International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223691 Volume 10, Issue 6, November – December (2023)

SURVEY ARTICLE

# A Survey of Current Detection and Prevention Techniques for Black Hole Attack in AODV of MANET

Mohamed A. Ryan
Systems and Computer Engineering Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt.
Eng_ryan2016@outlook.com

Sayed Nouh
Systems and Computer Engineering Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt.
sayed.nouh07@gmail.com

Aly M. El-Semary
Systems and Computer Engineering Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt.
aelsemary@azhar.edu.eg

Received: 11 August 2023 / Revised: 24 October 2023 / Accepted: 27 November 2023 / Published: 30 December 2023

**Abstract – "Mobile Ad Hoc Network" (MANET) comprises a set of mobile nodes that communicate wirelessly and operate in a self-organized environment that requires no infrastructure. This network type dynamically forms its topology in which the nodes' mobility leads to rapid, unpredictable, and frequent changes in the dedicated topology. Routing process in such environment is a challenge. In addition, the lack of centralization administration makes MANET subject to intrusions. "Ad Hoc On-Demand Distance Vector" (AODV) protocol is among the most widely deployed routing protocol in MANET. Unfortunately, is susceptible to black hole attacks in which intruders utilize the protocol nature to infiltrate the network and execute their malicious activities. Therefore, the paper discusses and analyzes the latest existed solutions used to protect against black hole attacks. In addition, it categorizes the current solutions according to the deployed technology to provide the reader with state-of-the-art approaches.**

**Index Terms – AODV, Attack, Black Hole, MANET, Malicious, Reputation, Route Discovery, RREP, RREQ, Sequence Number, Trust Value.**

## 1. INTRODUCTION

Wireless networks comprise a set of mobile nodes utilizing electromagnetic waves as a mean for communicating data with each other. These types of networks allow users to effortlessly connect various devices without the requirement of purchasing, connecting, or carrying cables [1]. These networks offer advantageous features like mobility and reducing time and cost required for installation. Generally, wireless networks are categorized into two main types: Infrastructure and infrastructure-less Networks.

Infrastructure networks utilize a central node or device called a base station to manage communication among different network nodes. Specifically, the base station allocates specific channels for communication between each pair of communicating nodes or devices [2]. This implies that the routing algorithm among communicating nodes is controlled by a centralized manner. Such networks are commonly referred to as "centralized networks" [3].

In contrast, infrastructure-less networks operate without central management. This results in a distributed routing mechanism among devices [4]. MANET is an example of such networks, where nodes possess the liberty to move and autonomously organize in an arbitrary manner. [5]. Accordingly, MANET is widely employed in several field such as disaster areas, personal area networks, military sector and sensor networks [6]. Unfortunately, the unrestricted movement of nodes in MANET results in a highly challenging problem in its routing protocols [7].

In general, the routing mechanism or protocol is in charge of forwarding data or packets from one node to a next node toward a target or destination node. Routing protocols in MANET are categorized according to how mobile nodes obtain and maintain routing information into three primary categories. These categories are reactive, proactive, and hybrid routing protocols [8] as depicted in Figure 1. Reactive or on-demand routing protocols are bandwidth-effective routing protocols. In reactive routing approaches, nodes maintain routes to only those nodes that are in an active communication with them [9]. In this kind of routing process,

SURVEY ARTICLE

a path between an origin and a target is discovered only when the origin is in need to exchange data with the target and at the same time, there is no valid route between them [1]. The nature of MANET allows any node to join the network including nodes that behave maliciously. A malicious node might take place on the routing path at the time the path discovery procedure and perform attacks during the data forwarding procedure. AODV is among the well-known reactive routing protocols.

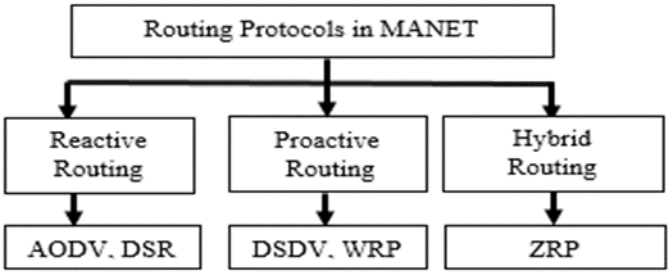


Figure 1 Routing Protocols Classification in MANET

In proactive or "table-driven" routing schemes, every node maintains a current updated view of the entire network through an update packet that is periodically sent among network nodes. Also, when any topology change occurs, an update packet gets propagated through the network to notify all nodes regarding the modification [10]. Examples of such proactive schemes are “Destination-Sequenced Distance Vector Routing” (DSDV), “Wireless Routing Protocol" (WRP) and “Fisheye State Routing” [11].

The hybrid routing schemes implement the on-demand and table-driven approaches to leverage their advantages. For example, ZRP is one of the hybrid routing protocols [8].

### 1.1. AODV

AODV is considered as the most famed on-demand routing scheme [12]. In the AODV, a route is discovered only when the route is needed. In other words, when an origin node needs to talk to a target node, the origin node launches the path discovery procedure if it has no path in its routing table to the destination [11]. To identify a rout in the AODV protocol, the protocol creates what is called a Route Request (RREQ) packet which is subsequently disseminated to neighboring nodes through flooding. Upon receipt of the RREQ packet, a neighbor node updates its routing table by establishing a reverse path to the origin node. The neighbor node might be either a target node or an intermediate node. In case, it is the target node, it starts what is called a Route Reply process by creating a Route Reply (RREP) packet and sending it to the origin node through the reverse path. On the other hand, if the neighbor node is an intermediate node, it looks for a route to the target node in its routing table. If the intermediate or transit node finds a path to the target node, it triggers the Route Reply process by establishing a RREP packet and forwarding it to the origin node via the reverse route. Otherwise, the transit node broadcasts the received RREQ packet to its neighbor nodes in the direction of the target node. The intermediate nodes iteratively broadcast the RREQ packet until it is delivered to either the final target node or a transit node that has a path to the target. After receiving a RREQ packet, the target node or the intermediate node that has a path to the target launches the Route Reply procedure by sending a RREP packet to the origin node via the reverse path. Finally, upon receipt of the RREP by the origin node, it starts to transmit its data to the target node via the discovered route. If the origin node gets another RREP with either a higher sequence number or the identical sequence number but a lower hop count, the origin node will update its routing details and may opt to employ this revised route [13].

