Simulation Based Comparative Study of Routing Protocols in Mobile Ad Hoc Network

*Selladevi.M, Research scholar, Department of Computer Science, chikkanna Govt Arts College, Tirupur, Tamilnadu, India, mschella30@gmail.com.

Duraisamy. S, Assistant Professor, Department of Computer Science, chikkanna Govt Arts College, Tirupur, Tamilnadu, India, sdsamy@gmail.com

Abstract - A manet is a gathering of self-arranged node associated with remote connections. Every node of a mobile ad hoc network goes about as a switch and discovers an appropriate route to forward a packet from source to destination. Manet can be seen as an open type of network where nodes turn out to be a part of any network at any time so that susceptible by various kinds of attack. A wormhole attack is unsafe attack against routing protocols in ad hoc network where nodes attract the packet from one location and retransmit them then onto the next area utilizing long range connect inside the network. A wormhole opening can be effortlessly propelled between two attacker nodes without trading off the portable nodes. In this paper we study and analyse the performance of AODV and DSR under the effect of numerous wormhole attacker nodes. we evaluate the performance in terms of throughput, packet delivery ratio, packet loss and average end-end delay by using Network simulator (NS2) tool. Finally based on the simulation result we investigated the foremost affected routing protocol in terms of network metrics under wormhole attack.

Keywords — Mobile ad-hoc network (manet), Wormhole attack, AODV protocol, Security, Router, Infrastructure-less.

I. Introduction

A mobile ad hoc network (manet) (manet) is a group of devices or nodes that transmit across a wireless communication medium mainly primarily based on radio frequency with none constant infrastructure or centralized manage. Cooperation of nodes is critical to forward packets on behalf of every unique once other destinations are out in their direct wi-fi transmission vary. There might be no centralized control or community infrastructure for a manet to be installation, as a consequence making its deployment short and cheaper. The nodes facility to move generously ensures a flexible and accessible vibrant community topology that's any other critical feature of a manet [1]. A number of the manet programs includes emergency disaster, army operations over a battlefield (vulnerable infrastructure), and wasteland expeditions (temporary networks), and community networking via fitness monitoring the usage of scientific sensor community (msn). Each node in an ad hoc network ought to be inclined to ahead packets for different nodes. Every node act each as a number and as a router for the topology of ad hoc networks varies with time as nodes flow, be a part of or go away the community, with this topological lack of confidence calls for a routing protocol to run on each node to create and preserve routes most of the nodes. Mobile ad-hoc networks may be deployed in areas where a stressed-out network infrastructure can be unwanted due to motives which include value or comfort. This will be fast deployed to help emergency requirements, on the spot needs and coverage in emergent regions [1]. Each routing protocol uses different algorithms to look a route [7]. In conventional routing protocols, path for each route from host to host have to be retained in the routing tables earlier. Network topology changes, route updation and route protection can be reflected in routing tables through periodic updates [9–11]. As each mobile communication range is confined, communication beyond the limitation make route maintenance costly. Frequent adjustments inside the paths between different hosts might not be contemplated in the routing tables. As outcomes packets are undeliverable and network overall performance communication degrades. Some other drawback is that every node has restricted battery electricity, so right utilization of power consumption is an crucial issue. To assist the dynamic kind of communication in ad hoc networks proactive and reactive routing protocols were proposed primarily based at the traditional routing algorithms. Due to dynamic nature of routing protocols they are additionally at risk of distinctive types of attacks like blackhole, wormhole, packet replication, dos, flooding, session hijacking and spamming and many others. In this paper, our first complete fulfilment is to evaluate reactive (AODV, DSR) routing protocol with most dangerous routing assault wormhole. The aim of the paper isn't always only simulating the routing protocols towards more than one attacker nodes but additionally compare overall performance against every other. To

DOI : 10.18231/2454-9150.2018.1050

evaluate the overall performance of routing protocols widespread network metrics like throughput, packet delivery ratio, packet loss and average end-to-to end delay.

II. Related Work

Song et al. [12], proposed a statistical analysis approach that have a look at the have an effect on of wormhole on multipath routing. SAM uses statistical analysis tool to have a look at the drastic adjustments in routes because of wormhole attack.

Wang et al. [13], proposed a respectable plan MDS-VOW (Multi-Dimensional Scaling-Visualization of Wormhole) to see the wormhole by visualizing deterioration caused from counterfeit connections. It requires separate message between each combine, with the goal that erroneous separation can be estimated. The primary disadvantage of this plan is to identify wormhole under genuine conditions more unpredictable situations are required.

