Wireless Networks (2020) 26:1981–2011
https://doi.org/10.1007/s11276-019-01966-z

A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability

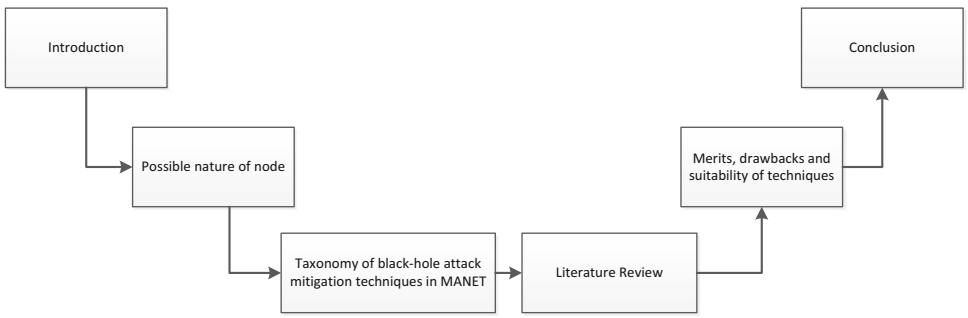
Shashi Gurung[1,2] · Siddhartha Chauhan[1]

Published online: 27 February 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

Mobile Ad-hoc Network (MANET) is a prominent technology in the wireless network in which the mobile nodes operate in a distributed manner and collaborate with each other in order to provide the multi-hop communication between the source and the destination node. Generally, the main assumption considered in the MANET is that each node is a trusted node. However, in a real scenario, there are some unreliable nodes which misbehave and launch the attack in network like black-hole in which the misbehaving nodes attract all the traffic towards itself by giving false information of having a shortest path towards the destination with a very high destination sequence number. In this paper, we discussed different possible nature of the nodes in the network that can lead to the different possible attacks. We have also presented the different classification of the techniques and discussed the merits, drawbacks, and suitability of the various techniques in different scenarios which need to be taken into consideration while designing an efficient protocol.

Graphical Abstract



Keywords MANET · Black-hole · AODV · Overhearing · Clustering · IDS · Sequence number threshold · Cross checking · Byzantine attacks

1 Introduction

Mobile Ad-hoc Networks (MANETs) are the collection of independent mobile nodes which operate in distributed manners and coordinate with each other in providing communication between the source and the destination node. These networks can be set up easily and quickly at a low cost without requiring any type of fixed infrastructure like base station which is required in case of setting up the cellular network. It provides multi-hop communication

✉ Shashi Gurung
gurungshashi68@gmail.com

Siddhartha Chauhan
siddharthachauhan1@gmail.com

[1] Department of Computer Science and Engineering, National Institute of Technology, Hamirpur, India

[2] Computer Centre, Jawaharlal Nehru Government Engineering College, Sundernagar, India

through the intermediate node which plays an important role in providing the communication path between the source and the destination node as well as in forwarding the data packets. It is a self-configurable, temporary and infrastructure-less networks [1] of mobile devices that communicate with each other if within the direct radio transmission range of each other or through the intermediate nodes. The nodes in MANET have limited computation power due to its small size, small memory, and low processing power capabilities. Each node not only acts as a host and but also as a router. In order to communicate with each other, the routing protocol such as Ad-hoc On-demand Distance Vector (AODV) [2], Dynamic Source Routing (DSR) [3] etc is used which helps in finding the optimal route between the source and the destination node. The conventional MANET routing protocols assume that all nodes are trusted node and cooperate with each other but in a real situation, the behaviour of the nodes can be different and hence may not cooperate with other nodes. Due to this assumption, MANET's routing protocols have many weaknesses that can be exploited by the attacker in order to disturb the communication process. Therefore, MANET's routing protocols are more vulnerable to a denial of service (DoS) attacks. In this paper, the main contributions are that we have discussed about the different possible nature of the node, classification of techniques, and provided merits, drawbacks, and suitability of the various mitigation techniques in MANET.

The remainder of the paper is organized as follows. Section 2 explains about black-hole attack and different possible nature of the node in the network. In Sect. 3, we describe various techniques that deal with the black-hole attack and its classification into various categories. In Sect. 4, we discuss the merits and drawbacks of various schemes that need to be considered for designing efficient routing protocols and also discuss the suitability of scheme in the scenarios as per the simulation result in the available literature. At last, Sect. 5 concludes the paper.

2 Black-hole attack

Black-hole attack is also known as packet dropping attack which seriously degrades the performance of the network [4–6]. In this type of attack, there can be a single legitimate node or multiple legitimate nodes in the network. When there are two or more than two legitimate nodes which collaborate with each other in order to disrupt the communication, they are called as cooperative black-hole attack. The attacks which are launched by the authorized nodes are known as byzantine attacks [7]. In normal AODV routing protocol, whenever the source node wants to communicate with the destination node, it broadcasts route request packet if it does not have a path towards the destination. The destination node sends back reply packet on receiving the route request from the intermediate node. But in black hole attack, the black hole node on receiving route request packet sends reply packet with false information of having a minimum path towards the destination with a very high sequence number. The high sequence number indicates the freshness of the path. On receiving reply packets from the malicious node, the source nodes start sending the data packets from the path which contains malicious node and then the malicious node starts dropping the data packet.

In order to launch a black-hole attack in MANET, the main thing is that the attacker should have knowledge of about attracting the traffic towards itself which is possible by giving false route information in the reply header packet to the source node. In any routing protocol, the source node always communicates with the destination node through the optimal path and that path should not be a stale path. In AODV routing protocol, the two main field's information in reply header packet plays the important role in selecting the final established path which is hop count and destination sequence. The high destination sequence number indicates the freshness of the path. Therefore, the attacker always utilizes the vulnerability of the underlying routing protocols which are generally designed by considering the mutual cooperation among the nodes in the network. The attacker always gives the false information by providing the minimum hop count to 1 with a very high destination sequence number in the reply packet due to which the source node selects the path which contains malicious node and thereby leads to the packet dropping attack. Thus, any node in MANET can easily misbehaves and creates a severe damage to the network. There can be different nature of the node in a mobile ad-hoc network which is represented in Table 1 [8]. If a node is not malicious; it will not send incorrect information of having the shortest path and incorrect information about destination sequence number. In the Table 1, 0 represents incorrect information and 1 represents correct information. If a node is malicious, it can send incorrect information of having the shortest path with incorrect destination sequence number leading to black-hole attack in the network and start dropping the data packet when receiving the data packets. If a node is malicious, it can send correct information regarding destination sequence number but with incorrect information of having the shortest path toward destination due to which source node starts sending data packets and then malicious node drops it. If a node is malicious, it can send the correct information of having the shortest path with incorrect information of the destination sequence number that can also lead to the black-hole attack in the network. At last, if a node is malicious, it can send correct information of

Table 1 Nature of the node

Malicious	Destination sequence no.	Shortest path	Packet drop	Attack	Type of attack
No	1	1	No	No	No attack
Yes	0	0	Yes	Yes	Black-hole
Yes	0	1	Yes	Yes	Black-hole
Yes	1	0	Yes	Yes	Black-hole
Yes	1	1	Yes	Yes	Gray-hole

having the shortest path with correct destination sequence number but even then it can also lead to the gray-hole attack in the network which is a selective packet dropping attack by behaving normally during route discovery process and then behaving as malicious.

3 Literature review

There are various techniques as proposed by many researchers for combating with the black-hole attack in MANET which are described in detailed in the Sect. 3.3. These techniques have been classified into various categories as shown in Fig. 1.

3.1 Classification of techniques

3.1.1 Cryptography based scheme

It includes all those solutions in which cryptography technologies such as symmetric key cryptography, digital signature or hashing are used for encryption, verification and integrity purpose so as to be able to secure the network from the possible attacks.

3.1.2 Overhearing based scheme

It consists of all the solutions in which each node can overhear its neighbour's transmission to check its honesty. If its neighbor node is found to be doing some unexpected event, it is declared as a malicious node and the information is propagated in the network.

3.1.3 Sequence number threshold based scheme

In this category, the source node calculates a threshold value by using the destination sequence number parameter of the reply packet and drops the reply packet if it contains the sequence number greater than the threshold.

3.1.4 Acknowledgment based scheme

In this category, an acknowledgment packet is sent by the node to confirm about the well reception of the packets.

3.1.5 Clustering based scheme

In this scheme, the network is divided into the cluster in which the cluster head detect the black hole attack and inform about it in the network.

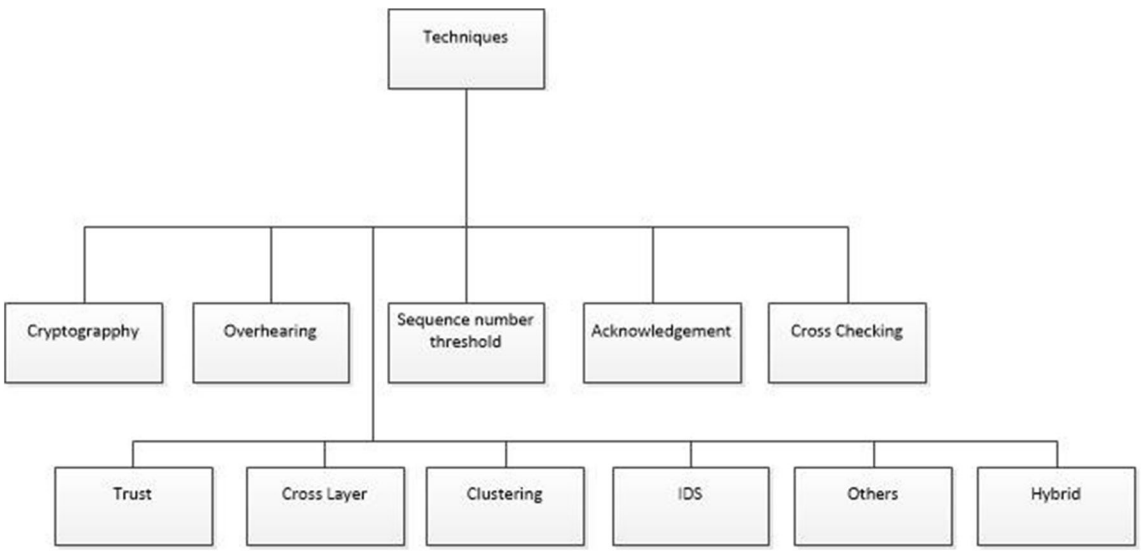


Fig. 1 Classification of techniques

3.1.6 Cross-layer collaboration based scheme

In this section, it encompasses all those solutions in which more than two layers cooperate with each other to detect the malicious activity in the network.

