Performance Analysis of MANET under Security Attacks

Pushpender Sarao
Sharad Institute of Technology College of Engineering, Ichalkaranji-416121, Maharashtra, India
Email: drpushpendersarao@gmail.com

Abstract—In Mobile Ad hoc Network (MANET), performance of the routing protocols is degraded by various network attacks such as black hole attack and rushing attack. Mostly all layers of mobile ad hoc networks are vulnerable to several attacks. Routing protocols used in mobile ad hoc networks are designed by considering that all the nodes are trustable in communication mode. MANET is less secure network due to its features like no centralized administration control and no infrastructure is required. In this paper, Ad hoc On Demand distance Vector (AODV) routing protocol is evaluated under rushing attack, black hole attack, and grayhole attack. Under multiple attacking, single attacking, and without attacking modes, performance of network has been evaluated. By varying the speed, network size, node density, and number of attacking nodes, four different network scenarios have been generated. Performance metrics are considered as average throughput, average end to end delay and packet delivery ratio. Network simulator 2 is used to simulate the attacks over AODV routing protocol. Results show that all the above attacks are responsible for the poor throughput, heavy dropping packets and higher end to end delays in the network. Throughput is degraded as the numbers of attacking nodes are increased. AODV is less affected by rushing attack as compared to black hole and grayhole attacks.

Index Terms—Network attacks, rushing attack, grayhole attack, black hole attack, packet delivery ratio, average E2E delay, malicious node, active attacks

I. Introduction

MANETs [1] refers to mobile ad hoc networks in which there is no need of infrastructure and centralized control system. MANET has so many features such as: self-organizing, decentralized, self-configured, ad-hoc in nature, nodes in the network can freely move to establish a link. MANET was initially developed for military operations and some other rescue operations. Nowadays, it is very popular due to its low space requirement, less time to deployment, low installation cost, less infrastructure requirements, and its various applications in data communication. Network topology is dynamic i.e. topology is certainly changed as nodes in the network changes their speeds. Nodes in the network are movable and are free to join and leave the network. All nodes are connecting with a wireless link and can communicate to each other directly. Each node acts as a host as well as router and can receive or send messages to its neighbours. Link breakage is frequently taken place in MANET due to the high speed of the nodes. Due to dynamic topology, no any centralized authentication system, and freedom of the nodes to join and leave the network, mobile ad hoc networks are vulnerable to various network attacks i.e. these networks are less secure. Besides, these limitations, the routing protocols used in mobile ad hoc networks are designed by considering that all nodes participating in communication are trustworthy and will cooperate to each other honestly. Due to such type of reasons, chances of introducing the malicious nodes in the network are more and performance of the network will be affected.

A. AODV

AODV [2] refers to ad hoc on demand distance vector routing protocol. AODV was designed (in July, 2003) for especially mobile ad hoc networks to reduce the processing time, network utilization and network overhead. It is a reactive, loop free routing protocol and works well as compare to DSR (dynamic source routing). In AODV, only path is established when data have to be transmitted from source to destination. Mainly three types of messages are generated in AODV communications: route request, route reply, and route error message. When a communication link has to be established, source node broadcasts a route request message in the network. For each node in the network, a routing table is established with some specific fields like hop count, destination IP address, destination sequence number, network interface and next hop node in the network. The route error message of AODV contains the following fields: unreachable destination IP address, unreachable destination sequence number, additional unreachable destination IP addresses, and additional unreachable destination sequence numbers. A node that is the part of an active route, continuously broadcasts a 'Hello' message in the network. For all types of the message communications port number 654 is used through UDP (user datagram protocol). Performance of AODV is degraded in scalable networks. AODV is designed by considering that all nodes in the network are trustworthy and will cooperate to each other during data communication. It is assumed that there is no any malicious intruder node in the network. AODV supports only unicasting and does not support multicast routing. In view of security, AODV is vulnerable to various network attacks such as blackhole and grayhole attacks. To mitigate its vulnerability to various attacks, a number of enhanced algorithms have been proposed by researchers. Some research work is designed against blackhole attack while some secure models have been proposed by

Manuscript received September 1, 2021; revised February 17, 2022.
Corresponding author email: drpushpendersarao@gmail.com.
doi:10.12720/jcm.17.3.194-202

keeping in view of cooperative grayhole, rushing, jellyfish, and flooding attacks in ad hoc networks.

B. Rushing Attack

In rushing attack [3], performance of the network is affected specially in terms of the end to end delay. It is denial of service attack in which attacker node forwards the entire packets without processing it for the particularly authentication. Attacker node sends the packet to its neighbor node with a high speed as compared to a normal node in the network. As a result in the network traffic queues are overflowed and due to the heavy traffic, high levels of end to end delays are taken place. A normal node takes more time to process the received packets and messages. As well as the numbers of malicious nodes are introduced in the network, performance of the network will also be degraded. As compared to gray hole and black hole attacks, performance of the network is less affected in rushing attack. In single attacking mode and cooperative attacking mode, rushing attack may be introduced in the network. In rushing attack, behavior of the malicious node is frequently changed and it is very difficult to identify it.

C. Grayhole Attack

A grayhole attack [4] is a kind of blackhole attack in which data packets are dropped time to time or as per criteria settled by the attacker. Initially, malicious node acts like a normal node and works well as per network protocol. But, suddenly, it acts as an attacker node and starts dropping the packets passing to it. Data dropping may be taken place for a specific time or for specific node type. Due to its uncertain behavior of the attacker node in grayhole attacker, it is very difficult to identify it. Performance of the network is affected by the grayhole attack in terms of throughput, packet delivery ratio, end to end delay, and overhead of the network. Grayhole attack may be taken place in single attacker or cooperative attacking mode. As well as number of attacker nodes are introduced in the network, performance of the network is more affected. Performance of the network is less affected by the grayhole attack as compared to blackhole attack because in blackhole attack, the attacking node regularly dropping all the packets passing to it while in grayhole attack, dropping of the packets is not in a regular mode.