Mahajan et al. [14], examined self-contained in-band wormhole analysis based on the successful, unsuccessful and uninteresting scenarios. Observation proved that the placement of compromised nodes plays important role in the wormhole attack. The results prove that increasing wormhole strength end to end delay also increases.

Awerbuch et al [15], a secure unicast routing protocol ODSBR is compared with AODV routing protocol under wormhole attacks. The analysis proved that the centre area of a network is most effective attack position

Arora et al [16], examined the weakness of AODV routing protocol under the wormhole attack. The study considered a network of size 1000 m x 1000 m having 33 mobile nodes. The performance evaluated with varying node speed under wormhole attack. The result shows that under wormhole attack throughput and average end to end delay decreases abruptly.

Sanaei et al [17], studied AODV and DSR in the presence of wormhole and without wormhole attack using scenarios like mobility. Performance analysis based on throughput, packet delivery ratio and end to end delay metrics. The results proved that DSR is more affected by the wormhole attack.

Vandana et al. [18], compared the impact of the wormhole on AODV using different network parameters like network throughput, packet delivery ratio, average end to end delay and packet drop using NS2 simulator. The results proved that as more wormhole nodes exist in the networks the performance degrades in terms of network parameters. To provide security to above defined routing protocols various wormhole detection and prevention schemes have been proposed.

Chen et al. [19], defined DV-HOP localization mechanism that makes use of label to provide at ease area accuracy. The nodes are mark by using distinctive labels to violate different communication properties. Pseudo neighbors are identified and communication between them is forbidden. The scheme can’t work properly in which packet loss and radii of the nodes aren't same.

Madria et al. [20], proposed SERWA that makes use of symmetric key cryptography mechanism for creating the secure path. It doesn’t require any unique hardware or clock synchronized. The key factor of SERWA is it offers secure routing towards the wormhole attack after detecting its presence.

III.TYPES OF ROUTING PROTOCOLS

Mobile ad hoc network is classified into table driven (proactive), on demand (reactive) and hybrid. Manet routing protocols classified into three classes

3.1 Proactive Routing Protocol

Proactive routing protocol maintain consistent and contains update regarding each node within the routing table. These protocols used periodic event-driven algorithmic program for route discovery and route maintenance similar to every request when some predefined amount, routes are updated mechanically within the routing tables according to topological changes of the host table-driven routing protocol have fascinating properties that make them applicable for the time period applications [22]. DSDV and OSLR are the proactive type of routing protocols.

3.2 On Demand /Reactive Routing Protocol

On demand are source-initiated routing protocols. Once source needed path the route discovery occurs between source to destination within the network [13]. When route discovery, route maintenance mechanisms continuous unless the destinations are unapproachable [24]. AODV and DSR are the reactive routing protocol.

3.3 Hybrid Routing Protocol

ZRP divides the network into small manageable zones. ZRP is hybrid routing protocol which combines the best features of both proactive and reactive routing protocols [13].

3.2.1 AODV (Ad Hoc On Demand Distance Vector Routing Protocol)

AODV is improved version of DSDV as a result of it minimizes the broadcasting method by permitting the on-demand routes [4]. As there's no route maintenance and no exchange between the routing tables that’s why it's hop to hop, unidirectional on demand routing protocols [22]. In AODV, route discovery method starts once source node initiates and floods the network with RREQS (route request). The node next to source node acts as an intermediate and sends RREPS (route reply) back to the previous node along with the route information by establishing reverse path in unicast manner. This method continues unless the packet reaches its destination RREP (route reply) are generated correspondence to every RREQs. Every node stores the sequence number of received route request, if same RREQ copies reaches multiple times, it's discarded by intermediate nodes. This unique sequence number helps to construct loop free surroundings. It has one

DOI : 10.18231/2454-9150.2018.1050

entry per destination and table entries show activeness of accessible path. In AODV, path with the shortest hop counts are most popular to transfer the information from source to destination. If any node moves alone or with path route maintenance aspect starts by notifying the upstream nodes regarding the broken links. Then broken or invalid path are removed from the routing tables. Link breakage between totally different path may be simply detected with the help of RERR (route error).