3.1.7 Cross-checking based scheme

In this scheme, cross-checking is done by the source node with the next hop or previous hop of the intermediate node so that the nature of the intermediate node can be found out.

3.1.8 Trust-based scheme

It includes the solutions that compute the node trust values based on neighbour transmission which helps in identifying the nature of the node whether malicious or normal. If a trust value of a node is less than a threshold, it is declared as malicious otherwise normal nodes.

3.1.9 IDS based scheme

This scheme is based on special nodes called as IDS nodes which have the capability to detect the malicious activities by overhearing its near transmission and when an anomaly is detected, it broadcast the message in the network to isolate it.

3.1.10 Other schemes

In this section, there are many solutions which do not come under the above categories.

3.1.11 Hybrid scheme

These are those schemes which can be the combination of above categories.

3.2 Parts

The summary of existing techniques has been done on the following basis and is presented in Table 2.

3.2.1 Reference

In this part, the reference of the existing technique is provided.

3.2.2 Base protocol

In order to deal with packet dropping attack in the mobile ad-hoc network, many researchers have used the different protocol as a base protocol which does not have any security mechanism for dealing black-hole attack. Mostly base protocols such as DSR and AODV have been used.

3.2.3 Protocol modification

In order to add security features to the base protocol, many researchers have made some modifications. Some of these modifications have mitigated the impact of black-hole attack. Some modifications are able to detect the malicious node while others are able to prevent the malicious node from doing any malicious activity in the network. Any modification done in the base protocol is marked by 'Y' (Yes) and where there is no modification in a base protocol is marked by 'N' (No).

3.2.4 Extra control packets

In order to make the network secure from the malicious nodes, some modifications led to the addition of new extra control packets. These extra control packets help in mitigation, detection, and prevention of the malicious nodes in the network. Any extra control packet added in the base protocol or used in methodology is shown as 'Y' i.e. Yes and where there is no extra control packet, it is shown as 'N' i.e. No.

3.2.5 Control packets name

Many researchers have proposed the different approach for dealing with black hole attack. Some of them have given the special name to their control packets that help in coping up the problem of black hole attack in MANET. There are some protocols where no extra control packets are added. They are represented by the term 'Not used'.

3.2.6 Proposed protocol or scheme

Some researchers have proposed protocol by adding security features in the base protocol and have given new name while some have made changes in the base protocol but have not mentioned the new protocol name which is mentioned as MAODV (modified AODV) protocol. Others have proposed a scheme that helps in the security of the network.

3.2.7 Merits

The existing techniques have some merits which can be taken into consideration in designing an efficient protocol for the different environment.

Table 2 Summary of various techniques

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Marti et al. [11]	DSR	Y	Y	Send route request (SRR)	Watchdog pathrater	Detect single or multiple black-hole nodes	Routing overhead due to extra route request	Random waypoint model	2000	Berkeley's network simulator (ns)
						Increased throughput during extreme mobility	May fail to detect under ambiguous collision, receiver collision, limited transmission power, false misbehaviour, collusion, and partial dropping	Pause time 0 and 60 s Maximum speed of node: 20 m/s Malicious node fractions: 0.1, 0.2, 0.3, 0.4 Metric: throughput versus fraction of misbehaving node, routing overhead versus fraction of misbehaving node and effect of false detection		
Deng et al. [26]	AODV	Y	Y	Further request and further reply	SAODV	Detect single and multiple black-hole nodes	Fail in cooperative black hole attacks	Metric: throughput and routing overhead	2002	Not discussed
						Increased throughput with minimal routing overhead	Delay increases for large network			
						Avoid high false positive rate problem	Malicious node can give fake reply on behalf of destination node			
Lee et al. [44]	DSR	Y	Y	CREQ	EXACT	Packet delivery is high when mobility is low	May fail in cooperative black-hole attack	Random waypoint model	2002	NS-2
				CREP	DIFF_ONE	Low data transmission overhead than DSR by around 10%		Maximum speed of node: 10 m/s Pause time 10,20,30,40 s Malicious node: 0, 2, 4, 8 Metric: packet delivery ratio, data transmission overhead and control overhead with respect to number of malicious nodes		

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Ramaswamy et al. [27]	AODV	Y	Y	Further request and further reply	MAODV	Detect multiple cooperating black-hole nodes Discover secure paths	High routing overhead	Simulation of proposed approach is not done	2003	Not used
Balakrishnan et al. [21]	DSR	Y	Y	Acknowledgement packet	Two ACK	When malicious node is around 40% even then there is good packet delivery ratio	TWOACK packets may contribute to the traffic congestion	Random waypoint model	2005	NS-2
					S-TWOACK	Similar end to end delay compared to DSR under high traffic	Detects only misbehaving links	Maximum speed of node: 20 m/s Pause time 0 s (high mobility) Metric: packet delivery ratio and routing overhead with respect to percentage of misbehaving nodes		
Peng et al. [31]	DSR	Y	Y	Broadcasting malicious ID	Common neighbour listening	Reduces delay about 50%	Fail in highly dynamic network topology	Random waypoint model	2006	NS-2
						High throughput and PDR when pause time is 300 s	Assumed high density of nodes	Maximum speed of node: 20 m/s Pause time: 0, 100, 200, 300, 400, 500, 600 s Metric: packet delivery ratio, average throughput and average end to end delay with respect to pause time		
Tamilselvan et al. [45]	AODV	Y	N	Not used	SAODV	PDR is high and delay is low in static network	Check replies from all nodes so end-to-end delay increases	Random waypoint model	2007	Glomosim
							Packet delivery decrease as node mobility speed increases	Metric: packet delivery and average end to end delay with respect to node mobility		

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Kurosawa et al. [13]	AODV	Y	N	Not used	Dynamic learning method	Effective in anomaly detection Detection rate is low when mobility is high	False positive Processing overhead will be more for shortening updating interval and more battery will be consumed	Random waypoint model Maximum speed of node: 20 m/s Pause time: 10 s Metric: detection rate and false positive with respect to node mobility	2007	NS-2
Yu et al. [28]	AODV	Y	Y	Check packet	DCM	Detect multiple cooperative black-hole nodes High detection rate and packet delivery rate	Need improvement in the voting mechanism which can deal with the gray-hole attack	Random waypoint model Maximum speed of node: 10 m/s Pause time: 200 s Metric: detection rate, packet delivery rate and overhead with respect to network traffic	2007	NS-2
Liu et al. [22]	DSR	Y	Y	Acknowledgment packet	2ACK	Flexibility of controlling overhead with the use of the Rack parameter Overcomes ambiguous collision, receiver collision and limited transmission powers	Focused only on link misbehaviour Higher routing overhead is due to acknowledgment packets	Maximum speed of node: 20 m/s Malicious node fractions: 0.1 to 0.4 Metric: packet delivery ratio and overhead with respect to misbehaviour ratio	2007	NS-2

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Dokurer et al. [46]	AODV	Y	N	Not used	IDSAODV	Does not require any additional overhead No modification in packet format Reduced the packet loss due black hole attack to 71.09% which is an improvement of 18.86% compared to the AODV protocol	The assumption that first reply always comes from the black-hole	Node positions and movements are randomly generated Metric: packet loss percentage	2007	NS-2
Fahad et al. [35]	Not used (proposed solution)	Y	Y	FAP	SMDP	Low complexity Reduce communication overhead	Need an extension of the solution to support node's mobility during the session	Simulation of the proposed approach is not done	2007	Not used
Weerasinghe [29]	AODV	Y	Y	FREQ and FREP packet	MAODV	Can accurately prevent cooperative black-hole attacks Better throughput rate Minimum packet loss percentage	High end-to-end delay High routing overhead Lower throughput in high mobility	Random waypoint model Pause time: 30 s Metric: throughput, end-to-end delay, route request overhead and packet loss with respect to the number of nodes, node mobility, and terrain area	2008	Qualnet
Medadian et al. [12]	AODV	Y	Y	Opinion alarm packet	MAODV	Packet delivery and throughput is high when mobility is high	Opinion is not always correct Delay is high when static i.e. node mobility speed is 0 m/s as compared with dynamic	Metric: packet delivery ratio, delay, control overhead, and throughput and with respect to node mobility	2009	Glomosim

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Lu et al. [47]	AODV	Y	Y	SRREQ SRREP	SAODV	Maintain high routing efficiency	Routing overhead due to multiple reply packets and additional control packets	Randomly generated simulation scenarios Metric: packet delivery ratio, delay, control overhead, and throughput and with respect to node mobility	2009	NS-2
Raj et al. [14]	AODV	Y	N	Not used	DPRAODV	Increases PDR with minimum increase in average end to end delay and normalized routing overhead	Increase in average end-to-end delay and normalized routing overhead	Random waypoint model Pause time: 2 s Mobility speed: 10 to 70 m/s Number of nodes: 10 to 60 Metric: packet delivery ratio, average end to end delay and normalized routing overhead with respect to node mobility, number of nodes and traffic load	2009	NS-2
Ameza et al. [49]	AODV	Y	Y	Alert	AODVSABH	Delivery of high ratio of data Consumes less route establishment delay	Routing overhead	Random waypoint model Maximum speed: 12 m/s Metric: packet delivery ratio, control traffic, and route establishment delay	2010	NS-2

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Mistry [48]	AODV	Y	N	Not used	MAODV	Achieves a good rise in packet delivery ratio with acceptable rise in end to end delay	Increase in average end-to-end delay and normalized routing overhead	Random waypoint model	2010	NS-2
						Does not add any control packets to AODV protocol		Mobility speed: 10 to 70 m/s		
						Simple and efficient in implementation		Node varying: 10 to 80		
								Pause time: 2 s		
								Metric: packet delivery ratio, delay, control overhead, and throughput and with respect to node mobility		
Al-Roubaiey et al. [23]	DSR	Y	Y	Acknowledgment packet	AACK	Solves limited transmission power and receiver collision problem	Routing overhead	Random waypoint model	2010	NS-2
						Performs better than TWOACK and Watchdog methods	Suffers from gray-hole attack	Pause time: 0 s		
								Maximum Mobility speed: 1 to 20 m/s		
								Number of nodes: 10 to 60		
								Metric: packet delivery ratio, average end to end delay and routing overhead with respect to malicious node percentage		

