Wireless Pers Commun (2017) 96:47–63
DOI 10.1007/s11277-017-4150-2

Simulation Based Comparative Study of Routing Protocols Under Wormhole Attack in Manet

Parvinder Kaur[1] · Dalveer Kaur[2] · Rajiv Mahajan[3]

Published online: 28 April 2017

Abstract A Mobile Ad hoc network (manet) has emerged as an autonomous, multi-hop, wireless and temporary type of network which works within the constraints like bandwidth, power and energy. Manet can be observed as an open type of network where nodes become a part of any network at any time that's why it is susceptible to different types of attacks. Wormhole attack is most threatening security attack in ad hoc network where an attacker node receives packet at one location and replay them at other location which is remotely located far. In this paper, we study and compare the performance of AODV, DSR and ZRP under the impact of multiple wormhole attacker nodes. Diverse scenarios are characterized as like average of 50 runs and mobility. By statistical placement of multiple wormhole nodes across the network, we evaluate the performance in terms of throughput, packet

Parvinder Kaur's research area is mobile ad hoc and wireless networks. The paper focus on how the performance of various routing protocols degrade due to wormhole attack. AODV, DSR and ZRP evaluated together with group of source and destination nodes by including more than one wormhole nodes in the network. Simulation results identify the most effective routing protocol in the term of network metrics based on different scenarios. The motivation behind performance analysis serves as a cornerstone for the development of secure detection and prevention scheme for wormhole attack based on simulation results.

✉ Parvinder Kaur
Jassi33@gmail.com

Dalveer Kaur
dn_dogra@rediffmail.com

Rajiv Mahajan
rajivmahajan08@gmail.com

[1] Department of Research, Innovation and Consultancy, Punjab Technical University, Jalandhar-Kapurthala Highway, Kapurthala, Punjab, India

[2] Punjab Technical University, PIT University Campus Jalandhar-Kapurthala Highway, Kapurthala, Punjab, India

[3] Department of Computer Science and Engineering, Golden College of Engineering and Technology, Gurdaspur, Punjab, India

delivery ratio, packet loss, average end to end delay and jitter. Finally based on the simulation we investigated the most affected routing protocol in terms of network metrics.

Keywords Mobile Ad hoc network (Manet) · Routing protocols · Wormhole · Metrics · Network simulator · Throughput · Packet loss · Packet delivery ratio · Jitter · Random mobility model

1 Introduction

Wireless ad hoc networks have become popular in recent years for research purposes [1]. There are two types of mobile networks—Infrastructure wireless networks and Infrastructure-less mobile ad hoc network [1]. In Infrastructure wireless network, nodes reply upon predefined access points for working. Fixed base stations are assigned and nodes can move within its topology range. In Infrastructure-less or ad hoc networks both terms are interchangeably use. In ad hoc networks, no fixed base stations are allotted and nodes can move in any area without the restriction of infrastructure [2–4]. Each host performs the task of route maintenance or creation by itself. Manet is collection of wireless nodes where each node is dynamic in nature. No fixed wired connections are available and nodes work without the restriction of any physical location. In manet, each host act as a router to transfer data into multihop manner. Nodes are self-sufficient and independent to work individually as a result route maintenance, route tracking and path link breakage detection is done by itself [5, 6]. Two hosts which came in the same topology range can share information with one another easily and if two nodes are far away from each other then intermediate nodes can transfer the data between them [2, 7]. With the emergence of Manet, many real-time communication problems have been solved which require formation of immediate networks within a short span of time such networks are feasible in battlefield, military, conference etc. [4–9].

Manet use peer to peer communication scheme between hosts on the other hand radio waves are meant for data transfer between peer to peer nodes. But as radio communication is unreliable and insecure so to make this communication more reliable, robust and efficient; the secure routing protocols must be created. The lack of fixed infrastructure and mobility nature of nodes, manet are vulnerable to different types of malicious activities. To utilize the limited computational and communication resources in the effective manner security is required. In this research article, we focus on one of the sever wormhole attack, which potentially destroys network communication.

As many routing protocols have proposed for mobile ad hoc network. Each routing protocol uses different algorithms to search a path [7]. In traditional routing protocols, path for each route from host to host must be retained in the routing tables in advance. Network topology changes, route updation and route maintenance can only be reflected in routing tables through periodic updates [9–11]. As each mobile communication range is limited, communication beyond the limitation make route maintenance is costly. Frequent changes in the paths between different hosts may not be reflected in the routing tables. As consequences packets are undeliverable and network performance communication degrades. Another drawback is that every node has limited battery power, so proper utilization of power consumption is an important factor. To support the dynamic type of communication in ad hoc networks proactive and reactive routing protocols have been proposed based on the traditional routing algorithms. Due to dynamic nature of routing protocols they are also susceptible to different types of attacks like blackhole, wormhole, packet replication, DOS, flooding,

session hijacking and spamming etc. As per our knowledge in the literature performance evaluation of different routing protocol have been studied with a variety of attacks under diverse scenarios like mobility, multiple attacker nodes and varying nodes speeds. In this paper, our first comprehensive achievement is to evaluate two reactive (AODV, DSR) and one hybrid (ZRP) routing protocol with most harmful routing attack wormhole. The aim of the paper is not only simulate the routing protocols against multiple attacker nodes but also compare performance against each other. To evaluate the performance of routing protocols significant network metrics like throughput, packet delivery ratio, packet loss, average end to end delay and jitter. Our purpose is to investigate impact of wormhole on routing protocols under different scenarios like average of 50 runs and varying mobility.