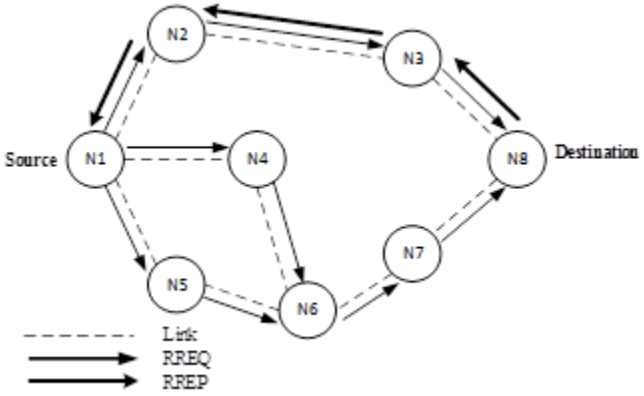


Figure 2 AODV Routing Mechanism

To illustrate the process, Figure 2 is created to depict the process of discovering the route in AODV protocol. In the Figure, N1 serves as the origin node, while N8 functions as the destination node. N1 initiated a route discover to N8 by flooding a RREQ message to its neighbors N5, N4, and N2, in this case. Each of the nodes N5, N4, and N2 updates its routing information with the reverse route to the origin node and then floods its received RREQ packet to its neighbors. In this case, N3 receives the RREQ from its neighboring node N2 while N6 receives two RREQ packets from its neighboring nodes N4 and N5. Since each of N3 and N6 is an intermediate node, each of them broadcasts its received RREQ to its neighboring nodes. In this case, N3 broadcasts its packet to N8 while N6 broadcasts its packet to N7. Once the target node N8 obtains the RREQ from N3, it creates a RREP and forwards it to the origin node through the reverse discovered path N3, N2, and N1 in this case. On the other hand, once the transit node N7 gets the RREQ from N6, it broadcasts the packet to N8, which in turns ignore the packet because it received the same RREQ from N3. Finally, when the origin node N1 receives the RREP from the target node

SURVEY ARTICLE

N8, both nodes can start forwarding their data though the discovered route N1, N2, N3, and N8 in this case.

The article is structured as the following: Section 2 discusses the Attacks in MANET while Section 3 introduces the black hole Attack. The solution techniques and their categorizations are demonstrated in Section 4. Ultimately, the paper is concluded in Section 5.

## 2. ATTACKS IN MANETS

Attacks in MANET can be classified into two primary categories: Passive and active attacks. In passive attacks, the enemy is not involved in the communication but just listen or eavesdropping to the communication. This type of attacks includes eavesdropping attack and traffic analysis attack. In the active attacks, on the other hand, an attacker is involved in the communication to make malicious modification. These types of attacks include acknowledgement spoofing, wormhole, selective forwarding, black hole, sinkhole, and Sybil attacks as shown in figure 3.

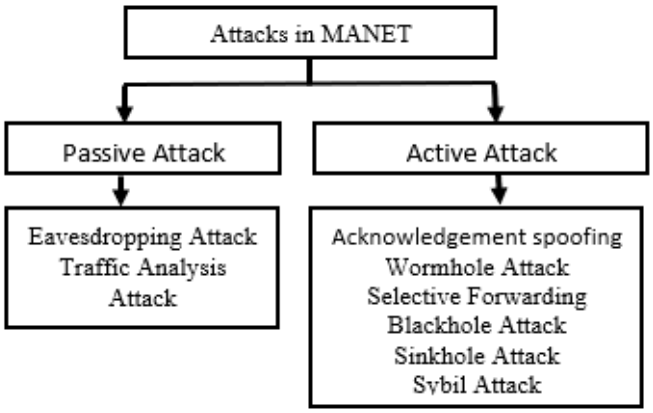


Figure 3 Attacks in MANET

### 2.1. Passive Attacks

The passive attacks are types of attacks that do not include themselves in the network operation. In other words, they do not alter the main operation of the network. These types of attacks include traffic analysis attacks and eavesdropping attacks. In eavesdropping attack, an attacker secretly listens to communications of others aiming to gather information exchanged between them. The detection of the eavesdropping attacks is a challenge but they can be prevented by implementing an effective or strong encryption mechanism [14]. On the other hand, the traffic analysis attack is the process of capturing and investigating network data or packets aiming to extract information from the intercepted data. The traffic analysis can be employed to discover the concealment of the anonymous network. In general, the traffic analysis attack is a passive attack but, in some cases, it might be an active attack. For example, when an attacker changes the timing of a set of flow packets based on a defined pattern to link the flows between the two sides [15].

### 2.2. Active Attacks

In the active attacks, an enemy tries to change or destroy the exchanged data which could disturb the main operation of the network. Denial of Service DoS and routing protocol attacks are examples of active attacks.

The DoS attacks can be lunched across various network layers including physical, data link, or network layer. In case of a physical layer, an attacker may persistently send an electromagnetic signal to disrupt the radio frequency utilized by nodes, causing jamming and resulting in DoS attack, rendering the network sensors. At the data link layer, the DoS attack can be achieved by violating the protocol. For instance, an attacker constantly transmits messages in order to cause collision or exhaust the energy of the target nodes. In addition, the DoS attacks can be generated at the network layer attacking the routing protocols of MANET [15].

In contrast, attacks on routing protocols take place through different types of routing protocol attacks including acknowledgement spoofing, wormhole, selective forwarding, black hole, sinkhole, and Sybil attacks. The remainder of this section presents these types of attacks.

In the "Acknowledgement Spoofing Attack" ASA, an enemy or a malicious node may falsify acknowledgement to motivate that a feeble link is robust or an inactive node is operational. This leads to a feeble link might be selected for routing. As a result, the transmitted packets via that link might be corrupted or lost. A malicious node implementing the ASA can efficiently perform a selective forwarding attack by attracting its aimed node to forward its packets via those feeble paths.

The wormhole attack significantly threatens MANETs by employing two cooperated adversaries to tunnel data between them. The first adversary placed at one network location receives messages from network nodes over a low-latency channel and tunnels these messages to the other adversary at different network location. After establishing the wormhole, the attacker can easily manipulate routing to manage packets through the wormhole [16]. This type of attack is risky because it can be achieved even if the network nodes employ effective authentication and confidentiality algorithms. Specifically, the attack does not necessitate compromising any node within the network [17].

The selective forwarding is a routing protocol attack whereby an enemy node puts itself on a routing path through the routing procedure. Then, it selectively discards certain received packets while in the process of data forwarding. One form of the selective forwarding is referred to as grayhole attack when the attacking node selectively gets rid of some of the received data packets.

SURVEY ARTICLE

Detecting this kind of attack is challenging as the malevolent node has the ability to discard packets from particular nodes while forwarding packets from others, or it might intermittently drop packets while behaving normally at other times. The combination of these tactics complicates the identification of the attacking node responsible for the attack [17].

The Black hole attack is a form of routing protocol attack, wherein an attacking node inserts itself into a routing path as part of the routing procedure. Then, the attacking node rejects to forward any received packets by simply drops them. Two or more attacking nodes are cooperated with each other to perform the black hole attack aiming to avoid their detection.

The sinkhole attack is a routing protocol attack where an attacking node tries to involve itself on the routing path. The attacking node achieves its goal by enticing its neighbor nodes that it has the best routing metrics to forward their traffic via the attacking node. By including itself on the routing path at the time of the routing process, the attacking node has the ability to form a sever attacks including modifying or dropping received packets through the date forwarding procedure. When the attacking node drops a specific type of packets, it behaves, in this case, like the selective forwarding attack.

In the Sybil attack, an attacking node generates a large number of malicious identities, one for each Sybil node. The attacking node can generate an identity for the Sybil node by one of two approaches. In the first approach, the attacking node launches a Sybil node by creating its address from the network address space. In the second approach, the attacking node obtains a Sybil node by spoofing the identity of a legitimate node. The second approach is preferred when the address space of the network is limited. After each Sybil node is allocated an identity, it can start communication with the underlying legitimate network nodes either directly or indirectly through the attacking node. This makes the Sybil attack significantly influences the network routing process [15].

