of security. Security is the major concern for basic functionality of MANETs. Due to lack of any central authority, all of the security issues are handled by nodes themselves to resist different type of security attacks. Our aim is to understand the behavior of attacker nodes toward OLSR, AODV and to analyze the impact of Sybil attack towards throughput in MANETs.

Routing is a method which involves the sending and receiving of information among various nodes in the network. Routing protocols can be classified in many ways, but mainly these protocols are categorized on the basis of structure of the network and routing strategy. Various routing protocols can be classified as proactive routing protocols, reactive routing protocols and hybrid routing protocols. Proactive routing protocols are table driven protocols in which every node keeps a separate routing table and whenever any node wants to transmit packets to another node, it knows the router already. Reactive routing protocols are is the protocols in which the updating of routing table is done on-demand basis and when any node wants to transmit any packet, it has to establish path currently. Hybrid routing protocols are combination of proactive and

reactive routing protocols. Some routing protocols are discussed next.

A. AODV

AODV is a reactive routing protocol. In ad-hoc on demand distance vector routing (AODV) protocol, whenever any node wants to send any data to another node, it has to find the route to the destination node currently on demand [2]. For discovery and maintenance off routes, three types of control messages used in AODV are described as:

Route Request Message (RREQ)

Any source node in the network that wishes to send data to another node sends RREQ message. This message is transmitted by source node to its neighboring nodes, which then again retransmit this message to its nearby nodes. This process of retransmission is continued until a node is found that has path to destination.

Route Reply Message (RREP)

A node that has any intermediate node which has a path to the destination node sends the route reply message back to the source node.

Route Error Message (RERR)

The nodes in the network periodically checks their link status to neighboring nodes and whenever any node finds a crack in an active path, RERR message is sent by node to inform other nodes about the link failure.

Route Discovery Mechanism in AODV

When any node wishes to start the communication with any other node in the network, it creates an RREQ message and floods it to other nodes. This message is forwarded by sender node to its neighboring nodes and neighboring nodes again retransmits it to its neighbors. This process of retransmission continues until a node is found that has path to destination. When the destination is found or an intermediate node is found which has path to destination, it sends the RREP message to the sender node. When the sender node receives the RREP, a path is formed between the sender node and destination node. Once the path is formed, the sender and destination nodes can transmit/receive information to one another.

Route Maintenance in AODV

When any crack is found in link between source and destination, the RERR message is transmitted back to source node for informing the source node about a path error. When the source node will receive this message then either it will not send any data more on this path or it will request for a new path for transmission of data by broadcasting a new RREQ message.

B. OLSR

An OLSR is also a proactive routing protocol, known as link state routing protocol. The link-state routing algorithms help in selecting the best route by calculating the various parameters like delay, bandwidth and so on [9]. These Link-state paths are more reliable, stable and accurate for computation of the best route. Each node in the network broadcasts the periodic message for updating the topological information. In this protocol, the multipoint relays are used in the network to support efficient flooding of the control message to the nodes. Here in the network, the multipoint relays do the roué calculations to establish the path from a source to destination. It is intelligent protocol and it can sense paths before transmission. It has various control intervals to sense various parameters of the network like 'hello' interval, 'take-care' interval etc.

For the proper functionality of any network in MANETs, security is the most vital concern. Ad-hoc networks mostly suffer from various security attacks due to its characteristics like absence of centralized control, absence of any defense mechanisms, and random change in topology of network and so on.

Types of Security Attacks

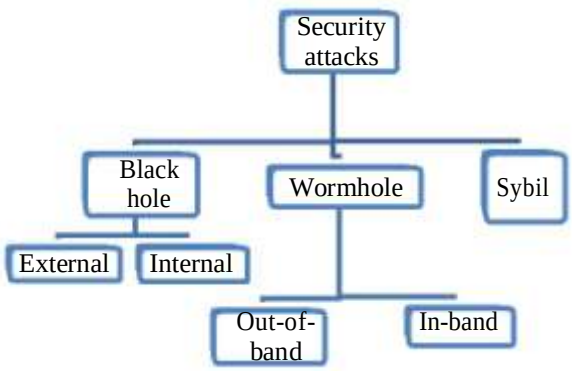


Fig. 1 Security attacks in MANETs

Black hole Security Attack

In black hole attack, an attacker node claims that it has the shortest route to the destination [3]. Hence the attacker will send response back to the sender node before any legal node. Hence the sender node will assume that it is the shortest path and it will discard every other route to destination node. In this way all the packets are sent by the sender to the malicious node, then either these packets are dropped by the malicious node or it will send these packets to any other unknown address.

In fig. 2, let node "A" wants to transmit packets to some destination node "E" and starts the route discovery. Hence if there is another node "C" which is malicious node and when it receives the RREQ packets then this node will claim that it has the shortest path destination. Thus it will send response (RREP packet) back to the node "A" before any other legal node. In this way node "A" will assume that this is the shortest path and hence route discovery is completed.