The rest of the paper is organized as follows: The Sect. 2, we briefly review the related literature work. In Sect. 3, contains Classification of Routing Protocols. In Sect. 4, describes the wormhole attack and its types. In Sect. 5, describes Simulation Environment. In Sect. 6, Performance Evaluation and Results are discussed. In Sect. 7, Conclusion and Future work discussed.

2 Related Work

Past studies investigated the routing protocols with wormhole presents in the research and various solutions have been proposed to defend against wormhole. The details of literature survey are as follow:

Mahajan et al. [12], examined self-contained in-band wormhole analysis based on the successful, unsuccessful, doubtful, interesting and uninteresting scenarios. Observation proved that the placement of compromised nodes play important role in the effectiveness of wormhole attack. The results prove that as with the increase in the wormhole strength end to end delay also increases.

Awerbuch et al. [13], a secure unicast routing protocol ODSBR is compared with AODV under different attacks like wormhole, blackhole and rushing attacks. The analysis proved that the center area of a network is most effective attack position. Observation also proved that center area in mulicast routing is more vulnerable to attacks.

Arora et al. [14], examined the vulnerability AODV under the wormhole attack. Their study considered a network of size 1000 m × 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.

Garg et al. [15], compared the reactive routing protocols with wormhole under mobility and non mobility environment using Qualnet 4.5. The analysis proved threshold wormhole attack is more severe than all pass and all drop because packet drop is more. The results proved that AODV is more vulnerable to wormhole attack in case of mobility and also performance degrades in terms of throughput, average end-to-end delay, average jitter and packet delivery ratio.

Sanaei et al. [16], studied AODV and DSR in the presence of wormhole and without wormhole using scenarios like mobility. Performance analysis based on throughput, packet delivery ratio and end to end delay metrics. The study considers 500 × 500 m^2 square areas with 30 nodes and packet size is 52 bits. The results proved that DSR is more affected by the wormhole attack.

Vandana et al. [17], 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. This study considered 1000 m × 1000 m having 50 nodes with the existence of five wormhole nodes. 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.

Dong et al. [18], demonstrated unusual behavior of network due to the wormhole underlying topology nodes. Based on the simulation results new approach has been proposed which rely upon network connectivity without the need of any specialized hardware that help to detect and locate the wormhole attack. Hu et al. [19], Packet leashes defense mechanism against wormhole by adding geography or time information into the packet. Pooverdran et al. [20], proposed a graph based model to characterize the wormhole. Nodes must be equipped with a GPS receiver and create a necessary and required condition to prevent the wormhole attack. Chiu et al. [21], proposed a algorithm which uses the delays and number of hops different disjoint paths to locate the wormhole attack. The delay of normal path is compared with the path under wormhole attack. Xu et al. [22], proposed a WADD approach that uses a hop count technique to detect the wormhole attack. Abnormalities in the diameter are used to detect the wormhole attack.

The main contribution the paper by using out of band wormhole link behavior of AODV, DSR and ZRP are simulated. The purpose is to simulate above defined protocols by including more than one source, destination and attacker nodes in the simulation area. Our experiment compare and analysis performance of AODV, DSR and ZRP routing protocols based on throughput, packet delivery ratio, packet loss, average end to end delay and jitter metrics using different scenario like mobility and average of 50 runs. The simulation results generate the most affected routing protocol in terms of network metrics.

3 Classification of Routing Protocols

Mobile Ad hoc Network can be classified into Table Drive (proactive), On Demand (reactive) and Hybrid [11]. Regardless of all routing protocols that are designed for same underline network, but each routing protocol has different set of characteristics. According to Mbarushimana et al. [23], Saeed et al. [24] routing protocols can be classified into the following categories as illustrated in Fig. 1.