## 3. BLACK HOLE ATTACK IN AODV

In AODV, the black hole attack is an active attack that can take place through twofold. During the first fold, an enemy node includes itself on the routing path at the time of the route discovery phase. During the second fold, the attacking node performs its goal during the forwarding process by rejecting to forward any received packet [18]. To illustrate the operation of the black hole attack, Figure 4 is constructed to show the general behavior of the black hole in AODV with a single attacking node. The figure has five nodes *A, B, C, D,* and *F* along with the malicious black hole node *M*. The sold arrows indicate a route request discovery while the doted arrows designate the route reply. Also, node *A* in need to communicate with the node *E* and it currently has no route path between them. Therefore, the node *A* should discover the route to the target node *E*.

To discover the route from *A* to *E*, the node *A* triggers a route request procedure by flooding a RREQ to its neighbors towards the target node *E*. Each of its neighbors *B* and *D* along with *M* will receive the RREQ. Each of *B* and *D* floods its received RREQ to its neighbors; In this case, *E* will receive RREQ from *B* while *F* will receive RREQ from *D*. In contrast, *M* immediately triggers the route reply procedure by replying with a RREP to the origin node via the established reverse route (in this case, *M* sends the RREP to *A*). In addition, the node *E* will initiate the route reply process by replying with a RREP packet to *A* through *B*, which in turn forwards it to *A*. In this case, *A* receives two RREP packets, one from *M* and the other one from *E*. Because *M* enticed *A* that it has the best path metrics to *E* (i.e., *A* receives a RREP with a smaller number of hop-counts from *M* before *E*), the node *A* marks *M* as the next hop towards the target *E*. In this case, the discovered route is *A, M,* and *E*. The attacking node *M* managed to insert itself on the route from *A* to *E*. This enables *M* to achieve its goal during the forwarding process by rejecting to transmit any received packets.

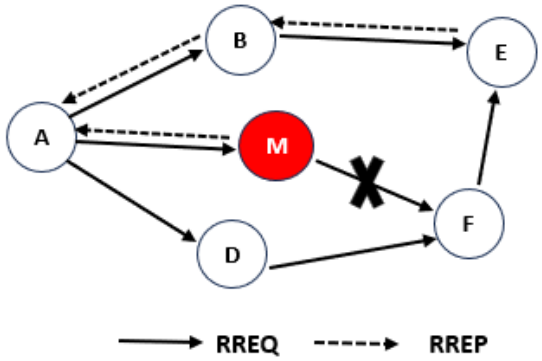


Figure 4 Black hole Attack in AODV

To transmit data packets from the origin node *A* to the target node *E* through the discovered route *A*, *M*, and *E*, *A* forms each required data packet and forwards it to the attacking node *M* which in turn gets rid of each received data packet. This method enables the black hole node to intercept and discard all incoming data packets. In certain situations, the attacking node operates friendly through the path discovery phase and shows its malevolent actions through the data forward process [19].

Concluding the black hole behavior, Figure 4 illustrates the black hole scenario with a single attacking node. In this scenario, an enemy node manipulates the routing protocol by falsely pretending that it possesses the shortest route to the target node to involve itself on the route path [20]. On the

**SURVEY ARTICLE**

other hand, the cooperative black hole attack uses two or more attacking nodes to perform the attack. The attacking nodes cooperate to include at least one attacking node on a route path. The black hole attacks scenarios with cooperative malicious node are hard to be detected [20].

## 4. SOLUTIONS AND TECHNIQUES

This paper categorizes the current black hole protection techniques into three categories. Trusted value-based techniques, Sequence Number-Based Techniques and Miscellaneous techniques.

### 4.1. Trusted Value-Based Techniques

The researcher in [21] - introduced a secure scheme named TSAODV that depends on assessing the trustworthiness of every node in the routing path. The trustworthiness is determined by criteria such as success and failure which describe the status of the transmission. The term RREQS represents the route request success rate demonstrated by the number of adjacent nodes that have successfully received the route request packets. In contrast, the term "RREQF" denotes the failure rate of route request determined by the number of neighboring nodes that have not received the RREQ packet. Also, the RREPS represents the success rate of route reply determined by the number of route reply packets received by the initiator node. On the other hand, the RREPF denotes the failure rate of route reply and it can be calculated as the number of neighboring nodes that refused to transmit the route reply packet as a response to the pre-received RREQ packet. In addition, DATAS refers to the number of data packets successfully conveyed to its destination while DATAF indicates the number of data packets that have not successfully reached its intended destination. Table 1 provides a synopsis of the aforementioned parameters.

Table 1 Parameters of TSAODV

| COMMUNICATION TYPE | Route Request | Route Reply | DATA |
|---|---|---|---|
| SUCCESS | RREQS | RREPS | DATAS |
| FAILURE | RREQF | RREPF | DATAF |

The intermediate values *RRR*, *RPR* and *RDR* calculate the rates of route request, route reply and route data respectively. The trusted value $TV = (RRR + RDR + RPR) / 3$ is calculated for each node during the routing process. Next, the value *TV* of each node is compared with a predefined threshold to determine the node reliability. Table 2 indicates the different threshold values. The shortcoming of the underlying scheme is adding overhead due to periodically sending control packet in order to calculate the number of packets that have reached the neighbors. This conflicts with the nature of reactive routing protocols.

Table 2 Threshold Values

| Trustworthy Value | Action | Node Behavior |
|---|---|---|
| 0.0 to 0.4 | Ban | untrustworthy Node |
| 0.4 to 0.7 | Accept | trustworthy Node |
| 0.7 to 1.0 | Accept | Most trustworthy |

Authors in [22] proposed a new secure scheme called BP-AODV (Black hole Protected AODV). The scheme recognizes the hurtful nodes during route discovery process. In addition, it detects the attacking nodes that behave friendly during the path discovery phase while behave unfriendly during the data transfer phase. The authors implemented an algorithm called challenge-response-confirm pattern to create a reliable path between the origin and destination nodes. The originating node sends a modified RREQ that includes a random number (challenge), every node receives the RREQ will store the challenge value and then flood it to its neighbors toward the target node. Once the target node gets the RREQ, it employs the Logistic chaotic map to produce a response value derived from the received challenge along with secret values. Next, it encapsulates the response into a modified RREP packet and propagates it to the origin node via the established reverse routes while keeping the secret values. Each node gets the route RREP will save the response value and forwards it to the origin through the reverse path. In addition, the node sets a path with non-operational state to the node that sent the RREP. After a pre-calculated time pointer, the destination launches the confirm process by sending a RCON packet to convey and reveal the secret values to the origin and the intermediate nodes.

Each node receives the RCON packet will use the secret values along with the pre-stored challenge value to recalculate the response value which is compared with the previously stored value. If they are equal, the node activates the path to an operational state which can be used to forward data packets between nodes. Otherwise, the node considers the forwarding node as an attacking node and eliminates its route from the routing table. The BP-AODV system safeguards against not only black hole attacks using an attacking node but also collaborative black hole attacks generated by multiple attacking nodes. This is true under the assumption made by the authors that the number of trusted nodes that send the RCON are more than the number of attacking nodes. The BP-AODV scheme uses a trust value mechanism to prevent the hurtful node that works friendly during the path discovery while gets rid of the data packets at the time of date forwarding phase. The main issue in BP_AODV is the delay during the route discovery phase, as the calculations take place at every node that participates in the path between the origin and target node.

