Evaluation of Traffic Models under Multiple Black hole Attack in Wireless Mesh Network

Pushpender Sarao
Sharad Institute of Technology College of Engineering, Ichalkaranji, India
Email: drpushpendersarao@gmail.com

***Abstract*—Wireless networks are the networks in which data communication is done through the wireless channels and wireless nodes. In such type of the networks, cooperation of the all nodes is required. Due to which, chances of security attacks is possible and network performance and security is badly affected. Black hole attack is a security attack comes under the active, internal as well as external attacks. In black hole attack, malicious node presents a suitable, shortest and low cost path. If the above path is selected for data transmission, malicious node drops the received packets and as a result performance of the network is degraded. In this paper, impact of Random Direction (RD) and Reference Point Group Mobility (RPGM) models have been analyzed for wireless mesh network in the presence of multiple black hole attacks. By varying the number of network connections and node density, (Ad hoc on demand distance vector) AODV routing protocol is evaluated. Normalized routing load, average end to end delay, average throughput, and total number of packets received are considered as performance metrics. Bonn-motion tool has been used to create the scenario of mobility models. In the presence of black hole attack, and under RPGM mobility model, AODV routing protocol presents better results in respect of average throughput, normalized routing load. Simulation work has been carried out on network simulator version NS-2.35.**

***Keywords*—Random direction, reference pint group mobility, black hole attack, throughput, normalized routing load**

I. Introduction

Wireless mesh networks are the networks in which wireless nodes can communicate to each and every node directly and indirectly. Mostly military applications have been developed through wireless mesh network. In such type of network, router works as the connecting device as well as access point. Due to large network and expectation of cooperation of the nodes during the communication, possibility of attacks is possible. Security attacks can be classified into two categories-active attacks and passive attacks. Active attacks can be further classified into two categories-internal attacks and external attacks. In internal attack, attack belong to same domain while in external attack, attacker does not belong to same domain. In passive attack, message content will not be changed while in active attack, message contents will be changed i.e. packet modification is possible. In passive attack, information collection about path, source node, and destination node has been done. Wormhole attack and black hole attack are the two main network layer security attacks which directly affects the performance of the network and dangerous to the network security. In wormhole attack, attacker receives packets at one location in the networks and tunnels where the above packets are resent into the network. Due to the wormhole attack two things happened in the network-delay in the packet delivery and failure to find the valid route. Wormhole attack can be launched without the knowledge of the network. Black hole attack is another very important network layer attack. A malicious node falsely advertises well shortest and low cost path to the destination node during the path-finding process. Packets are dropped by malicious nodes. Black hole attack comes under the active attack and DoS (Denial of Service) attack. In this attack, performance of the network is badly affected. In this paper, we have performed simulation based study to analyze the impact of mobility models (random direction mobility model and reference point group mobility model) [1, 2] on the performance of mobile ad hoc networks (in the presence of multiple black hole attacks). Routing protocol for this study is considered as (ad hoc on demand distance vector routing) AODV [3].

The mobility parameters manly introduce us about the mobility patterns in different network scenarios.

Networks attacks directly degrade the performance of a network [4]. Black hole attack is one of the network attack due to which number of packets are lost on the way and not reachable at the destination [5]. Performance of a protocol is also depends upon the node mobility i.e. type of mobility model has been applied in the network. Different mobility models have their own characteristics in different networks.

Rest of the this research work is organized as follows: Section II presents about the related work of impact of black hole attack with respect to network performance. Research methodology and simulation generating parameters have elaborated in Section III. In Section IV, results and evaluation process have been mentioned by using tables and graphs as different network scenarios. This paper has been concluded in Section V.

Manuscript received August 15, 2022; revised September 28, 2022; accepted February 1, 2023.

II. Related Work

In literature, effect of black hole attack has been already analyzed for AODV routing protocol [6-9]. Most of the work is simulated in one mobility model. No work has been conducted with simultaneously in two mobility models.

In this work, effect of multiple black hole attack has been simulated for two mobility models and at the same time performance is been observed.

Barinderpal singh and kulbir kaur evaluated the AODV routing protocol under black hole by varying the number of packets, and performance metrics like packet delivery ratio, throughput and delay, protocol is analysed under black hole attack in mobile ad hoc network [10]. Simulation work was conducted in network simulator NS-2.35 environment by using different models like mode model, deployment model, mobility model, and radio model. It has been observed that in the presence of black hole attack, performance of AODV is degraded. As the packet size is increased, the throughput of the network is degraded.