3.2.2 DSR (Dynamic Source Routing Protocol)

DSR is a loop free, source initiated on demand routing protocol [23–25]. It helps to search the path in multihop surroundings dynamically. In DSR, mobile nodes are aware of sequence of nodes to be followed through which packets are passed and route caches and update new routes entries on frequently basis [4]. There are two phases “route discovery” and “route maintenance”. In route discovery source has packet to send it initial ask routing cache for available path. If ways are given in route cache, the source node makes use of this path for transfer information otherwise” route discovery’’ part is initiated. It broadcast request by as well as individual identification number, source and destination address. Every intermediate node verifies the incoming packet, if it is aware of the address of destination; it replies back otherwise it will forward the request to its destination. Route replies are generated by the destination or intermediate node. Route discovery ends with sequence of hops used for data transfer. DSR has multiple entries for every destination in routing tables [2]. To avoid process of same request again and again, every node maintains the list of recently seen requests and discards that specific request. ‘‘route maintenance’’ starts with the detection of broken or invalid links that can't be use for data transfer [23]. DSR reduces power consumption and is additionally time economical. The disadvantage of DSR is that it uses multi hop path discovery policy to search path, same RREQ (route request) is forwarded to multiple hops at identical time.

IV.WORMHOLE ATTACK

Wormhole is a trivial type of attack that uses a combine of colluding nodes to transfer a packet from one location to a different location using long range high speed private link [4]. Figure 1, explains, how data transfer take place if the malicious nodes is presented [37].

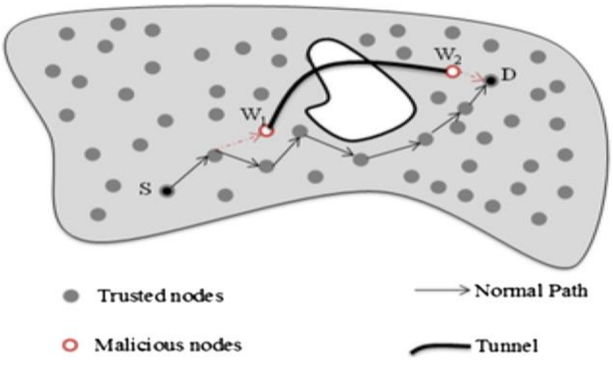


Figure 1 The Wormhole attack model

The primary attacker node is placed among the network that transfer the packet to next attacker node situated on the opposite location. This long-range tunnel tend to wormhole link. These attacker nodes acting as neighbour nodes to other nodes however actually, they are many hops off from one another [5,6]. Within the presence of wormhole attack, hop count value decreases however delay will increases. Wormhole attack exploits network communication by performing DOS attack or overburden the network communication with flooding of packets.in wormhole attacker nodes don’t modify packets contents; thus, cryptography strategies can’t observe and prevent wormhole attack. The wormhole is launched among the network in three ways which is represented in fig 2[5].

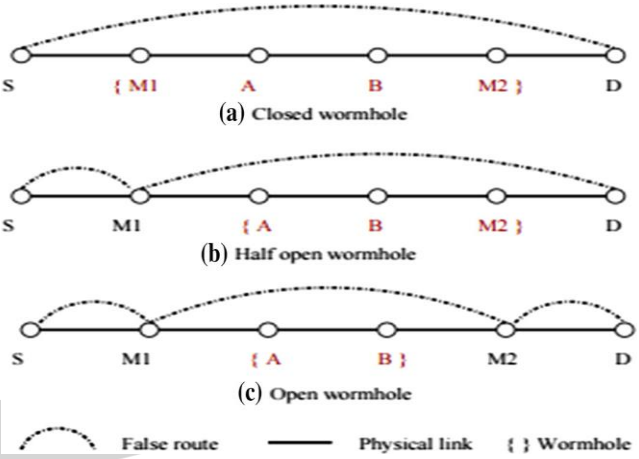


Figure 2 Categorization of wormhole attack

4.1 Hidden/Closed Wormhole Attack

The malicious nodes don’t modify the packet content and packet header [5, 6]. The malicious node at one area merely transfer the packet an alternative area within the network long rang tunnel. The malicious nodes fake as they're neighbors of legitimate nodes [6]. Malicious nodes hide their identities within the created path. As shown in the figure 2 (S, A, B, D) are the legal nodes and M1, M2 are the malicious nodes. Source node tunnels the packet to destination by using M1, M2 are the direct neighbors.

