International Journal of Computer Applications (0975 - 8887)
Volume 183 - No.29, October 2021

# Black Hole Attack in Mobile Ad Hoc Networks: Challenges and Directions

Noble Arden Kuadey
Ho Technical University (HTU)
Department of Computer Science

Lily Bensah
Ho Technical University (HTU)
Department of Computer Science

Baidenger Agyekum Twumasi
Ho Technical University (HTU)
Department of Electrical/Electronics Eng.

Carlos Ankora
Ho Technical University (HTU)
Department of Computer Science

Gerald Tietaa Maale
McCoy College of Education
Department of ICT

Anthony Mawuena Kuadey
St. Francis College of Education
Department of Mathematics/ICT

## ABSTRACT

A mobile ad hoc network (MANET) is a dynamic wireless network with no fixed infrastructure. The nodes move arbitrarily and are capable of communicating with each other without a central authority. MANETs are well suited for several situations such as emergencies, vehicular networks, and military operations. However, the flexible nature of MANET exposes it to attacks such as black hole attacks. The black hole attack is considered as one of the most predominant attacks that poses a threat to MANET. In this attack, an illegitimate node informs a source node of having the optimal route to the destination node, resulting in data packets being redirected and eventually dropped by this illegitimate node. Several works have been carried out to address this issue. This paper presents an overview of solutions proposed to mitigate black hole attacks, research limitations to the proposed works, and future works that need to be carried out.

### General Terms

Security, Mobile Ad Hoc Network (MANET), Routing Protocol

### Keywords

Black Hole Attack, Cooperative Black Hole Attack, Malicious Node, Packets

## 1. INTRODUCTION

MANET is a type of network in which nodes are mobile, their network topology changes dynamically and has no fixed infrastructure [1]. The mobile nodes in MANET can enter or leave the network at any time. Furthermore, they use a multi-hop wireless network to communicate with each other. Also, the nodes in MANET communicate by using routing protocols. This enables the nodes to discover the shortest route between the source and destination nodes. In addition, during communication between two mobile nodes in a multi-hop network, each node can act as a router. MANET's infrastructure-less, multi-hop communication, mobile, and dynamic features make it suitable for several scenarios such as emergencies, vehicular networks, meetings and military operations. However, due to the features of MANET, nodes in the network are vulnerable to a wide range of attacks, such as black hole attack. Black hole attack is very common and one of the security threats in MANETs. Thus, it is important to detect and prevent black hole attacks in MANET. Attacks in MANETs can be generally classified into two main groups, passive and active [2]. In a passive attack, an attacker keeps track of the information between the nodes without modifying or disrupting the flow of information between the nodes [2]. On the other hand, an attacker modifies or changes the information exchanged between the nodes in active attacks [2]. Furthermore, the attacker can disrupt the routing process by dropping packets, injecting the packets, modifying the packets, etc. Security mechanisms are required to mitigate various attacks, such as a black hole in MANET. Several research works have been carried out in order to propose security mechanisms and other techniques for detecting and mitigating black hole attacks and their variants. However, these security mechanisms have their drawbacks in mitigating black hole attacks in MANET. This paper discussed several security mechanisms that researchers proposed to mitigate black hole attacks, their existing challenges, and proposed future work that can be carried out to mitigate black hole attacks in MANET.
The rest of the sections in this paper are organized as follows. Section II explains routing protocols and discusses black hole attack in MANET. Section III presents research works proposed to address black hole attacks. Section IV presents research gaps and future directions. Section V finally concludes the paper.

## 2. ROUTING PROTOCOLS AND BLACK HOLE ATTACK

### 2.1 Routing Protocols

In MANET, routing protocols are responsible for determining the optimal route to carry out communication between the source and destination node [3]. They can be grouped into three major categories: proactive, reactive and hybrid [3], [4], [5]. Proactive routing protocols have routing tables that store information about all the

nodes residing in the network, which is updated whenever there is a change in the network [3]. Furthermore, each node has a routing table from which it checks the next hop node in the route for a destination node before sending a packet to that node [6]. Proactive routing protocols are useful in network topologies that do not have a large number of nodes. Landmark ad hoc routing (LANMAR), Destination Sequence Distance Vector (DSDV), Fisheye State Routing (FSR), Global State Routing (GSR), Optimized State Link (OSLR) routing protocol, Hierarchical State Routing (HSR), Cluster Gateway Switch Routing Protocol (CGSR), Wireless Routing Protocol (WRP) and Zone-Based Hierarchical Link State routing protocol (ZHLS) are examples of proactive routing protocols [3], [5], [6]. Reactive routing protocol, also known as on demand routing protocol, establishes routes for communication between a source node and a destination node only when there is a need to send a packet [3], [5], [6]. Also, reactive routing protocols do not periodically transmit topological information of the network. Temporary Ordered Routing protocol (TORA), Cluster-Based Routing Protocol (CBRP), Signal Stability-Based Adaptive routing protocol (SSA), Ad hoc On-demand Distance Vector routing (AODV), Dynamic Source Routing (DSR), and Associativity Based Routing (ABR) are some examples of reactive routing protocols [3], [5], [6]. The features of proactive and reactive routing protocols are combined to form the hybrid routing protocol. This routing protocol reduces the control traffic overhead that occurs from proactive systems. Also, the hybrid routing protocol reduces the route discovery delays that occur in reactive systems by maintaining a routing table [3]. Some examples of hybrid routing protocol are Dual-Hybrid Adaptive Routing (DHAR), Adaptive Distance Vector routing (ADV), Zone Routing Protocol (ZRP), Sharp Hybrid Adaptive Routing Protocol (SHARP), and Neighbor-Aware Multicast Routing Protocol (NAMP) [3], [5], [6].