D. Blackhole Attack

In blackhole attack [4], all the data packets are dropped by the malicious node passing to it. In this attack, malicious node broadcast false information that it has a reliable and shortest path for the destination. And as a result, source node or intermediate node sends packets to it. Performance of the network especially throughput and packet delivery ratio is affected by the blackhole attack. Blackhole attack comes under active attack in ad hoc networks. blackhole attack may be implemented in single or cooperative mode. In cooperative mode, a number of malicious nodes introduced in the network and collectively data packets are dropped by the malicious nodes. Blackhole attack is more dangerous attack as compared to rushing and grayhole attacks.

This research work has simulated gray hole, rushing, and black hole attacks on existing AODV routing protocol with four approaches: normal AODV, AODV with gray hole attack (G-AODV), AODV with rushing attack(R-AODV), AODV with black hole attack (B-AODV). To simulate the above attacks, AODV in NS 2.34 has been updated as per particular attack type. By considering the performance parameters as average throughput, packet delivery ratio, and average end to end delay, simulation results have been investigated.

The main objective of this research work is to implement and analyze the rushing attack, gray hole attack and black hole attack for understanding the impact of above attacks on the performance of AODV in MANET.

Rest of this work is organized as follows: Section II summarized the literature survey regarding several security attacks and their impact on network performance. To implement the proposed work, simulation setup with different network scenarios and performance parameters are presented in Section III. Further results are discussed with the help of graphs in Section IV. Section V concludes this research work.

II. Related Work

Mobile ad hoc networks are very popular networks due to its various application areas in real world wireless scenarios such as personal area networks, military operations, and vehicular networks. For reliable wireless communications, mobile ad hoc networks are most appropriate network; although, there are certain security issues regarding confidentiality and loss of the data.

In literature, security attacks and their impact on the performance of routing protocols has been discussed by researchers. Meenakshi Tripathi et al. analyzed the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol under wormhole and blackhole attacks in wireless sensor networks [5]. Individually blackhole and grayhole attacks have been simulated in NS 2.35 by considering the network performance parameters such as network lifetime, data sent at base station, and extended energy. Also a comparatively study have been conducted and it is declared that as well as the network size is enlarged, the effect of attacks is more. Impact of blackhole attack is more on the performance of the network as compared to grayhole attack.

A study for impact of blackhole and rushing attacks has been conducted in mobile ad hoc networks [6]. Performance of the network is observed by considering the metrics like throughput, packet delivery ratio, and average end to end delay. It was concluded that end to end delay and throughput in case of rushing attack is higher as compared to blackhole attack. Impact of

blackhole attack is more on the performance of the network.

DSR and AODV routing protocols have been evaluated under flooding and rushing attacks in mobile ad hoc networks [7]. For 25-150 node density, DSR and AODV protocols have been simulated for 500 seconds in network simulator NS 2.35. By considering the performance parameters like throughput and packet delivery ratio, it was declared that AODV is less affected by flooding and rushing attacks as compared to DSR routing protocol. Flooding attack is more harmful as compared to rushing attack both for AODV and DSR protocols.

Performance of AODV under rushing attack has been analyzed by Shukla and Khondekar in [8]. By varying the network size and node densities, rushing attack is simulated in NS 2.35 and has been evaluated by considering performance metrics as control overhead, packet delivery ratio, normalized routing load, throughput, and delay. It was observed that network performance is affected by the rushing attack in terms of the above metrics. It degrades the efficiency of the protocol and increases the unnecessary delays in the network.

Detection and mitigation schemes for the security attacks have been proposed to resolve several security issues in ad hoc networks [9]-[14]. Some routing protocols also have been enhanced so that securely data transmission should be possible [15], [16]. Some authors compared the impact of network attacks such as blackhole, rushing, flooding attacks on AODV routing protocols by considering performance parameters like throughput, packet delivery ratio and end to end delay in the network [17], [18]. AOMDV (Ad hoc on demand multi-path distance vector) is the extended version of AODV which facilitate for discovering multiple routes from source to destination [19]. The multicast routing feature of AOMDV routing protocol reduce the impact of blackhole attacks.

III. Simulation Setup

AODV routing protocol is simulated with and without blackhole, grayhole, and rushing attcaks for maximum simulation time of 100 seconds. To implement grayhole, blackhole, and rushing attacks, two files (aodv.cc and aodv.h) in NS 2.34 [20] has been modified. Network simulator 2 (NS 2.34) has been used for generating the wireless scenario by pause time 0 second, packet queue size 50, antenna as omni antenna. Network simulator 2 is very popular simulator among the academicians and researchers. Front end is written in TCL while back end works on C++. Routing protocols can be simulated in several wireless network scenarios like wireless sensor network, wireless mesh network and mobile ad hoc networks. NS2 is object oriented and event driven simulator. Trace file (.tr) and network animator (.nam) files are generated when tcl file is executed. In our simulation work, four different network scenarios have been configured by varying the motion, number of attacking nodes, network size, and node density. For data transmission, both TCP and UDP traffics have been used. Performance metrics (average throughput, packet delivery ratio, and average end to end delay) are calculated by executing the awk scripts and particular scenario's trace file.

In all the scenarios, attacking nodes are kept in motion. In our all experimental work, attacking nodes are selected randomly in the network. To generate the simulation environment, parameters with their respective values have been mentioned in Table I.