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Li et al. [9]	AODV	Y	N	Not used	SEAODV	Lightweight and computationally efficient due to symmetric cryptography operations	Memory constraint due to the requirement of pre-distribution of key	Assumed network throughput of 400 kbps for a single flow	2010	Not discussed
						Performs better as compared with ARAN and SAODV in terms of computation cost and route acquisition latency	May fail in internal attack due to shared key	Metric: computation cost and route acquisition latency		
Su [40]	AODV	Y	Y	Block message	ABM MAODV	With 9 IDS the detection rate is 100% and false positive rate is 0% if proper threshold is set	Cannot detect the gray-hole attack If the IDS nodes do not cover the entire network, detection and isolation of gray hole nodes may not be possible	Random waypoint model Maximum Mobility speed: 20 m/s Pause time-0,5, 10, 15 s Malicious node: 1 or 2 (fixed/moved) Metric: packet loss rate with respect to pause time	2011	NS-2
Marchang et al. [32]	AODV	Y	Y	Trust packet	LTB-AODV	Lightweight Scalability PDR is highest when mobility is low i.e. when speed is 1 m/s	Increases delay with the increase in mobility speed due to overhead of periodically broadcasting of TRUST control packet by the node	Random waypoint model Pause time: 0 s Mobility speed: 1 to 15 m/s Metric: packet delivery ratio, packet drop ratio, average end to end delay, route frequency, routing load and average throughput with respect to mobility speed	2012	NS-2

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Lacey et al. [33]	DSR	Y	N	Not used	Ripsec	Multi-layer security Protection from external and internal threats Robust against attacks	Designed for CLOSED MANET	Random waypoint model Node speed: uniform 0-10 m/s Metric: total request error sent, throughput and load	2012	OPNET
Jhaveri et al. [15]	AODV	Y	N	Not used	R-AODV	During route discovery process, it isolates multiple malicious nodes Select short and secure path	Routing overhead due to the forwarding of reply packet back to the source node	Random waypoint model Pause time: 1 to 5 s Mobility speed: 10 to 50 m/s Number of nodes: 10 to 50 Malicious node: 1 to 5 Metric: packet delivery ratio, average end to end delay and normalized routing overhead with respect to network size, mobility speed, pause time, traffic load and effect of malicious node	2012	NS-2
Jhaveri et al. [16]	AODV	Y	N	Not used	MR-AODV	Reliable against multiple attackers Uses default control packets	Need to deal with cooperative black hole attack	Metric: packet delivery ratio, average end to end delay and routing overhead	2012	NS-2
Saha et al. [36]	DSR	Y	Y	Alert packet	TSR	Double layer scheme Resilient against protocol compliant attacks and insider attacks	Various assumption	The simulation designed in java Assumed initial congestion window size to be 5	2012	The platform to perform the simulation is designed in Java

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Yerneni et al. [50]	AODV	Y	Y	MREQ and MREP	SAODV	Better security as compared with AODV Better packet delivery ratio as compared with AODV	Routing overhead due to multiple reply packets and additional control packets	Random waypoint model Mobility speed: 5 to 40 m/s Number of nodes: 20 to 50 Metric: packet delivery rate, throughput, and control packets with respect to the number of nodes and node mobility speed	2012	NS-2
Baadache et al. [25]	AODV, OLSR	Y	Y	Acknowledgment packet	TA, RA	Detection ratio is constant whether network is dense or not High delivery of data packets and high detection ratio as compared with 2-hop ACK and Watchdog methods	Additional overhead due to acknowledgement packets	Random waypoint model Metric: detection ratio, overhead, throughput, and delay	2012	OPNET
Tan et al. [17]	AODV	Y	N	Not used	SRD-AODV	PDR increases for small, medium and large environment with node mobility and is high when mobility is low	Cannot prevent black hole attack if the sequence number is less than the fixed threshold for the different environment	Random waypoint model Maximum Mobility speed: 20 m/s Pause time-0,5, 10, 15 s Metric: packet delivery ratio, Packet drop, overhead and delay	2013	NS-2
Katal et al. [38]	AODV	Y	N	Not used	CBDCDDPT	Efficient Intra cluster intrusion detection Secure Reliable due to data stream based approach	Increases delay The malicious node can become CH due to high residual energy Not suitable for highly mobile network	Random waypoint model Network size: 30 Metric: throughput	2013	OPNET

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Shi et al. [37]	AODV	Y	Y	Routing check request	Clustering	Prevent single and multiple collusive black-hole attacks	Complex due to the computation of various values	Random walk mobility model	2013	NS-2
				Route check affirmation		Packet delivery increases as traffic loads increases	Cannot tackle gray-hole attack because the gray-hole can become CH	Random mobility speed: 0 to 30 m/s		
							Overhead	Metric: packet delivery ration with respect of the number of black-hole nodes and traffic load		
Mohanapriya et al. [41]	AODV	Y	Y	QREQ, QREP, MNREQ, and ALARM	MDSR	Lightweight solution	High routing overhead due to extra control packets such as QREQ, QREP, MNREQ and ALARM packets	Random waypoint model	2014	Glomosim
						Less energy loss	If the IDS nodes do not cover the entire network, detection and isolation of gray hole nodes may not be possible	Mobility speed: 0 to 80 m/s		
						Suitable for resource-constrained MANET		Pause time-0 to 80 s		
								Metric: packet delivery ratio, with respect to node mobility speed		
Gurung et al. [53]	AODV	Y	N	Not used	ANB-AODV	Lightweight	The assumption that first reply from the malicious node	Random waypoint model	2014	NS-2
						Easy and simple implementation	Without attack, source node does not able to communicate with destination initially as the first reply is always rejected	Mobility speed: 5 to 55 m/s		
								Metric: packet delivery rate, throughput with respect to node mobility		

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Barani et al. [42]	AODV	Y	N	Not used	GAIIS	Better performance with DCAD and WPCA Detect flooding, black-hole, neighbor, rushing and wormhole attack	False positive	Random waypoint model Maximum Mobility speed: 35 m/s Pause time: 5 s Metric: average detection rate	2014	NS-2
Dhiman et al. [24]	DSR	Y	Y	Acknowledgment packet	Enhanced 2ACK	Low energy consumption due to use of RSA High PDR at low packet size	High routing overhead in comparison to exiting 2ACK	Random waypoint model Mobility speed: 5 to 55 m/s Metric: packet delivery rate, throughput, delay, overhead, and energy consumption	2014	NS-2
Dhanalakshmi et al. [10]	DSR	Y	N	Not used	IKGM	Prevents the attackers from initiating forged acknowledgment attacks Reduces the memory constraint	Battery consumption as new keys are to be generated instantly by every node when it takes part in the communication	Random waypoint model Maximum mobility speed: 20 m/s Metric: packet delivery ratio, throughput and packet drop	2014	NS-2
Kumari et al. [34]	Not discussed	Y	Y	S-Ack F-Ant Challenge and monitoring packets	ADMSFA	Secure transmission of acknowledgement packets Perform better than SACK	High routing overhead due to additional control packets	Malicious nodes: 2,4,6,8, 10 Metric: packet delivery ratio, delay, overhead and residual energy with respect to the number of malicious nodes	2015	NS-2

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Salunke et al. [18]	AODV	Y	N	Not used	DSNT	Secure the network in the multiple black-hole attacks	Needs a more detailed study of message exchange in their specific network for which fine-tuning of λ is carried out	Metric: packet delivery ratio	2015	NS-2
Dorri et al. [30]	AODV	Y	Y	Data control packet	Cross check	Low processing time and packet overhead as compared with base work under different number of malicious nodes	Delay rises	Random waypoint model	2015	OPNET
				Alarm packet		No false positive detection	Needs to be extended to detect the gray-hole attack	Maximum mobility speed: 5–20 m/s Pause time: 15 s Malicious nodes: 2,4, 6 Metric: packet overhead and processing time with respect to the number of malicious nodes		
Chang et al. [51]	DSR	Y	Y	RREQ'	CBDS	Based on dynamic threshold	Requires more time to detect and trace malicious nodes	Random waypoint model	2015	Qualnet
						Perform better than DSR, 2ACK and BFTR protocols in terms of PDR and routing overhead	Need to address other types of collaborative attacks	Maximum Mobility speed: 20 m/s Metric: packet delivery ratio, routing overhead, average end to end delay and throughput with respect to malicious node ratio and node mobility speed		

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Gurung et al. [43]	AODV	Y	Y	Alert packet	MGAM	Cover maximum area to detect malicious nodes Does not use any additional control packets in base protocol High PDR, throughput and low routing overhead at low mobility speed	Static threshold value	Random waypoint model Mobility speed: 5, 15, 25 and 35 m/s Metric: packet delivery rate, average throughput, routing overhead, normalized routing overhead with respect to node mobility speed	2016	NS-2
Kumar et al. [19]	AODV	Y	N	Not used	Proposed AODV	Reduces routing overhead and provides faster communication due to use of HELLO packet	High delay and routing overhead than normal AODV	Random waypoint model Mobility speed: 20 m/s Number of nodes: 20, 30, 40, 50, 60 Pause time: 2, 5, 10, 20 Metric: packet delivery rate, average end to end delay, dropped packets and routing overhead with respect to node mobility speed and malicious node percentage with respect to the number of nodes and pause time	2016	NS-2

Table 2 (continued)

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Panos et al. [54]	AODV	Y	Y	Alarm packet	CUSUM	Accurate detection of black-hole nodes at minimal false positives even when nodes are performing partial dropping attack	Assume that no attack takes place during the training phase	Random waypoint model	2016	NS-3
						High detection at static network when node speed is 0 m/s	The false positive ratio of the standard CUSUM increases when speed increases and decreases	Mobility speed: 0 to 10 m/s		
						Does not have significant computational overhead so CUSUM test is suitable for infrastructure-less networks		Number of nodes: 25, 50,75, 100 Metric: PRW and packet delivery ratio with respect to black-hole intensity		
Singh [39]	AODV	Y	Y	Alert packet	Mobile trust points with Clustering	Performs better than AODV under attacks	Energy consumption due to monitoring of cluster head activities	Malicious nodes: 5, 10, 15, 20 Metric: detection rate, packet delivery rate, average end to end delay and average throughput with respect to malicious node	2016	NS-2
Gurung et al. [20]	AODV	Y	Y	Alert packet	MBDP-AODV	Based on dynamic threshold value of the sequence number	Cannot detect the gray-hole attack	Random waypoint model	2017	NS-2
						Detects black-hole node during route discovery phase	High routing overhead	Mobility speed: 5, 15, 25 and 35 m/s		
						Performs better than IDSAODV protocol in terms of PDR and throughput		Metric: packet delivery rate, average throughput and routing overhead with respect to node mobility speed and malicious node percentage		