Now node "A" will discard all other different RREP packets and will start sending packets to node "C". In this fashion all information packet will be consumed or lost.

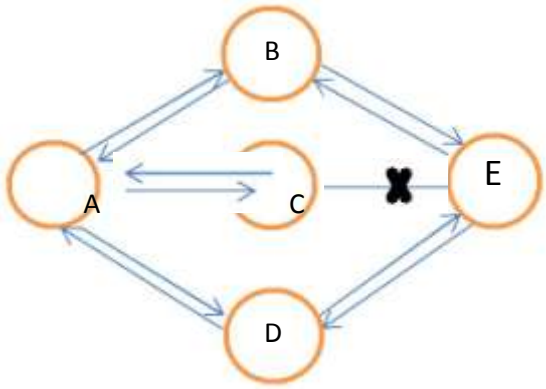


Fig. 2 Black Hole Attack

Wormhole Attack

In this attack, an attacker captures information packets at some point in the ad-hoc network and then tunnels those packets to a remote location, where the attacker replays those packets without any modification [4]. In wormhole attack, the two attacker nodes are present to launch the attack, which behaves as legal nodes to the destination nodes and various other nodes in mobile ad-hoc network. To launch this type of attack, one of the attacker nodes is near the sender node and the other attacker node is near the destination node. The malicious node near the sender will receive all the information packets from the sender node and then it will tunnel those packets to the other malicious node near the destination node. Here, the malicious nodes are linked with each other via medium that is not present to other normal nodes [5].

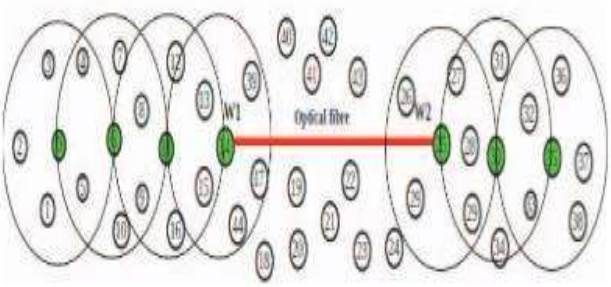


Fig. 3 Wormhole attack

Here in fig. 3, if the sender node-0 wants to transmit packets to destination node-35, transmission will take place through the wormhole link. The two malicious nodes behaves in such manner so that, they seem to be neighboring nodes to the other nodes in the network. The wormhole link advertises for having the shortest route to the destination node and attracts whole the information packets towards it and thus take the control of whole traffic that is flowing through the ad-hoc network. After taking the control, the malicious nodes can modify the information packets, drop the information packets to destination node or they can selectively drop those information packets.

Sybil Attack

In this attack a node in the wireless network can claim multiple identities. Here, an attacker node does not behave like just a node as in various other attacks like black hole attack, wormhole attack etc. Rather the attacker node behaves as multiple nodes (two or more nodes). Hence the Sybil nodes are created by series of fake identities in an ad-hoc network and thus the

malicious node attempts to behave as various fake identities (nodes) instead of one [2].

The rest paper is organized as follows. The section II discusses the literature survey, section III explains the research methods and various assumptions of simulation set up. Section IV discusses the analysis and section V presents the discussion and conclusion of the work.

II. LITERATURE SURVEY

Various issues related to the challenges of mobile ad-hoc networks have been solved by many researchers.

Dema Aldhobaiban et al. [1] proposed a new method and formed a mechanism for prevention of wormhole attacks by using an algorithm for the managing a number of nodes in the network using node ID. Zolidah Kasiran et al. [2] analyzed the performance of AODV in terms of throughput under Sybil and wormhole attack. They found that in case of presence of these attacks, the throughput was lesser than that in case of absence of these attacks. Also they found that the Sybil attack affected the performance of MANET more badly rather than wormhole attack. Kriti Patidar et al. [3] have suggested protocols that can protect MANETs from wormhole attacks, black hole attacks and also they can improve the network stability. Anal Patel et al. [4] surveyed several techniques to detect the presence of wormhole attack in the network and they proposed an approach for detection and prevention of wormhole attack.