TABLE I: PERFORMANCE PARAMETERS

Simulation Parameter	Value
Simulator with Version	Network simulator 2 NS 2.34
Routing protocol	AODV
Types of Attacks	Blackhole attack, Grayhole Attack, Rushing Attack
Network Size	500×500m, 800×800 m, 1000×1000m, 1500×1500m
Network Topology	Random
Size of the packet queue	50
Data Rate	2.0 Mbps
Maximum speed	20,40,60,80,100 m/s
Maximum number of nodes	10,20,40,60
Antenna Type	Omni Antenna
Simulation time	100 seconds
Traffic type	FTP, CBR(Constant Bit Rate)
Traffic Connections	TCP, UDP
Mac type	802.11
Link Layer type	LL

Scenario-1: Varying the nodes

By varying the nodes from 10 to 60 and introducing the 4 malicious nodes, AODV is simulated for 100 seconds for black hole, rushing, and grayhole attacks. Malicious nodes are randomly selected in the network. Random topology is used to layout the nodes in the network having size of 745m×700 m. Total II network traffic connections has been established: one TCP connection (traffic type FTP) and other UDP connection (traffic type CBR). In TCP and UDP connections, packet size is decided as 1500 bytes. In UDP connection, CBR traffic is configured with packet size 1000 bytes, data rate as 2.0 Mb. Traffic time is decided from 1-100 seconds both for FTP and CBR traffics. No. of attacking nodes-4, node 10(1,3,5,8), node 20(1,2,12,14), node 40(6,12,19, 26), node 60(6,15,16,37). In case of 10 nodes, TCP connection is established with node 0 as source node while node 7 as destination node. UDP connection is established with node 2 and node 9 as source node and destination node respectively. In TCP connection establishment for 20, 40, and 60 nodes, node number 0 are settled as source nodes while node number 18, 37, and 59 are considered as destination nodes respectively. In UDP traffic connection establishment, for 20, 40, and 60 nodes, node number 11, 13, and 40 are decided as

source nodes while node number 4, 31, and 56 considered as destination nodes. Traffic starting time and stop time is decided as 1 second and 100 seconds respectively both for TCP and UDP connections.

Scenario-2: Varying the Speed

By varying the motion of the speed from 20 m/s to 120 m/s, 60 nodes are simulated for 100 seconds in network size 500m×500m. Layout of the nodes in the network is kept as random topology. All the nodes including 4 attacking nodes are kept in moving mode with pause time 0 second. In blackhole, grayhole, and rushing attacks simulation, attacking nodes are selected randomly in the network. TCP and UDP traffic connections have been established with FTP and CBR traffics respectively. Traffic starting and stop time is kept as 1 second and 100 seconds respectively for FTP and CBR traffics. Size of the packet is kept as 1500 bytes for both types of connections. CBR traffic is configured with packet size 1000 bytes, data rate as 2.0 Mb. In TCP and UDP connections, node number 0 and 40 are decided as source nodes while node 59 and 56 play a role of destination nodes.

Scenario-3: Varying the Network Size

In simulation work, scenario 3 is configured with maximum 60 nodes, network size(500×500 m^2, 800×800 m^2, 1000×1000 m^2 , 1500×1500 m^2), pause time 0 second, and simulation time as 100 seconds. All the nodes (including 4 attacking nodes) have maximum speed of 20 m/s. nodes number 6,15,16,37 are randomly selected as attacking nodes to simulate the grayhole attack, blackhole attack, and rushing attack. Three active attacks (grayhole, blackhole, and rushing attacks) have been simulated for AODV routing protocol. Random topology is used to layout the nodes in the wireless network scenario. TCP and UDP traffic connections are established with FTP and CBR traffics. For both types of connections, packet size of 1500 bytes is decided. Maximum traffic time is kept as 100 seconds. CBR traffic is configured with packet size 1000 bytes and data rate 2.0 Mb. Node number 0 and 40 are considered as source nodes while nodes 59 and 56 play a role of destination nodes.

Scenario-4: Varying the Number of attacks

By varying the number of attacking nodes from 0 to 4, network scenario 4 is generated with network size 745m×700m, pause time 0 second, and maximum simulation time as 100 seconds. By using the random topology, 60 nodes under blackhole, grayhole, and rushing attacks have been simulated by introducing 1-4 attacking nodes. Attacking nodes are kept in moving mode. Simulation environment is configured with packet queue size 50, antenna model as omni antenna, and 2 network connections (1 TCP and 1 UDP connection). Packet size is decided as 1500 bytes. CBR traffic is configured with 1000 bytes packet size and 2.0 Mb data rate. Traffic is generated for maximum time of 100 seconds both for FTP and CBR traffics. Number of attacks with malicious nodes is depicted in table 2. Node number 0 and 40 are decided as source nodes while destination nodes are decided as node number 59, and 56. Maximum packet size of 1500 bytes is decided for both TCP and UDP traffic connections. CBR traffic is configured with packet size 1000 bytes and 2.0 Mb data rate.

TABLE II: NO. OF ATTACKS WITH MALICIOUS NODES

No. of Attacks	Malicious Nodes
1	6
2	6,37
3	15,16,37
4	6,15,16,37

IV. RESULTS AND DISCUSSION

Rushing, blackhole, and grayhole attacks are simulated for AODV routing protocol in mobile ad hoc network for 100 seconds of simulation time. Performance metrics are considered as average throughput, average end to end delay (E2E Delay), and packet delivery ratio (PDR):

1. *Throughput:* It is defined as "the amount of packets passing through a link." In short, you can say it as flow rate.
2. *Packet Delivery Ratio (PDR):* It can be measured as the ratio of number of packets delivered in total to the total number of packets sent from source node to destination node in the network.
3. *End to End Delay (E2E Delay):* It is the sum of the delays experienced at a sequence of intermediate nodes on the way to the destination.

Graphical results have been generated by using the xgraph tool in NS2.34. Results have been analysed and discussed in terms of particular attack and performance metric.