In [11], fuzzy based intrusion detection system to detect the black hole attack has been proposed by Mohammed Abdel Azim in mobile ad-hoc network. Forward packet ratio and average destination sequence number parameters were taken as input for fuzzy based system to detect the black hole attack. Total nine fuzzy rules were designed for the system. The proposed system has the number of modules like extraction of the fuzzy based parameters module, fuzzy inference module, fuzzy decision module and response module. The proposed system is verified and evaluated in a network simulator OMNET ++. Evaluation parameters were considered as packet delivery ratio, routing overhead. It was claimed that proposed optimal system has good detection ability in terms of black hole attack.

In [12], effect of black hole attack in the performance of OLSR (optimized link state routing) has been evaluated in different mobility model scenarios (random way point mobility model and constant waypoint mobility model). The performance metrics were considered as throughput and number of packets received. It was claimed that OLSR produces better results for random waypoint mobility model in the presence of black hole attack.

In [13], performance of MANET is evaluated in the presence of black hole attack. Also features and vulnerability issues in MANET has been discussed by the authors. AODV routing protocol is analyzed with and without black hole attack. Simulation work was carried out in the network simulator NS-2.35. Packet loss metric was considered as main metric for evaluation of the network. It was observed that packet loss percentage has been increased with respect to number of black hole attacks. Black hole attack will degrade the performance of the network.

Sharma Hitesh Omprakash *et al*. has analysed the impact of black hole attack in the random mobility model for mobile ad hoc network [14]. AODV routing protocol was simulated in the network simulated NS-2.35 environment for mobile ad hoc network. The main performance parameters were considered as: throughput, packet delivery ratio, packet dropping ratio, routing overhead in the single network traffic connection as well as multiple network traffic connections. Mobility model was considered as random mobility model. It was concluded that multiple network traffic connections reduce the effect of black hole attack in terms of dropping packets ratio.

By considering the AODV and AOMDV routing protocols, impact of RPGM (Reference Point Group Mobility) model has been studied in vehicular ad-hoc network (VANET)[15]. Node density is taken as main performance parameter to evaluate the network. By varying the node density and constituting the group size as 5, throughput, end to end delay and normalized routing overhead was calculated.

Simulation environment was generated by using the network simulator NS-2.34 for VANET (Vehicular Ad hoc Network). It was claimed that AOMDV (Ad-hoc on – demand Multipath Distance Vector) routing protocol works well as the node density is going to higher levels. Also in terms of throughput and normalized routing overhead, performance of AOMDV is better than AODV routing protocol.

In [16], Megat Zuhari *et al*. analysed the efficiency of mobile ad-hoc network in terms of various mobility models like gauss Markov mobility model, reference point group mobility model and Manhattan mobility model. Brief overview of three mobility models has been described. To investigate the performance the performance of mobile ad-hoc network, AODV routing protocol has been used. Simulation work was carried out by using network simulator NS-2. By varying the speed of nodes and by using performance of the protocol has been observed. The performance parameters are considered as: number of unidirectional links, average route request packets sent, transmission range, probability of link connectivity, probability of route connectivity. Simulation results visualized the impact of mobility models on the performance of AODV routing protocol.

III. Research Methodology

By generating two network scenarios (by varying the number of connections and number of nodes), simulation work was planned for two mobility models. Detailed simulation parameters and their respective values are mentioned in Table I.

Simulation setup:

Table I. Simulation Parameters

Simulator Version	NS 2.35
Mobility Models	Random Direction, Reference Point Group Mobility
Simulation time	100s
No. of Connections	5,10,15,20,25,30,35,40
No. of Nodes	40,50,60
Network attack	Multiple Black hole Attack
MAC type	802.11
interface queue type	PriQueue

antenna model	Omni Antenna
max packet in ifq	100
Routing Protocol	AODV
dimension of topography	316×303, 315×318,
Max. Speed	20m/s
Traffic connection type	TCP
TCP-Packet size	512 bytes
Initial Energy	50 J
txPower	0.75 V
rxPower	0.25 V
Idle Power	0.04 V

In this research work, simulation work has been carried out in two different scenarios:

Scenario-*I:* By varying the number of connections (5-40 traffic connections)

*RPGM(*Reference *Point Group Mobility)-Connections:*

TCP traffic connections 5,10,15,20,25,30,35 and 40 are considered with mobility model as RPGM. Packet size is taken as 512 bytes for all the TCP connections. MAC protocol is taken as 802.11. Network topology size is created as 316m×303m for maximum 60 numbers of mobile nodes having maximum speed as 20m/s. simulation time is carried out as 100 seconds. All the energy parameters are taken as described in Table I. For all simulations, three black hole nodes (node number 10, 20, 30) have been introduced to evaluate the performance of the network.