**SURVEY ARTICLE**

In [23], the authors proposed an approach relying on the reliability factor of the route. Initially, all nodes have the same initial value of reliability factor *r*. When a node is in need to send data, it starts the normal route discovery process. Once the node receives a RREP, it checks the value of r. If the value of *r* is near to zero, this indicates that the RREP sent by an attacking node. If the value of ***r*** is greater than 0.5, the originating node utilizes the route to transmit the data packets. The concept of fake RREQ is used when the value of *r* is equal to or less than 0.5. This concept is considered as an additional confirmation step to deduce whether the node is a malicious or genuine. To achieve the concept, the source sends a fake RREQ and the attacking node will send RREP. The authors of the underlying scheme strive to thwart black hole attacks in the route discovery phase but the collaborative black hole attack still can play a role during the data forwarding phase.

In [24], the authors identify and mitigate the collaborative black hole attacks by computing the trustworthiness value of every node in the network and comparing that trust value with a predefined threshold. They categorized the nodes as unreliable, reliable, and most reliable based on the trust value. An unreliable node is the node that just joined the network or has a minimum trustworthiness value while a reliable node is defined by the fact that its neighboring node has received packets through it. The designation of most reliable is given to a node that has a high trust value. This trust value indicates that the neighbors of the node have received numerous packets through it. In this scheme, every node keeps a trustworthiness table to store the trust status of each adjacent node. When the node gets a RREP it consults its trustworthiness table to choose the reliable route. The authors use fake RREQ to update the status of nodes in the trust table. The shortcoming of the underlying scheme is the overhead of the fake RREQ to build the trust. In addition, the cooperative black hole attack can take place in this scheme.

In [25], the researchers introduced a strategy to prevent the collaborative black hole attacks by employing a trust-based avoidance technique. Every node within the network keeps a trust table that includes the trustworthiness scores of its adjacent nodes. The neighboring nodes in this scheme are categorized into three types according to their trust level which is Unknown, Known, or Companion. The trustworthiness of individual neighbor is determined by analyzing its track record of successfully forwarded packets. A neighbor's trust value increases as the neighbor has effectively transmitted packets in the past. Accordingly, when a node needs to transmit data packets to a particular target node, it consults its trust table to identify the most reliable neighbor that is capable of forwarding the packets to the target node. The authors tried to eliminate the overhead in the network so they do not use any additional management packets. The findings indicate that the E2E delay in the suggested approach is identical to the standard AODV although calculating the trust value at each node during the route discovery might increase the delay. Even though the underlying scheme is designed to protect against the collaborative black hole attacks, the collaborative black hole attacks might take place in this scheme. To achieve this, a malicious node *A* can build its trust by sends all of its received packets to another malicious node *B*. This entices the source to forward its data packets through the node *A* which in turn performs its goal by refusing to forward its received packets.

In [26], the authors provided a trust detection mechanism to distinguish between the malicious and benign nodes. They added an accessible trust authority node (TA) which observes network activities and logging every event that occurs in the network. When a new node becomes part of the network, it takes the whole information that was recorded by the authority node. The suggested scheme called ETERE (Efficient Trust Establishment-based Routing Evidence) is employed to evaluate the routing information. The I-Trust technique is utilized to identify misbehavior or malicious nodes that transmit inaccurate information. The suggested scheme distinguishes between benign and malicious nodes based on their attack history. The authors have not revealed the authority technique that they used to authenticate the trusted node. Accordingly, what if an attacking node pretends that it is the trusted node?

In [27], the researchers proposed an approach that depends on the trust value of every node within the network. Initially, every node has a maximum trustworthiness value for all of its neighbors. When a node *N* transmits a data packet, it initiates a timer and waits for a reply from the next hop. If the timer runs out and there is no reply, the node *N* will decrease the trustworthiness value of that next hop. The node *N* will share the new trustworthiness value of its neighbors with other nodes within the network. If a node keeps dropping the data packet, it means that its trustworthiness value will continue to decrease. If a node's trustworthiness value drops below the min_trust value, then this node will be blocked from sending data where all the nodes in the network will put it into the blacklist. In this scheme, extra control packets are used to share the trust value of the nodes. This causes overhead to the network. In addition, the underlying scheme completes the process of the route discovery and detects the malicious node during the data forwarding process. This means that if an attacking node is detected along the route, the origin node will initiate the process of route discovery again. As a result, an extra delay is added to the network.

In [28], a secure trust AODV has been introduced where every participating node has trust level table along with malicious node *MN* table. The trust level table maintains the trust value of each node. Initially, all nodes are considered trustworthy and their trust values will be updated when

SURVEY ARTICLE

receiving route replies. The authors use a threshold technique to validate the route replies. The threshold is established by considering both the received sequence number and the sequence numbers presented in the routing information of the transmitting node. Upon receiving the RREP, the origin node examines its *MN* table to check if the originator of the RREP has an entry. If it has an entry, the RREP will be discarded. Otherwise, the origin node checks the safety status of the received RREP. The trustworthiness level of the RREP originator node of the unsafe route reply will be decreased. If the trust value became negative, the originator node will be added to the malicious table. In the proposed technique, the authors calculate the threshold based on the previously received sequence number that might be not fresh enough. This might result in a wrong threshold.

In [29], the authors introduced an algorithm to collect data about network nodes. The collected information includes the number of transmitted and received packets and the number of replies received by each node. The collected information is analyzed to take a decision whether a node is malicious or benign. Upon receiving a RREP from the transit node *N*, the transmitting node sends a request to the adjacent nodes of *N* to get their opinions about the sender of RREP. The authors established specific criteria to detect malicious nodes. For example, the node that sends RREP with a high sequence number and minimum hop count or the node that gets a large volume of packets but transmitting only a single packet could potentially be a malicious node. A collaborative black hole attack would break this approach by giving incorrect opinions about another malicious node. Also, the additional control packets that are used to gather information will increase the network overhead.

In [30], the researchers proposed a routing scheme named RORP that eliminates the broadcasted packets to the trusted nodes only. The scheme aims to reduce the memory wastage and power consumption as well as isolate malicious nodes. Initially, the scheme sets all nodes with reputation value $REP_{init}$ increases if the corresponding node forwards packets successfully; otherwise, it gets decreased. Nodes with higher reputation attract more neighboring nodes to forward their messages through them. This results in significantly increasing the likelihood of the intended messages reaching their destination safely. The reputation model periodically updates the reputation value of the nodes. Therefore, the unsuitable neighboring node will be filtered out. After reputation model is achieved by filtering the unsuitable nodes, the suggested scheme applies reputation threshold on the remaining nodes to select the forwarding set. To enhance the selection process of relay nodes, the proposed protocol uses Q-learning and reinforcement learning technique. The Q-learning technique enables nodes to learn and adapt to their routing decision according to the behavior of neighboring nodes. Accordingly, nodes in MANET continuously assess the outcomes of their routing decisions. They learn from these outcomes and adapt their strategies to choose relay nodes that maximize the chances of successful and secure data transmission. This adaptive approach ensures that the routing decisions are not static but they evolve over time. Even though the routing decisions adapt to changing network conditions and the presence of attacking nodes, the learning process imposes an overhead on the network.