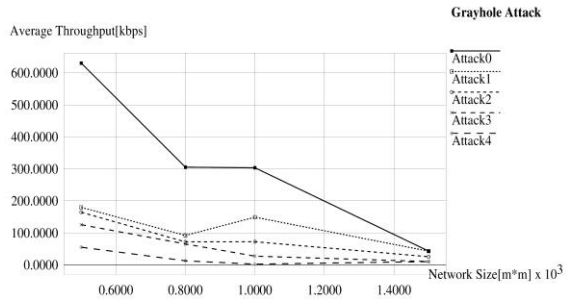

Fig. 1. Network size Vs average throughput

Average throughput is analysed with and without grayhole attack for AODV routing protocol (see Fig. 1). Without grayhole attack, average throughput is decreasing as the network size is increased. For all network size, as well as number of attacking nodes are increased, average throughput is decreased. In case of 3 and 4 attacking nodes, average throughput is decreased as the network size is increased. Average throughput is fluctuating in case of 1 and 2 attacking nodes as the size of the network is changed.

Packet delivery ratio in respect of number of attacking nodes has been depicted in Fig. 2 for grayhole attack. For 2, 3, and 4 attacks, packet delivery ratio is decreased as the network size is increased while it is fluctuating for 0,

1 attacks. As the numbers of attacking nodes are increased, packet delivery ratio is also fluctuating with small differences.

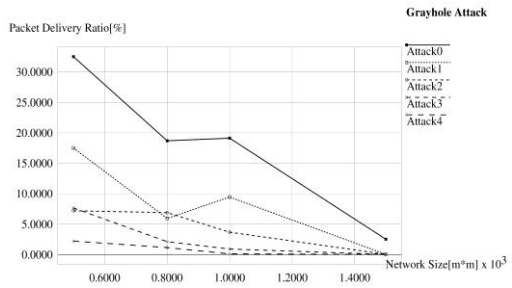

Fig. 2. Network size Vs packet delivery ratio

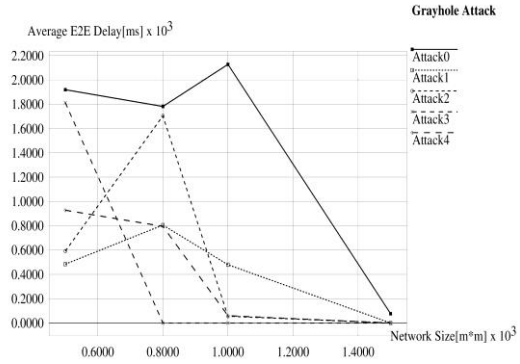

Fig. 3. Network Size Vs average E2E delay

Impact of grayhole attack for average end to end delay in respect of network size is shown in Fig. 3. Without any attack, average E2E delay is fluctuating in respect of network size. As grayhole attacks are increased, average end to end delay is fluctuating for all network sizes from 500m×500m to 1000m×1000m while it is 0 for network size 1500m×1500m.

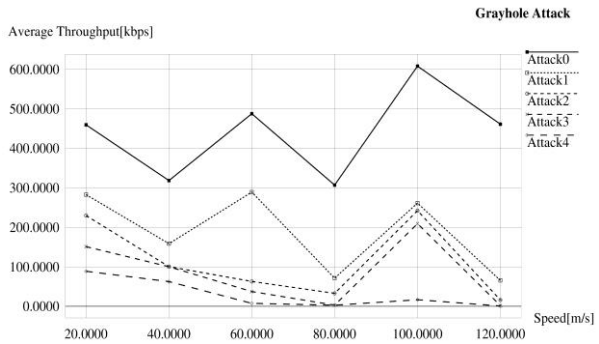

Fig. 4. Speed Vs average throughput

Average throughput in respect of speed is presented for grayhole attacks (see Fig. 4). Without any attack, average throughput for AODV is fluctuating as the speed is increased. As well as the attacking nodes in the network are increasing, the average throughput of the network is decreased for speeds 20-120 m/s. Impact of single to multiple grayhole attacks has been evaluated and presented through the graph. Average throughput is 22% with single grayhole attack while with multiple grayhole attacks (4 attacks) it is only 4%.

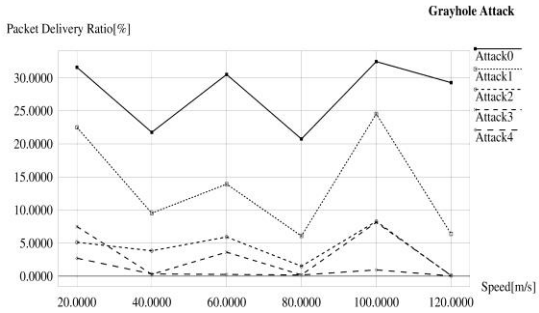

Fig. 5. Speed Vs packet delivery ratio

As illustrated in Fig. 5, in the presence of grayhole attack, packet delivery ratio (PDR) in terms of speed 20-120 m/s is presented. PDR is fluctuating for all speed ranges in the absence of grayhole attack. As the attacker nodes are introduced, PDR is degraded. As well as the numbers of attacker nodes are increased, PDR is decreasing at speed 20-120 m/s. In presence of grayhole attacker nodes, as the speed is increased, PDR is fluctuating. In presence of multiple 4 attacker nodes, PDR is highly affected. PDR in normal AODV is 57% while it is degraded from single grayhole attack to multiple grayhole attacks i.e. 29% to 2%. This is due to the fact that presence of multiple malicious nodes will become a cause for heavy dropping of the packets.

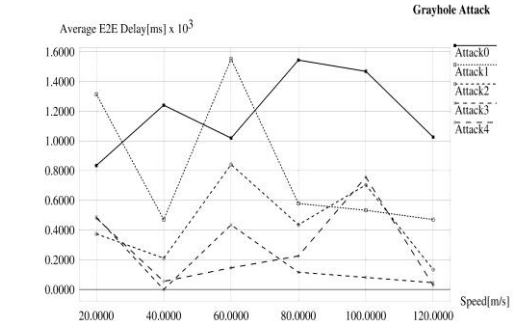

Fig. 6. Speed Vs average E2E delay

In the presence of grayhole attack, average E2E delay in terms of speed is shown in Fig. 6. Graph presents the effect of single to multiple grayhole attacks with respect to various speed values (20-120 m/s). Without any attack, average E2E delay for AODV routing protocol is fluctuating as speed of the network will vary, but as the grayhole attacker nodes are introduced, it is surprisingly decreasing and at the same time it is also fluctuating. As speed and number of attacking nodes are increased, average E2E delay is fluctuating. In case of multiple (4 attacking nodes) attack, average E2E delay is very less because due to multiple grayhole malicious nodes, maximum packets are dropped. Average end to end delay for normal AODV is 40% while it is 10% in case of multiple grayhole attacks.