### 2.2 Black Hole Attack

The black hole attack is one of MANET's most predominant and dangerous attacks [6]. This attack occurs on the network layer [1]. In addition, it is an attack that enables an illegitimate node to receive a route request (RREQ) packet and reply with a fake route reply (RREP) packet. The RREP packet contains a small hop count and destination sequence number, thus making the source node believe that the malicious node is trustworthy and has the shortest route to that particular destination node [6], [7]. Therefore, if the source node transmits a data packet to the malicious node, which happens to be the black hole node, the packets are dropped and not forwarded by the malicious node [6], [7]. A black hole attack is illustrated in Figure 1, where node 1 represents the source and initiates an RREQ packet to find a path to node 7, the destination node.The nodes 2, 3, 4, 5, and 6 are intermediary nodes. When node 6 receives the RREQ packet from node 1, it generates a fake RREP packet and transmits it to node 1. Thus, upon receiving the fake RREP packet from node 6, node 1 gets assurance that the shortest route to node 7 is through node 6. Subsequently, it sends a data packet to node 7. However, node 6, upon receipt of the data packets from node 1, drops it and does not forward further to node 7. Thus, node 6 is considered a malicious node that has initiated a black hole attack. A variant of a black hole attack is a cooperative black hole attack in which two or more illegitimate nodes collude together to drop packets received [6]. One of the illegitimate nodes serves as a forwarding node which replies the source node with a fake RREP packet. As a result, when the source node sends the data packet through that particular illegitimate node, it transmits the received

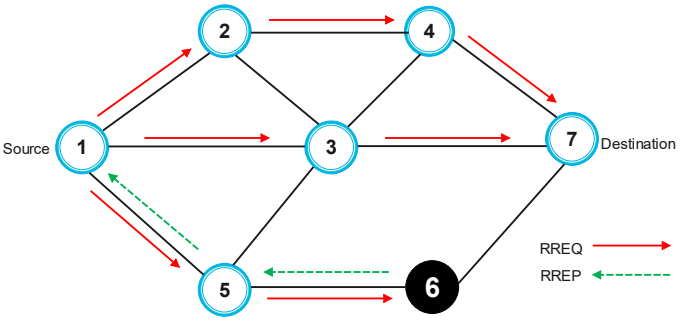


Fig. 1. A Black hole attack: Node 6 acting as black hole by sending fake RREP

data packet to its co-operative partner in attack, who then drops the forwarded data packet.

## 3. LITERATURE REVIEW

The authors in [8] proposed a mechanism that mitigates against both the cooperative black hole and black hole attacks. Their work incorporated check bit into the data routing information (DRI) table and modified the AODV protocol. Their proposed solution detects and eliminates black hole attacks and provides a secure path to the destination node. Similarly, an identification mechanism was proposed to identify malicious nodes [9] in MANETs. In their work, "N" route request messages, further request messages, and further reply messages were used in cross verification to identify malicious nodes. Also, in [10], the authors proposed a tracking mechanism that detects black and gray hole attacks.Their proposed solution consists of two phases. In phase 1, data is securely transmitted to the destination node. However, if there is a drop in packet forwarding, data transmission is stopped and the detection process is initiated. The second phase consists of detecting illegitimate nodes and rendering the network inaccessible to them. However, their proposed mechanism results in computational complexity. The authors in [11] presented a detection mechanism using an Adaptive Neuro Fuzzy Inference System (ANFIS) and Particle Swarm Optimization (PSO) to detect black hole attack. However, their mechanism leads to an increase in computational load on the nodes in the network and an increase in routing overhead due to accuracy in decision making based on information sharing among participating nodes. Also, in [12], a detection mechanism was proposed to prevent black hole attack. In their work, each node has a detection mechanism that determines the suspicious value in order to detect the high capability node in the network. Suppose the detection mechanism detects that a neighboring node has a suspicious value that exceeds the threshold. In that case, it is flagged as an illegitimate node and isolated from the network to prevent other nodes from forwarding their packets to it. However, an illegitimate node will not be detected as a black hole node if it can intelligently keep its value within the acceptable threshold value. Saurabh *et al*. [13] proposed a clustering technique in the AODV routing protocol to mitigate black hole attack. The nodes are grouped into clusters, with each cluster having a head. Furthermore, the cluster head is randomly selected. Check points are deployed in the network to compare the number of received data packets to the number of packets sent by the nodes. If the probability of packets reaching the specified destination is less than the threshold value, then the node is flagged as an illegitimate node. However, due to the mobility nature of MANET, there may be some complications result-