*RD(*Random *Direction)-Connections:*

By varying the TCP traffic connections as 5, 10, 15, 20, 25, 30, 35, and 40 for 60 mobile nodes (having max. speed as 20m/s) network scenario has been generated. Topology size as 316m×303m is taken for the above scenario with simulation time as 100 seconds. Three malicious nodes have been introduced. Remaining parameters are taken as per Table I.

Scenario-II: By varying the number of nodes (40-60 nodes)

RPGM(Reference Point Group Mobility)-Nodes:

By varying the nodes (40, 50, and 60) and considering the mobility model as RPGM, network scenario has been generated. Maximum speed of nodes is taken as 20m/s. two TCP traffic connections has been generated with packet size as 512 bytes. Network topology size is taken as 315m×318m. routing protocol for evaluation purpose is taken as AODV. Energy parameters are settled as per Table I.

RD-Nodes:

By varying the nodes (40-60) and network topology size as 315m×318m network scenario has been created. Maximum simulation time is taken as 100 seconds by considering maximum speed of nodes as 20m/s. Two TCP (Transmission Control Protocol) connections have been established with packet size as 512 bytes. Three black hole nodes have been introduced in the network.

In both the scenarios, traffic connection is TCP type. Performance of AODV is evaluated with and without black hole attacks. Three black hole nodes have been introduced for each scenario. Random direction and reference point group mobility models have been used for the movement of thee nodes in the simulation work.

Average throughput, average end to end delay, normalized routing load, and total number of packets are the metrics which have been used to evaluate the network performance.

IV. Results and Discussions

As simulation work was carried out on network simulator NS-2.35 and result has been recorded in tabular forms. In this section visualization of the simulation result is presented as discussed below:

Varying the connections:

Connections versus Average E2E(End to End) Delay:

TABLE II. CONNECTION VS AVERAGE E2E DELAY

Connections	Average E2E Delay[milliseconds]			
	RD (Random Direction)	RD(Random Direction)-Black hole	RPGM (Reference Point Group Mobility)	RPGM (Reference Point Group Mobility)-Black hole
5	268.564	281.396	284.404	242.08
10	305.293	201.783	322.02	153.914
15	330.371	80.2182	350.072	25.64
20	457.902	174.978	437.064	101.166
25	795.477	125.612	813.784	371.067
30	837.251	320.049	836.369	217.804
35	849.984	236.672	949.57	240.098
40	1056.54	221.414	1063.93	372.275
Total	4902.382	1642.122	5057.213	1724.044
Average	612.798	205.265	632.151	215.5055

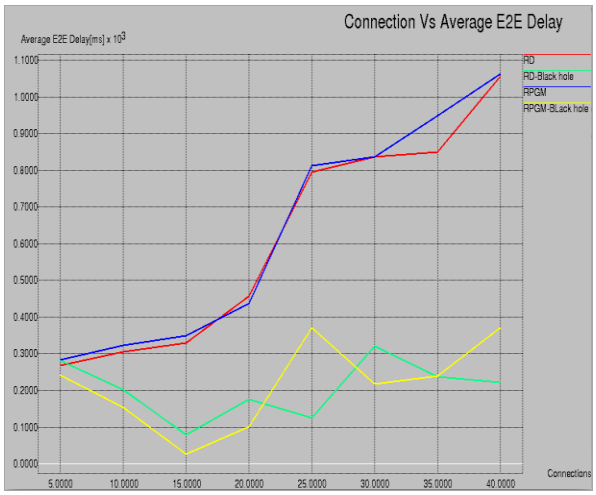

Figure 1. Connection Vs average E2E delay

Average E2E(End to End) delay for AODV is visualized in Fig. 1 by varying the number of traffic connections (5-40 connections). RD and RPGM traffic models have been compared with and without black hole attack (see Table II). In case of RD model, as the connections are increased, average E2E delay is also increased. In the presence of black hole attack, average

end to end delay is very less in respect of connections. This is because of maximum packets have been lost on the way during communication.