4.2 Half Open Wormhole

The attacker node modifies the packet contents solely at one aspect. Attacker node doesn’t change the packet content throughout the route discovery method [5]. As shown in Figure the source node directly transfers the packet to malicious nodeM1 because M1 acting as a neighbor of source node S. Then M1 directly tunnel the packet to destination D by hiding its details in the packet header. Just one node visible in half open mode wormhole.

4.3 Exposed / Open Mode Wormhole

Malicious nodes don’t modify the packet contents and mark their presence within the packet header by as well as themselves [5]. Nodes are aware about presence of malicious nodes in the created path but cannot detect their exact location in the network. Figure 2c illustrates the malicious nodes M1 and M2 are visible to source S and destination D.

V.SIMULATION ENVIRONMENTS

5.1 Simulation Model

The main goal of our experiment is to analysis impact of wormhole on routing protocols. Using NS2 simulator AODV and DSR protocols are simulated. NS2 contains physical level, mac, data link layer and routing protocols to perform comparison. The nodes move in a simulation area at a uniform speed with the help of random waypoint. After some pause time nodes changes their random position or change their destinations. Communications between the mobility nodes established using constant bit rate (CBR). To generate the ample traffic group of sources and destinations are randomly placed within network area. More than one malicious node is randomly placed within the network to study the impact of wormhole attack in more extent, two more victim nodes are randomly placed within the network they may choose any location within the network.

Protocols	AODV, DSR
Simulation area	1100 X1100
Number of nodes	50
Simulation time	30 S
Range for normal network	200 M
Range for wormhole network	500m
Mobility model	Random Way point
Queue length	500
Packet size	256 bytes
Maximum speed	20m/s

5.2 Performance Metrics

Throughput

Throughput means the total number of bits transferred over the destination in per unit time [29, 30]. Throughput depends upon the capacity of the channel.

Packet Delivery Ratio

Packet Delivery Ratio (PDR) is the number of packets received over number of packets sent [29,30]. The more packets received by the destination node better is the performance.

Packet Loss

Packet loss means total packets lost during the transmission [30]. It defines the number of packets that never reach the destination. Packet loss occurs due to congestion, disturbance and weak radio signals.

Average End-to-End Delay

It defines the total delay over number of packets received by destination. Average E2E delay defines the average time taken by the packets to reach the destination [29,30]. Average E2E delay includes time like propagation, transmission, queuing, and processing delay.

VI. RESULTS AND DISCUSSION

6.1 Analysis Based on Average of 50 Runs

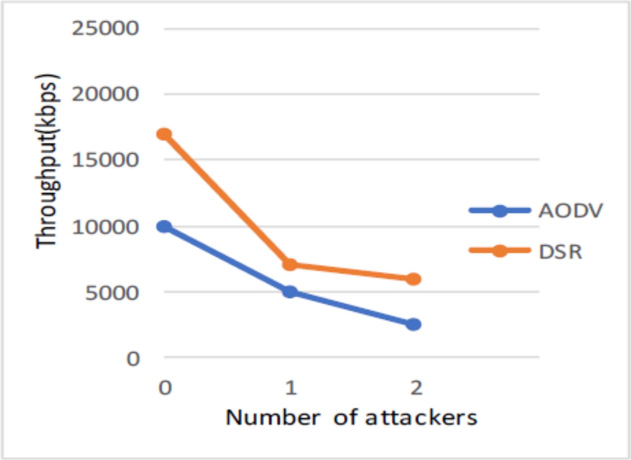
In this scenario, to obtain average simulation results experiment repeated 50 times with same sets of parameters as mentioned in Table 1 for simulation purpose in each routing protocols. The implementation of routing protocol is done in NS2 for the simulation purpose [31]. the simulation parameters are used table2 adapted from kumar et al [28].

Table 1 Simulation parameters for evaluation

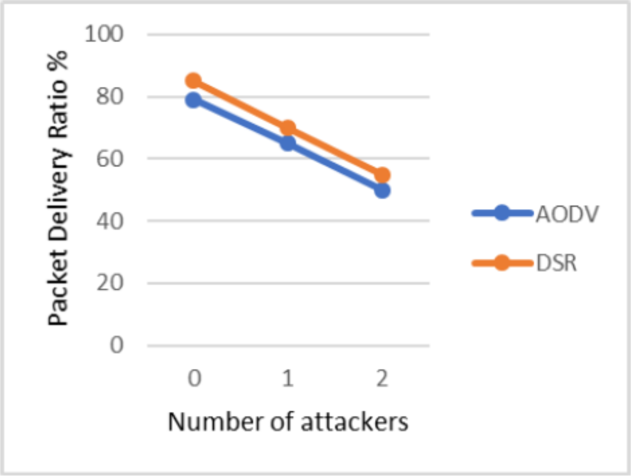
6.1.1 Results

Figure 3 a, b, c, d shows performance of AODV and DSR with and without wormhole.