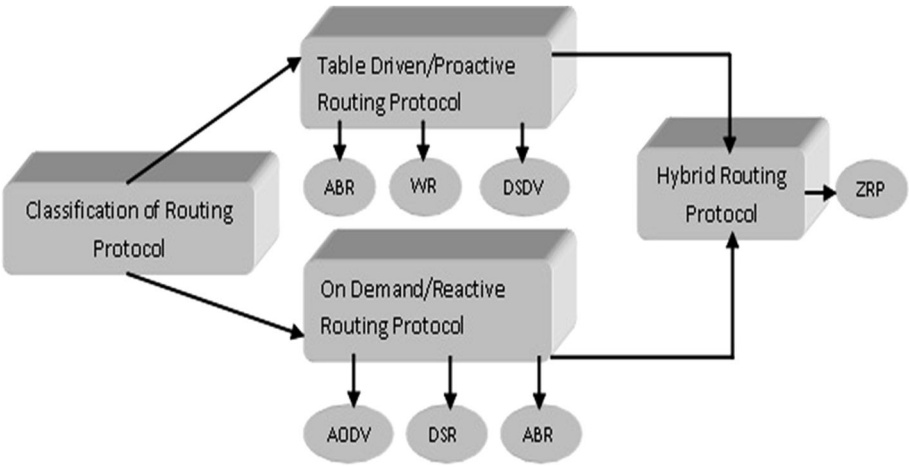

Fig. 1 Classification of routing protocols

3.1 Table Driven/Proactive Routing Protocol

Proactive Routing Protocols maintains consistent and contains update information about every node in the routing tables [23, 24]. These protocols used periodic event-driven algorithm for route discovery and route maintenance corresponding to each request. After some predefined period routes are updated automatically in the routing tables according to topological changes of the host [23]. Table driven routing protocols have desirable properties which make them applicable for the real-time applications [24]. DSDV and OSLR are the proactive type of routing protocols.

3.2 On Demand/Reactive Routing Protocol

On Demand are source initiated routing protocols. When source required path then route discovery take place between source to destination within the network [11, 24]. After route discovery, route maintenance mechanisms continuous unless the destinations are unreachable [24]. AODV and DSR are the reactive routing protocols.

3.2.1 AODV (Ad hoc on Demand Routing Protocol)

AODV is improved version of DSDV because it minimizes the broadcasting process by allowing the on demand routes [4]. As there is no route maintenance and no exchange between the routing tables that's why it is hop to hop, unidirectional on demand routing protocols [25, 26]. In AODV, route discovery process starts when source node initiates and floods the network with RREQs (Route Request) [27]. 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 process continues unless the packet reaches its destination. RREPs (Route Reply) are generated correspondence to each RREQs. Each node stores the sequence number of received request, if same RREQs copies reaches multiple times, it is discarded by intermediate nodes. This unique sequence number helps to construct loop free environment. It has one entry per destination and table entries show activeness of available paths. In AODV, paths with the shortest hop counts are preferred to transfer the data from source to destination. If any node move alone or with path route maintenance face starts by notifying the upstream nodes about the broken links. Then broken or invalid paths are removed from the routing tables. Link breakage between different available paths can be easily 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 [28–30]. It helps to search the path in multihop environment dynamically. In DSR, mobile nodes are aware about sequence of nodes to be followed through which packets are passed and route caches and update new routes entries on continually 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 paths. If paths are presented in route cache, the source node makes use of this path for transfer data otherwise "route discovery" phase is initiated. It broadcast a request by including unique identification number, source and destination address. Each intermediate node verifies the incoming packet, if it knows the address of

destination; it replies back otherwise it will forward the request to its destination. Intermediate node only processes the packet when the address is unknown or previously packet never visited the same node. 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 each destination in routing tables [2]. To avoid processing of same request again and again, each node maintains the list of recently seen requests and discards that particular request. "Route Maintenance" starts with the detection of broken or invalid links which cannot be use for data transfer. To reduces the packet overhead in DSR "No Beacon" and "Hello" message is incorporated [28]. DSR reduces power consumption and is also time efficient. The drawback of DSR is that it uses multihop path discovery policy to find paths, same RREQ (Route Request) is forwarded to multiple hops at the same time.

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 [11, 24]. The path discovery within the network zone uses proactive routing algorithm. Different updated paths from source to destination are available in the routing table so deliveries of packets are instant. Reactive protocols algorithm establishes paths outside the network zones by means of flooding requests. ZRP (Zone wise routing protocol) and CEDAR are an example of the hybrid protocol.

3.3.1 ZRP (Zone Wise Routing Protocol)

In ZRP, each node works within the local and outside the scope with different communication strategies. To support the larger range of communication between the different zones ZRP came into existence [31]. ZRP adapts the best features of table driven and on demand routing protocols that's why underline problems packet overhead and long waiting delays has been reduced. ZRP supports two types of communication. Routing performed with nearby nodes is done using IARP (Intra Zone Routing Protocol). It uses routing tables that stores information about all the paths within the zone in advance using proactive method [31, 32]. Due to availability of paths in the routing tables from source to destination message delivery is immediate. Communication between the farther nodes is performed by reactive method. IERP (Inter Zone Routing Protocol) handles the path creation between the different zones with the help of intermediate nodes which lies on the

Table 1 Comparison of AODV, DSR and ZRP based on protocols properties

Protocols property	Routing protocols		
	AODV	DSR	ZRP
Multicast routes	No	Yes	Yes
Loop free	Yes	Yes	Yes
Periodic broadcast	Yes	No	Yes
Unicast support	Yes	Yes	Yes
Area coverage	Small	Small	Large
Flooding of messages	No	Yes	Yes
Path creation	Hop by hop	Total sequence of hops known	Depends on local and outside zone

boundaries of each zone using reactive technique. In IERP, request can be easily reach out without searching and query the whole network. In Table 1. Based on the behavior, communication model, routing method and different characteristics of AODV, DSR protocol and ZRP routing protocols the comparative analysis is represented as follow [7].