By varying the network size, average throughput for normal AODV, B-AODV (AODV with black hole attack), R-AODV (AODV with rushing attack) have been presented in Fig. 7. In case of normal AODV, average

throughput is decreased as well as the network size is increased. In the presence of rushing attack, performance of AODV in terms of average throughput is better than B-AODV (AODV with black hole attack). Graph presents that impact of rushing attack in respect of throughput is less as compared to black hole attack. Average throughput for R-AODV (AODV with rushing attack) is 36% and for B-AODV (AODV with black hole attack), it is 23%.

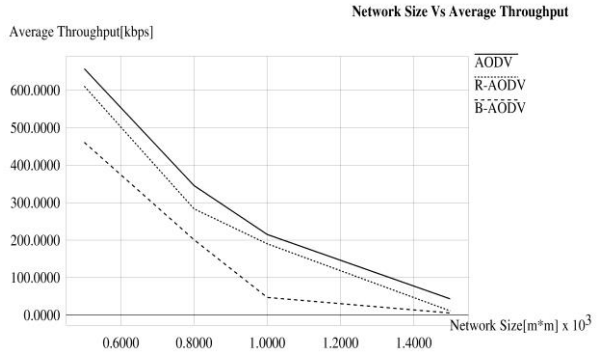

Fig. 7. Network size Vs average throughput

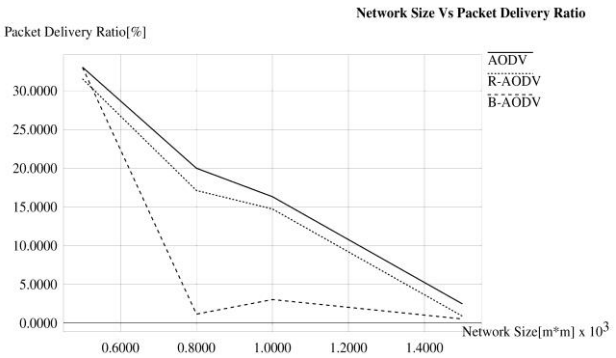

Fig. 8. Network size Vs packet delivery ratio

By varying the network size with respect to packet delivery ratio [PDR] is illustrated in Fig. 8. In the presence of rushing and black hole attacks on AODV, PDR is evaluated. In case of normal AODV (i.e. no any attack), as the network size is varying from 500m×500m to 1500m×1500m, PDR is decreasing dramatically. It is highest at 500m×500m network size while it is lowest at network size of 1500m×1500m. In case of R-AODV (AODV with rushing attack) and B-AODV (AODV with black hole attack), PDR is fluctuating as the network size is varying. Overall average PDR for R-AODV (16.06%) is higher than B-AODV (9.42%).

Average end to end delay (average E2E delay) with respect to network size is presented for R-AODV(AODV with rushing attack), B-AODV(AODV with black hole attack) and normal AODV routing protocols (see Fig. 9) . In normal AODV(without any attack), average E2E delay is increasing from 500m×500m to 800m×800m network size, but suddenly it is decreasing from 800m×800m to 1500m×1500m network size. In case of R-AODV (AODV with rushing) and B-AODV (AODV with blackhole) attacks, average E2E delay is fluctuating as well as network size is varying. Overall average E2E delay for B-AODV (680.43 ms) is lower than R-AODV (2171.88 ms) because maximum packets have been dropped and less data has to be transmitted in case of B-AODV while in case of R-AODV, packets are forwarded with high speed without checking any authenticity. As a result, due to heavy traffic in the network, more delays are taken place.

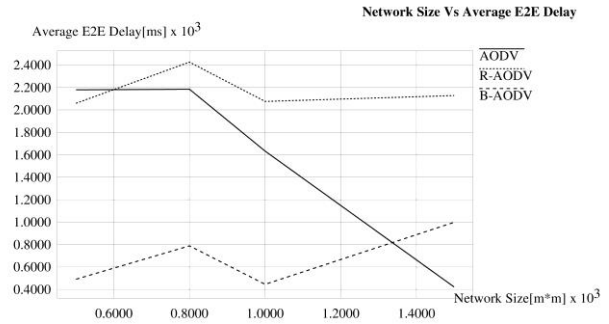

Fig. 9. Network size Vs average E2E delay

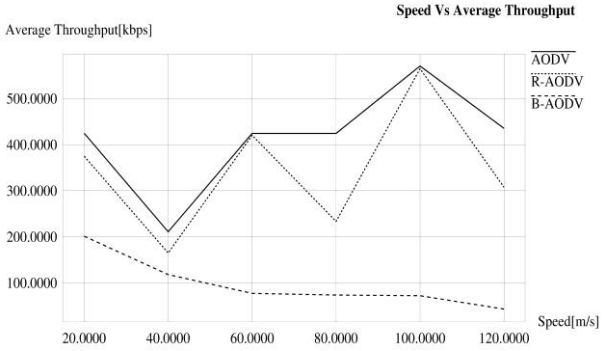

Fig. 10. Speed Vs average throughput

As shown in Fig. 10, with and without rushing and blackhole attacks on AODV, average throughput in respect of speed is presented. In the absence of any attack, average throughput for AODV routing protocol is fluctuating as well as speed of the nodes is varying from 20m/s to 120m/s. In case of B-AODV (AODV with black hole attack), average throughput is decreasing as the speed in the network is increasing while it is totally different in case of R-AODV (AODV with rushing attack). Throughput is fluctuating with respect to the certain values of the speed. Average throughput is affected both in R-AODV and B-AODV. In case of R-AODV, it is less affected as compared to B-AODV. Average throughput for R-AODV is 41% while in case of B-AODV it is 11%.