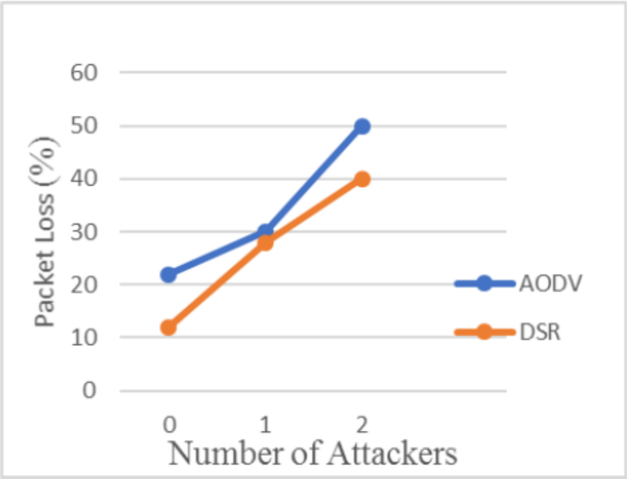
a)



b)



c)



DOI : 10.18231/2454-9150.2018.1050

d)

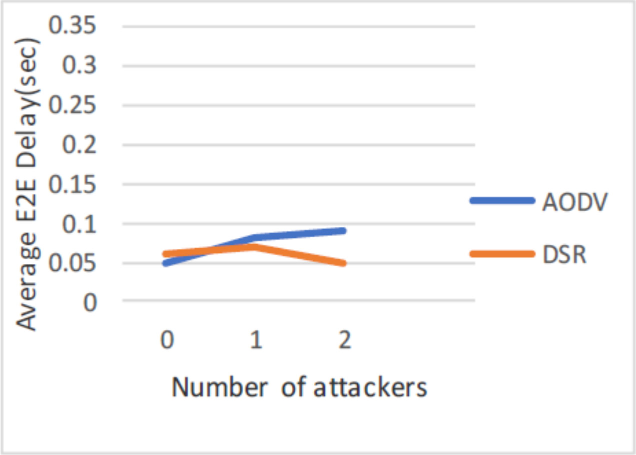


Figure 3 a shows throughput of AODV is worse than DSR. On the same lines, Fig. 3b. AODV exhibits more fall rate in PDR than DSR. Fig. 3c. AODV has maximum packet loss as compared to DSR.

6.2 Analysis Based on Mobility

In this scenario, same sets of parameters are used for simulation purpose as mentioned in Table 2 with varying speed of network nodes. The performance of AODV and DSR analyzed using the simulation. The simulation is carrying out using NS2 with mobility.

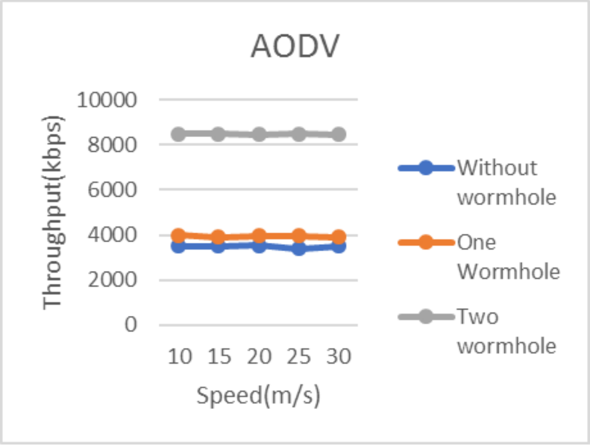
Table 2 Simulation parameters for evaluation

Protocols	**AODV, DSR**
Simulation area	1100 X1100
Number of nodes	50
Simulation time	30 S
Range for normal network	200 M
Range for wormhole network	500m
Mobility model	Random Way point
Queue length	500
Packet size	256 bytes
Maximum speed	20m/s
Pause time	0.1m/s
Mobility model	10 m/s to 30 m/s

6.2.1 Results

Simulated results are presented in Figs. 4, 5, 6, and 7. They show performance trade-off in some metrics.