Anju et al. [5] proposed a technique for detection and prevention of wormhole attack in two phases by using an AODV protocol in ad-hoc networks. Vinesh Teotia et al. [6] suggested a new mechanism for wormhole detection in MANETs consisting of COTA mechanism with its implementation on location aided routing protocol (LAR1), which is known as COTA-LAR1 scheme. Juhi Biswas et al. [7] suggested an algorithm for detection of wormholes. Shiyu Ji et al. [8] proposed an algorithm known as DAWN (Defending against wormhole attack in wireless coding systems) for detection of wormhole attack in wireless network coding systems. Chaitali Biswas Dutta et al. [9] analyzed the impact of wormhole attack on a proactive routing protocol OLSR. Guoxing Luo et al. [10] presented a system, Pworm. It is system of passive wormhole detection and localization which is based upon the fact that wormholes will attract huge amount of network traffic through it. Phillip Lee et al. [11] presented a framework (passivity-based control-theoretic framework) for mitigation of wormhole attack on NCS (networked control system). Kuan Zhang et al. [12] surveyed Sybil attacks and various defense schemes in Internet of Things (IoT) in this paper. Wei Dong et al. [13] proposed an RTSP protocol (robust and secure time-synchronization protocol) for Sybil defense in WSNs. Ruixia Liu et al. [14] proposed a new technique known as RSSI (received signal strength indicator) based technique to recognize Sybil nodes even when they carry out their power control. Xia Feng et al. [15] suggested a system known as EBRS (event based reputation system) in this paper. In communication process, EBRS can recognize Sybil attack with stolen and fabricated identities. The results of simulation showed that this technique is able to detect and defend Sybil attacks with good performances.

III. METHODOLOGIES

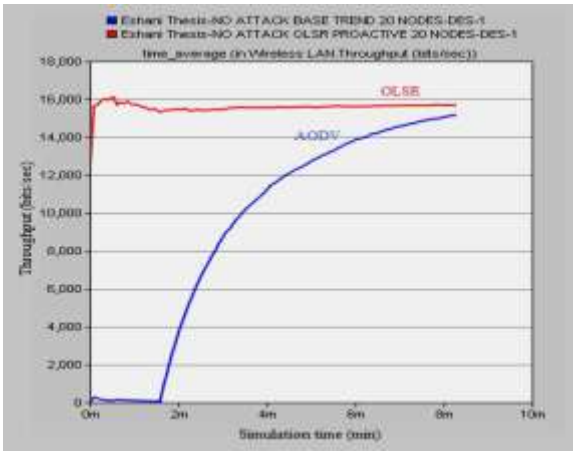
The simulation model is created by various node set ups that consist of variable number of nodes (20, 60 and 100). The different numbers of nodes are selected to analyze the performance of network with increase in number of nodes to analyze the impact of scalability. This research work focuses on evaluating the performance of proactive routing protocol i.e. Optimized link state routing (OLSR) and reactive routing protocol i.e. Ad-hoc On-demand Distance Vector (AODV) against Sybil attack. Twelve scenarios are created with different number of nodes under no attack and Sybil attack for AODV and OLSR routing protocols. We took mobile nodes and all the nodes are configured by making use of predefined parameters of OPNET or done manually.

IV. SIMULATION RESULTS

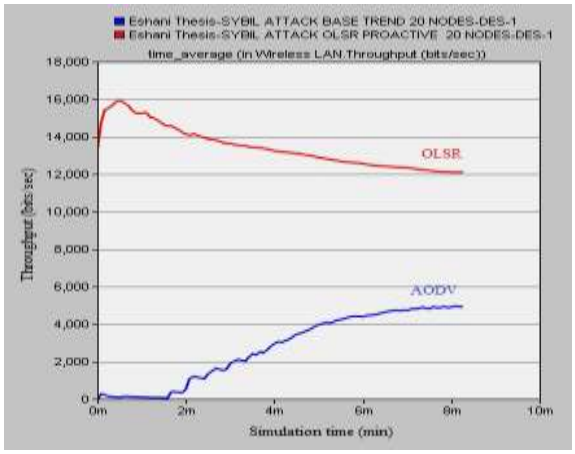
The performance of various network parameters like throughput, delay and load of OLSR and AODV routing protocols in the absence and presence of Sybil attack is presented in this

section. Throughput represents the total number of bits (in bps) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network. Delay represents the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. Load represents the total load (in bits/sec) submitted to wireless LAN layers by higher layers in all WLAN nodes of the network.

From fig. 4(a) and fig. 4(b), it can be observed that in absence of attack OLSR and AODV have comparable throughputs. However, in the presence of attack there is 25% decrease in throughput of OLSR and 67% decrease in throughput in AODV. This result is in consonance of those available in literature [2].