4 Wormhole Attack

Wormhole attack is launched at the network layer. It is one of denial of service attack which can affect the performance of routing protocol on large extent. Wormhole is serious, sophisticated and hazardous type of attack which destroys the network communication [33, 34]. In wormhole attack, a pair of nodes which are remotely located far away from each other creates long range link and tunnel the information through it. An attacker node prevents legal nodes to discover legitimate path. Wormhole nodes at different locations in the network are responsible for replays of the selected packets to new locations, delay data transfer and denial of service attacks. In hidden attack, malicious nodes don't modify the packet header and its contents. Malicious nodes hide their identities in created route [21, 35]. Long range tunnel is used to transfer the data between two malicious nodes. This type of attack gives assurance to the receiver that sender is its immediate neighbor. In Exposed Attack, node doesn't modify the packet header. By making themselves part of the created path they append their identities in packet contents. The legal nodes are aware about the presence of the malicious node in the formed route but they imitate that malicious nodes are direct neighbors [21, 35, 36]. Figure 2, Illustrates, how data transfer take place in the presence of malicious nodes [37]. There are four types of wormhole attacks.

4.1 Packet Encapsulation

In this type of attack, without incremented the hop count data transfer take place between the wormhole nodes lying at the distant point using legitimate path. Packet encapsulation brings the packet into its original form.

4.2 Out of Band

In this type of attack, high transmission link is used to form the tunnel between the two wormhole nodes.

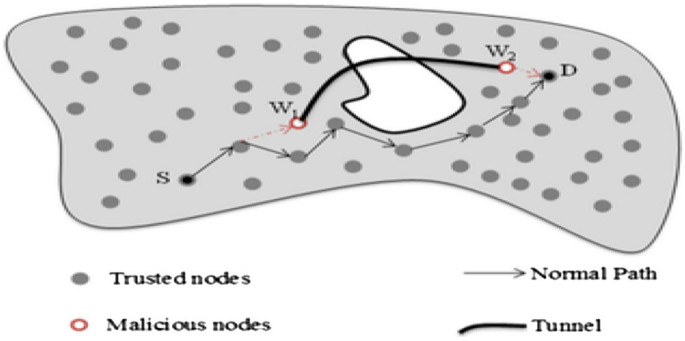

Fig. 2 The Wormhole Attack Model. http://dx.doi.org/10.1371/journal.pone.0115324.g002

4.3 High Power Transmission

In this type of attack, only one malicious node is present. Malicious nodes uses high power transmission link to extract the data toward itself.

4.4 Packet Relay

These attacks can be launched using two malicious nodes. The data transfer happens between two malicious nodes which are far located from each other. But convince other nodes they are neighbor nodes.

5 Simulation Environment

5.1 Network Model

Consider a set of sensors dispersed in a field. We make the following assumptions:

(a) All sensors are mobile, having similar capabilities and equal significance.
(b) All sensors are aware of their own residual energy.
(c) Links are symmetric, and the radio signal has identical energy attenuation in all directions.
(d) Data exchanged between two communicating sensors that are not within each other's radio range are forwarded by other sensors.
(e) All sensors are capable of operating in forwarding mode and sensing mode.

5.2 Simulation Model

The main goal of our experiment is to analysis impact of wormhole on routing protocols. Using NS2 AODV,DSR and ZRP 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 there 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. At first instance only one attacker node is used to form the attack by placing it at any location randomly within the network. The source node has some data to send, it broadcasts RREQ messages to find path to destination node. During the route reply phase, the wormhole node in the network tends to reply back to source pretending to have path to destination node. Malicious node then becomes an intermediate between source and destination. Upon receiving the data from the source node, it tends to drop the packets. 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. Long-range wireless link deploy between the colluding nodes to transfer the data.

5.3 Performance Metrics

5.3.1 Throughput

Throughput means the total number of bits transferred (b_i) over the destination in per unit time (t_i) [38, 39]. Throughput depends upon the capacity of the channel. The throughput capacity of channel is n and i represent sequence number.

$$\text{Throughput} = \frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{t_i}$$

5.3.2 Packet Delivery Ratio

Packet Delivery Ratio (PDR) is the number of packets received ($PktR_i$) over number of packet sent ($PktS_i$) [38, 39]. The more packets received by the destination node better is the performance. The packet delivery ratio of channel is n and i represent sequence number.

$$\text{Packet delivery ratio} = \frac{1}{n}\sum_{i=1}^{n}\frac{PktR_i}{PktS_i}$$

5.3.3 Packet Loss

Packet loss means total packets lost during the transmission [39]. It defines the number of packets that never reach the destination. Packet loss occurs due to congestion, disturbance and weak radio signals. It can be calculated in percentage of packet loss (L_i) over percentage of packet sent ($PktS_i$). The packet delivery ratio of channel is n and i represent sequence number.