Table 2 continued

References	Base protocol	Protocol modification	Extra control packets	Control packets name	Proposed protocol/ scheme	Merits	Drawbacks	Parameters and metric used	Year	Simulator used
Pu et al. [55]	DSR	Y	Y	RREQ'	EBAD	High PDR when network is static Performs better than CBDS and 2ACK scheme Reduces the energy consumption and detection latency	EBAD is not originally designed to deal with an adversarial scenario that the malicious node is located in the shortest path to the destination node	Random waypoint model Maximum mobility speed: 20 m/s Metric: packet delivery ratio, detection rate, detection latency, energy consumption etc.	2017	OMNeT++
Delkesh et al. [56]	AODV	Y	Y	Fake packet Modified request and reply packet	EAODV	Nodes execute uniform algorithm independently Detect single, multiple black-hole, internal and external black-hole attack in the network Performs better than IDSAODV protocol in term of delivery, loss rate, throughput and delay	Cannot detect the smart gray-hole attack due to genuine participation in route discovery process	Random waypoint model Number of nodes: 50, 60, 70, 80, 100, 200 Maximum mobility speed: 50 m/s Metric: Packet delivery rate, packet loss rate, end to end delay and routing overhead with respect to different nodes	2018	NS-2
Ndajah et al. [57]	AODV	Y	N	Not used	SBAODV	Detect single and multiple black-hole nodes	Cannot detect the smart gray-hole attack due to genuine participation in route discovery process	Random waypoint model Metric: Packet delivery rate, overhead and throughput with respect to time	2018	NS-2
Veeraiah et al. [58]	AODV	Y	Y	Information of detected malicious node communicated to cluster head through sink node	Trust-aware FuzzyClus-Fuzzy NB	Minimum delay, minimum energy consumption, maximum detection rate and maximum throughput as compared with KmeansNB and NBTrust methods	May not be suitable for highly mobile environment due to frequent clustering overhead and maintenance	Number of nodes:100 Metric: Delay, throughput, detection rate and energy consumption with respect to time	2019	NS-2

3.2.8 Drawbacks

All the techniques which have been proposed by the researcher also have some drawbacks which have been discussed.

3.2.9 Parameters and metrics

In this, the various parameters and metrics used by the researcher for the evaluation of techniques are discussed.

3.2.10 Year

In this, the year is mentioned in which different researchers have proposed a protocol or scheme.

3.2.11 Simulators

Network simulators like NS-2, Glomosim, and OPNET etc have been used by many researchers for validating the efficiency of their proposed protocol or scheme. It has been found that NS-2 is used many times by different researchers.

3.3 Schemes

3.3.1 Cryptography based schemes

In [9], the author has designed new protocol named Security Enhanced AODV protocol for wireless mesh networks that makes use of Blom's key pre-distribution scheme for computing the pairwise transient key (PTK) through the broadcasting of extended HELLO packet and then uses the established PTK to distribute the group transient key (GTK). In order to authenticate the unicast and broadcast routing messages, PTK and GTK key are used respectively. Each pair of nodes shares a unique PTK key, while GTK key is secretly shared between the node and all its one-hop neighbours. In this technique, the standard AODV routing message is extended to include message authentication code (MAC) for the guarantee of the message's authenticity and integrity in a hop-by-hop fashion. The simulation results show that SEAODV avoids routing attacks in the network and perform better in comparison with ARAN and SAODV in terms of route acquisition latency and computation cost. The disadvantage of this approach is that it incurs high communication cost due to the exchange of keys.

A new key exchange mechanism called Instant Key Generation Mechanism [10] is proposed for eliminating the pre-distributed keys requirement. In the pre-distributed scheme, keys are already installed at the nodes between group members to set up common secret key which requires memory and are distributed over the network due to which the attackers can identify the key and make forge acknowledgment. In order to avoid this pre-distribution of key requirement, they proposed a new scheme in which new keys are generated instantly by every node when it takes part in the communication. All acknowledgment packets generated by the nodes are digitally signed before they are sent out and are verified. Therefore, in this technique forging of acknowledgment packet by the attacker is not possible. The simulation results show that the proposed approach is having better performances as compared to other acknowledgment schemes. The disadvantage of this approach is huge computation cost due to frequently computation of new keys by the nodes.

3.3.2 Overhearing based schemes

In [11], the authors have proposed a scheme that is the combination of two major components, termed watchdog and path-rater, for detecting and mitigating routing misbehaviour node in the network. In this scheme, all nodes are in a promiscuous mode in which it overhears the activity of its neighbor node. If the next hop node is cooperating and working as a normal node by forwarding the data packet then the data packet is cleared from the buffer of the node which is watching its neighbor activity. If a data packet continues to be in the buffer for a long time, the watchdog component declares its next hop neighbor as a misbehaving node whereas the path-rater component rates every path in its cache and finally selects the path that best avoids malicious node. But there is some limitation of this technique that fails to detect malicious node and gives false information of its next neighbor node as a misbehaving node in the presence of ambiguous collisions, limited transmission power, and receiver collisions. This false information about the genuine node as a misbehaving node is termed as false positive.

In [12], the author proposed an approach to mitigate the black hole attack by judgment process. In this approach, each node gives their opinion about the honesty of its neighbor's nodes by overhearing its activities. Whenever a node gets all the opinions of neighbors, it decides whether the replying node is the malicious node or not based on number rules. If a node is the first receiver of a reply (RREP) packet, it forwards packets to source and starts the judgment process on about replying node. Therefore, the judgment process is totally dependent on the opinion of the network's nodes about the replying node. The disadvantage of this approach is that opinions are not always correct because any node can give a false opinion of others.

3.3.3 Sequence number threshold based schemes

Dynamic Learning Method is proposed in [13] which based on a threshold that calculates the dynamic threshold value at the regular interval of times according to changing network environment. It used a multidimensional feature vector to express the state of the network at each node. In traditional schemes, static training data is used for defining the state of the network. Due to dynamic network topology characteristic of mobile ad hoc networks, such static training method could not be efficiently used. In order to define the state of network, three features are used i.e. number of sent out request packet, number of received reply packet and the average of difference of destination sequence number in each time slot between the sequence number of reply packet and the one held in the node list which is maintained by each node.

Dynamic threshold based protocol is proposed by [14] in which the threshold value is dynamically updated in every time interval. This solution also removes the limitation of those solutions which were using a static threshold value. According to their solution, the source node checks to find out whether the reply's sequence number is higher than the threshold value. If it is found to be higher than the threshold value, the node is declared as a malicious and it adds the node to the blacklist and broadcasts the alarm packet to inform other nodes about its id so that further communication by this node is discarded. The threshold value is computed by taking an average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the reply packet.

In [15], a new protocol called Reverse Ad-hoc On-demand Distance Vector (R-AODV) is proposed which not only deals with black hole attack but also deals with the gray-hole attack in the network. The authors have modified the functionalities of node receiving request (RREQ) packet, sending the request (RREQ) and receiving the reply (RREP) packet. It dynamically calculates PEAK value which is based on the number of RREQ packet sent, number of received reply (RREP) packet and sequence number in the routing table. After every RREP packet received, the value of PEAK is calculated by the addition of these three parameters to the previous value of PEAK. Before a route is to be established, each node checks the destination sequence of RREP packet with the PEAK value. If it is greater than PEAK value then the node marks this RREP as DO_NOT_CONSIDER and marks the node sending RREP as a malicious node. Therefore, RAODV not only detects the malicious node but also isolates the multiple malicious nodes present in the network during the route discovery phase which helps in the establishment of the short and secure route towards the destination. The advantage of this approach is that it has low routing overhead as it does not use any extra control packet for notifying other nodes regarding the black-hole or malicious node. It uses standard RREQ and RREP packet to notify other nodes about the presence of malicious node.

In order to further enhance the performance of MANET, the author made some modification in the functionality of node receiving reply (RREP) packet in R-AODV protocol and proposed an extension of above protocol called as Modified Reverse Ad-hoc On-demand Distance Vector (MR-AODV) [16]. In this protocol, the intermediate node does not forward the reply (RREP) packet back to the source node on the reverse path once it detects the node sending RREP as a malicious and also it does not require DO_NOT_CONSIDER parameter. Therefore all RREPs packet reaching source node are from the genuine node and the RREP packet containing the shortest and fresh path is selected for the data transmission. The main advantage of MR-AODV is that it has low routing overhead as compared to R-AODV by not forwarding RREP packet after detection of the misbehaving node in the network.

Secure Route Discovery for the AODV protocol (SRD-AODV) is proposed in [17] for dealing with black hole attacks. In this protocol, it is required that the source node and the destination node has to check the sequence numbers in the route request and route reply packet respectively with threshold value before creating a connection with the destination node for transmission of data packets. Three fixed threshold values have been defined for classifying real nodes and malicious nodes in three different types of environments which is small, medium and large. The drawback of this approach is that the threshold value is fixed which may not be feasible in a high mobility environment.

Dynamic Sequence Number Threshold protocol is proposed in [18] in which sequence number based threshold value is calculated which is compared with the reply packet sequence number. An additional field named grade is added in the routing table. When a node receives an RREP packet it checks reply packet's destination sequence number with the sequence number threshold value. If the value of sequence number in reply packet is less than the threshold value then the packet is accepted otherwise the node grade in the routing table is changed to malicious' from which the reply packet is received and finally reply packet is dropped.

In [19], the packet processing technique of normal AODV is improved in order to detect routing misbehaviour and alert other nodes by using default AODV control packets i.e. HELLO packets so that there is no additional overhead. In this approach, the authors have calculated the threshold value based on a number of requests sent and reply packet received.

Mitigating black-hole attack through detection and prevention Ad-hoc On-demand Distance Vector (MBDP-

AODV) protocol based on dynamic threshold value of the destination sequence number is proposed in [20]. In this approach, the source node sends the data packets after receiving the reply packet. Whenever it receives the minimum three replies packets, it calculates the threshold value and detects the black-hole attack. The drawback of this approach is that it has high routing overhead due to multiple replies packets sent by the destination node.