ing in nodes exiting and joining new clusters. Thus, it could lead to false detection of the black hole node. Relief classification algorithm was adopted to mitigate black hole attacks [14]. In their work, they have an offline and online phase. In the offline phase, the most important features from the black hole detection dataset is used to improve the level of the detection rate. In the online phase, network nodes with the previous features are frequently identified. If an identified network node exceeds a predefined threshold value, then it is flagged as a malicious node and excluded from the routes. However, a malicious node will not be detected as a black hole node if it can intelligently keep its value within the acceptable threshold value. Naveena $et\ al.$ [15] presented a trust-based routing scheme to prevent black hole attacks. Their solution consists of the data retrieval (DR) table phase and the route formation phase. The DR table phase identifies and manages data transfer of each node, while the route formation phase predicts a safe path for the transfer of data packet to the destination node. However, due to the periodic update of trust values, their proposed solution leads to routing overhead. Similarly, Arulkumaran and Gnanamurthy [16] proposed a fuzzy logic rule scheme to detect black hole attack. In their work, each node maintains its neighbor node's trust value. The trust value is computed prior to packet transmission. Further, the route trust is computed based on the route trust and the trust value is updated in each node's routing table. If the valid route is valid, then the most trusted node route is selected for transmission of packets. However, due to the periodic update of trust values, their proposed solution leads to routing overhead. Also Veeraiah and Krishna [17] proposed a detection mechanism using fuzzy clustering and Bayesian rule to mitigate black hole attacks. In their work, the nodes are grouped into clusters using a fuzzy clustering technique, which uses the optimal centroid. Furthermore, the node trust table consists of all trust values associated with each node in the network. The detection mechanism analyses the node trust table and if a node is found not to be trustworthy, it is flagged as an illegitimate node. However, their proposed solution leads to maintenance overhead. Furthermore, this detection mechanism is not suitable for networks with many mobile nodes due to the clustering of nodes. Gurung and Chauhan [18] presented a solution using a dynamic threshold value to mitigate against black hole attack. Their proposed solution consists of a dynamic threshold computing module, a detection module and a prevention module. In the dynamic threshold computing module, the source node calculates the dynamic threshold value for the destination sequence number. The source node sends the SUSPECT packet to find an illegitimate node in the detection module and then transmits the ALERT packet in the network. The illegitimate node does not participate in the route discovery process in the prevention module, and other nodes ignore its reply. However, their proposed solution cannot detect a black hole attack if the calculated value is within the threshold value. Furthermore, their detection scheme leads to a high routing overhead. Similarly, the authors in [19] proposed a mechanism to mitigate black hole attack. They defined a threshold value and verified RREP messages using the defined threshold value. The source node verifies the destination sequence number of the RREP messages. If the destination sequence number is less than the defined threshold value, the node is flagged as a malicious node. However, their proposed system is susceptible to black hole attacks if the attacker can intelligently keep its destination sequence number within the defined threshold value. A solution that modifies the AODV routing protocol and provides a secured communication in the network was presented by the authors in [20]. In their work, each node stores the node's identifier, the number of data packets, the number of RREQs and RREPs in an activity table. Furthermore, the public keys of each node are stored in a directory. In addition, each node digitally signs a packet before sending it to another node. A node is flagged as an illegitimate node if it is not a trusted node and its packet is not digitally signed. However, due to the involvement of keys, their proposed solution leads to a high computational overhead. The authors in [21] presented MBDP-AODV protocol, a protocol that uses dynamic sequence number threshold to mitigate black hole attacks. Their protocol has three phases. The source node computes the mean and standard deviation in the first phase using the destination sequence number. The computed standard deviation number represents the threshold value. The source node sends the suspect packet to the next hop to identify a malicious node with a suspected destination sequence number in the second phase. If any node has a hop count of 1 and a suspected sequence number, an alert packet that has a suspected sequence number and illegitimate ID is transmitted by the source node. The malicious node is stopped from taking part in the route discovery process in the final phase. However, their proposed solution results in a high routing overhead. Similarly, the authors in [22] proposed an agent-based AODV protocol to mitigate black hole attacks. In their work, when a route reply message is received, a node designated as an agent examines the probability of all the nodes in the incoming route request message. The nodes with the highest probability are forwarded to the blacklist and further examined to see whether they are already part of the list. ALERT packets are transmitted across the networks. Subsequently, route reply from the nodes that are blacklisted is avoided. Panos $et\ al.$ [23] developed a detection mechanism that detects sudden changes in AODV's sequence number parameter's normal behaviour. Their mechanism has training and normal phase. In the training phase, the cumulative sum algorithm computes a random sequence $X_n$. This is transformed into another random sequence $Z_n$. Furthermore, the algorithm computes the random sequence $Y_n$. In addition, the threshold value $N$ is calculated. The cumulative sum algorithm computes $X_n$, $Z_n$, $Y_n$ at each time interval in the normal phase. If $Y_n$ crosses the threshold value $N$ at any time interval, a black hole attack is detected. Thus, the normal phase triggers an alarm and notifies other nodes on the network. However, should there be an attack during the training phase of their detection mechanism, the attack cannot be detected since they assume there was no attack during the training phase. The authors in [24] presented a routing algorithm that sends forged packets. In their work, the source node sends a forged RREQ packet that does not have a legitimate destination node address. If a node with a fake RREP packet responds to the source node, it is flagged as a black hole node. Furthermore, it is separated from the routing table of nodes from the network by sending a legitimate RREP message. An algorithm based on reliability factor to prevent black hole attacks was developed by the authors in [25]. The algorithm initially assigns each node a reliability factor value of $0.5$. When a source node receives an RREP packet, it verifies the reliability factor and the sequence number. If the reliability factor is less than $0.5$, the source node further sends a fake RREQ. If a node replies, that node is flagged as a black hole node and the attack is prevented. Similarly, Pathan $et\ al.$ [26] implemented a detection mechanism that modified the AODV routing protocol to detect black hole attacks. A bait timer is placed in the source code with a value of $T$ seconds randomly chosen. The source node generates a false RREQ packet and broadcasts it with an illegitimate destination address randomly created when the timer reaches $T$ seconds. Thus, a node that replies to the fake RREQ packet is considered an illegitimate node. Furthermore, to determine the illegitimate node that responded to the fake RREQ packet, its identity is traced from the RREP generator address field and added to a list of black hole nodes. A source node broadcasts a genuine RREQ packet with an