(a)



b)

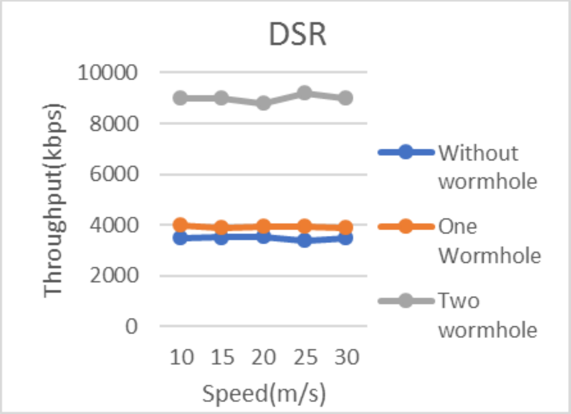
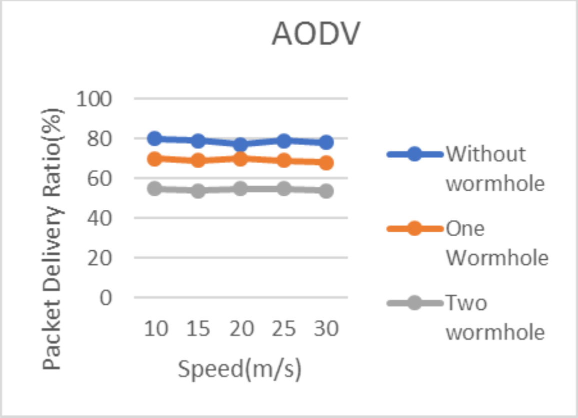


Figure 4 a, b Illustrates, throughput for AODV and DSR with and without wormhole under mobility

(a)



b)

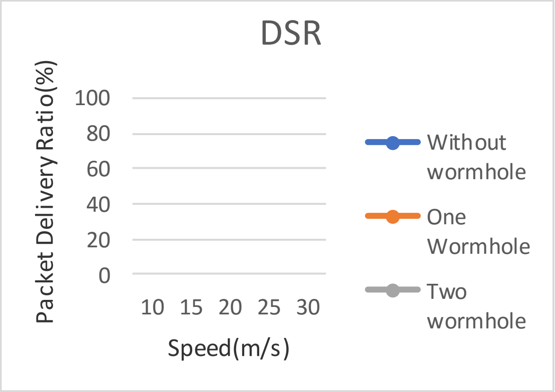
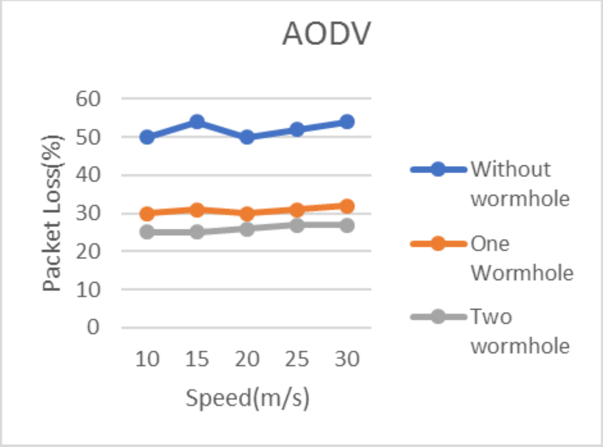


Figure 5 a, b Illustrates, Packet Delivery Ratio for AODV and DSR with and without wormhole under mobility

a)



DOI : 10.18231/2454-9150.2018.1050

b)