In [31], the authors introduced a secure and energy-efficient routing scheme that guarantees successful delivery of information between the origin and destination nodes in MANET. The protocol is based on an adaptive trust model that considers various node parameters to estimate a highly suitable trust level. Fuzzy clustering is employed to partition the whole network into distinct clusters along with a designated cluster head (*CH*). The *CH* is chosen based on the highest levels of direct, indirect, and current trust within each cluster. Detection of attacking nodes is accomplished through the utilization of a dynamic threshold value. This dynamic threshold is calculated using ANN model that acquires knowledge about various parameters of the network. These parameters include the proportion of route modifications, node degree, connectivity, the stability of node, pause time, remaining power, mobility, and mean neighborhood trustworthiness.

The scheme explicitly diagnoses every intermediary node involved in network transmission. The diagnosis prevents the intentional dissemination of falsified data by suspected nodes and enables the identification of trusted paths after the identification of suspicious nodes. The simulation outcomes demonstrate that the suggested protocol outperforms the schemes TEAR, ETRES, ETRS, and C-SSA in terms of PDR, energy consumption, and E2E delay. Unfortunately, cooperative black hole attacks might take place in this scheme by giving fake parameters that would end up with selecting a malicious node as a trust node.

In [32], the researcher presented a trust-based scheme to enhance the security of the service discovery process in MANETs; targeting prevention against denial-of-service attacks. The underlying model both packet dropping attacks and flooding attacks by managing the trustworthiness of each node within the network. The RREP and RREQ packets of original AODV have been expanded as SREQ and SREP messages, respectively. These messages include additional two-hop service information. Consequently, the routing table of each node has been extended to accommodate this additional service information.

Every node within the network retains a neighbor cache that contains information about its immediate neighbors along with their respective trust values. Initially, the scheme sets the trust value of each node to one that refer to the minimal level of trust on a scale from 0 to 3. The trustworthiness value of a

SURVEY ARTICLE

node is increased only when the node cooperates in forwarding packets and it has a trust value of one or two. In other words, cooperation of a node with a trust value of zero does not result in an increment. Periodically, the neighbor cache is cleared or reset to its default values (i.e., set the trust value to one). This approach encourages nodes to responsibly forward packets from their neighbors in order to potentially earn higher trust levels in the process. The trust values of nodes that have not cooperated in forwarding packets are reduced. This leads to their exclusion from secure pathways. On the other hand, nodes exhibiting high trust levels are chosen at each hop to guarantee a secure route between the consumer and the server. The trustworthiness value that assigned to a node is continuously adjusted in real-time based on its performance in forwarding packets and adherence to the protocol's requirements. The suggested approach is compared with the standard AODV, AIF AODV, and SNRM in terms of control message overhead and service discovery latency. The outcomes show that the suggested approach provides better performance where it is 4% less than AIF_AODV while it is 16% less than SNRM in terms of message control overhead. In addition, the proposed approach prevents the intermediate nodes from creating RREPs to eliminate the malicious. This makes the suggested approach to experience some delay which makes the original AODV outperforms the proposed scheme in term of E2E delay.

The introduced scheme in [33] is a trust-based fuzzy method that aims to thwart black hole attacks in MANET. The method considers four main factors to identify and avoid black hole nodes: energy auditing, neighboring node trust, packet integrity, and node member authentication. The first factor is the energy auditing which involves monitoring the energy consumption of every node in the network. Nodes with low energy levels are considered less trustworthy and they are given a lower priority in the routing process. This helps to prevent black hole nodes from consuming too much energy and disrupting the network.

The second factor is the neighboring node trust which involves evaluating the trustworthiness of each node's neighbors. Nodes with more trustworthy neighbors are given higher priority in the routing process. This helps to prevent black hole nodes from forming alliances with other nodes and disrupting the network.

The third factor is the packet integrity which involves verifying the integrity of each packet transmitted in the network. Packets that are found to be tampered with or corrupted are discarded and the nodes transmitted these packets are marked as untrustworthy. This helps to prevent black hole nodes from intercepting and modifying packets in the network.

Finally, the node member authentication involves verifying the identity of every node in the network. Nodes impersonating other nodes or using fake identities are marked as untrustworthy. This helps to prevent black hole nodes from disguising themselves as legitimate nodes and disrupting the network.

The underlying approach employs a collection of fuzzy rules to assess the trustworthiness of every node in the network based on the aforementioned factors. The authors executed a performance test to compare their scheme TFAODV with the original AODV. The results indicate that the TFAODV surpasses AODV in terms of PDR, throughput, E2ED, and overhead.

In [34], the authors introduced a Machine Learning trust-based scheme called ML-AODV to eliminate black hole. In ML-AODV, each mobile node initially maintains a list of immediate or 1-hop neighbors through periodic HELLO packet exchanges. Subsequently, the source or originator node verifies the existence of a path to the target node in its routing table. If a route is found, the source triggers the transmission of data packets. Otherwise, it broadcasts a new RREQ packet to immediate 1-hop neighbors to establish a route. Upon receiving the RREQ by a neighbor node, the node verifies whether it is the destination or not. If it is not the destination, it calculates the trustworthiness value of the node and then compares the value with process a predefined threshold. If the trustworthiness value exceeds the threshold, the trustworthiness value is stored in the ML-AODV RREQ. This procedure ensures the utilization of trust values to improve the reliability of route discovery process. The trustworthiness value is determined according to the residual energy *RE* and "Link Expiration Time" *LET*. The scheme uses ANN to recognize the most efficient and optimal route while utilizes the VSM classifier to detect intruders within the selected route. The structure of ANN involves input, hidden and output layers. The enhanced route is established at the input layer according to the measured features of the node. These features include *LET*, *RE*, and hop-count. The hidden layer aids in capturing the relationships among the node features provided as inputs to the ANN. In output layer, the ANN computes the input values and presents the optimal path with enhanced *LET* and *RE* while minimizing delay. The authors conducted experiments to assess the performance among ML-AODV, original AODV, and Trust AODV in terms of reliability, overhead, throughput, E2ED, and packet loss. The results indicate that ML-AODV exhibits superior performance in relation to the mentioned metrics. The ML-AODV is well-suited for networks characterized by medium capacity and moderate node speeds, but it may not be suitable for networks featuring high-speed nodes or high-density configurations.

In [35], the authors provided a scheme to identify black hole attacks by leveraging node credibility and Andrews plot. In the initial phase, the node credibility for each network node is computed by assessing its behavior and performance. All

SURVEY ARTICLE

nodes start with an initial credit value of 3. Upon receiving a counterfeit RREP, an origin node initiates the transmission of data packets and waits a specific timeframe for acknowledgment (CACK) from the destination. In the absence of receiving CACK, the credit assigned to the node responsible for the fraudulent RREP is subsequently reduced.