alert field, an intermediary node upon receipt of the RREQ packet verifies the black hole node entry and marks it in the routing table. Thus, all RREP packets from the black hole node are discarded. Khan $et\ al.$ [27] proposed a detection mechanism using an Ant Colony Optimization technique to mitigate black hole attack. Similarly, the authors in [28] proposed a detection scheme using hybrid Weighted Trust Based Artificial Bee Colony (WTABC) algorithm to detect black hole attacks. Also, a detection scheme based on Gray Wolf Optimization and trust setup data aggregation was proposed to mitigate black hole and gray hole attacks [29]. In their work, one node is selected as a trusted authority. All nodes' information is investigated and processed automatically by the trusted authority. If malicious nodes are detected, the trusted authority rearranges them. The authors in [30] presented a detection mechanism based on data control packet and a black hole check table that mitigates and eliminates black hole nodes. Their work introduced a data control packet that verifies the path taken by all nodes in all steps. Furthermore, each node maintains a black hole check table to decide which nodes are trustworthy. Zardari $et\ al.$ [31] proposed a dual attack detection mechanism based on intrusion detection system (IDS) and connected dominating set (CDS) technique to detect black hole and gray hole attacks in MANET. In their work, the CDS technique creates small groups of nodes within the network. The proposed technique then selects the IDS set of nodes from the CDS subsets of CDS nodes that have sufficient energy. The IDS node with the highest energy and that is trusted is then chosen to frequently transmit status packets in order to detect the malicious node. If an IDS node suspects a node to be malicious, it broadcasts a block message to all nodes. Subsequently, all nodes stop communicating with the suspected malicious node. Yasin and Abu Zant [32] incorporated a timer and baiting technique in the AODV routing protocol to mitigate black hole attacks. In their work, each node has a bait-timer that is set to $T$ seconds at random. When it reaches $T$ seconds, the source node generates and sends a bait request with a randomized fake id. When a node replies to the source node with a fake request, that node is marked as a black hole node and further added to a list created for black hole nodes. In addition, they have deployed a hello message transmission mechanism that enables adjacent nodes to know each other. Thus, when a source node receives a reply, it verifies the node's ID with the node that has the optimal path. In addition, if the verified node's ID is in the list created for black hole nodes, then it is dropped; otherwise, it verifies the node's id in the created neighbour nodes list and responds if it is in the list. A detection mechanism called Secure-DSR was proposed to mitigate black hole attack and to enable secured communication in the network [33]. In this detection mechanism, the black hole nodes are identified by examining the control packets used in network routing. The drawback to this work is that they assumed all participating nodes in the network are legitimate. In [34], an intrusion detection system was proposed to mitigate black hole attacks. An Identification and Confirmation system was proposed in [35] to identify black hole attacks in MANET. In their work, they constructed an attack tree for a black hole attack. Further, the authors adopted a honeypot that makes use of the black hole attack tree to identify various kinds of black hole attacks. Once a black hole attack is identified, it is confirmed using the attack history database's record of previous attacks. However, their proposed system will not be able to identify a black hole attack if prior information about the black hole attacker is not captured in the constructed tree for the black hole attack. In their work, Hossain $et\ al.$ [36] proposed a cryptography solution to mitigate the black hole attack in MANET. However, their proposed mechanism may lead to high computation overhead in the network due to the computation of keys and ciphers. Furthermore, the authors in [37] proposed a secure routing protocol called SAODV to prevent black hole attack. In SAODV, a requesting node does not immediately respond to a node with an RREP data packet but waits until all other neighboring nodes reply with their next hop details. A timer is set in the Timer Expired Table upon receipt of the first request and collecting other requests from different nodes. The requesting node stores the sequence number and packet's arrival time from each node in a Collect Route Reply Table (CRRT). The time at which the first route request is received is used to compute a timeout value. Furthermore, the requesting node checks from CRRT whether there is any repeated next hop node after the timeout value. Thus, if there is any repeated next hop node present in the reply path, then it is assumed the path is safe, otherwise the path is flagged as malicious. However, their proposed SAODV is vulnerable to cooperative black hole attacks. El-Semary and Diab [38] improved upon the works of the authors in [37] to mitigate cooperative black hole attack. They proposed a protocol called BP-AODV that mitigates both black hole and cooperative black hole attacks initiated during the process of routing. Their proposed work implemented a technique that established trusted routes. The source node creates a challenge value and transmits it to a destination node during a route request. Upon receipt of the challenge value by the destination node, it calculates the response value as a function of the received challenge value and other generated secret values. Furthermore, it transmits the response value to the source node during the route reply while keeping the secret values. In addition, it verifies the route by sending the secret values. Mistry $et\ al.$ [39] focused on improving the secure AODV. They proposed a protocol called MOSAODV to guard against black hole attack. In MOSAODV, the source node does not respond immediately to the first RREP received. It rather stores all the RREPS received from neighboring nodes. It analyses all the stored RREPS and discards RREPS that have very high destination sequence numbers. Also, any node that transmits RREP with such a high destination sequence is flagged as a malicious node. The MOSAODV protocol maintains the identity of the malicious node to prevent further packets from such a malicious node. However, their proposed protocol leads to high computation and may also lead to false positives where the proposed protocol classifies legitimate nodes as malicious nodes. A detection mechanism called CBDAODV was introduced by the authors in [40]. A source node in CBDAODV accepts at least two RREP packets from different neighboring nodes. In addition, it uses an alternative route to validate the selected optimal route. If the destination node confirms that no route exists between the selected route, then the source node flags that node as an illegitimate node that executes a black hole attack. Furthermore, it discards the earlier selected optimal route and chooses another routing path for onward transmission of data packets. The authors in [41] proposed a solution by modifying the AODV protocol thus preventing any intermediate or destination nodes from modifying their default operations. In their work, the source node stores all RREP messages and calculates peak value. In addition, if the RREP's sequence number is higher than the peak value, then that node associated with the high sequence number is flagged as a malicious node. However, their solution involves high computation and comparison of sequence numbers against peak value in determining a malicious node. It can also lead to false positives. In their work, Chavan $et\ al.$ [42] modified AODV protocols to prevent black hole attacks. The modified protocol uses two message techniques sent from the source node to a destination node for verification. A source node first sends a VERIFY packet to a destination node via an intermediate node and subsequently sends CHECKVRF. When the destination node receives the CHECKVRF packet, it verifies whether