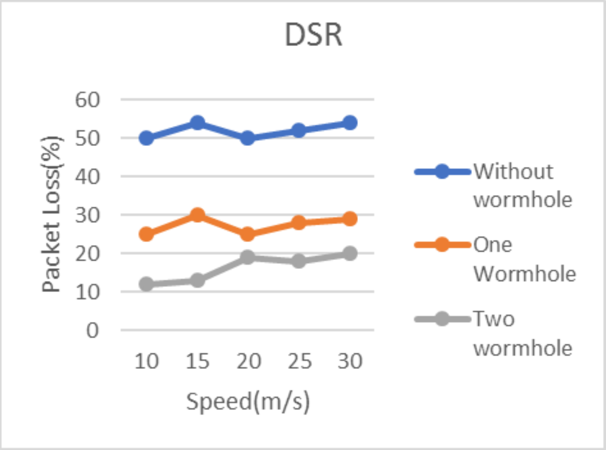
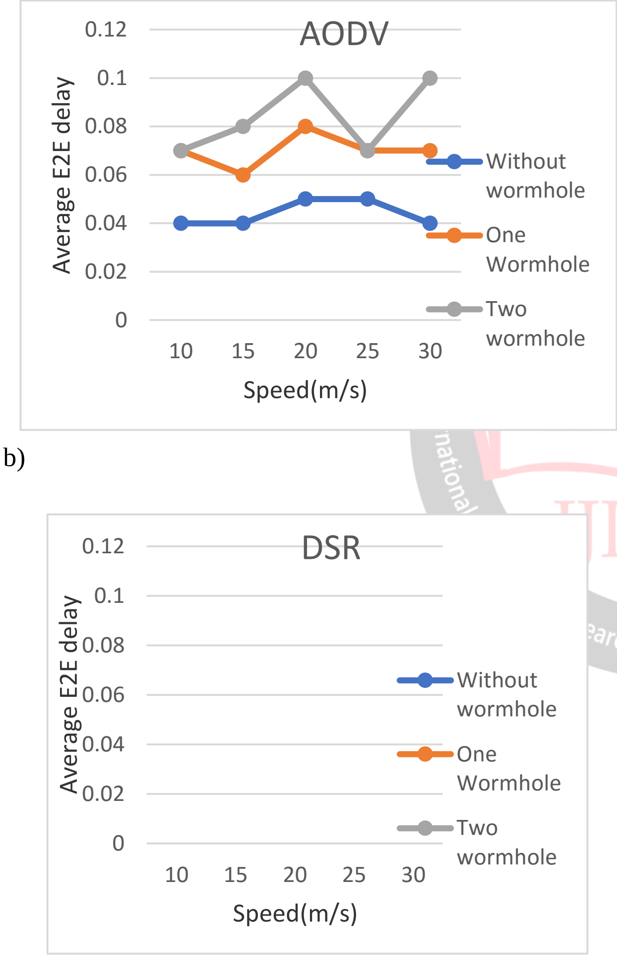


Figure 6 a, b Illustrates, Packet Loss for AODV and DSR with and without wormhole under mobility



b)

Figure 7 a, b Illustrates, average E2E delay for AODV and DSR with and without wormhole under mobility.

From Figs. 5, 6 and 7, it can be concluded from results AODV performance is comparatively poor than DSR. As mobility increases more link breakage occur, paths are unreachable and packets don't reach at their destinations. Due to the presence of attacker nodes RREQs are hacked by them and transferred to other unknown location. Those RREQs never reach to its intended location so directly affect throughput, packet delivery ratio and packet loss. The average E2E delay for all the routing protocols is illustrated in Fig. 5. The average E2E delay increase as mobility goes high in the network more link breakage occurs more frequently and the new path creation takes time. Each routing protocols route buffering mechanism also affect the performance.

VII. CONCLUSION

Performances of routing protocols depend upon several factors like number of senders, receivers and attacker nodes. The NS2 simulator provides accurate results which can be used for comparison of different routing protocols. After reviewing all the above figures, it can be clearly judged that performance of AODV routing protocol is more affected by the wormhole attack in terms of throughput, packet delivery ratio, and Packet Loss. The simulation results clarify if multiple attacker nodes are present in the network then the performances of the routing protocols degrade. In our future work, based on the above simulation results a secure wormhole detection and prevention technique can be developed which will improves the performance AODV in terms of Packet Delivery Ratio, Throughput and Packet Loss.

REFERENCES

[1] Ho, Yao H., Ho, Ai H., & Hua, Kien A. (2008). Routing protocols for inter-vehicular networks: A comparative study in high-mobility and large obstacles environments. Computer Communications,31(12), 2767–2780.

[2] Ramanathan, R., & Redi, J. (2002). A brief overview of ad hoc networks: Challenges and directions' Communications Magazine, 40(5), 20–22.

[3] Bansal, M., Rajput, R., & Gupta, G. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. The internet society.

[4] Royer, E. M., & Toh, C. K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE, 6(2), 46–55.

[5] Giordano, S. (2002). Mobile ad hoc networks, In Handbook of wireless networks and mobile computing (pp. 325–346).