3.3.4 Acknowledgment-based schemes

Two hop ACK [21] approach is proposed which is based on acknowledgment scheme that use a special acknowledgment packet called as TWOACK packets, that are given a fixed path of two hops (or three nodes) in the direction opposite to that of data packets. In order to implement this approach, an authentication mechanism is used so that the next hop is prevented from sending a forged ACK packet on behalf of the intended two-hop neighbor. If no acknowledgment is received from the two-hop neighbor, it suspects the link as misbehaving links which is not chosen in the next route discovery process. The drawback of this method is that it has cannot detect misbehaving nodes and has high routing overhead.

2ACK is proposed by [22] that help in detecting routing misbehaviour and mitigating its adverse effect. The 2ACK methodology is based on the idea of sending two-hop acknowledgment packets in the opposite direction of the routing path. The receiving node only sends two hop acknowledgment packets for a fraction of received data packets. It can be incorporated as an add-on to the standard routing protocols for MANETs, such as DSR for detecting routing misbehaviour in the network.

The AACK [23] is a scheme which is based on network layer acknowledgment and consists of the combined approach of Enhanced-TWOACK and an End-to-End acknowledgment scheme. It enhances the performance of TWOACK scheme by using end-to-end acknowledgment scheme for reducing the routing overhead of TWOACK and maintaining good performance. In this approach, if the source node receives the acknowledgment, it means there is no malicious node in the network. It has also taken timeout threshold value as a parameter which is used to detect the misbehaving node when it is dropping the data packets more than this timeout threshold value. The advantage of this approach is that its detection efficiency is increased as compared to TWOACK by applying node detection algorithm for detecting malicious node more accurately.

In [24], the author proposed an approach for detecting the malicious node. According to this approach, when a path is established the source node forms different sets that consist of three consecutive nodes which are left, middle and right node. Each node of the network maintains a list of misbehaving nodes. When LeftNode forwards the packets; it makes entry of forwarded packets in list data structure and waits for two acknowledgment packets. If none of the acknowledgment packets is received within their threshold time limit T1 and T2 respectively, that set is considered as a malicious set. Within threshold time T1, if E-2ACK1acknowledgment packet is received then LeftNode waits for E-2ACK2 acknowledgment packet else observers its MiddleNode by rating the behavior in promiscuous mode and if rating falls threshold Time TS, LeftNode declares its MiddleNode as misbehaving nodes and if not, Left node declares its RightNode as misbehaving nodes and then flood this information. Within threshold time T2, if E-2ACK2 acknowledgment packet is not received then after time T2 both MiddleNode of that group starts rating their next hop nodes (i.e. RightNode) for time T3 and if number of dropped packets exceeds threshold TS within time T3 then that RightNode is declared as malicious node otherwise LeftNode of second set is declared as malicious node. At last, information of the malicious node is broadcasted across the network and separated. The drawback of this approach is that routing overhead is increased due to 2ACK packets.

The authors in [25] proposed a new approach in which all intermediate nodes have to send acknowledgment on receiving the data packets. Through these acknowledgments, the source node creates a Merkle tree and compares the tree root value with a precalculated value. The end-to-end route is free from packet droppers if both values are equal but this approach is quite resource-demanding. Through simulation, it has been found that the detection efficiency and performance of the proposed approach is better as compared to watchdog approaches in terms of the best delivery ratio of packets and the highest detection ratio.

3.3.5 Cross-checking based schemes

In [26], the author has dealt with the black hole problem and proposed a solution in which it is required that each intermediate node has to send back the information about its next hop whenever it sends back a reply packet. This solution requires the addition of next hop information in the original AODV header. In this solution, it ignores the further reply from the inquired intermediate node. The drawback of this solution is that it works by making an assumption that malicious node does not cooperate with each other which is called as cooperative black hole attack, as it always checks only one next hop node. Although in a real scenario it can be possible.

In [27], a new approach is proposed which is used to identify multiple black-hole nodes cooperating with each other. It removes the limitation of the above solution by

making use of two bits of additional information in data routing information (DRI) table which is maintained by each node. In data routing information (DRI) table, 1 means 'true' and 0 means 'false'. The first bit "From" convey information on routing the data packet from that node while the second bit "Through" convey information on routing data packet through that node. As the black hole node does not forward the data packets to its next hop, the "Through" field in DRI table of the next hop would be zero which means it has not routed the data packets through its next hop but the black-hole node gives false information in DRI table of having routed the data packets through its next hop. The source node verifies with the next hop of the intermediate node whether the intermediate node is has routed the data packers or not by comparing the DRI table of an intermediate node with the DRI table of next hop. If there is the mismatch in the DRI table information of the intermediate node and next hop, then the intermediate node is declared as a malicious node. The drawback of this approach is that it increases average end to end delay along with routing overhead when mobility increases due to frequent path break up. The author proposed the approach for cooperative black hole detection and prevention but did not test this approach in any network simulator or in a real environment.

A distributed and cooperative mechanism is proposed by [28] for combating with the multiple black-hole attack that consists of four steps i.e. local data collection, local detection, cooperative detection, and global reaction. This approach uses an estimation table similar to DRI table with extra two fields of RTS/CTS and Suspicious field. According to this approach, the first local data is gathered through overhearing for detecting the suspicious node. If there is suspicious one, the detecting node initiates the local detection procedure to check whether the suspected one is a malicious black-hole node. After that, the initial detection node starts cooperative detection by first broadcasting and informing all the nearby neighbors of the possible suspicious node to participate cooperatively whether the suspicious node is a malicious node. When it is found to be a malicious node, the global reaction is started immediately to alert the other nodes of the malicious node identity.

The authors in [29] proposed a solution for the prevention of cooperative black-hole attack. It has been found that the solution resulted in good performance in terms of minimum packet loss percentage and throughput. It can accurately detect and prevent the cooperative black-hole attacks. The drawback of this approach is that the routing overhead and delay increases when mobility increases because it uses more route request and further requests packet to check every next hop.

The authors in [30] presented a solution for mitigating the black-hole attack in the network that consists of three steps in which the first step is about finding the freshest path, second is about checking the path and last is about eliminating the malicious node. In this approach, when a node sends the reply packet it must put its next hop information and previous hop information along with the DRI entries for both of them in the reply packet. The source node firstly checks the next hop of reply generator and request for next hop id and DRI table entries for previous node and its own next hop in the path. On receiving DRI tables, the source checks whether the intermediate node is a malicious node or not. Through the simulation results, it has been found that this approach has reduced the packet overhead and processing time of detecting black hole nodes by 56% and 64% respectively. The drawback of this approach is that it increases the average end to end delay of data packets due to cross-checking.

3.3.6 Trust-based schemes

In [31], the authors proposed a common neighbour listening mechanism for combating with black hole problem in which common neighbour is selected that neighbour of two different nodes. The common node with a higher trust value is chosen when there are two common neighbours and listen to the network to check the neighbour transmission. If any node is dropping packet the common node will decrease its trust value and checks with trust threshold value. If any trust value is less than the threshold value, it is declared as a malicious node otherwise normal node. The drawback of this approach is that it has taken an assumption that the density of node in the network should be high and there is not much change in the neighbour set during route discovery but when mobility speed increases the neighbour set keep on changing and the chances of common neighbour becomes very less. Therefore, this approach cannot work in the highly dynamic network topology.

In [32] the author has proposed a trust-based routing protocol in which every node maintains a trust value for each of its neighbors. In order to maintain the trust value, a new control packet is used called as trust packet which is periodically exchanged between the nodes. This approach deals with two kinds of attacks, namely, the black-hole attack and the gray-hole attack. In this protocol, only the destination node is allowed to send reply packet due to which average end to end delay of data packets increases. It also has drawbacks of routing overhead due to a periodic exchange of trust packet.

In [33], the author has proposed a new framework called as Reputation-based internet protocol security framework which provides not only protection from external attacks but also provides security from internal attacks. The

external attacks are prevented through encryption while internal attacks are mitigated by behavior grading that assigns trust values to nodes based on their participation during the routing process. In this technique, the sender and relay nodes overhear downstream nodes to check whether the packets have been received and acknowledged or not. The upstream nodes increase the reputation index for downstream relay nodes that acknowledge receipt of packets. The simulation result shows that the number of routing errors was reduced by approximately 52% but due to the security provided by the framework, the throughput of the network decreases which is acceptable for increasing the security. The advantage of this approach is that it improves the network availability by using round-robin multipath routing algorithm.

In order to overcome with black hole attack problem, the authors proposed an enhanced Ant-based defense mechanism for selective forwarding attack [34] in MANET. In this mechanism, the trust model is used that defines the trustworthiness of the node based on the number of time the packet is dropped. The authors have used two ant agents which are forward ant agent that performs trust mechanism and the backward agent that detects the misbehaving node in the path. The forward ant agent establishes the path to the source whereas the backward ant agent establishes the path to the destination. In order to send secure acknowledgment packet, S-ACK scheme is implemented. The forward ant agent collects the information of S-ACK packet and when it reaches the destination; it sends back the digitally signed S-ACK packets through the backward ant agent to detect the malicious node by comparing trust value of S-ACK packet with the predefined threshold value. In this approach, the challenge and monitoring packet is also sent by the source node for monitoring the neighbor node. The drawback of this technique is that routing overhead is increased due to extra control packets.

3.3.7 Cross-layer collaboration based schemes

In [35], the author introduced a new approach for detecting the malicious node in which session layer interacts with the network layer for detecting misbehaving nodes that drop data packets in MANET. There are two stages in this approach, the first stage is the monitoring stage in which each node checks its direct neighbours whether they are forwarding data packets of a traffic session in the network or not, and the second stage is the decision stage in which decision is taken whether the monitored node misbehaving or not. The advantage of this approach is that it is able to detect malicious activity in the network under power control employment with a low communication overhead. However, the disadvantage of this approach is that it does not deal with the mobility of nodes and cooperative attack.

Two-level secure re-routing (TSR) is a two-level approach [36] that deals with black hole node by detecting it at the transport layer and then communicating it at the network layer. The detection of malicious activity is done by observing any variations in the size of the transmission control protocol (TCP) congestion window. If there is any abnormality then re-routing process takes place at the network layer to find a new route towards the destination. Two modules have been used i.e. local supervision and congestion window surveillance (CWS) modules that confirm the presence of any malicious activity in the network.