$$\text{Packet loss} = \frac{1}{n}\sum_{i=1}^{n}\frac{L_i}{PktS_i}$$

5.3.4 Average E2E Delay

It defines the total delay (d_i) over number of packet received by destination ($PktS_i$). Average E2E delay defines the average time taken by the packets to reach the destination [38, 39]. Average E2E delay includes time like propagation, transmission, queuing, and processing delay. Performance of routing protocol is better if E2E delay is less. The average end to end delay with channel capacity is n and i represent sequence number.

$$\text{Average E2E delay} = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{PktS_i}$$

5.3.5 Jitter

It is the variation in delay of received packet. Jitter defines the difference between receiving ($PktR_i$) and sent ($PktS_i$) time of all the packets divided by the total number of

packet available ($PktN_i$) [39]. Jitter is the delay caused by the network congestion. It is also caused by long queue of packets, if there is more delay it means that particular protocol is over burdened with packet length. The jitter in channel capacity n and i represent sequence number.

$$\text{Jitter} = \frac{1}{n}\sum_{i=1}^{n}\frac{(PktR_i - PktS_i)}{PktN_i}$$

6 Performance Evaluation and Results

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 2 for simulation purpose in each routing protocols. The implementation of routing protocol is done in NS2 for the simulation purpose [12, 40]. NS2 is discrete network simulator that helps us to simulate the behavior of both type of routing protocols wired and wireless networks for both single hop and multi-hop [29]. To simulate behavior of mobile nodes the area under consideration is 1100 m × 1100 m with 50 mobile nodes [1]. Nodes are randomly placed within the square field. Transmission range of normal network is 200 and 500 m for wormhole. Random Way Point mobility model is used to randomly generate its position in given simulation area move with maximum velocity speed, after some pause time they move to new location within the square field [41]. Wormhole nodes are not neighbors in the simulation environment. The simulation parameters are used in Table 2 adapted from Kumar et al. [42].

6.1.1 Results

Figure 3 shows performance of AODV, DSR and ZRP with and without wormhole. Figure 3a shows throughput of AODV is worse than two. On the same lines, Fig. 3b. AODV exhibits more fall rate in PDR than DSR and ZRP and in Fig. 3c. AODV has maximum packet loss as compared to DSR and ZRP. This can be attributed to the fact that since AODV routing protocol would store the routes once formed, the same attacker nodes would appear in the paths saved in the cache memory. So every time the saved path is fetched to forward the data, the wormhole attackers would drop it, thereby making the

Table 2 Simulation parameters for evaluation

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

throughput, packet drops and packet delivery ratio values worse. Figure 3d shows average E2E delay which is more for ZRP than DSR and AODV. ZRP shows more delay as of the fact that the zonal head would first aggregate the data from the zonal member and then it would forward the data to the destination node located in some other zone. The aggregation at the zonal head of the source node and then dissemination by the zonal head of the destination might attribute to more end to end delays of the zonal routing protocol. Figure 3e show jitter for AODV, DSR and ZRP protocol. DSR shows more delay in the case of without wormhole because in DSR no routes are store in the cache memory. So every time source node needs to forward the data to the destination, it has to look out for the new or fresh paths to the particular destination nodes. From the Fig. 3 it can be clearly analyzed that as numbers of attacker nodes are increased the performance degrades in terms of metrics.