In case of RPGM model, as the connections are increased, the average E2E delay is also increased. While in the presence of black hole attack, average E2E delay is decreased for all the connections. In the presence of black hole attack, average E2E delay for RD model is 2,055.265 ms while it is 215.50 in case of RPGM model. Connections versus normalized routing load:

TABLE III. CONNECTION VS NORMALIZED ROUTING LOAD

Connections	NRL(Normalized Routing Load[%]			
	RD (Random Direction)	RD(Random Direction)-Black hole	RPGM (Reference Point Group Mobility)	RPGM (Reference Point Group Mobility)-Black hole
5	0.022	0.16	0.022	0.172
10	0.052	0.066	0.046	0.112
15	0.102	0.439	0.089	0.09
20	0.233	0.103	0.116	0.12
25	0.303	0.708	0.236	0.276
30	0.317	0.457	0.233	0.309
35	0.458	0.4759	0.478	0.359
40	0.59	0.644	0.458	0.368
Total	2.077	3.0529	1.678	1.806
Average	0.259	0.3816	0.2097	0.22575

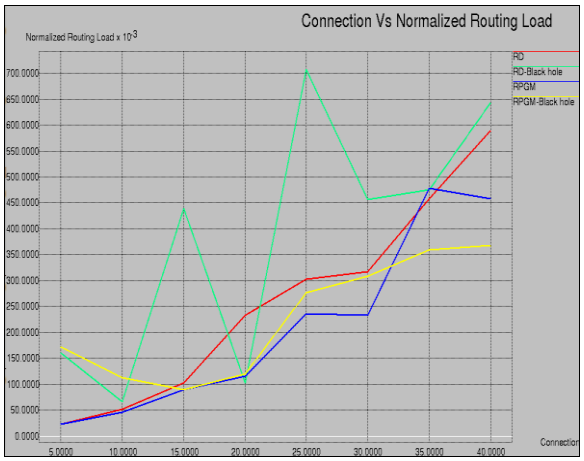

Figure 2. Connection Vs NRL.

As shown in Fig. 2, normalized routing load is presented with respect to number of connections. In case of RD model, as the traffic connections are increased, the NRL is also increasing. In the presence of black hole attack, NRL is varying as the number of connections is increased.

In case of RPGM model, from traffic connections 5 to 25, NRL is respectively increasing, but suddenly, it is varying from 30-40 connections. In the presence of black hole attack, from 5-20 connections, NRL is varying while traffic connections 25 to 40, it is regularly increasing (see Table III).

Overall average NRL for RD is 2.077 while it is 1.678 in case of RPGM traffic model. In a different network scenario, in the presence of black hole attack, average NRL for RD model is 0.3816 while in the presence of black hole attack, it is 0.2257 for RPGM traffic model. Connections versus packet received:

TABLE IV. CONNECTION VS PACKET RECEIVED

Connections	Packet Received			
	RD (Random Direction)	RD(Random Direction)-Black hole	RPGM (Random Direction)	RPGM (Random Direction)-Black hole
5	21746	5221	21806	4848
10	23272	18115	23265	12921
15	21111	4101	21418	2
20	13344	15111	14298	14988
25	21327	6562	21858	14322
30	22361	10210	22129	13957
35	19057	1250	17223	17384
40	18460	11557	778	20043
Total	160678	72127	142775	98465
Average	20084.5	9015.875	17846.875	12308.125

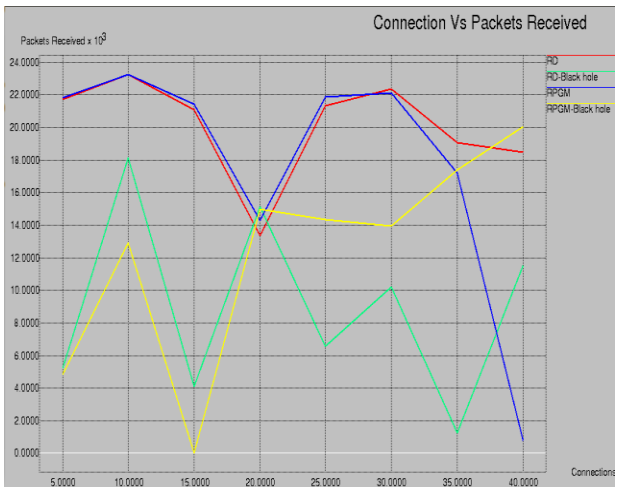

Figure 3. Connection Vs packet received.

Packet received with respect to number of connections is shown in Fig. 3. Packets received are presented with and without presence of black hole attack for RD and RPGM traffic models from 5 to 40 connections. Numbers of packets are varying as the numbers of connections are varying. In the presence of black hole attack, numbers of packets received are less for network connections (5-40 connections). Black hole attack degrades the performance of network, hence numbers of packets received have been reduced.

In case of RPGM traffic model, as the number of traffic connections are varying, the received packets are also varying (Table IV); same case is repeated in the presence of black hole attack. Performance of network is degraded by the black hole attack; numbers of received packets are very less. As the numbers of connections are varying, received packets are also varying, but with degraded performance.