3.3.8 Clustering based schemes

Clustering based approach is proposed in [37] for the prevention of black-hole attack in which the network is divided into clusters and cluster head (CH) is elected from the cluster for the detection of black hole attacks locally. The authors have used three parameters to give weight to each node for the election of the cluster head. In the first parameter, i.e., relative stability value, the longer time life of clusters can be guaranteed. In the second parameter, i.e., connectivity value, the good connectivity used to shape communication between cluster head and cluster members can be achieved. In the third parameter, i.e., the credit value, the packets dropping behavior is taken into consideration so that it impossible for black hole nodes to be elected as CHs. As the network is monitored by the cluster head, this technique is able to prevent black hole attacks even in the network where many separate or collusive black hole nodes exist. The drawback of this technique is that gray hole can become as cluster head because it behaves genuinely sometimes due to which if it is selected then it can cause degradation of the network.

In [38], the author proposed Cluster-Based Datagram Chunk Dropping Detection and Prevention technique in which the cluster head (CH) detects the malicious node. The node is elected as a cluster head which has high battery back up in the cluster. In this approach, the data to be transmitted is divided into chunks. Each chunk is assigned a number and then transmitted from source to destination through the optimum path chosen within the cluster. These chunks which have been sent from source make their entry in a buffer at the source node. The source node sends its buffer to the cluster head which compares its values with the buffer values maintained at each intermediate node. If the values of the chunk number do not match at a particular intermediate node, it means there is a malicious node in the network dropping datagram chunks. The drawback of this technique is that there can be chances that the gray-hole

node becomes a cluster head which can lead to performance degradation of the network. This approach also introduces some delay and requires high battery backup.

The authors in [39] proposed a solution for mitigating the black-hole attack in MANET by using mobile trust points with clustering. The proposed scheme uses some mobile trust points which monitor the activities of cluster heads in order to detect the attack and then generate ALERT in the network if any black hole node is detected. The drawback of this approach is that monitoring of activities is required due to which there will be energy consumption in such resource constraint network.

3.3.9 IDS based schemes

In [40], a new mechanism called as Anti Black Hole mechanism is proposed in which special node i.e. IDS node is deployed in the network. According to this mechanism, the IDS node increases the suspicious value of node according to the abnormal difference between the request and reply packet transmitted from the node. The intermediate nodes are forbidden to send the reply to the request packet. If any intermediate node is not the destination and that has never broadcasted a request packet for a specific route, but forwards a reply packet for the route, then nearby IDS node will increase its suspicious value by 1 in the nearby IDS node's suspicious node table. When the suspicious value of a node exceeds the threshold value, IDS node broadcast block message to all nodes in the network for isolating suspicious node from the network. In this approach, if the reply is sent by a node which does not forward the corresponding request packet previously, they are suspected to be malicious nodes and if the suspected value exceeds the threshold, they are isolated. But the gray hole nodes behave normally during the route discovery process by sending true information about destination sequence number and hop count. Once the path is established containing that node, it drops data packets selectively. The drawback of this approach is that it cannot detect gray-hole nodes.

In [41], the author has given a new solution for detecting the gray-hole node based intrusion detection system (IDS). When destination node does not receive the actual number of data, it sends a query request packet to the node which is at a 2-hop distance from it and waits for query reply. The query reply packet contains information about the number of data packets a node has forwarded to its next hop neighbor in the source route. After receiving query reply packet, the destination node checks whether its previous hop neighbor has forwarded all the data packets that it received from its previous node. If not the makes its entry into the suspected list and notifies to the nearby IDS nodes about the suspected nodes present in the network. The IDS nodes that are deployed in the network monitor the malicious node's transmission and broadcast the block message to all the nodes whenever it finds an anomaly in the network and then isolates the misbehaving node from the network. The Glomosim simulator is used to validate the effectiveness of the proposed intrusion detection system. The advantage of this approach is that it helps in less energy loss due to the fact the IDS nodes are set into promiscuous mode only when destination node notify it which makes it suitable for the resource-constrained network. The simulation results have shown that the packet loss rate in the proposed approach is better than DSR in presence of multiple gray-hole nodes.

In [42], an approach called Genetic Algorithm and Artificial Immune system (GAAIS) based on genetic algorithm (GA) and artificial immune system (AIS) is used for dynamic intrusion detection in an AODV-based network. Each normal feature vector taken from network traffic is represented by a hypersphere with fix radius. The features are divided into four categories in which three features are related to the constant bit rate (CBR) traffic, ten features are related to routing discovery process, five features are related to path disruption and four features are related to routing protocol specific, which is used for anomaly detection in network traffic. In order to detect the anomaly in network traffic, spherical detectors are used which is generated by using the algorithm for covering the nonself space. The advantage of this approach is that GAAIS adapts itself according to changes in network topology by making use of two updating methods: partial and total. The performance of GAAIS has been evaluated in the ns-2 simulator under different types of routing attacks such as black-hole, flooding, rushing, and worm-hole. The drawback of this approach is that some genuine nodes are detected as malicious node i.e. false positive problem.

In [43], the authors have launched the smart gray-hole attack and proposed a new mechanism for mitigating the impact of the smart gray-hole attack. The special nodes called as Gray hole-intrusion detection system (G-IDS) have been used for detection and prevention of smart gray-hole attack. These special nodes overhear the transmission of its neighbouring nodes and when it detects that the node is dropping the data packets which are greater than the threshold value then it broadcast the alert message in the network. The drawback of this approach is that it is based on the static threshold value. The threshold value may be different for the different scenario.

3.3.10 Other schemes

The authors in [44] proposed a mechanism in which the intermediate node sends the reply packet to the source if it

has a route towards the destination. After that, it would send a confirmation request to its next hop. If the next hop has a route towards the destination it would send confirmation reply packet back to the source node and the source node compares the information contained in reply packet which is sent by the intermediate node with the information contained in confirmation reply packet so that it is able to learn whether the path in reply (RREP) is valid or not. If the intermediate would be black hole node then its next hop would send correct information in the confirmation reply (CREP) packet about the hop count towards the destination and sends it to the source node. The assumption made in this approach is that the CREP packet cannot be modified. This approach has the drawback as it cannot detect the cooperative malicious node because the intermediate node and its next hop can give false information.

According to the approach proposed in [45], the source node waits and checks the replies from all the neighbouring nodes to find a safe path. After expiry of the timer, it first checks in collect route reply table whether there is any repeated next hop node. If any repeated next hop node is found in the reply paths it assumes the paths are correct or the chance of malicious paths is limited. The drawback of this approach is that it increases the average end to end delay due to waiting for multiple replies coming from neighbours.

In [46] Intrusion detection system Ad-hoc On-demand Distance Vector (IDSAODV) protocol is proposed in which the impact of black hole attack is mitigated by ignoring the first reply and responding to the second reply. According to this protocol, the author has made an assumption that the first reply always comes from black hole node whenever there are multiple replies. The drawback of this protocol is that there may be a scenario in which malicious node is far away from the source node and the destination node is near to source node. In that case, the first reply will come from original destination node and according to the protocol it would ignore the first reply and responds to next reply which is coming from black hole node and it is accepted by source node resulting into black hole attack. Their solution improved the network performance by about 19% in the presence of a black hole.

In SAODV which is proposed in [47] for combating with the black hole attack, the destination node is verified by using a random number. In this protocol, when source node receives a reply packet, it stores the reply packet in its routing table, and immediately sends a verification packet to the destination node along the opposite direction route of received reply packet. Each SRREQ (request) packet contains a random number which is generated by the source node. When destination nodes receive two requests (SRREQ) packets from multiple neighbour nodes, it directly stores them in the table and compares the content of request (SRREQ) packets whether it contains same random number or not. Similarly, the source node also gets more than two SRREP packets from the neighbour nodes and compares the data to check whether the random number is the same or not. If any of the reply packets are having the different random number, it means that the path contains the malicious node. The drawback of this approach is that the extra control packets are used and routed through different paths due to which routing overhead increases. The delay also increases due to verification of the multiple paths.

In [48], the author proposed a new solution for dealing with the black hole attack in which all the reply packets are collected and stored in the newly created table for a specific time period. Once the timer is expired, it starts analyzing the sequence number of the received reply packets from the table. If there is any reply packet which contains a very high sequence number, that reply packet is discarded. The proposed approach also maintains the identity of the misbehaving node as so that in future, it can discard any control packets coming from that node.

In AODV Secured Against Black Hole attack (AODV-SABH) [49], the destination node rejects the packet which contains the sequence higher than its sequence number. Every node receiving the request packet is required to include its address and the sequence number of the destination node. When black hole nodes receive the request packet, it sets the sequence number of the destination to a high value and forwards the request packet. On receiving this request packet, the destination compares the sequence number with its own sequence number. If it is less than its own sequence number it sends back the reply otherwise it would reject the request packet. The drawback of this approach is that it increases routing overhead.

Secure Adhoc On-demand Distance Vector (SAODV) protocol is proposed in [50] for dealing with black hole attack. It has two phase namely suspicion and confirmation. Through random number, the destination node is verified for each received reply packet by the source node which indicates that multiple paths that are identified are verified. In the first phase, source node extracts the sequence number from each reply packet and also delay is calculated for each of these. If anyone of the value is greater than the average of other value and delay for that reply packet is also low then that source node suspects about the existence of a malicious node in the network. In order to confirm the malicious node, additional control packets are used which are MREQ and MREP which contain an extra field of random numbers. The source node sends MREQ packet with the different random number for the different route and on receiving this packet by the destination node, it sends MREP packet containing the same random number for each MREQ packet. There is a very low probability that

the malicious node will send the same random number as that of the destination node.

In [51], the author proposed a cooperative bait detection scheme for the black hole attack detection which consists of three stages namely the initial bait stage, reverse tracing stage and reactive defense stage. In this scheme, the source node stochastically selects an adjacent next hop node and cooperates with it by taking the address of this next hop node as bait destination address to make malicious nodes to send a reply message. By using a reverse tracing technique, malicious nodes are detected and prevented from the participation in the route discovery process. In this approach, it has taken assumptions that whenever there is a significant drop in the packet delivery ratio (PDR), an alarm packet is sent by the destination node back which makes source node to start the detection mechanism again. In this scheme, proactive detection is done in the initial stage and reactive response at the subsequent stage in order to reduce the resource wastage. The drawback of this approach is that it can take its adjacent next node as a bait address which can be malicious node [52].