In Fig. 11, packet delivery ratio [PDR] is depicted for normal AODV, R-AODV (AODV with rushing attack), and B-AODV (AODV with black hole attack). When speed in the network is increased, the PDR for normal AODV is fluctuating. At speed 100 m/s, it is highest while at speed 40m/s, it is lowest. As rushing and blackhole attacks are introduced in the AODV routing protocol, PDR of the network is affected. It is highly affected in case of B-AODV while it is less affected for R-AODV. PDR is fluctuating as well as speed of the nodes is varying 20-120m/s both for the R-AODV and B-

AODV. PDR for R-AODV is 43% while it is 11% for B-AODV.

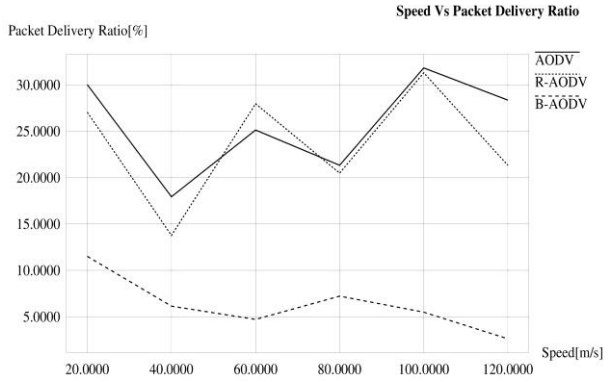

Fig. 11. Speed Vs packet delivery ratio

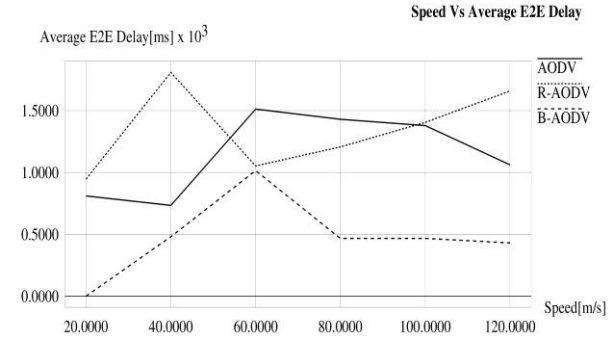

Fig. 12. Speed Vs average E2E delay

In Fig. 12, average end to end delay (average E2E delay) in respect of speed is shown. By varying the speed, average E2E delay is depicted for normal AODV, B-AODV (AODV with black hole attack), and R-AODV (AODV with rushing attack). Without any attack, delay for AODV is decreasing from speed 60 m/s to 120 m/s while in case of R-AODV, it is increasing from speed 60 m/s to 120 m/s. Average E2E delay is fluctuating at various values of speed in the network. Average E2E delay for R-AODV is 45% while it is 16% for B-AODV.

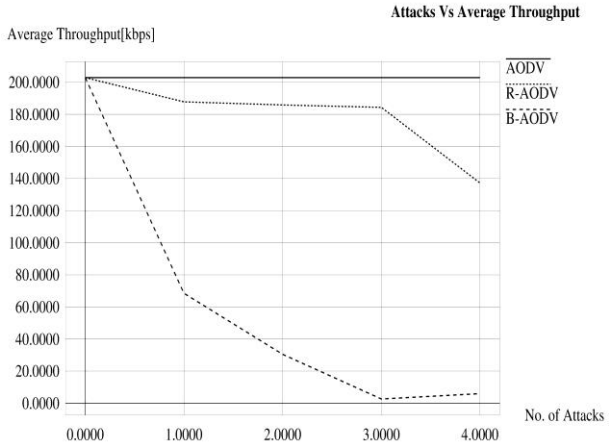

Fig. 13. Attacks Vs average throughput

By varying the number of attacking nodes from 0 to 4, average throughput is investigated (see Fig. 13) for normal AODV, R-AODV (AODV with rushing attack) and B-AODV (AODV with black hole attack). In the absence of any attack, average throughput is 202.92 kbps for AODV routing protocol. As well as attacks are increased in the network, average throughput is decreased both for the R-AODV and B-AODV. In the presence of R-AODV (179.63 kbps), average throughput is less affected as compared to B-AODV (62.09Kbps). This is due to the fact that in B-AODV; all the packets are dropped that are passing to attacker nodes whereas in rushing attack, randomly dropping of packets is taken place.

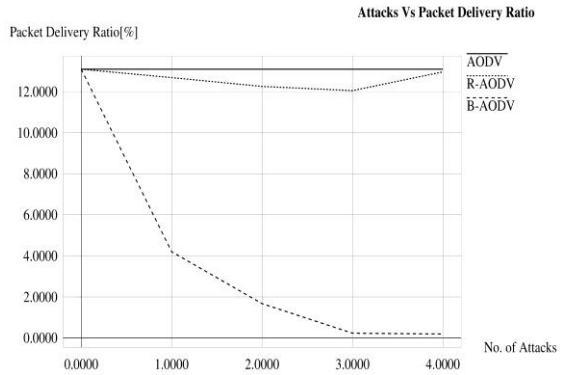

Fig. 14. Attacks Vs packet delivery ratio

In Fig. 14, performance of AODV under rushing and black hole attacks is analyzed by varying the number of malicious nodes in the network. PDR is investigated from 0-4 attacker nodes. Without any attacker node, PDR for AODV is 13.09% but as well as numbers of attacking nodes are increased in the network, PDR is decreased both in the presence of above attacks. In case of R-AODV (AODV with rushing attack), PDR is decreasing with very small variations while is totally different in case of B-AODV (AODV with black hole attack). Here, PDR is badly affected and is very low (13%) as compared to R-AODV (43%).