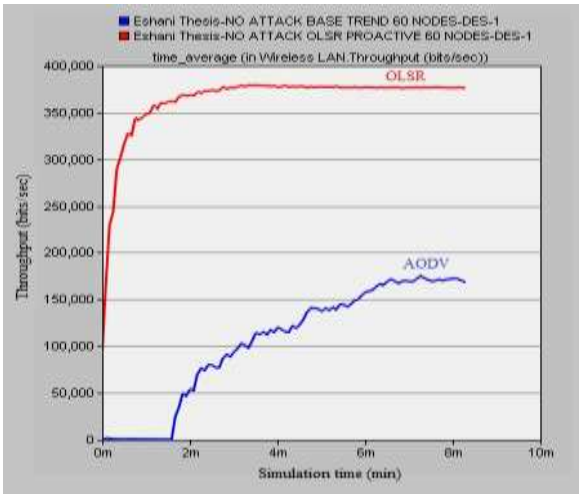
(a)



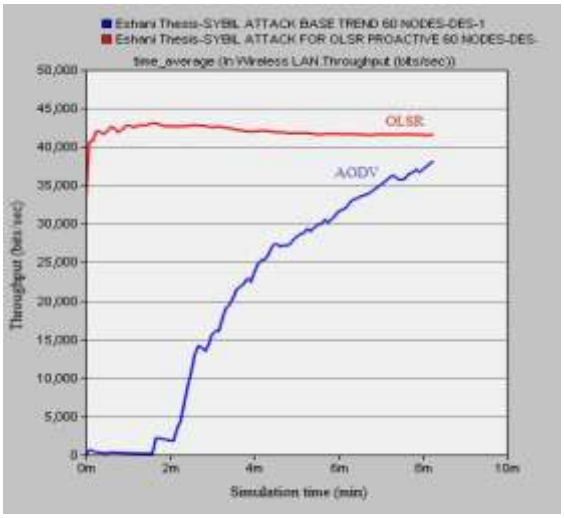
(b)

Fig. 4 (a) Throughput in absence of attack (#nodes = 20) (b) Throughput in presence of attack (#nodes = 20)

In fig. 5(a) and fig. 5(b), it can be observed that for network containing 60 nodes, the OLSR has higher throughput than AODV in absence of attack but in the presence of attack, decrease in throughput of OLSR is 89% and that in AODV is 78 %.



(a)

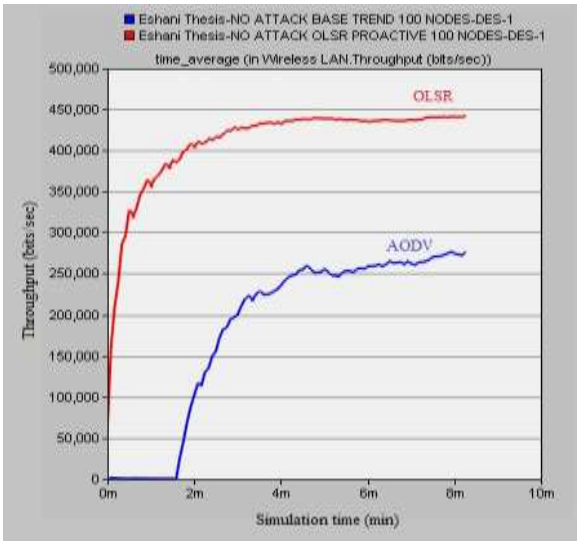


(b)

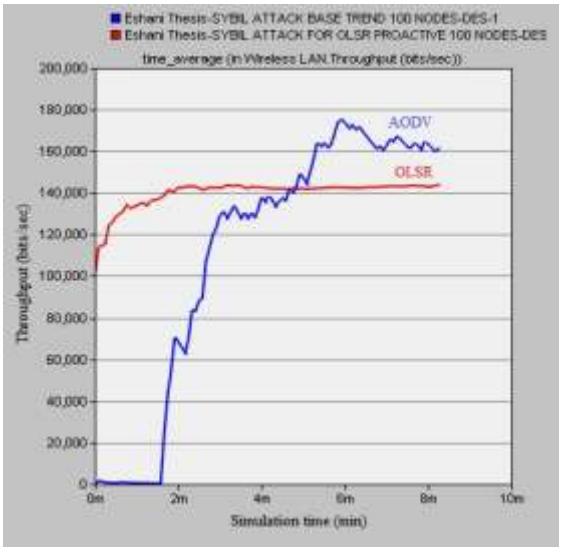
Fig. 5(a) Throughput in absence of attack (#nodes = 60) (b) Throughput in presence of attack (#nodes = 60)

Fig. 6(a) and fig. 6(b) show the throughput comparison for 100 nodes in absence and presence of attack. It can be observed that the OLSR has higher throughput than AODV in absence of attack. However, in the presence of attack decrease in throughput of OLSR is 69%

which is more than that in AODV in which decrease in throughput is 42%.