In the next phase, the nodes within the network are sorted into three distinct categories according to their node credibility scores. These categories comprise Good Nodes, Suspected Nodes, and Malicious Nodes. The Good Nodes exhibit high node credibility scores and are deemed reliable. The Suspected Nodes are characterized by moderate node credibility scores and a suspicion of potential malicious behavior. The Malicious Nodes are identified by low node credibility scores and classified as inherently malicious. The scheme utilizes the Andrews plot to graphically illustrates the node credibility scores which help in the identification of nodes exhibiting abnormal behavior.

Even though the authors utilized the Andrews plot to graphically illustrate node credibility over a series of transactions, they did not present a method for preventing black holes. In addition, they have not provided performance evaluations or comparisons with current routing schemes. Accordingly, the proposed scheme could be used to detect the attacking nodes but not to prevent them.

In the context of [36], the STABA scheme is introduced for the identification of Black hole nodes. STABA begins with selecting specific node parameters including the total number of lost packets, energy utilization, and buffer length. These parameters play a crucial role in determining the trustworthiness of each node. In the STABA scheme, an origin node initiates a RREQ to a target node. Next, intermediate node receiving the RREQ establish a reverse route. Next, for each hop on the route, the positive and negative trust values of the node are calculated. If the negative trust value exceeds the negative threshold, the node is identified as malicious. On the other hand, if the positive trust value surpasses the positive threshold, the node is marked as genuine and proceed to the next hop.

STABA is compared with the traditional AODV in terms of E2ED, PDR, and Throughput. The findings demonstrate that the introduced scheme exhibits superior performance when compared to AODV.

In [37], the authors proposed a solution to detect black hole attacks in MANETs using the KNN clustering or grouping technique with fuzzy inference. The scheme detects attacks based on the received data from nodes by tracking sent packets. By utilizing KNN grouping, the nodes calculate neighborhoods, form groups, and assess trust levels among neighboring nodes. Group heads are nominated based on trust thresholds and fuzzy inference to select the node with the most trustworthy neighbors at the required energy level. After network formation and group calculation, trust is established between group heads and nodes through initiating closed routing and identifying malicious nodes.

The reputation of a node is established by the trust it harvests from other nodes. Periodically, nodes within a group convey their trustworthiness values to every node in the trust table that is maintained by the group head. Once a group head accumulates a specific number of opinions about a node, it updates the node's reputation value in its trust table. Additionally, the group head periodically generates a list of unreliable nodes based on its reputation table. This list is then disseminated within the cluster to prompt other nodes exercising caution when engaging in communication with these identified unreliable nodes.

Upon the establishment of the trusted network together with the computation of groups, group heads, and mutual trust among nodes, the packet routing within the network is initiated to facilitate the identification of malicious nodes.

The results of conducted experiments show that the introduced approach excels in comparison to the ANN-SVM and ANFIS+PSO schemes in terms of throughput, PDR, and total delay.

Finally, Table 3 provides summarized comparison for the schemes in the references from 21 to 37 in the same order as in Section 4.1.

Table 3 Summarized Comparison of Trusted Value-Based Techniques

| Scheme | Detection Type | Year | Defect |
|---|---|---|---|
| Detection and Avoidance of Unified Attacks | Cooperative & Single detection | 2016 | Control packets need to be sent timely which causes overhead to the network |
| BP-AODV | Cooperative & Single detection | 2019 | Delay during the route discovery process, as the calculations take place at every node |
| Reliability Factor Based AODV Protocol | Single detection | 2018 | The malicious node still can play a role during the data-forwarding process |

**SURVEY ARTICLE**

| | | | |
|---|---|---|---|
| Detecting and avoiding of collaborative black hole | Cooperative & Single detection | 2016 | Fake RREQs are sent periodically to update the trust table which causes overhead. |
| Avoidance of collaborative black hole | Cooperative & Single detection | 2016 | Calculating the trust value of every node during the route discovery should increase the delay |
| efficient trust establishment | Cooperative & Single detection | 2022 | A central node is used to authenticate the newly joined nodes, the technique will fail if this node failed |
| BH-Detection | Cooperative & Single detection | 2015 | Overhead because of the control packets, and extra delay |
| STAODV | Cooperative & Single detection | 2017 | Wrong threshold could happen. |
| Modified algorithm to improve security | Cooperative & Single detection | 2016 | The nodes exchange control packets to gather information, that causes overhead |
| RORP | Cooperative & Single detection | 2023 | The learning process imposes an overhead on the network. |
| ANN-C-SSA | Single Detection | 2022 | Cooperative malicious nodes can break the scheme by giving fake parameters |
| AODV- SSD | Cooperative & Single detection | 2021 | The scheme prevents intermediate nodes to create RREP that would add extra delay to the network. |
| TFAODV | Cooperative & Single detection | 2022 | No comparison with the recently existing schemes. |
| ML-AODV | Cooperative & Single detection | 2023 | Not suitable for networks featuring high-speed nodes or high-density configurations. |
| Node Credit | Cooperative & Single detection | 2023 | The introduced technique used to only detect the malicious nodes not to prevent them. |
| STABA | Cooperative & Single detection | 2022 | Cooperative attack can break the introduced technique. |
| KNN | Cooperative & Single detection | 2021 | Many malicious nodes can cooperate to give wrong trust value to break the scheme. |

4.2. Sequence Number-Based Techniques

In [38], the researchers suggested an approach to identify and prevent single and cooperative black hole attacks by filtering the RREP at the origin and intermediate nodes. When the intermediate node gets RREP from another intermediate node, it verifies the sequence number by sending an inquiry to the target node asking for its current sequence number. After the intermediate node gets the reply from the target node, it updates its destination sequence number and forwards RREP to the origin node. The origin node will consider the RREP with a minimum sequence number as an indication that this is the valid route.

In [39], the researchers provided an approach to detect the attacking node by verifying the sequence number in the RREP. They assume that the attacking node generates the sequence number with an arbitrary maximum number $Arbt_{max}$ of 100. The origin node tries to reveal the malicious behavior of the black hole node by comparing the received sequence number in RREP with the sequence number in the RREQ. If the received sequence number is arbitrarily high, the origin node adds the received source number to a RREQ and rebroadcasts it. If the source receives a RREP from the same node with arbitrary high sequence number, then the route is discarded. The researchers assume that the source node has a destination sequence number near the actual sequence number

SURVEY ARTICLE

of the destination. Consequently, they compare that sequence number with the received sequence number but this assumption is not always true.

In [40], the researchers proposed a threshold-based technique to prevent black hole attack. They identify the node as a malicious node if it sends a RREP equal to or greater than the threshold. The source node calculates the threshold dynamically. When the origin node gets different RREPs from different paths, it first checks the number of received sequence numbers and based on that it calculates the threshold which is the average value of the received sequence numbers. The technique discards the route if the received sequence number is equal to or greater than the threshold. Otherwise, the originating node starts the transmission of data packets to the target. The findings show that the introduced technique provides better throughput than that of SAODV [41].

In [42], the researchers introduced a methodology that only modifies the behavior of the origin node without any modifications to the intermediate or destination nodes. The pre-request receive reply procedure is used and a new RREP_Tab table is added. Upon receiving the initial route reply, the origin node initiates a timer, saves all received RREPs to the RREP_Tab, identifies and excludes the malicious node, and then chooses the response with the highest destination sequence number. Unfortunately, the cooperative black hole attacks can play a role where two or more malicious nodes can send RREP that will affect the proposed scheme.