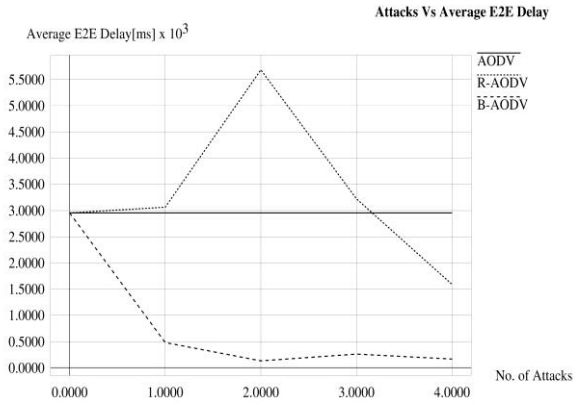

Fig. 15. Attacks Vs average E2E delay

As shown in Fig. 15, Average end to end delay (average E2E Delay) is presented for rushing and blackhole attacks. In the absence of the attacker node, average E2E delay in the network is 2954.63 milli-seconds. Total average E2E delay in the presence of the rushing attacks (R-AODV) is higher while it is low in case of black hole attack (B-AODV). As the numbers of attacker nodes are increased in the network, average E2E

delay is fluctuating both for the above attacks. Total average E2E delay for R-AODV is 3303.11 ms while it is 798.46 ms for B-AODV. Average end to end delay is high as compared to AODV and B-AODV; this is due to the fact that in case of R-AODV, all the receiving packets are forwarded at very high speed as compared to normal node without processing it and due to high traffic in the network, normal node takes more time in processing the packets before forwarding it to the neighbour node.

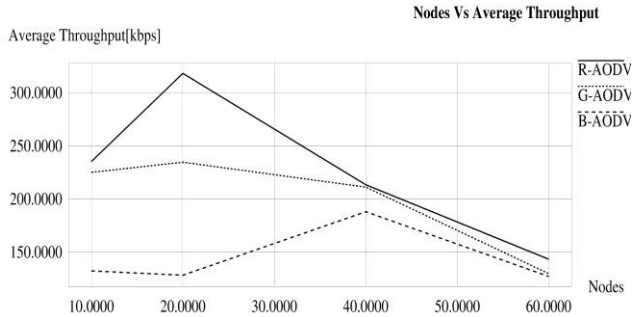

Fig. 16. Nodes Vs average throughput

In Fig. 16, B-AODV (AODV with black hole), G-AODV (AODV with grayhole attack), and R-AODV (AODV with rushing attack) have been analysed by varying the node densities; average throughput is presented in respect of nodes. Average throughput is fluctuating as the numbers of nodes are increased in the network for B-AODV, G-AODV and R-AODV. Total average throughput is highest in case of R-AODV i.e. 227.50 Kbps while in case of B-AODV, it is lowest i.e. 143.78 Kbps as compared to G-AODV and B-AODV. Because during implementing B-AODV, the malicious node drops all the packets passing through it while in case of G-AODV, only selected packets or as per defined criteria, packets are dropped. Therefore grayhole attack gives less impact on the throughput of the network as compare to black hole attack.

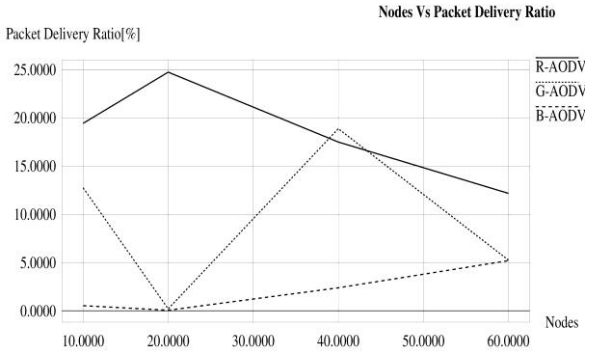

Fig. 17. Nodes Vs packet delivery ratio

Packet delivery ratio (PDF) has been analyzed in terms of node density as depicted in Fig. 17. For B-AODV (AODV with black hole attack), G-AODV (AODV with grayhole attack) and R-AODV (AODV with rushing attack), PDF is presented in respect of number of nodes. In case of B-AODV and G-AODV, PDF is decreasing from node density 10 to 20 while it is increasing from node density 20 to 60. This scenario is totally different in case of R-AODV; PDF is increasing from node density 10 to 20 but suddenly it is decreasing from node density 20 to 60. Grayhole attack has less impact on the PDF as compare to blackhole attack. Out of above three attacks, there is highest PDF in case of rushing attack i.e. 18.46%.

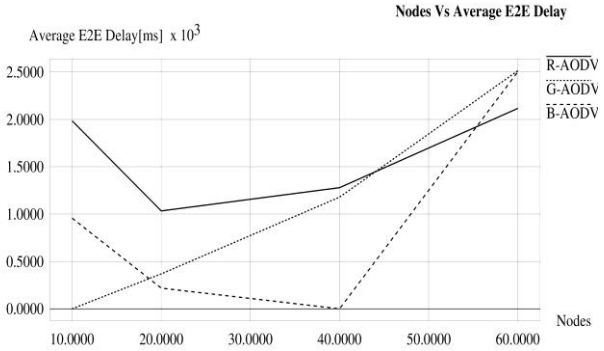

Fig. 18. Nodes Vs average E2E delay

Fig. 18 illustrates the average E2E delay in terms of node densities for B-AODV (AODV with black hole attack), R-AODV (AODV with rushing attack), and G-AODV (AODV with grayhole attack). For all the node densities (10-60), average E2E delay is fluctuating in case of B-AODV, R-AODV, and G-AODV. Among B-AODV, R-AODV, and G-AODV, there is highest total average delay for R-AODV i.e.1603.15 ms. This is expected because the rushing attacker nodes in the network instantly forward packets without conducting a check on its routing table. In case of B-AODV, total average E2E delay is very less i.e. 919.30 ms; because maximum packets has been dropped by the malicious nodes and further there is no more data transmission work.