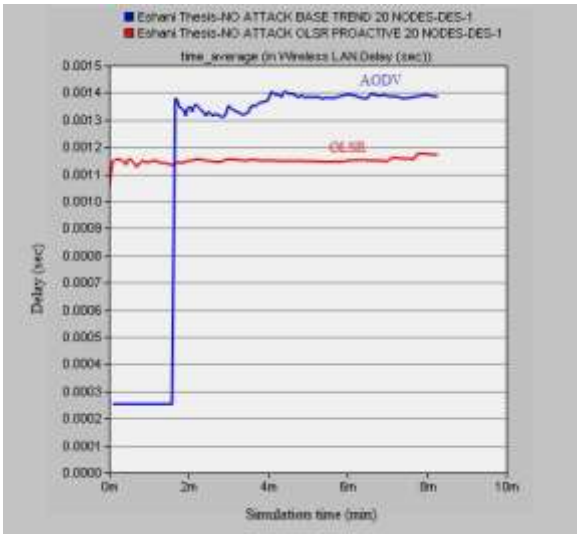
(a)



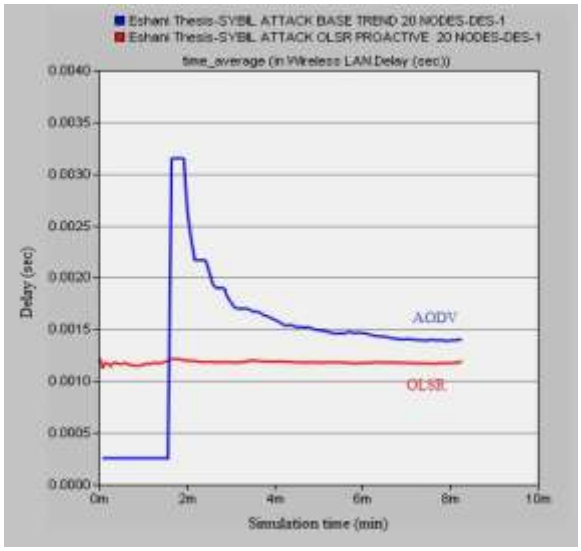
(b)

Fig. 6(a) Throughput in absence of attack (#nodes = 100) (b) Throughput in presence of attack (#nodes = 100)

Fig. 7(a) and fig. 7(b) show the delay comparison for the 20 nodes in absence and presence of Sybil attack. It can be observed that the delay in AODV is more than that in OLSR in absence of attack. In presence of attack also delay in AODV is more than that in OLSR i.e. Sybil attack has no impact on delay parameter in AODV as well as OLSR for the network having 20 nodes.



(a)



(b)

Fig. 7(a) Delay in absence of attack (#nodes = 20) (b) Delay in presence of attack (#nodes = 20)

In fig. 8(a) and fig. 8(b), delay is compared for the network having 60 nodes in the absence and presence of Sybil attack respectively. It can be observed that the delay in OLSR is more than that in AODV in absence of attack. However in the presence of attack, it can be observed that delay in OLSR is increased by 91% whereas it is decreased in AODV by 40%.

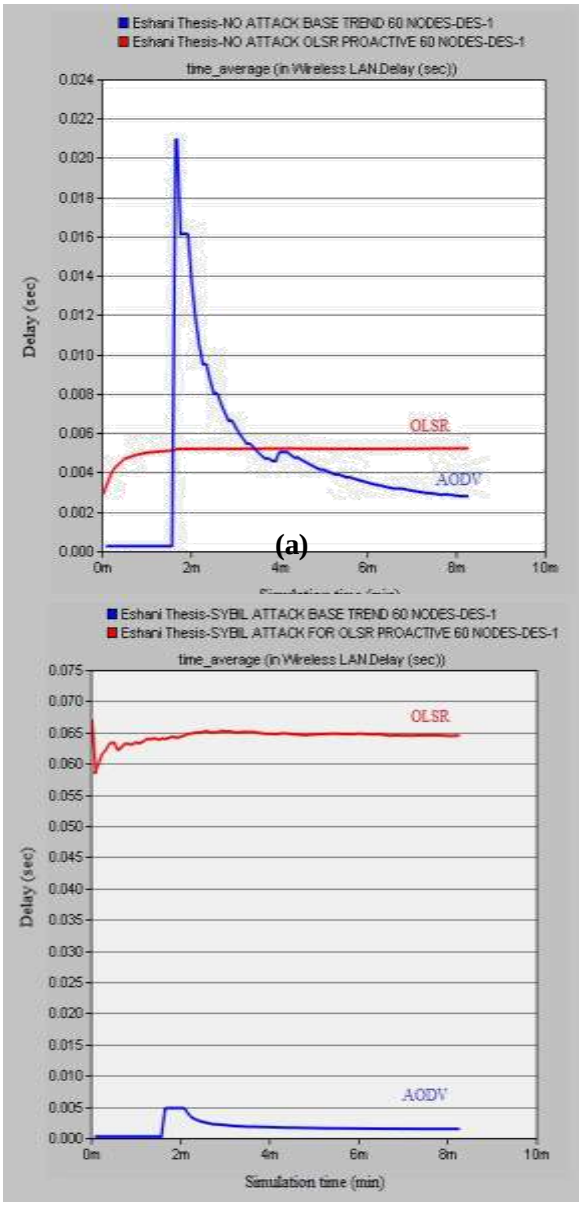


Fig. 8(a) Delay in absence of attack (#nodes = 60) (b) Delay in presence of attack (#nodes = 60)

Fig. 9(a) and fig. 9(b) show the delay comparison for 100 nodes in absence and presence of attack. It can be observed that the delay in OLSR is more than that in AODV in absence of attack. However in the presence of attack, it can be observed that delay in OLSR is increased by 20% whereas it is decreased in AODV by 50%.