the VERIFY packet received earlier from the intermediate node matches the source node ID. Thus, if there is a match, it sends a FINALREPLY packet to establish a legitimate path. However, if there is no match and the destination node does not reply with a FINALREPLY packet, the intermediate node is flagged as a black hole node. In [43], a secure AODV routing mechanism was proposed to mitigate and eliminate black hole attacks. They introduced a validity value in RREP. The source node verifies the validity value of an RREP packet it receives it. Thus, if the validity value is null, the source node flags that particular node as an illegitimate node and drops the RREP packet. Their work is based on the assumption that the illegitimate node has no idea about the validity value in RREP. However, if the illegitimate node uses the same protocol, it can analyze it and set a validity value before launching an attack. Tamilselvan and Sankaranarayanan [44] introduced a protocol called PCBHA to mitigate against cooperative black hole attack. They proposed a fidelity table that will contain fidelity levels of every node that participates. When a source node broadcasts RREQ packets to its neighbouring nodes, it awaits RREP packets from its neighbouring nodes. It chooses a neighbouring node with a higher fidelity level and exceeds a predefined threshold value, and then transmits data packets to the destination node. Furthermore, upon receipt of the packet, the destination node sends an acknowledgement to the source node. Subsequently, the source node increases the fidelity level of the intermediate node to ensure a safe path to the destination node. However, suppose the source node does not receive any acknowledgement from the destination node. In that case, it reduces the fidelity level of the intermediate node and considers a possible black hole node on this path. The PCBHA protocol is based on the source node receiving acknowledgement from the destination node. However, a malicious node could send a forged acknowledgment packet upon receiving the RREQ packet from the source node, increasing its fidelity level. Dokurer $et\ al.$ [45] presented a modified AODV routing protocol that mitigates black hole attack. When a source node transmits an RREQ packet, it discards either the first RREP or the first two RREP packets receive from neighboring nodes. It rather chooses any subsequent RREP packets from the next hop. However, their solution is vulnerable to cooperative black hole attacks. An authentication mechanism using enhanced certificates was proposed by the authors in [46]. In their work, nodes authenticate each other by creating certificates and issuing them out to neighboring nodes. In addition, without the use of centralized authority, they generate a public key. Furthermore, to support certification, they used Multicast Ad-hoc On-Demand Distance Vector Routing protocol. However, due to the generation and involvement of keys, their proposed solution leads to a high computational overhead. The authors in [47] presented a secure AODV routing protocol that is able to mitigate black hole attack. Their work enables the verification process directly between a source node and a destination node through an exchange of random numbers. Similarly, the authors in [48] formulated a detection mechanism that mitigates black hole attack. In their work, the trueness level helps avoid packet drop attacks by generating a trust hierarchy and cooperation among legitimate nodes. Furthermore, their cryptography mechanism enables the confidentiality of information in data packets. In addition, it ensures that there is secured communication between two nodes and helps in the authentication. However, due to the calculation of keys, their solution involves a high computational overhead. A TRACEROUTE mechanism was introduced by the authors in [49] to mitigate the source of collaborative black hole attack. The mechanism breaks the collaboration between the illegitimate nodes by eliminating and marking the source of collaboration. In their work, the source node transmits a trace packet to the destination node and then sets a timer for Reversetrace. Furthermore, the trace packet is forwarded by each intermediate hop and also sets the timer for Reversetrace upon receipt of the trace packet. Thus, if the timer set expires before the Reversetrace is received, that particular next hop is marked as a collaborative black hole node and the Reversetrace is sent through previous nodes to the source node. However, their solution results in communication overhead. Venkanna $et\ al.$ [50] proposed a modified AODV routing protocol that achieves cooperative routing. Their proposed mechanism computes the final trust value (FTV) and the remaining energy value of neighbouring nodes in the network. The computed values determine a cooperative and trustworthy route between a source and a destination node. However, their solution leads to an increase in the consumption of energy as well as routing overhead.