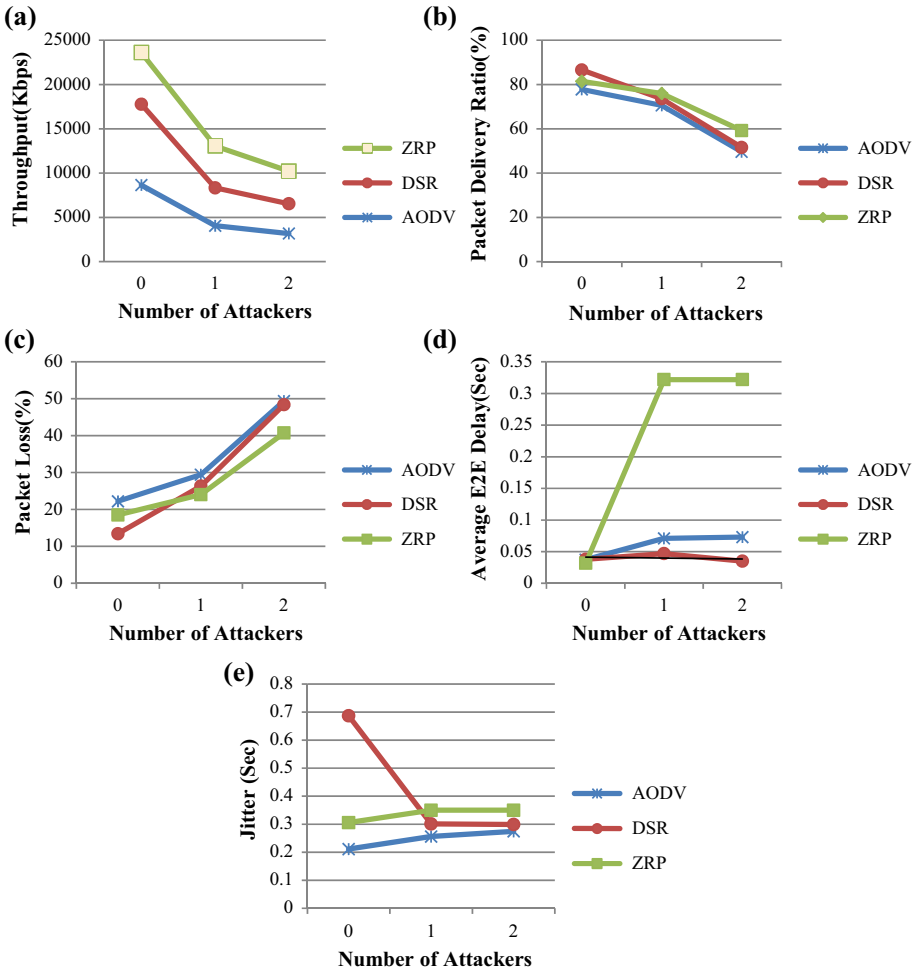

Fig. 3 Illustrates, performance evaluation for average of 50 runs with and without wormhole **a** throughput **b** packet delivery ratio **c** packet loss **d** average E2E delay **e** jitter

6.2 Analysis Based on Mobility

In this scenario, same sets of parameters are used for simulation purpose as mentioned in Table 3 with varying speed of network nodes. The performance of AODV, DSR and ZRP analyzed using the simulation. The simulation is carrying out using NS2 with mobility. The random way point model is used [4]. Nodes are moving within the define terrain range toward the destination with minimum speed 10 m/s to maximum speed of 30 m/s in any direction using random mobility model with a 0.1 m/s pause time [42]. After pause time it moves to the new destination randomly. The network consists of 50 nodes with the network area 1100 × 1100 m. The performance comparisons of different protocols are based on the values generated with and without wormhole under mobility. The simulation results are based on the output generated in the NS2.

6.2.1 Results

Simulated results are presented in Figs. 4, 5, 6, 7 and 8. They show performance trade-off in some metrics. From Figs. 4, 5 and 6, it can be concluded from results AODV performance is comparatively poor than DSR and ZRP. 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. 7. 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. ZRP demonstrates the worst performance than AODV and DSR. ZRP causes delay due to search discovery of the path out of zone; if the tunnel is created between the wormhole nodes within zones the delay become double. In Fig. 8, DSR shows more jitter than AODV and ZRP. DSR uses multihop and source initiated technique for packet transfer so data rotated is unwanted in the network that may cause jitter. AODV performance is superior for jitter than DSR and ZRP.

Table 3 Simulation parameters for evaluation

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

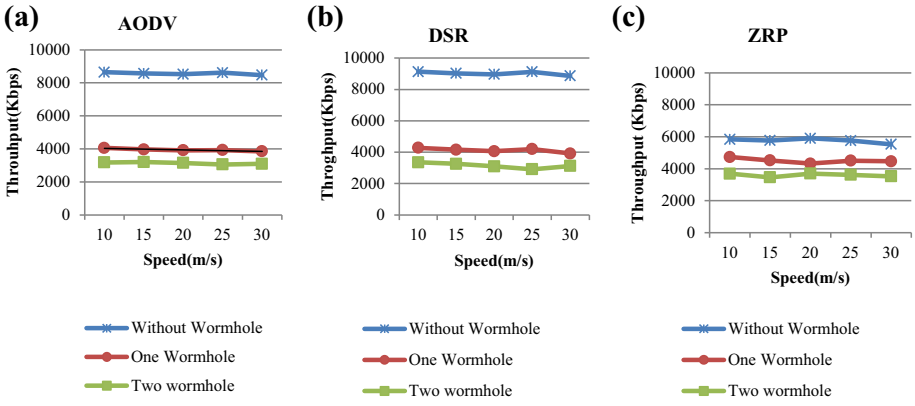

Fig. 4 Illustrates, throughput for AODV, DSR and ZRP with and without wormhole under mobility

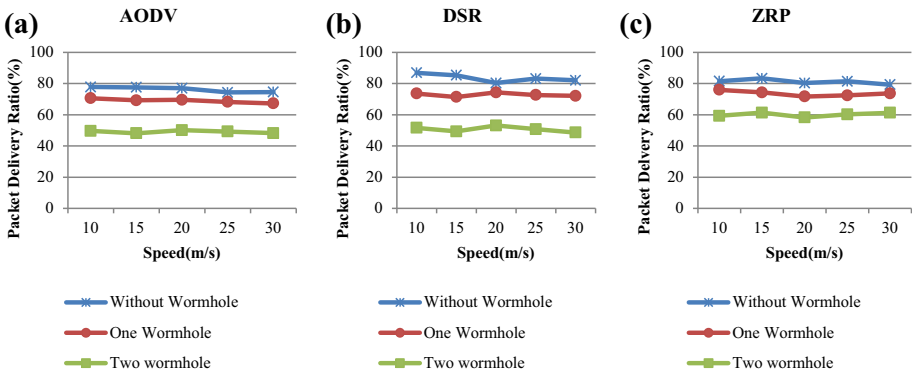

Fig. 5 Illustrates, packet delivery ratio for AODV, DSR and ZRP with and without wormhole under mobility