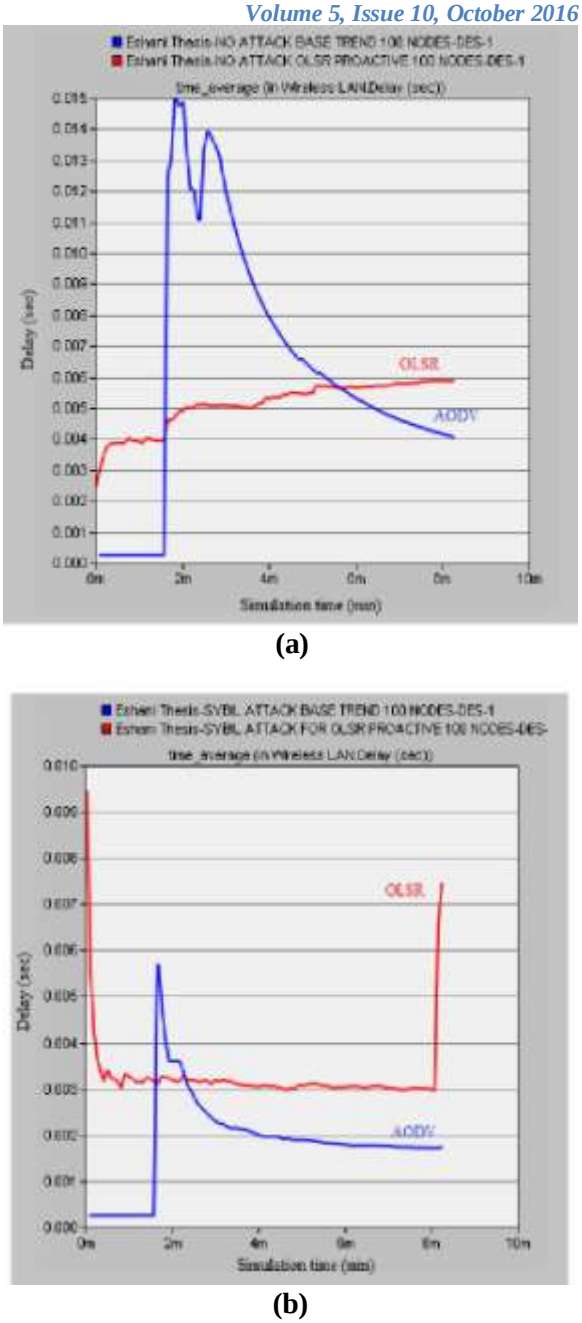
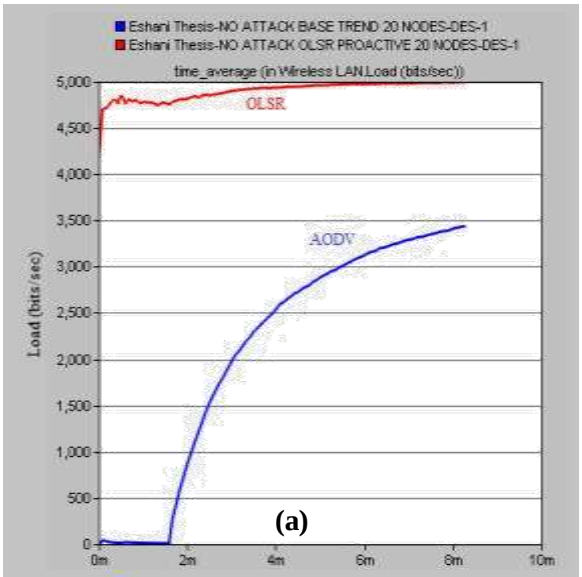
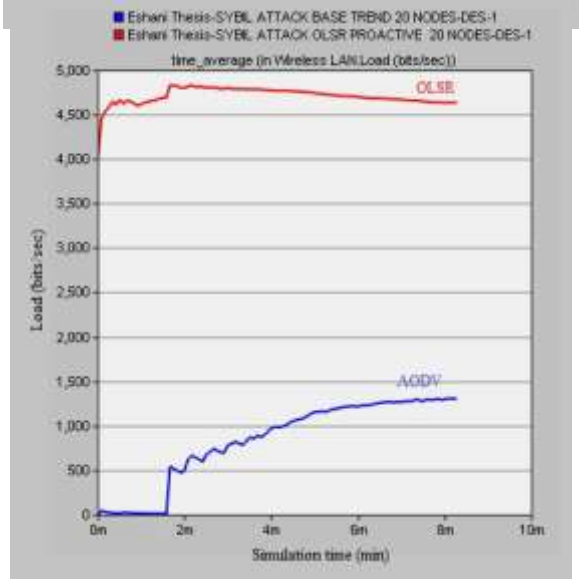