Overall average packet received for RD model is 20,084 while it is 17,847 for RPGM traffic model. In the

presence of black hole attack, performance of network is very poor for both the traffic models i.e. RD and RPGM models. Received packets for RD model in presence of black hole attack are 9,016 while it is 12,308 for the RPGM traffic model. RPGM model works ell as compared to RD model in the presence of black hole attack as numbers of received packets are more as compared to RD model.

Connections versus Average throughput:

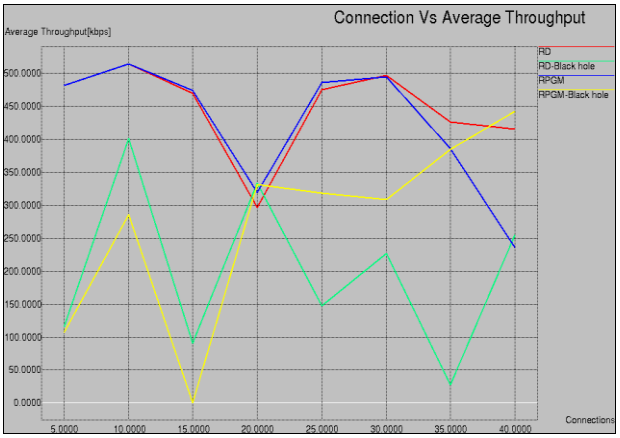

Figure 4. Connection Vs average throughput

TABLE V. CONNECTIONS VS AVERAGE THROUGHPUT

Connections	Average Throughput[kbps]			
	RD (Random Direction)	RD(Random Direction)-Black hole	RPGM (Random Direction)	RPGM (Random Direction)-Black hole
5	481.43	115.92	482.32	107.53
10	514.87	400.74	514.47	285.45
15	469.82	90.59	474.16	0
20	297.03	334.09	319.51	331.34
25	475.63	147.07	486.68	318.28
30	496.89	227.01	494.6	308.2
35	426.52	27.21	386.19	384.63
40	415.02	255.62	235.34	442.71
Total	3,577.21	1,598.25	3,393.27	2,178.14
Average	447.151	199.78	424.158	272.2675

Average throughput with respect to number of traffic connections is evaluated for AODV routing protocol in the presence of RD model and RPGM models (as shown in Fig. 4). In case of RD model, as the number of connections are varying, average throughput is also varying. In the presence of black hole attack, same case is repeating i.e. average throughput is varying. Performance of average throughput is degraded as the numbers of connections are varying (5-40 connections).

In case of RPGM model, as the connections are varying, average throughput is also varying. In the presence of black hole attack, from 5-25 traffic connections, average throughput is also varying. But suddenly, as the traffic connections 30-40, average throughput is also increased regularly. It is lowest for 15 connections while at 40 connections, it is highest (Table V).

Overall average throughput for RD model is 447.15 kbps while for RPGM model, it is 424.16 kbps. in the presence of black hole attack, average throughput for RD model is 199.78 kbps while it is 272.27 kbps in case of RPGM model. RPGM model works well in respect of average throughput as compared to RD model in the presence of black hole attack.

Varying the number of nodes: At different node densities with respect to other performance parameters, simulation work has been implemented. Detailed work has been elaborated as below:

Nodes versus Average E2E Delay: By varying the node density in respect to the average end to end delay simulation work as carried out and results has been depicted in a tabular form as shown below:

TABLE VI. NODES VS AVERAGE E2E DELAY

Nodes	Average E2E Delay[ms]			
	RD (Random Direction)	RD (Random Direction) -Black hole	RPGM (Random Direction)	RPGM (Random Direction)-Black hole
40	17.672	30.821	19.06775	119.958
50	22.1846	133.662	230.948	163.788
60	52.2495	60.4738	16.1922	77.6599
Total	92.1061	224.956	266.2079	361.4059
Average	30.70	74.98	88.7359	120.468

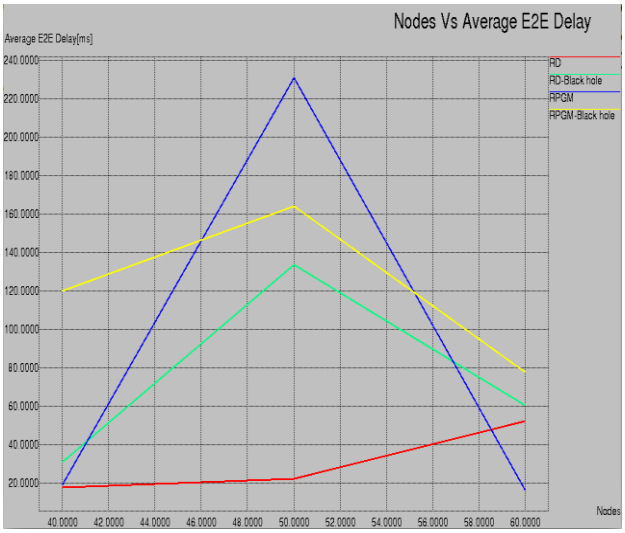

Figure 5. Nodes Vs average E2E delay.