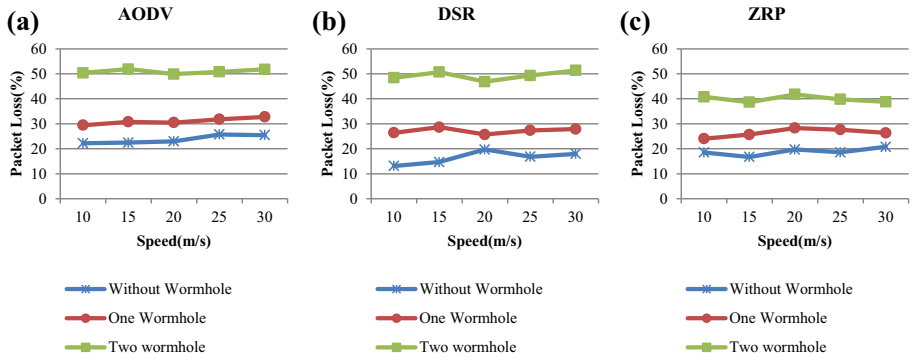

Fig. 6 Illustrates, packet loss for AODV, DSR and ZRP with and without wormhole under mobility

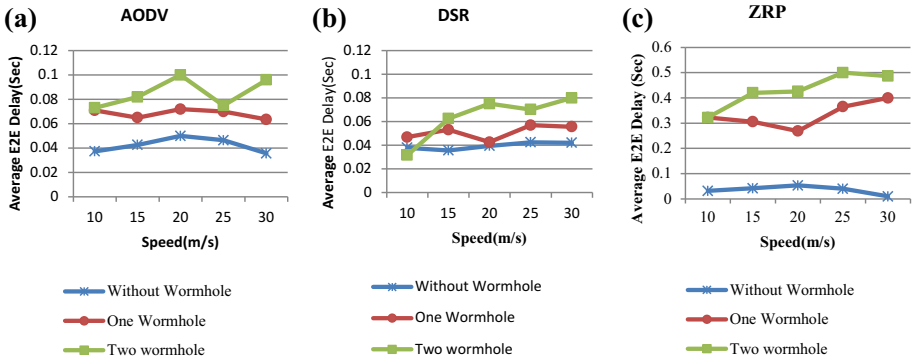

Fig. 7 Illustrates, average E2E delay for AODV,DSR and ZRP with and without wormhole under mobility

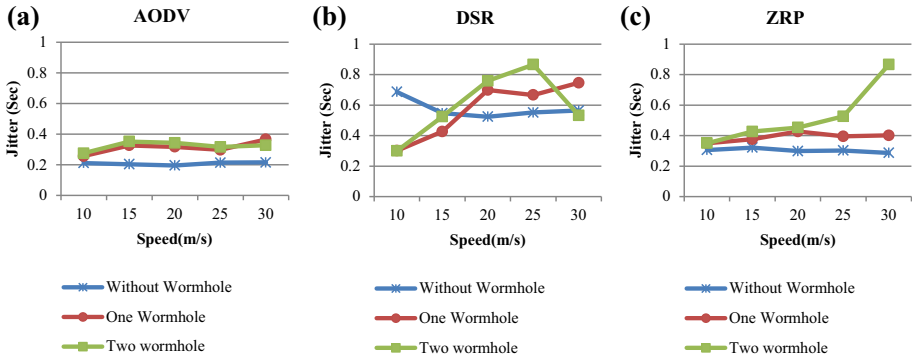

Fig. 8 Illustrates, jitter for AODV,DSR and ZRP with and without wormhole under mobility

7 Conclusion and Future Work

Performances of routing protocols depend upon several factors like number of senders, receivers and attacker nodes. The NS2 simulator provides accurate and fare values which can be used for comparison of different routing protocols. After reviewing all the above figures it can be clearly judged that the performance of AODV is more affected by the wormhole in terms of throughput, packet delivery ratio, and Packet Loss. Whereas ZRP exhibits more average end to end delay and DSR demonstrates more jitter. The simulation results in this paper clarify that if multiple attacker nodes are present in the network then the performances of the routing protocols degrade.

In our future work, simulation and comparison of different routing protocols can be performed under different types of wormhole attacks. 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.

Acknowledgements The authors are thankful to the Department of RIC, I.K.G. Punjab Technical University, Kapurthala, Punjab, India and providing me opportunity to carry out my research work.

Conflict of Interest The authors declare that there is no conflict of interest regarding the publication of this paper.