Fig. 9(a) Delay in absence of attack (#nodes = 100) (b) Delay in presence of attack (#nodes = 100)

Fig. 10(a) and fig. 10(b) show the comparison of load in case of AODV and OLSR protocols for 20 nodes in the absence and presence of Sybil attack. It can be observed that the OLSR has higher load on the network than AODV in absence of attack. However, in the presence of Sybil attack it can be observed that there is slightly decrease in load by 6% in OLSR while in AODV, decrease in load is by 63%.



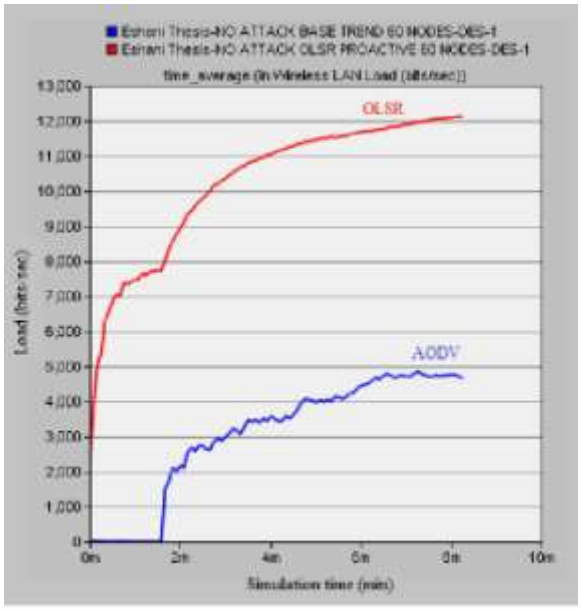
(a)



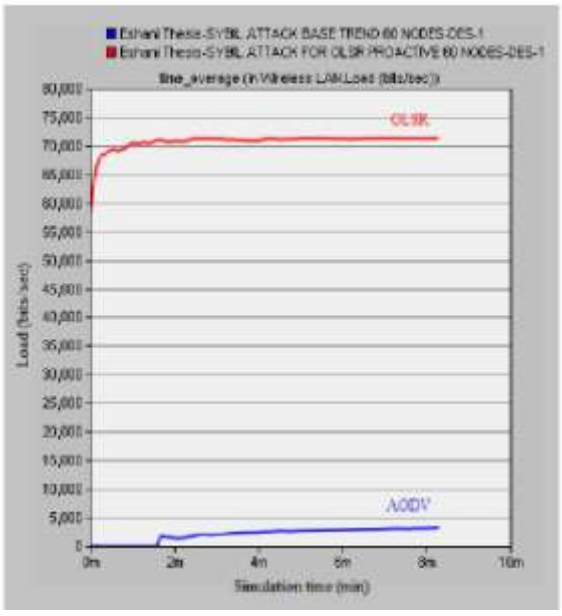
(b)

Fig. 10(a) Load in absence of attack (#nodes = 20) (b) Load in presence of attack (#nodes = 20)

Fig. 11(a) and fig. 11(b) show the comparison of load in AODV and OLSR protocols for 60 nodes in absence and presence of attack. It can be observed that the OLSR has higher load than AODV in absence of attack. However in the presence of attack it can be observed that the load is increased in OLSR by 83% and decreased in AODV by 18%.



(a)



(b)

Fig. 11(a) Load in absence of attack (#nodes = 60) (b) Load in presence of attack (#nodes = 60)

Fig. 12(a) and fig. 12(b) show the load comparison for 100 nodes in absence and presence of attack. It can be observed that the OLSR has higher load than AODV in absence of attack. However, in the presence of attack it can be observed that load is increased in OLSR by 54% and decreased in AODV by 47%.