As shown in Fig. 5, average end to end delay with respect to node density is evaluated. In case of RD model, as the number of nodes are increased, average E2E delay is varying. In the presence of black hole attack, average E2E delay is also varying.

In case of RPGM model, average E2E delay is varying as the node density is varying. In the presence of black hole attack, as the node density is varying, average E2E delay is also varying.

Overall average E2E delay for RD model is 30.70 ms while it is 88.736 ms in case of RPGM model. In the presence of black hole attack, average E2E delay for RD model is 224.956 ms while for RPGM model it is 361.406 ms (See Table VI).

Performance of RD model is better as compared to RPGM model, in respect of average E2E delay with and without presence of black hole attack.

Nodes versus normalized routing load: normalized routing load has been analyzed in terms of node densities. The results have been recorded in tabular form as depicted in Table VII.

TABLE VII. NODES VS NORMALIZED ROUTING LOAD

Nodes	Normalized Routing Load[%]			
	RD (Random Direction)	RD (Random Direction)-Black hole	RPGM (Random Direction)	RPGM (Random Direction)-Black hole
40	0.010	40 .010	0.010	0.386
50	0.021	50 .911	0.103	0.063
60	0.116	60 .062	0.010	0 .073
Total	0.147	150.983	0.123	0.522
Average	0.049	50.327	0.041	0.1774

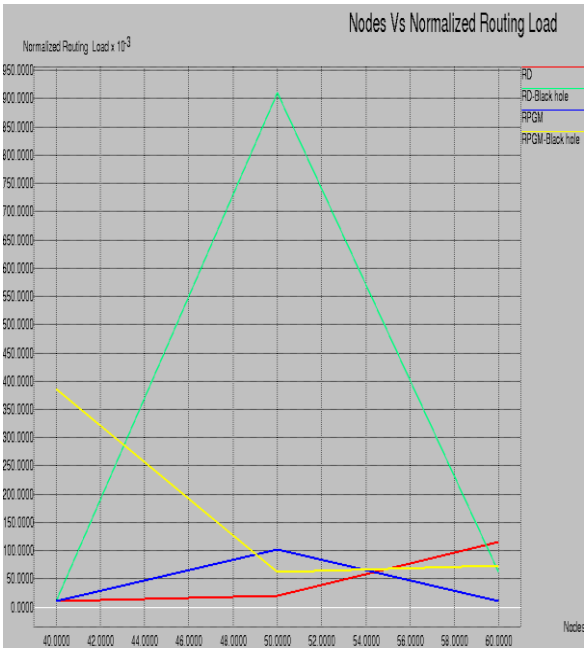

Figure 6. Nodes Vs NRL.

Normalized routing load is presented through the graph (See Fig. 6) with respect to node density. In case of RD model, as the node density is increased, NRL is also increased respectively. In the presence of black hole attack, same case is repeated i.e. normalized routing load is increasing.

In case of RPGM model, normalized routing load is fluctuating as the node density is varying. In the presence of black hole attack, from node density 50-60, normalized routing load is increased. It is lowest at node density 50 while at node density 60, it is highest.

Overall average normalized routing load for RD model is 0.049 while it is 0.041 in case of RPGM model. In presence of black hole attack, normalized routing load for RD model is 50.327 while in case of RPGM model, it is 0.1774(as shown in Table VII).

RPGM model works well in respect of RPGM node density (as compared to RD model) in the presence of black hole attack.

Nodes versus packet received:

Packet received with respect to node density is presented in figure. In case of RD model, as the node density is increased, packet received is decreased respectively. In the presence of black hole attack, packet received is fluctuating (as shown in Fig. 7).

In case of RPGM model, received packets fluctuating as the node density is varying. In the presence of black hole attack, as the node density is increased, received packets also increased.