## 4. RESEARCH GAPS AND FUTURE WORKS

Some of the research works proposed mechanisms that address single black hole attacks. However, their proposed detection mechanisms could not address cooperative black hole attacks. Furthermore, some other proposed mechanisms result in routing overheads. Similarly, other proposed solutions result in computational overhead due to the generation and involvement of keys. Furthermore, some other proposed solutions result in false positives where legitimate nodes are flagged as black hole nodes. Also, some detection mechanisms use threshold values to prevent black hole attacks. However, such mechanisms cannot prevent black hole attacks if malicious nodes can keep their values within acceptable threshold values. Future work should propose solutions that address the increase in computation and routing overheads while preventing black hole and cooperative black hole attacks. Furthermore, future proposed works should address the drawbacks of threshold values and false positives. To the authors' best of knowledge, few research works have proposed using blockchain technology to mitigate attacks in MANETs. However, not much work has been done on using blockchain technology to mitigate black hole attacks in MANETs. Blockchain technology, which has key features such as decentralized, immutable, transparent and secure, can be leveraged to implement a security mechanism that addresses black hole and cooperative black hole attacks in MANET. The authors propose that future works adopt blockchain technology to address some weaknesses identified in the discussed research works.

## 5. CONCLUSION

MANET's dynamic and infrastructure-less nature exposes it to some security attacks, such as a black hole attack. Some research works have proposed several variants of secured AODV routing protocols. Others proposed cryptography techniques, optimization techniques, statistical threshold approach, control packets approach, and other detection mechanisms to detect black hole attacks. This paper presented various proposed solutions that address black hole attacks and cooperative attacks. In addition, this paper identified some weaknesses in the proposed solutions. Furthermore, it proposes future research work that needs to be carried out to detect and prevent black hole and cooperative black hole attacks in MANET.

## 6. REFERENCES

[1] S. Sharma and A. K. Gupta, "A comprehensive study of dymo routing protocol," *International Journal of Computer Applications*, vol. 73, no. 22, 2013.

[2] J. Kumar, M. Kulkarni, and D. Gupta, "Effect of black hole attack on manet routing protocols," *International Journal of Computer Network and Information Security*, vol. 5, no. 5, p. 64, 2013.

[3] D. N. Patel, S. B. Patel, H. R. Kothadiya, P. D. Jethwa, and R. H. Jhaveri, "A survey of reactive routing protocols in manet," in *International Conference on Information Communication and Embedded Systems (ICICES2014)*. IEEE, 2014, pp. 1–6.