V. Conclusion

Mobile ad hoc networks are vulnerable to several network attacks and there is serious issue regarding security. Routing protocols used in MANET are less secure for data transmission. AODV routing protocol is also vulnerable to attacks and presence of any malicious node will degrade its performance. In this paper, AODV has been analyzed under rushing, black, and grayhole attacks. The experimental results signify that MANET is highly affected by multiple attacking nodes as compare to single attacking node. As the numbers of attacking nodes are increased, network performance is also degraded in respect of packet delivery ratio and average throughput. AODV is less affected by rushing attack. The results show that black hole attack is the attack due to which performance of AODV is heavily affected as compared to G-AODV (AODV with grayhole attacks) and R-AODV (AODV with rushing attacks).

Conflict of Interest

The author declares that there is no any conflict of interest.

REFERENCES

[1] P. I. I. Ismail and M. H. F. Ja'afar, "Mobile ad hoc network overview," in *Proc. Asia-Pacific Conference on Applied Electromagnetics*, 2007, pp. 1-8.

[2] Perkins, E. Belding-Royer, and S. Das, Ad Hoc On-demand Distance Vector (AODV) Routing (No. RFC 3561), 2003.

[3] G. S. Chandel and R. Chowksi, "Study of rushing attack in MANET," *International Journal of Computer Applications*, vol. 79, no. 10, pp. 43-45, October 2013.

[4] Usha and Bose, "Comparing the impact of black hole and gray hole attacks in mobile adhoc networks," *Journal of Computer Science*, vol. 8, no. 11, pp. 1788-1802, 2012.

[5] M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN," in *Proc. 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN), Procedia Computer Science*, 2013, pp. 1101–1107.

[6] R. Kuri, S. Islam, M. J. Hossain, and M. H. Kabir, "Simulation-based comparative analysis on the effect of Black-hole attack and Rushing attack on the mobile ad-hoc network," *International Journal of Applied Engineering Research*, vol. 14, no. 10, pp. 2383-2387, 2019.

[7] M. Verma and N. C. Barwar, "Study and evaluation of DSR and AODV MANET routing protocols under flooding and rushing attacks," *International Journal of Engineering Research & Technology*, vol. 3, no. 11, pp. 532-535, November 2014.

[8] S. Mondal and K. L. Hassan, "Performance analysis of MANET under rushing attack," *International Journal of Recent Technology and Engineering*, vol. 8, no. 4, pp. 8506-8510, November 2019.

[9] M. Radha and M. N. Rao, "Gray hole attack detection prevention and elimination using Sdpegh in Manet," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 3, pp. 605-614, February 2019.

[10] P. Rani, Kavita, S. Verma, and G. N. Nguyen, "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network," *IEEE Access*, vol. 8, pp. 121755-121764, July 2020.

[11] S. V. Vasantha, A. Damodaram, and S. R. Krishna, "Path-hop based secure AODV to detect blackhole and gray-hole attacks in MANET," *Journal of Critical Reviews*, vol. 7, no. 18, pp. 1077-1093, 2020.

[12] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks," *Computers*, vol. 5, no. 16, pp. 1-18, 2016.

[13] B. Sen, M. G. Meitei, K. Sharma, M. K. Ghose, and S. Sinha, "Mitigating black hole attacks in MANETs using a trust-based threshold mechanism," *International Journal of Applied Engineering Research*, vol. 13, no. 7, pp. 5458-5463, 2018.

[14] N. Song, L. Qian and X. Li, "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach," in *Proc. 19th IEEE International Parallel and Distributed Processing Symposium*, 2005, p. 8.

[15] S. S. Narayanan and S. Radhakrishnan, "Secure AODV to combat black hole attack in MANET," in *Proc. International Conference on Recent Trends in Information Technology*, 2013, pp. 447-451.

[16] S. R. Deshmukh, P. N. Chatur, and N. B. Bhople, "AODV-based secure routing against blackhole attack in MANET," in *Proc. IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, 2016, pp. 1960-1964.

[17] S. Sivanesh and V. R. S. Dhulipala, "Comparitive analysis of blackhole and rushing attack in MANET," in *Proc. TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks*, 2019, pp. 495-499.

[18] K. S. Praveen, H. L. Gururaj, and B. Ramesh, "Comparative analysis of black hole attack in ad hoc network using AODV and OLSR protocols," in *Proc. International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science*, 2016, pp. 325–330.

[19] P. Sarao, "Ad hoc on-demand multipath distance vector based routing in ad-hoc networks," *Wireless Personal Communications*, vol. 114, pp. 2933–2953, 2020.

[20] The Network Simulator - ns-2. [Online]. Available: https://www.isi.edu/nsnam/ns/

Prof. Pushpender Sarao is associated as a Professor in Computer Science & Engineering department, Sharad Institute of Technology College of Engineering, Ichalkaranji, Maharashtra India. He is BE, M.Tech, Ph.D in Computer Science and Engineering. He earned his doctorate degree from Shri Venkateshwara University, India in June, 2016. He is author of five books in computer science, modern software engineering, and wireless networks. He is a member of IEEE, ACM, ICSES, RES, and IAENG, and life member of ISTE, CSI and IEI. He got published more than 72 research papers in national and international reputed journals. Also he shared his research experience in more than 23 national and international conferences. He attended several FDP and seminars/workshops in engineering institutions and state universities. He is member of editorial board for 19 national and international journals. His main research work focuses on routing protocols in wireless mesh networks, mobile ad-hoc network. He has 9 years of teaching experience and 10 years of industrial experience.