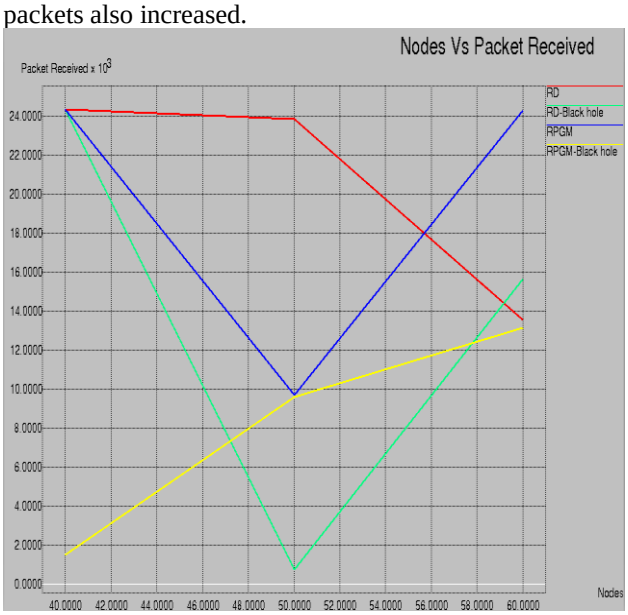

Figure 7. Nodes Vs packet received.

TABLE VIII. NODES VS PACKET RECEIVED

Nodes	Packet Received			
	RD (Random Direction)	RD (Random Direction) -Black hole	RPGM (Random Direction)	RPGM (Random Direction) -Black hole
40	24,374	24,337	24,334	1,470
50	23,847	712	9,694	9,579
60	13,531	15,642	24,327	13,142
Total	61,752	40,691	58,355	24,191
Average	20,584	13,563.66	19,451.66	8,063.66

Overall average received packets for RD model is 20,584 while it is 19,452 in case of RPGM model. In the presence of black hole attack, received packets for RD model is 13,564 while in case of RPGM model, it is 8,064 (See Table VIII).

Performance of RD model is better in respect of received packets in the presence of black hole attack.

Nodes versus average throughput:

Average throughput with respect to node density is presented in Fig. 8. In case of RD model, as node density is increased, average throughput is decreased. It is highest at node density 40 while at node density 60, it is lowest. In the presence of black hole attack, average throughput is fluctuating as the node density is varying.

In case of RPGM model, as the node density is increased, average throughput is fluctuating. In the presence of black hole attack, average throughput is increasing as the node density is increased.

Overall average throughput for RD model is 455.47 kbps while it is 347.72 kbps in case of RPGM model. In the presence of black hole attack, average throughput for RD model is 300.296 kbps while in case of RPGM model; it is 18.24 kbps (as shown in Table IX).

RD model works better (As compared to RPGM model) in respect to average throughput with and without black hole attack.

TABLE IX. NODES VS AVERAGE THROUGHPUT

Nodes	**Average Throughput[kbps]**			
	RD (Random Direction)	**RD (Random Direction) -Black hole**	**RPGM** (Random Direction)	**RPGM** (Random Direction) **-Black hole**
40	538.95	538.17	538.05	32.59
50	527.30	15.86	214.71	211.74
60	300.16	346.86	290.40	290.40
Total	1,366.41	900.89	1,043.16	534.73
Average	455.47	300.2966	347.72	178.2433

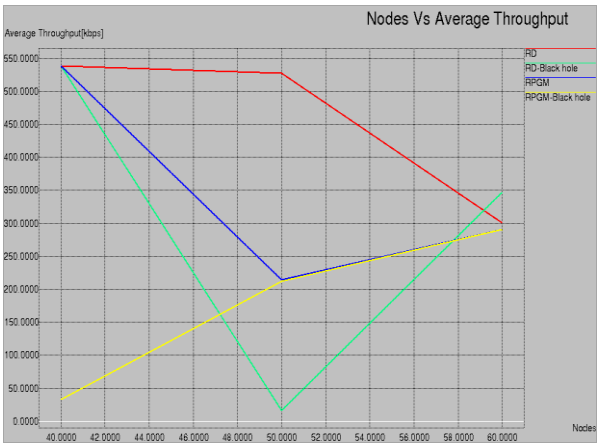

Figure 8. Nodes Vs average throughput.

V. CONCLUSION

In the presence of multiple black hole attack and two mobility models (Random Direction model and Reference Point Group Mobility model), and AODV routing protocol has been evaluated.

For RPGM mobility model, in the presence of black hole attack, E2E delay is decreased with respect to connections. In the above scenario, RPGM works well as compared to RD model. Overall average normalized routing load with respect to connections, in the presence of black hole attack, performance of RPGM model is better as compared to RD model. In case of connections versus, received packets scenario, RPGM model works well as compared to RD model. In the scenario, connection versus average throughput, in the presence of black hole attack, RPGGM model has better performance in terms of average throughput as compared to RD model. In the scenario, a node versus average throughput (in the presence of black hole attack), performance of RD model is excellence. In the scenario, nodes versus normalized routing load, (in the presence of black hole attack) RPGM model shows better results as compared to RD model. In the scenario nodes versus packet received (in the presence of black hole attack) RD model have better results as compared to RPGM model. In the scenario, nodes versus average throughput, RD model shows better performance as compared to RPGM model. In the presence of RPGM mobility model, AODV routing protocol works well and at the same time effect of malicious nodes on the performance of network is less as compare to random direction model.