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. *IEEE 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.
10. Das, Samir R., Castañeda, Robert, & Yan, Jiangtao. (2000). Simulation-based performance evaluation of routing protocols for mobile ad hoc networks. *Mobile Networks and Applications, 5*(3), 179–189.
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. Mahajan, V., Natu, M., & Sethi, A. (2008). Analysis of wormhole intrusion attacks in MANET. In *MILCOM 2008-2008 IEEE Military Communications Conference*. IEEE.
13. 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.
14. 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.
15. Garg, G., Kaushal, S., & Sharma, A. (2014, July). Reactive protocols analysis with wormhole attack in ad-hoc networks. In *2014 International Conference on Computing, Communication and Networking Technologies (ICCCNT),* (pp. 1–7). IEEE.
16. 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*, 1.
17. 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.
18. Dong, D., Li, M., Liu, Y., Li, X. Y., & Liao, X. (2011). Topological detection on wormholes in wireless ad hoc and sensor networks. *IEEE/ACM Transactions on Networking (TON), 19*(6), 1787–1796.
19. Hu, Y-C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless networks. In *INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies* (Vol. 3). IEEE.
20. 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.
21. Chiu, H. S., & Lui, K. S. (2006). DelPHI: Wormhole detection mechanism for ad hoc wireless networks. In *2006 1st International Symposium on Wireless Pervasive Computing* (pp. 6-pp). IEEE.
22. Xu, Y., et al. (2007) Detecting wormhole attacks in wireless sensor networks. In *International Conference on Critical Infrastructure Protection*. Springer US.
23. Mbarushimana, C., & Shahrabi, A. (2007). Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In *AINAW'07 21st International Conference on Advanced Information Networking and Applications Workshops*, *2007*, (Vol. 2). IEEE.

24. Saeed, N. H., Abbod, M. F., & Al-Raweshidy, H. S. (2012). MANET routing protocols taxonomy. In *2012 International Conference on Future Communication Networks (ICFCN),* (pp. 123–128). IEEE.
25. Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc *on-demand distance vector (AODV) routing* (No. RFC 3561).
26. Chaurasia, U. K., & Singh, V. (2013). MAODV: Modified wormhole detection AODV protocol. In *2013 Sixth International Conference on Contemporary Computing (IC3),* (pp. 239–243). IEEE.
27. Kim, Seongkwan, et al. (2011). Comparative analysis of link quality metrics and routing protocols for optimal route construction in wireless mesh networks. *Ad Hoc Networks, 9*(7), 1343–1358.
28. Johnson, D. B. (2003). The dynamic source routing protocol for mobile ad hoc networks. *Draft-ietf-manet-dsr-09. Txt*.
29. 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.
30. Boukerche, Azzedine. (2004). Performance evaluation of routing protocols for ad hoc wireless networks. *Mobile Networks and Applications, 9*(4), 333–342.
31. Haas, Z. J., & Pearlman, M. R. (1997). The zone routing Protocol (ZRP) for ad hoc networks, IETF Internet Draft http://www.ietf.org/internetdrafts/ draft-ietf-manetzone-zrp- 00.txt.
32. Beijar, N. (2002). *Zone routing protocol (ZRP)* (pp. 1–12). Espoo: Networking Laboratory, Helsinki University of Technology.
33. Sharma, D., Kumar, V., & Kumar, R. (2016). Prevention of wormhole attack using identity based signature scheme in MANET, In *Computational Intelligence in Data Mining—Volume 2* (pp. 475–485), Springer India.
34. Hu, Y. C., Perrig, A., & Johnson, D. B. (2006). Wormhole attacks in wireless networks. *Selected Areas in Communications, IEEE Journal on, 24*(2), 370–380.
35. 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.
36. 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*.
37. Sookhak, M., Akhundzada, A., Sookhak, A., Eslaminejad, M., Gani, A., Khan, M. K., Li, X., & Wang, X. (2015). Geographic wormhole detection in wireless sensor networks. *PloS one, 10*(1), e0115324.
38. Mohapatra, S., & Kanungo, P. (2012). Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 simulator. *Procedia Engineering, 30,* 69–76.
39. 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.
40. Issariyakul, T., & Hossain, E. (2011). *Introduction to network simulator NS2*. Berlin: Springer.
41. Bettstetter, C., Hartenstein, H., & Pérez-Costa, X. (2002). Stochastic properties of the random waypoint mobility model: Epoch length, direction distribution, and cell change rate. In *Proceedings of the 5th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems*, ACM.
42. 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.

Parvinder Kaur received the Master Degree in Computer Application from Amritsar College of Engineering and Technology, Amritsar in 2010 and pursuing Ph.D. in Computer Application as Research Scholar from Department of Research, Innovation and Consultancy, Punjab Technical University, Jalandhar, Punjab, India. Area of interests are wireless networks and mobile computing.

Dr. Dalveer Kaur received her Ph.D. in Electronic Engineering from Guru Nanak Dev University, Amritsar, Punjab, India in 2010. She is an Assistant Professor, Department of Electronics & Communication Engineering at the Punjab Technical University, PIT University Campus, Jalandhar-Kapurthala Highway, Punjab, India. She has published no. of research papers in national national/international conferences and journals.

Dr. Rajiv Mahajan is currently working as Director–Principal Golden College of Engineering & Technology, Gurdaspur, Punjab, india. His area of specialization is data communication and network security. He has worked as a professor and vice-principal Global institute of Management & Technology, Amritsar, Punjab and as Director-Principal in CT institutes shahpur, Jalandhar, Punjab. He has published no. of research papers in national/international journals and conferences. He is also associated with journals and conferences as an editorial board member and reviewer.