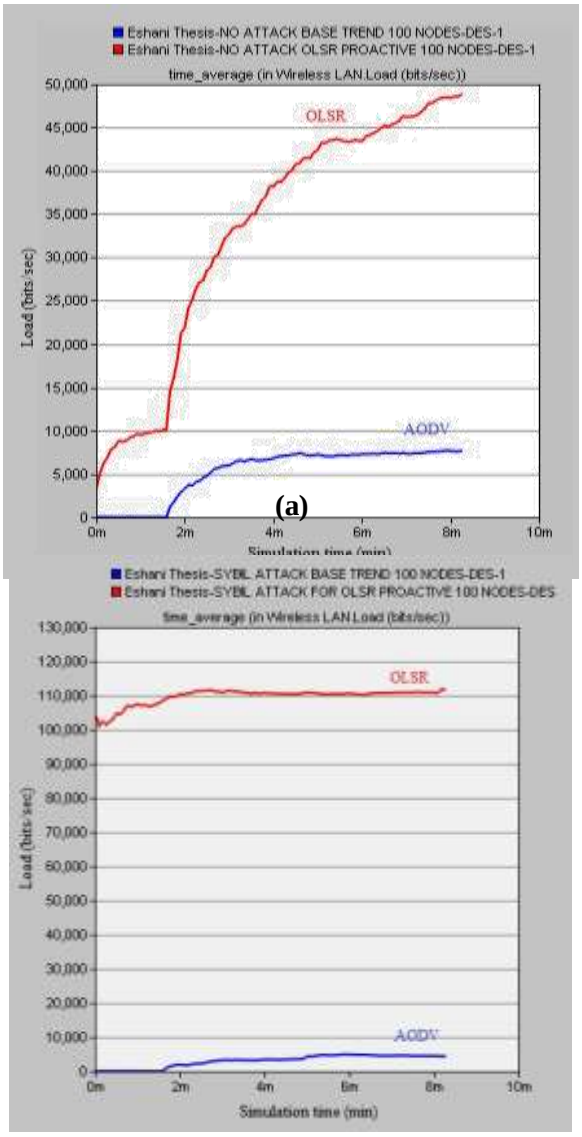


Fig. 12(a) Load in absence of attack (#nodes = 100) (b) Load in presence of attack (#nodes = 100)

V. CONCLUSION

The performance analysis showed that throughput of OLSR gets more reduced in the presence of Sybil attack in comparison to AODV, though this affect is more pronounced at higher number of nodes in the network. Similarly end to end packet delay of OLSR (proactive routing protocol) gets increased in the presence of Sybil attack especially at higher network size. Network load which is reflection of the total traffic (including payload and overhead) get substantially increased for OLSR in comparison to AODV. So it is concluded that proactive routing protocols are more adversely affected than reactive routing protocols under Sybil attack.

References

[1] D. Aldhobaiban, K. Elleithy, and L. Almazaydeh, "Prevention of Wormhole Attacks in Wireless Sensor Networks," in *2014 2nd International Conference on Artificial Intelligence, Modelling and Simulation*, 2014, pp. 287–291.

[2] Z. Kasiran and J. Mohamad, "Throughput performance analysis of the wormhole and sybil attack in AODV," in *IEEE 2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2014, pp. 81–84.

[3] K. Patidar and V. Dubey, "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 54, no. 7, 2014.

[4] A. Patel, N. Patel, and R. Patel, "Defending against Wormhole Attack in MANET," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 674–678.

[5] J. Anju and C. N. Sminesh, "An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET," in *2014 3rd International Conference on Eco-friendly Computing and Communication Systems*, 2014, pp. 149–154.

[6] V. Teotia and I. Woungang, "Wormhole Prevention using COTA Mechanism in Position Based Environment over

MANETs," in *IEEE ICC 2015-Communication Software, Services and Multimedia Applications Symposium*, 2015, pp. 8664–8668.

[7] J. Biswas, A. Gupta, and D. Singh, "WADP : A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol," in *Springer Information Communication and Embedded Systems*, 2008, pp. 1078–1085.

[8] S. Ji, T. Chen, S. Zhong, and S. Kak, "DAWN: Defending against wormhole attacks in wireless network coding systems," in *INFOCOM, 2014 Proceedings IEEE*, 2014, pp. 664–672.

[9] C. B. Dutta and U. Biswas, "Specification based IDS for Camouflaging Wormhole Attack in OLSR," in *2015 23rd Mediterranean Conferance on Control and Automation (MED)*, 2015, pp. 960–966.

[10] G. Luo, Z. Han, L. Lu, and M. J. Hussain, "Real-time and Passive Wormhole Detection for Wireless Sensor Networks," in *IEEE 2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2014, pp. 978–985.

[11] P. Lee, S. Member, A. Clark, S. Member, L. Bushnell, and S. Member, "A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3224–3237, 2014.

[12] K. Zhang, X. Liang, R. Lu and X.Shen, "Sybil Attacks and Their Defenses in the Internet of Things", IEEE Internet of Things Journal, Vol. 1, No. 5, October 2014.

[13] W. Dong and X. Liu, "Robust and Secure Time-Synchronisation Against Sybil Attacks for Sensor Networks", IEEE Transactions of Industrial Informatics, Vol. 11, No. 6, December 2015.

[14] R. Liu and Y. Wang, "A New Sybil, Attack Detection for Wireless Body Sensor Network", 2014 10th International Conference on Computational Intelligence and Security, 2014.

[15] X. Feng, C. Li, D. Chen and J. Tang, "A Method for Defensing Against Multi-Source Sybil Attacks in VANET", Springer, 29 January 2016.