CONFLICT OF INTEREST

The author declares no conflict of interest.

AUTHOR CONTRIBUTIONS

Corresponding author has conducted the all research work and observation has been recorded by him. Graphs and result discussion also has been carried out by same author. Final version of this work is approved by the corresponding author.

REFERENCES

[1] G. Jayakumar and G. Ganapathi, "Reference point group mobility and random waypoint models in performance evaluation of MANET routing protocols," *Journal of Computer Networks and Communications*, vol. 2008, p. 10, 2008.

[2] R. R. Roy, "Reference point group mobility," in *Handbook of Mobile Ad Hoc Networks for Mobility Models*, Springer, Boston, MA, 2011.

[3] Perkins, *et al*. "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003.

[4] Pooja and R. K. Chauhan, "An assessment based approach to detect black hole attack in MANET," in *Proc. International Conference on Computing, Communication & Automation*, 2015, pp. 552-557, doi: 10.1109/CCAA.2015.7148439

[5] F. H. Tseng, L. D. Chou, and H. C.Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Hum. Cent. Comput. Inf. Sci.*, 2011.

[6] E. E. Khin and T. Phyu, "Impact of black hole attack on aodv routing protocol," *International Journal of Information Technology, Modeling and Computing*, vol. 2, no. 2, pp. 9-17, May 2014, doi: 10.5121/ijitmc.2014.2202

[7] F. Mohammed, O. Mohamed, and E. Abdellah, "The impact of black-hole attack on AODV protocol," *International Journal of Advanced Computer Science and Applications, Special Issue on Advances in Vehicular Ad Hoc Networking and Applications*, 2014.

[8] A. K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks," in *Proc. International Conference on Pervasive Computing*, 2015, pp. 1-6, doi: 10.1109/PERVASIVE.2015.7087174.

[9] R. Chaudhary and P. R. Ragiri, "Implementation and analysis of blackhole attack in AODV routing protocol," in *Proc. Second International Conference on Information and Communication Technology for Competitive StrategiesMarch*, 2016, pp. 1–5, https://doi.org/10.1145/2905055.2905172

[10] B. Singh1 and K. Kaur, "Effect of black hole attack on the performance of AODV routing protocol under different traffic conditions in mobile AdHoc networks," *International Journal of Advanced Science and Technology*, vol. 115, 2018, pp. 11-22, http://dx.doi.org/10.14257/ijast.2018.115.02

[11] M. Abdel-Azim, H. El-Din Salah, and M. Ibrahim, "Black hole attack detection using fuzzy based IDS," *International Journal of Communication Networks and Information Security*, vol. 9, no. 2, pp. 187-195, August 2017.
[12] A. Nabou, M. D. Laanaoui, and M. Ouzzif, "Effect of black hole attack in different mobility models of MANET using OLSR protocol," *International Journal of Information and Computer Security*, vol. 18, no. 1-2, May 12, pp 219-235, 2022, doi:10.1504/IJICS.2022.10041136
[13] M. Elboukhari, M. Azizi, and A. Azizi, "Impact analysis of black hole attacks on mobile ad hoc networks performance," *International Journal of Grid Computing & Applications*, vol. 6, no. 1-2, June 2015.
[14] S. H. Omprakash and M. K. Suthar, "Implementation of black hole attack for random mobility for single and multiple connection in MANET," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 3, pp. 3299-3302, January 2020, doi: 10.35940/ijitee.C9035.019320
[15] R. S. Al-Qassas, "Routing and the impact of group mobility model in VANETs," *Journal of Computer Sciences*, vol. 12, no. (4), pp. 223-231, 2016, doi: 10.3844/jcssp.2016.223.231
[16] M. Zuhairi, H. Zafar, and D. Harle, "The impact of mobility models on the performance of mobile ad hoc network routing protocol," *IETE Technical Review*, vol. 29, no. 5, pp. 414-420, Sep-Oct 2012, doi: 10.4103/0256-4602.103175

Pushpender Sarao was born in Haryana, India. He received the PhD degree from Shri Venkateshwara University, India, in 2016 and the M.Tech degree from the Maharshi Dayanand University, Rohtak, India, in 2012. He is currently working as the professor and head, department of CSE, Sharad Institute of Technology College of Engineering, Ichalkaranji, Maharashtra, India. His research interests include wireless networks, data science, routing protocols, and wireless sensor networks.