In [43], the researchers introduced MBDP-AODV scheme in which the origin node gets multiple RREPs before sending the data packets. In this approach, the origin node calculates dynamic threshold of the received sequence numbers in the RREPs. It tries to identify the malicious node by sending a SUSPECT packet with a suspected sequence number. Accordingly, the source node will mark the node replayed with a hop-count of one along with the suspected sequence number as an attacking node which will be in the prevention phase, the considered attacking node is prohibited from participating in the upcoming path discovery processes. The researchers considered that the attacking node is one-hop far away from the origin node. Unfortunately, this is not the case in all scenarios where the attacking node would be far away from the origin node.

Finally, Table 4 summarizes the comparison of the schemes discussed in Section 4.2.

Table 4 Summarized Comparison of Sequence Number-Based Techniques

| Scheme | Detection Type | Year | Defect |
|---|---|---|---|
| Bulwark AODV | Cooperative & Single detection | 2015 | Considering the minimum sequence number as an indication of a valid route is not always true |
| Modified AODV | Cooperative & Single detection | 2020 | Comparing an old sequence number would break the scheme |
| Secure Routing-Based AODV | Single detection | 2021 | The collaborative attack would break the scheme |
| Receive Reply Method | Single detection | 2015 | A group of attacking nodes can break the scheme |
| dynamic threshold-based algorithm | Single detection | 2019 | The scheme assumes that the malicious node is at a one-hop distance from the origin node, which may not always be accurate. |

4.3 Miscellaneous Techniques

In [44], the researchers introduced an approach to identify and isolate the black hole in MANETs. In the proposed technique, each node periodically sends a "bait" request packet with setting TTL to one. The bait request packet is a fake RREQ packet to a fake destination. When a malicious node receives the bait request, it will reply with a RREP packet. Once the origin node gets the RREP, it recognizes that it was sent from an attacking node. Thus, the origin node adds that responded node to its malicious node list. In addition to the malicious node list, each node has a neighboring list. Accordingly, when a source node is in need to communicate with a target node, it floods a RREQ packet to its neighbors, which in turn flood it until reaching its destination or an intermediate node that has a route to the target. When the source node gets a RREP packet as a response to the RREQ, it checks its malicious node list. If the responded node is in the malicious node list, the source node discards the reply and consults its neighboring list. Also, if the reply came from unknown node, the origin node will discard the reply as well. The overhead of the extra traffic generated by bait packets is the drawback of the scheme.

In [45], the authors provided node-to-node authentication scheme to thwart single black hole attack in AODV. They use the encryption technique and hash function to authenticate every node during the route discovery phase to overcome the black hole attack. The scheme distributes a key *Nk* to all authenticated nodes before deployment. When a node *A* needs

**SURVEY ARTICLE**

to transmit data to a destination, it selects a session key *Sk*. Next, it forms a RREQ with the hash value of *Sk* and the encryption of both the *Sk* and the time stamp *TS* of sending the request using the key *Nk*. Then, it sends the RREQ to a neighbor node *B*. Upon receiving the RREQ packet, the node *B* recovers the key *Sk* and the time stamp *TS* by decrypting them with the key *Nk*. Next, the node *B* authenticates the request by computing the hash value of the recovered Sk and comparing it with the received hash value. If they are the same, the node *B* will exchange handshake with the node *A* by encrypting a random number with the *Sk*. The node A will verify the received reply. If it is valid, the node B will take place in the path route. Otherwise, it will be removed. The algorithm applies the process for each node through the path route up to the target node. This increases the E2E delay.

In [46], the researchers proposed a secure AODV (SAODV) scheme to detect black hole attacks through the route discovery phase. The approach utilizes a reputation technique in which each network node maintains an opinion table to save the reputation of its neighboring nodes. When the origin node gets a RREP from an intermediate node, it sends an opinion packet to the intermediate neighbor nodes to notify them about the reputation. Each node aggregates the received opinions by which the decision is made in choosing which nodes to be in the route path. Notably, this scheme does not address cooperative black hole attacks in which multiple malicious nodes collaborate to provide false opinions. It also adds some delay where the source node waits to consult the neighboring nodes about the reputation of the sender of RREP. Finally, the authors conducted experiments to measure the performance of the proposed SAODV against the AODV in terms of throughput, PDR, overhead, and End-to-End delay. The results reveals that the SAODV experiences better results in all metrics except the End-to-End dely.

In [47], the researchers introduced a scheme to identify the single black hole attack during the path discovery procedure. The scheme does not change the functions of AODV but it adds only a validity bit to the RREP packet. Upon receiving a RREQ by a transit node, if the transit node possesses a sufficiently recent path to the target node, it replies to the origin by transmitting a RREP packet with setting its validity bit to one. When the origin gets the RREP packet, it checks the validity bit. The origin node will starts sending the data packets only if the validity bit has a value of one. In the scheme, the authors assume that the malicious nodes send the default RREP and do not know about the validity bit. Unfortunately, this assumption is not valid because the security of an algorithm is not depended on the secrecy of the algorithm.

In [48], the authors proposed a scheme that avoids the black hole attack by ignoring the first received RREP. The underlying concept of this proposed approach allows a source node to store the received RREP packets during a period. The source node then ignores the first received RREP packet and considers that packet coming from malicious since a malicious node responds immediately by a RREP packet. The origin node chooses the route containing the maximum sequence number from the remaining RREP packets and utilizes that path to transmit the data packets.

The authors evaluate the performance of the standard AODV protocol and the proposed scheme based on the throughput, PDR, E2ED, and overhead metrics during attack scenarios. The findings indicate that the suggested schemes give better performance than that of AODV. Unfortunately, the proposed scheme is vulnerable against the collaborative black hole attacks. In addition, the scheme ignores the first received RREP which might come from a benign node.

In [49], the authors proposed an approach based on the reputation values of the participating nodes. The approach consists of three main phases. In the first phase, the scheme uses the Watchdogs and Pathrater techniques to collect the reputation value of every node in the network. The technique allows each node to monitor its neighbor nodes to calculate the reputation values that are shared among the nodes to come up with the network reputation. The reputation helps node to exclude malicious nodes from the route path. In the second phase, the scheme frequently updates and share the reputation values among the network nodes. In the third phase, the scheme forwards the data packet via the most reliable path that is determined by the reputation values of the participating nodes. The article does not provide performance evaluation for the suggested technique

In [41], the researchers proposed a secure AODV scheme that defends the black hole attacks by using a secure route discovery process. The origin node launches the rout discovery procedure by disseminating a RREQ to its neighboring node. If an intermediate node receives the RREQ and holds a valid path to the target, it responds by transmitting a RREP packet to the origin node. However, to prevent black hole nodes from responding, the proposed approach uses a digital signature to ensure that only legitimate nodes can respond. The route reply packet includes a digital signature generated by using the private key of the responding node. The source node uses the public key of the responding node to verify the digital signature of the received RREP packet to make sure that the route reply is generated by legitimate node.