[6] Nguyen, Hoang Lan, & Nguyen, Uyen Trang. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks, 6(1), 32–46.

[7] Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks, 2(1), 1–22.

[8] Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: Imperatives and challenges. Ad Hoc Networks, 1(1), 13–64.

[9] Sesay, S., Yang, Z., & He, J. (2004). A survey on mobile ad hoc wireless network. Information Technology Journal, 3(2), 168–175.

DOI : 10.18231/2454-9150.2018.1050

[10] Das, Samir R., Castan˜eda, Robert, & Yan, Jiangtao. (2000). Simulation-based performance evaluation of routing protocols for mobile ad hoc networks. Mobile Networks and Applications, 5(3), 179–189. M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.

[11] Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. Communications Surveys & Tutorials, IEEE, 10(4), 78–93.

[12] Song, N., Qian, L., & Li, X. (2005, April). Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach. In 19th IEEE international parallel and distributed processing symposium (p. 8). IEEE.

[13] Wang, W., & Bhargava, B. (2004, October). Visualization of wormholes in sensor networks. In Proceedings of the 3rd ACM workshop on wireless security (pp. 51–60). ACM.

[14] Mahajan, V., Natu, M., & Sethi, A. (2008). Analysis of wormhole intrusion attacks in MANET. In MILCOM 2008-2008 IEEE Military Communications Conference. IEEE.

[15] Awerbuch B., et al. (2004) Mitigating byzantine attacks in ad hoc wireless networks. Department of Computer Science, Johns Hopkins University, Tech. Rep. Version 1, p. 16.

[16] Arora, M., Challa, R. K., & Bansal, D. (2010). Performance evaluation of routing protocols based on wormhole attack in wireless mesh networks. In Second International Conference on Computer and Network Technology (pp. 102–104). IEEE.

[17] Sanaei, M. G., Isnin, I. F., & Bakhtiari, M. (2013). Performance evaluation of routing protocol on AODV and DSR under wormhole attack. International Journal of Computer Networks and Communications Security.

[18] Vandana, C. P., & Devaraj, A. F. S. (2013). Evaluation of impact of wormhole attack on AODV. International Journal of Advanced Networking and Applications, 4(4), 1652.

[19] Chen, H., Lou, W., Wang, Z., Wu, J., Wang, Z., & Xia, A. (2015). Securing DV-Hop localization against wormhole attacks in wireless sensor networks. Pervasive and Mobile Computing, 16, 22–35.

[20] Madria, S., & Yin, J. (2009). SeRWA: A secure routing protocol against wormhole attacks in sensor networks. Ad Hoc Networks, 7(6), 1051–1063.

[21] Poovendran, Radha, & Lazos, Loukas. (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Networks, 13(1), 27–59.

[22] Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

[23] Johnson, D. B. (2003). The dynamic source routing protocol for mobile ad hoc networks. Draft-ietfmanet-dsr-09. Txt.

[24] Chen, L., Yang R., & Huang, M. (2016). Ad hoc high-dynamic routing protocol simulation and research. In Wireless Communications, Networking and Applications (pp. 399–408). Springer India.

[25] Boukerche, Azzedine. (2004). Performance evaluation of routing protocols for ad hoc wireless networks. Mobile Networks and Applications, 9(4), 333–342.

[26] Maulik, R., & Chaki, N. (2010). A comprehensive review on wormhole attacks in MANET. In International Conference on Computer Information Systems and Industrial Management Applications (CISIM), IEEE.

[27] Kaur, G., Jain, V. K., & Chaba, Y. (2011). Wormhole attacks: Performance evaluation of on demand routing protocols in Mobile Ad hoc networks. In World Congress on Information and Communication Technologies.

[28] Kumar, J., Singh, A., Panda, M. K., & Bhadauria, H. S. (2016). Study and performance analysis of routing protocol based on CBR. Procedia Computer Science, 85, 23–30.

[29] Mohapatra, S., & Kanungo, P. (2012). Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 simulator. Procedia Engineering, 30, 69–76.

[30] Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015). Defending against collaborative attacks by malicious nodes in Manet: A cooperative bait detection approach. Systems Journal, IEEE, 9(1), 65–75.

[31] Issariyakul, T., & Hossain, E. (2011). Introduction to network simulator NS2. Berlin: Springer.

DOI : 10.18231/2454-9150.2018.1050