[4] H. Kaur, V. Sahni, and M. Bala, "A survey of reactive, proactive and hybrid routing protocols in manet: A review," *network*, vol. 4, no. 3, pp. 498–500, 2013.

[5] G. V. Kumar, Y. V. Reddyr, and M. Nagendra, "Current research work on routing protocols for manet: a literature survey," *international Journal on computer Science and Engineering*, vol. 2, no. 3, pp. 706–713, 2010.

[6] N. Khanna and M. Sachdeva, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in manets," *Computer Science Review*, vol. 32, pp. 24–44, 2019.

[7] P. Goyal, V. Parmar, R. Rishi *et al.*, "Manet: vulnerabilities, challenges, attacks, application," *IJCEM International Journal of Computational Engineering & Management*, vol. 11, no. 2011, pp. 32–37, 2011.

[8] R. Jaiswal, S. Sharma *et al.*, "A novel approach for detecting and eliminating cooperative black hole attack using advanced dri table in ad hoc network," in *2013 3rd IEEE International Advance Computing Conference (IACC)*. IEEE, 2013, pp. 499–504.

[9] M. C. Trivedi and S. Malhotra, "Identification and prevention of joint gray hole and black hole attacks," *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 10, no. 2, pp. 80–90, 2019.

[10] V. Sandhya Venu and D. Avula, "Invincible aodv to detect black hole and gray hole attacks in mobile ad hoc networks," *International Journal of Communication Systems*, vol. 31, no. 6, p. e3518, 2018.

[11] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, "Black hole attack detection using fuzzy based intrusion detection systems in manet," *Procedia Computer Science*, vol. 151, pp. 1176–1181, 2019.

[12] D. Nitnaware and A. Thakur, "Black hole attack detection and prevention strategy in dymo for manet," in *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)*. IEEE, 2016, pp. 279–284.

[13] V. K. Saurabh, R. Sharma, R. Itare, and U. Singh, "Cluster-based technique for detection and prevention of black-hole attack in manets," in *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, vol. 2. IEEE, 2017, pp. 489–494.

[14] F. Albalas, M. B. Yaseen, and A. Nassar, "Detecting black hole attacks in manet using relieff classification algorithm," in *Proceedings of the 5th International Conference on Engineering and MIS*, 2019, pp. 1–6.

[15] S. Naveena, C. Senthilkumar, and T. Manikandan, "Analysis and countermeasures of black-hole attack in manet by employing trust-based routing," in *2020 6th international conference on advanced computing and communication systems (ICACCS)*. IEEE, 2020, pp. 1222–1227.

[16] G. Arulkumaran and R. Gnanamurthy, "Fuzzy trust approach for detecting black hole attack in mobile adhoc network," *Mobile Networks and Applications*, vol. 24, no. 2, pp. 386–393, 2019.

[17] N. Veeraiah and B. T. Krishna, "Trust-aware fuzzyclus-fuzzy nb: intrusion detection scheme based on fuzzy clustering and bayesian rule," *Wireless Networks*, vol. 25, no. 7, pp. 4021–4035, 2019.

[18] S. Gurung and S. Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in manet," *Wireless Networks*, vol. 24, no. 8, pp. 2957–2971, 2018.

[19] A. Singh and M. Hasan, "An improved mechanism to prevent blackhole attack in manet," in *Progress in Advanced Computing and Intelligent Engineering*. Springer, 2018, pp. 511–520.

[20] P. Ndajah, A. O. Matine, and M. N. Hounkonnou, "Black hole attack prevention in wireless peer-to-peer networks: a new strategy," *International Journal of Wireless Information Networks*, vol. 26, no. 1, pp. 48–60, 2019.

[21] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of aodv under black-hole attack in manet," *Wireless Networks*, vol. 25, no. 4, pp. 1685–1695, 2019.

[22] H. Mahore, R. Agrawal, and R. Gupta, "Agent based black hole detection technique in aodv routing protocol," in *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*. IEEE, 2018, pp. 1–6.

[23] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Computer Networks*, vol. 113, pp. 94–110, 2017.

[24] T. Delkesh and M. A. J. Jamali, "Eaodv: Detection and removal of multiple black hole attacks through sending forged packets in manets," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 5, pp. 1897–1914, 2019.

[25] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability factor based aodv protocol: Prevention of black hole attack in manet," in *Smart Innovations in Communication and Computational Sciences*. Springer, 2019, pp. 271–279.

[26] M. S. Pathan, J. He, N. Zhu, Z. A. Zardari, M. Q. Memon, and A. Azmat, "An efficient scheme for detection and prevention of black hole attacks in aodv-based manets," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, pp. 243–251, 2019.

[27] D. M. Khan, T. Aslam, N. Akhtar, S. Qadri, I. M. Rabbani, and M. Aslam, "Black hole attack prevention in mobile ad-hoc network (manet) using ant colony optimization technique," *Information Technology and Control*, vol. 49, no. 3, pp. 308–319, 2020.