Anti Near Blackhole Adhoc On-demand Distance Vector (ANB-AODV) is proposed in [53] in which the author has made some modification in order to mitigate the impact of the black hole in the network. According to ANB-AODV protocols, it responds to the first reply and then responds to the subsequent replies packet. In this protocol, not only the source node but the intermediate node also updates its routing table whenever subsequent reply packets are processed.

The authors in [54] have proposed a mechanism that uses a dynamic threshold cumulative sum (CUSUM) test in order to detect abrupt changes in the normal behavior of AODV's sequence number parameter. The advantage of the proposed mechanism is that it accurately detects black-hole attacks with minimum false positives rate even if the malicious nodes are dropping the packets selectively. The drawbacks are that it assumes that no attack takes place during the training phase and the false positive ratio of the standard CUSUM increases when speed increases and decreases.

Explore-based active detection (EBAD) is proposed in which the basic idea is that a source node broadcasts a route request packet with a fictitious destination node to lure potential malicious nodes to reply a fake route reply packet. The EBAD is also incorporated with a digital signature technique in order to detect faulty information in the route reply packet. A route expiry timer is deployed to reduce the effect of route cache pollution caused by the fake route reply [55]. The drawback is that EBAD is not originally designed to deal with an adversarial scenario in which the malicious node is located on the shortest path to the destination node. According to solution proposed in [56], malicious nodes are identified by getting reply of the fake route request packet which contains the address of non-existing destination node. This scheme cannot detect the smart gray-hole attack in which malicious node participates genuinely in route discovery process. In [57], each node maintains an activity table and when it receives reply packet, it checks the value stored in activity table and decides whether the node is trusted or not. The drawback of this approach is that it cannot detect smart gray-hole attack in which malicious node participates genuinely in route discovery process and does not send any false reply packet. Hybrid schemes Trust-aware fuzzy clustering and fuzzy Naïve-Bayes (trust-aware FuzzyClus-Fuzzy NB) is proposed in [58] which is based on trust and clustering schemes. The drawback of this scheme is that it will be not suitable for high mobile-based network due to clustering formation & maintenance overhead.

4 Merits, drawbacks, and suitability of schemes

As we have described the drawbacks of various techniques in Table 2, some of the main drawbacks of these techniques are common which are presented in Table 3. Table 3 also discuss about merits and suitability of schemes as per simulation results in the available literature. In overhearing based schemes, the major drawbacks is that every node is required to be in sniffing mode due to which there will more energy consumptions and also in promiscuous mode, there are high chances of false positive.

Acknowledgment based schemes also result in high routing overhead due to extra control forwarding of acknowledgment packet by the node after receiving the data packets. Due to this, routing overhead increases and more energy is consumed which is not suitable for resource constraint network.

Trust-based solutions also have similar problems as there is the periodic exchange of trust values between the nodes which also results in routing overhead and more energy is also consumed due to monitoring and calculation of threshold values as compared to overhearing based schemes.

Sequence number threshold based schemes do not identify the malicious node completely due to openness nature of MANET, the smart attacker has an idea of ongoing communication between the nodes and based on communication, it will try to send a sequence number that is enough to attract the traffic towards itself and escape from detection.

Cryptography based scheme although provides protection from the external threats but an internal attacker can create havoc in the network. This scheme requires high

Table 3 Merits, drawbacks and suitability of various schemes

Schemes	Merits	Drawbacks	Suitability
Overhearing-based scheme	Detects single and multiple black-hole nodes	High False positive Energy consumptions	From the simulation results, it has been proved that during moderate and extreme mobility scenario, the overhearing based scheme gives good packet delivery ratio and throughput
Acknowledgment-based scheme	Good detection rate at low mobility speed	Huge routing overhead due to the extra control acknowledgment packets False positive increases in case of high mobility	From the simulation results, this scheme is mainly suitable for static or low mobility scenario because acknowledgment packet is sent after reception of data packets which may not be received by the source node when high mobility scenario is used leading to very high routing overhead
Trust-based scheme	Detects single and multiple black-hole nodes	Routing overhead due to the periodic exchange of trust values Energy consumptions due to monitoring the traffic of neighbor nodes and calculation of threshold values	In this scheme, the trust value of the node is calculated based on its activity in the network. From the simulation result, the performance is good in the static network rather than in a dynamic environment in which there is a high delay and routing overhead as the mobility speed increases
Sequence number threshold-based scheme	Detects single and multiple black-hole nodes	If within the threshold value, it will not able to detect and prevent the attack Delays and routing overhead increase in case of waiting for multiple reply packets by the source node	This scheme is suitable in both scenarios i.e. static and dynamic. Dynamic threshold values give better result as a comparison with static threshold value because MANET is dynamic in nature. In a highly mobile environment, destination sequence number keeps on increasing after frequent disconnection due to which static based threshold approach will not be efficient
Cryptography-based scheme	Good against external threats	Computation and communication overhead	The cryptography scheme is generally good for the static network and gives good PDR and throughput as the nodes have to share a key with other nodes secretly. In a dynamic environment, due to movements of nodes, the key sharing process will be difficult due to which malicious node will escape and there will be high communication and routing overhead
Clustering-based scheme	Good against the single black-hole, multiple black-hole and collusive black-hole attacks	Cluster formation and maintenance overhead in a high mobility scenario Possible chances for a malicious node to become CH because gray-hole node behaves sometimes as a genuine	This scheme is suitable in static or low mobility scenario because cluster head is elected among the nodes whereas, in case of high mobility scenario, there will be more computational overhead
Cross-layer-based scheme	Ensure High detection accuracy Low false alarms	Layer dependency Requires changes in multiple layers	This scheme is based on multi-layer cooperation and is generally suitable for the static network
Cross checking-based scheme	Good against cooperative black-hole attacks in case of cross-checking with DRI table	Increases routing overhead and delay Energy consumptions	This scheme is mainly suitable in static or low mobility scenario because due to less movement, the source node will be able to cross check with the intermediate nodes which will give good PDR and throughput but routing overhead will be high in high mobility scenario due to frequent disconnection and extra control packets. In high dynamic scenario, delay increases due to cross-checking
IDS-based scheme	Single and multiple black-hole attacks can be detected by IDS nodes	Randomly placement of IDS nodes will lead to less detection of the malicious nodes. Require full coverage of network area	The scheme is suitable for static as well as dynamic as the special nodes are to be deployed in the networks which monitor the activities of nodes in the network and have low routing overhead. The more is the IDS nodes in the area, the more is the detection rate with 100% packet delivery rate and zero false positives if the proper threshold value is set in case of black-hole attack

computation and communication cost which is not feasible in resource constraint network.

In the clustering based scheme, cluster maintenance is an overhead in case of high mobility scenario due to dynamic network topology. Sometimes cluster head (CH) is selected based on residual energy, if it has the high energy it will become CH. If the gray-hole node becomes cluster head of the cluster, it would cause performance degradation of the network.

In the cross-layer based scheme, more than two layers communicate with each other in order to detect the malicious nodes. This scheme may fail if there is an attack in other layers due to which intercommunication between layers will not be possible and hence attacker may escape from detection.

Cross-checking is another scheme that helps in identifying the nature of the node by doing cross-checking with its next hop or previous hop node. By sending an extra control packet for cross-checking, there is more consumption of energy and an increase in routing overhead.

IDS based schemes have a special node called IDS nodes which are always in sniffing mode. Although energy consumption is less due to fact that all other nodes in the network are not in promiscuous mode but if there is improper placement of IDS node then some of the malicious nodes cannot be detected. Full coverage by IDS can provide the security in the network.

These are the major drawbacks of various schemes which need to be taken into consideration for designing the effective protocols that can combat with the black-hole attack with fewer energy consumptions, minimum routing overhead, minimum delay and with accurate detection of malicious node.

5 Conclusions

In this paper, we have presented about the black-hole attack problem and different possible nature of the node in the mobile ad-hoc network. There are various techniques which have been proposed by the researcher for dealing with the black-hole attacks and these techniques have been classified into various schemes according to their basic operation. In this paper, we have also presented summary of various existing techniques with its merits and drawbacks. Finally, some important merits, drawbacks and suitability of the different techniques have been discussed that need to be taken into consideration for developing an efficient protocol. Moreover, the study done in this paper will be helpful for the researchers who are engaged in designing the protocols for combating with packet dropping attack in MANET.

References

1. Murthy, C. S. R., & Manoj, B. S. (2004). *Ad hoc wireless networks: Architectures and protocols*. Upper Saddle River: Prentice Hall PTR.
2. Perkins, C. E., Beliding-Royer, E., & Das, S. (2004). *Ad hoc on-demand distance vector (AODV) routing*. Roma: IETF Internet Draft, MANET working group.
3. Johnson, D. B., Maltz, D. A., & Hu, Y.-C. (2004). *The dynamic source routing protocol for mobile ad-hoc network (DSR)*. Roma: IETF Internet Draft.
4. Jhaveri, R. H., Patel, S. J., & Jinwala, D.C. (2012). DoS attacks in mobile ad-hoc networks: A survey. In *IEEE 2nd international conference on advanced computing & communication technologies.*
5. Gurung, S., & Chauhan, S. (2019). Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. *Wireless Networks, 25*(3), 975–988. https://doi.org/10.1007/s11276-017-1639-2
6. Gurung, S., & Chauhan, S. (2018). A dynamic threshold based approach for mitigating black-hole attack in MANET. *Wireless Networks, 24*(8), 2957–2971. https://doi.org/10.1007/s11276-017-1514-1
7. Sangi, A. R., Liu, J., & Zou, L. (2009). A performance analysis of aodv routing protocol under combined byzantine attacks in manets. In *Computational intelligence and software engineering. CiSE 2009. International conference on* (pp. 1–5). Piscataway: IEEE.
8. Gurung, S., & Siddhartha, S. (2017). A review of black-hole attack mitigation techniques and its drawbacks in mobile ad-hoc network. In *Proceedings of the 2nd IEEE international conference on WiSPNET* (pp. 2409–2415).
9. Li, C., Wang, Z., & Yang, C. (2010). SEAODV: A security enhanced AODV routing protocol for wireless mesh networks. *Transactions on computational science XI* (pp. 1–16). Berlin: Springer.
10. Dhanalakshmi, K. S., Kannapiran, B., & Divya, A. (2014). Enhancing manet security using hybrid techniques in key generation mechanism. In *Electronics and communication systems (ICECS), international conference on* (pp. 1–5). Piscataway: IEEE.
11. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on mobile computing and networking* (pp. 255–265). New York City: ACM.
12. Medadian, M., Yektaie, M. H., & Rahmani, A. M. (2009, November). Combat with black hole attack in AODV routing protocol in MANET. In *Internet, 2009. AH-ICI 2009. First Asian himalayas international conference on* (pp. 1–5). Piscataway: IEEE.
13. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *IJ Network Security, 5*(3), 338–346.
14. Raj, P. N., & Swadas, P. B. (2009). DPRAODV: A dyanamic learning system against blackhole attack in AODV based MANET. *International Journal of Computer Science, 2*(3), 54–59.
15. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). Improving route discovery for AODV to prevent blackhole and grayhole attacks in MANETs. *INFOCOMP, 11*(1), 1–121.
16. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). A novel solution for grayhole attack in aodv based manets. In *International conference on advances in communication, network, and computing* (pp. 60–67). Berlin: Springer.

17. Tan, S., & Kim, K. (2013). Secure route discovery for preventing black hole attacks on AODV-based MANETs. In *ICT convergence (ICTC), 2013 international conference on* (pp. 1027–1032). Piscataway: IEEE.
18. Salunke, A., & Ambawade, D. (2015). Dynamic sequence number thresholding protocol for detection of blackhole attack in wireless sensor network. In *Communication, information & computing technology (ICCICT), 2015 international conference on* (pp. 1–4). Piscataway: IEEE.
19. Kumar, J., Kulkarni, M., Gupta, D., & Indu, S. (2015). Secure route discovery in AODV in presence of blackhole attack. *CSI transactions on ICT, 3*(2–4), 91–98. https://doi.org/10.1007/s40012-016-0075-2.
20. Gurung, S., & Chauhan, S. (2017). A dynamic threshold based approach for mitigating black-hole attack in MANET. *Wireless Networks*. https://doi.org/10.1007/s11276-017-1514-1.
21. Balakrishnan, K., Deng, J., & Varshney, V. K. (2005, March). TWOACK: Preventing selfishness in mobile ad hoc networks. In *Wireless communications and networking conference, 2005 IEEE* (Vol. 4, pp. 2137–2142). Piscataway: IEEE.
22. Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *IEEE Transactions on Mobile Computing, 6*(5), 536–550.
23. Al-Roubaiey, A., Sheltami, T., Mahmoud, A., Shakshuki, E., & Mouftah, H. (2010, April). AACK: Adaptive acknowledgment intrusion detection for MANET with node detection enhancement. In *Advanced information networking and applications (AINA), 2010 24th IEEE international conference on* (pp. 634–640). Piscataway: IEEE.
24. Dhiman, D., & Sood, N. (2014, December). Enhanced 2ACK scheme for reducing routing overhead in MANETs. In *Parallel, distributed and grid computing (PDGC), 2014 international conference on* (pp. 120–125). Piscataway: IEEE.
25. Baadache, A., & Belmehdi, A. (2012). Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. *Journal of Network and Computer Applications, 35*(3), 1130–1139.
26. Deng, H. M., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communication Magazine, 40*(10), 70–75.
27. Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J., & Nygard, K. E. (2003, June). Prevention of cooperative black hole attack in wireless ad hoc networks. In *International conference on wireless networks* (Vol. 2003, pp. 570–575).
28. Yu, C. W., Wu, T. K., Cheng, R. H., & Chang, S. C. (2007, May). A distributed and cooperative black hole node detection and elimination mechanism for ad hoc networks. In *Pacific-Asia conference on knowledge discovery and data mining* (pp. 538–549). Berlin: Springer.
29. Weerasinghe, H., & Fu, H. (2007). Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In *Future generation communication and networking* (Vol. 2, pp. 362-367). IEEE.
30. Dorri, A., & Nikdel, H. (2015, May). A new approach for detecting and eliminating cooperative black hole nodes in MANET. In *Information and knowledge technology (IKT), 2015 7th conference on* (pp. 1–6). Piscataway: IEEE.
31. Peng, G., & Chuanyun, Z. (2006). Routing attacks and solutions in mobile ad hoc networks. In *Communication technology, 2006. ICCT'06. International conference on* (pp. 1–4). Piscataway: IEEE.
32. Marchang, N., & Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad hoc networks. *IET Information Security, 6*(2), 77–83.
33. Lacey, T. H., Mills, R. F., Mullins, B. E., Raines, R. A., Oxley, M. E., & Rogers, S. K. (2012). RIPsec–using reputation-based multilayer security to protect MANETs. *Computers & Security, 31*(1), 122–136.
34. Kumari, S. V., & Paramasivan, B. (2015, April). Ant based defense mechanism for selective forwarding attack in MANET. In *Data engineering workshops (ICDEW), 2015 31st IEEE international conference on* (pp. 92–97). Piscataway: IEEE.
35. Fahad, T., Djenouri, D., & Askwith, R. (2007, August). On detecting packets droppers in manet: A novel low cost approach. In *Information assurance and security, 2007. IAS 2007. Third international symposium on* (pp. 56–64). Piscataway: IEEE.
36. Saha, H. N., Bhattacharyya, D., Bandhyopadhyay, A. K., & Banerjee, P. K. (2012, August). Two-level secure re-routing (TSR) in mobile ad hoc networks. In *Advances in mobile network, communication and its applications (MNCAPPS), 2012 international conference on* (pp. 119–122). Piscataway: IEEE.
37. Shi, F., Liu, W., Jin, D., & Song, J. (2014). A cluster-based countermeasure against blackhole attacks in MANETs. *Telecommunication Systems, 57*(2), 119–136.
38. Katal, A., Wazid, M., Goudar, R. H., & Singh, D. P. (2013, April). A cluster based detection and prevention mechanism against novel datagram chunk dropping attack in MANET multimedia transmission. In *Information & communication technologies (ICT), 2013 IEEE conference on* (pp. 479–484). Piscataway: IEEE.
39. Singh, M., & Singh, P. (2016, August). Black hole attack detection in MANET using mobile trust points with clustering. In *International conference on smart trends for information technology and computer communications* (pp. 565–572). Singapore: Springer.
40. Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications, 34*(1), 107–117.
41. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Computers & Electrical Engineering, 40*(2), 530–538.
42. Barani, F. (2014). A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system. In *Intelligent systems (ICIS), 2014 Iranian conference on* (pp. 1–6). Piscataway: IEEE.
43. Gurung, S., & Chauhan, S. (2018). A novel approach for mitigating gray-hole attack in MANET. *Wireless Networks, 24*(2), 565–579.
44. Lee, S., Han, B., & Shin, M. (2002). Robust routing in wireless ad hoc networks. In *Parallel processing workshops, 2002. Proceedings international conference on* (pp. 73–78). Piscataway: IEEE.
45. Tamilselvan, L., & Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. In *Wireless broadband and ultra wideband communications, 2007. AusWireless 2007. The 2nd international conference on* (pp. 21–21). Piscataway: IEEE.
46. Dokurer, S., Erten, Y. M., & Acar, C. E. (2007). Performance analysis of ad-hoc networks under black hole attacks. In *SoutheastCon, proceedings on* (pp. 148–153). Piscataway: IEEE.
47. Lu, S., Li, L., Lam, K. Y., & Jia, L. (2009). SAODV: A MANET routing protocol that can withstand black hole attack. In *Computational intelligence and security, 2009. CIS'09. International conference on* (Vol. 2, pp. 421–425). Piscataway: IEEE.
48. Mistry, N., Jinwala, D. C., & Zaveri, M. (2010). Improving AODV protocol against blackhole attacks. In *Proceedings of the international multi conference of engineers and computer scientists* (Vol. 2).
49. Ameza, F., Assam, N., & Beghdad, R. (2010). Defending AODV routing protocol against the black hole attack. *International*

Journal of Computer Science and Information Security, 8(2), 112–117.
50. Yerneni, R., & Sarje, A. K. (2012). Enhancing performance of AODV against black hole attack. In *Proceedings of the CUBE international information technology conference* (pp. 857–862). New York City: ACM.
51. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Systems Journal, 9*(1), 65–75.
52. Jhaveri, R. H., & Patel, N. M. (2015). A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. *Wireless Networks, 21*(8), 2781–2798.
53. Gurung, S., & Saluja, K. K. (2014). Mitigating impact of blackhole attack in MANET. In *International conference on recent trends in information, telecommunication and computing, ITC* (pp. 229-237).
54. Panos, C., Ntantogian, C., Malliaros, S., & Xenakis, C. (2017). Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. *Computer Networks, 113,* 94–110.
55. Pu, C., Lim, S., Chae, J., & Jung, B. (2017). Active detection in mitigating routing misbehavior for MANETs. *Wireless Networks*. https://doi.org/10.1007/s11276-017-1621-z.
56. Delkesh, T., & Jamali, M. A. J. (2018). EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-018-0782-7.
57. Ndajah, P., Matine, A. O., & Hounkonnou, M. N. (2018). Black-hole attack prevention in wireless peer to peer networks: A new strategy. *International Journal of Wireless Information Networks*. https://doi.org/10.1007/s10776-018-0418-z.
58. Veeraiah, N., & Krishna, B. T. (2019). Trust-aware FuzzyClus-Fuzzy NB: Intrusion detection scheme basedon fuzzy clustering and Bayesian. https://doi.org/10.1007/s11276-018-01933-0.

Shashi Gurung received the M.Tech. degree in computer science and engineering in 2014 and the B.Tech. degree in computer science and engineering in 2011 from Punjab Technical University, Jalandhar, Punjab, India. He is currently pursuing the Ph.D. degree in computer science and engineering at National Institute of Technology Hamirpur, Himachal Pradesh, India. His research interests include mobile ad hoc network and network security. He has various publications in reputed journal of Springer i.e. Wireless Network.

Siddhartha Chauhan received the Ph.D. degree in computer science and engineering from National Institute of Technology Hamirpur, Himachal Pradesh, India, in 2013 and the M.Tech. degree in computer science and engineering from Indian Institute of Technology Roorkee, Uttrakhand, India, in 2003. He has published many research papers in international conferences and journal. He is currently with Department of Computer Science and Engineering, National Institute of Technology Hamirpur, Himachal Pradesh, India. His research interests include mobile ad hoc network and wireless sensor network.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.