[28] V. Keerthika and N. Malarvizhi, "Mitigate black hole attack using hybrid bee optimized weighted trust with 2-opt aodv in manet," *Wireless Personal Communications*, vol. 106, no. 2, pp. 621–632, 2019.

[29] R. Vatambeti, K. S. Supriya, and S. Sanshi, "Identifying and detecting black hole and gray hole attack in manet using gray wolf optimization," *International Journal of Communication Systems*, vol. 33, no. 18, p. e4610, 2020.

[30] A. Dorri, S. Vaseghi, and O. Gharib, "Debh: detecting and eliminating black holes in mobile ad hoc network," *Wireless Networks*, vol. 24, no. 8, pp. 2943–2955, 2018.

[31] Z. Ali Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain, and M. Q. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in manets," *Future Internet*, vol. 11, no. 3, p. 61, 2019.

[32] A. Yasin and M. Abu Zant, "Detecting and isolating black-hole attacks in manet using timer based baited technique," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[33] M. Mohanapriya and R. Santhosh, "Detection and elimination of black hole attacks in mobile ad hoc networks," *Materials Today: Proceedings*, 2021.

[34] N. Rajendran, P. Jawahar, and R. Priyadarshini, "Cross centric intrusion detection system for secure routing over black hole attacks in manets," *Computer Communications*, vol. 148, pp. 129–135, 2019.

[35] D. S. K. Tiruvakadu and V. Pallapa, "Honeypot based black-hole attack confirmation in a manet," *International Journal of Wireless Information Networks*, vol. 25, no. 4, pp. 434–448, 2018.

[36] S. Hossain, M. S. Hussain, R. R. Ema, S. Dutta, S. Sarkar, and T. Islam, "Detecting black hole attack by selecting appropriate routes for authentic message passing using sha-3 and diffie-hellman algorithm in aodv and aomdv routing protocols in manet," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2019, pp. 1–7.

[37] L. Tamilselvan and V. Sankaranarayanan, "The 2nd international conference on wireless broadband and ultra wideband communications," 2007.

[38] A. M. El-Semary and H. Diab, "Bp-aodv: Blackhole protected aodv routing protocol for manets based on chaotic map," *IEEE Access*, vol. 7, pp. 95 197–95 211, 2019.

[39] N. Mistry, D. Jinwala, and M. Zaveri, "Mosaodv: solution to secure aodv against blackhole attack," *IJCNS) International Journal of Computer and Network Security*, vol. 1, no. 3, pp. 42–45, 2009.

[40] N.-W. Lo and F.-L. Liu, "A secure routing protocol to prevent cooperative black hole attack in manet," in *Intelligent technologies and engineering systems*. Springer, 2013, pp. 59–65.

[41] D. R. Choudhury, L. Ragha, and N. Marathe, "Implementing and improving the performance of aodv by receive reply method and securing it from black hole attack," *Procedia Computer Science*, vol. 45, pp. 564–570, 2015.

[42] A. Chavan, D. Kurule, and P. Dere, "Performance analysis of aodv and dsdv routing protocol in manet and modifications in aodv against black hole attack," *Procedia Computer Science*, vol. 79, pp. 835–844, 2016.

[43] S. R. Deshmukh, P. Chatur, and N. B. Bhople, "Aodv-based secure routing against blackhole attack in manet," in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2016, pp. 1960–1964.

[44] L. Tamilselvan and V. Sankaranarayanan, "Prevention of cooperative black hole attack in manet." *J. Networks*, vol. 3, no. 5, pp. 13–20, 2008.

[45] S. Dokurer, Y. Erten, and C. E. Acar, "Performance analysis of ad-hoc networks under black hole attacks," in *Proceedings 2007 IEEE SoutheastCon*. IEEE, 2007, pp. 148–153.

[46] E. Mary Anita and V. Vasudevan, "Prevention of black hole attack in multicast routing protocols for mobile ad-hoc networks using a self-organized public key infrastructure," *Information Security Journal: A Global Perspective*, vol. 18, no. 5, pp. 248–256, 2009.

[47] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "Saodv: a manet routing protocol that can withstand black hole attack," in *2009 international conference on computational intelligence and security*, vol. 2. IEEE, 2009, pp. 421–425.

[48] N. Khanna, "Avoidance and mitigation of all packet drop attacks in manet using enhanced aodv with cryptography," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 37, 2016.

[49] N. Khana, "Mitigation of collaborative blackhole attack using traceroute mechanism with enhancement in aodv routing protocol," *International Journal of Future Generation Communication and Networking*, vol. 9, no. 1, pp. 157–166, 2016.

[50] U. Venkanna, J. K. Agarwal, and R. L. Velusamy, "A cooperative routing for manet based on distributed trust and energy management," *Wireless Personal Communications*, vol. 81, no. 3, pp. 961–979, 2015.