In addition, the approach uses a technique called hop-by-hop authentication to ensure the authenticity of each hop in the route. Each intermediate node that forwards a packet adds a hop-by-hop signature to the packet. The signature is generated using the private key of the forwarding node and includes the sequence number of the packet. The recipient node has the capability to validate the hop-by-hop signature by employing the forwarding node's public key and the packet's sequence

SURVEY ARTICLE

number. If the signature is approved, the packet is forwarded to the subsequent hop in the network. Otherwise, the packet is dropped. The authors conducted experiments to analyze the efficiency of the proposed approach against the AODV and BADOV in terms of throughput and packet loss rate. The findings indicate that the suggested approach perform better than that of BAODV but -the hop-by-hop signature could increase the end-to-end delay.

The authors in [50] proposed a scheme that divides the network into clusters, in each cluster there is a candidate cluster head. The role of the cluster head is to allocate resources into mobile nodes inside the corresponding cluster. The scheme works to prevent black hole attack using five different phases: setup, key generation, signature generation, communication, and verification. In the setup phase, the selected cluster head broadcasts the system parameters inside the cluster. When nodes receive the parameters, they start sending their identity to the cluster head which in turn sends the received identities to the key generation center KGC. The KGC is responsible for generating the private and public keys. The signature generation phase is responsible for securing the data communication. The cluster head play the role of the verifier in the verification phase. Accordingly, when a source node needs to communicate with a destination, it sends a RREQ to the cluster head which contacts with the destination, which replies with a RREP that includes its signature. Once the cluster head receives a RREP, it verifies the signature. If the signature is valid, the cluster head includes its signature in the RREP and then forwards it to the origin node which in turns identifies the preferred route recovered and verified from the received RREP. Next, the origin node starts the secure communication with the destination through the preferred route. On the other hand, if the signature is not valid, the cluster head marks the node as a malicious node. The proposed scheme is compared with the standard AODV, SAODV and CLS in terms of PDR, E2E delay, throughput, and routing overhead. The outcomes of the suggested approach surpass those of SAODV, AODV and CLS based on the aforementioned metrics. Unfortunately, using five algorithms in such battery-driven environment could exhaust and shorten the lifetime of network

In [51], the authors discuss the use of elliptic curve cryptography (ECC) to strengthen the security of MANETs by mitigating wormhole and black hole attacks. ECC is a public-key cryptography technique that utilizes elliptic curves over finite fields for key generation and data encryption. The authors proposed a scalable-dynamic elliptic curve cryptography (SDECC) method that uses a dynamic key generation algorithm to generate private and public keys for every node in the network. The SDECC method is designed to be scalable and efficient to be used in MANETs. The SDECC method is used together with SWBAODV protocol to mitigate wormhole and black hole attacks. The SWBAODV protocol is a secure routing protocol that employs cryptographic techniques to safeguard against diverse forms of security attacks. In order to assess the efficacy of the suggested approach, a comparison was done with the original AODV, Wormhole AODV (WAODV) and Black hole AODV (BAODV) in terms of several metrics such as routing overhead, PDR, E2E delay, energy, and throughput. The results indicate that the proposed scheme SWBAODV outperforms the BAODV and WAODV in terms of the aforementioned metrics while the original AODV outperforms SWBAODV with increasing the number of nodes in terms of Throughput, PDR, E2E delay and energy.

In [52], the researchers proposed detection black hole attack scheme LDAS to detect the malicious behavior by analyzing the generated data using a machine learning algorithm. The scheme accomplishes the detection process in three steps. The first step generates traffic data using an OMNET++ simulator. The simulator is crafted to mimic real traffic in presence of black hole attack. The produced data is collected in a specific format for subsequent analysis. The second next step gathers data and identifies the pertinent features used to identify malicious nodes. This accomplished through using SVM algorithm, a type of machine learning algorithms that is capable of classifying data into distinct categories based on specific features. Finally, once the algorithm selects the relevant features, the SVM algorithm starts to categorize traffic into normal and malicious categories. Through this analysis, it becomes possible to identify and subsequently block attacking nodes. The random forest classifier is also used to provide high accuracy and detection rates for identifying attacking nodes. The suggested scheme is highly effective in detecting black hole attacks compared with ABIP and DPBHA. The proposed scheme is able to detect black hole attacks but it cannot prevent them.

The authors in [53] presented a strategy for detecting and isolating black hole attacks in MANETs using the Response Time of Reply Generation (RTRG). In this scheme, when an origin node sends a RREQ packet to locate a destination node, intermediate nodes record the time of RREQ packet reception. Upon receiving the RREQ, the destination node or an intermediate node that has a recently established path to the target node replies with a RREP packet. Each node receiving the RREP will record the receiving time of RREP packet. Next, the initial next-hop node in the reverse route determines the response time by subtracting the time of receiving the RREQ packet from the time of receiving the RREP packet. If the response time is below a threshold, the first next hop node considers the originator node as a black hole and initiates the isolation process. The isolation process broadcasts a message to all nodes to notify them about the malicious node and advise them not sending any packets to it. This proposed scheme quickly detects and isolates black hole nodes as well as preventing them from disrupting the network.

**SURVEY ARTICLE**

For performance evaluation, the authors compared the proposed scheme with the traditional AODV under black hole attack in terms of PDR, E2E delay, Drop Packets, and Routing Overhead. The comparison reveals that the proposed solution outperforms the AODV with respect to the aforementioned metrics.

In [54], the researchers introduced DHMD routing scheme as a preventive measure against black hole attacks in MANETs. The protocol comprises four key phases: path discovery, route observation, primary data transmission, and termination phase. In the path discovery phase, the origin node transmits a RREQ to its neighboring nodes for seeking a path to the intended recipient. Each successive node in the path propagates the RREQ until it reaches the designated node. In the observation phase, every node transmits data through the most direct path to the target. The source node computes the digest of an input message and then encrypts the digested value *DM* of the message *M* using the Deffie-Hellman algorithm with the source private key. The result of the encryption is denoted by *EMD*. The source appends *EMD* at the end of *M* to form the complete message (*M*, *EMD*) and then sends it to the target node. Upon receiving the message (*M*, *EMD*), the destination node extracts the *EMD*. Subsequently, it calculates its own message digest (*dMD*) from the received message *M* and recovers the *MD* by decrypting the received EMD using the public key of the source node. The target node subsequently compares both message digests. During the primary data transmission phase, the transmitting node sends data to the target node the most reliable next-hop node. When the target node gets the date packet, it generates an acknowledgment packet called PAC and send it the origin node. In the termination phase, any node exhibits misbehavior is considered as a suspected malicious node. To assess the effectiveness of the proposed scheme, the authors perform a comparison between DHMD and AODV in the presence of a blackhole attack. The findings indicate that DHMD surpasses AODV in terms of PDR, throughput, E2E delay, and overhead.

In [55], the authors proposed ATOM scheme that works as a host-based "Intrusion Detection System" to identify the potentially harmful nodes within the network. The scheme employs assessment metrics like "Packet Drop" (PD) and RREP COUNT for the precise detection of suspicious activities. The nature of block hole node is to generate RREP packet when it gets a RREQ packet regardless it has a path to the target node or not. The algorithm conducts monitoring and analysis of the RREP count in the routing table of each node to identify the nodes that exhibit suspected behaviors. Nodes that exceed the predefined threshold in their RREP count are designated as suspicious nodes.

In an effort to mitigate false predictions, the algorithm takes into account the value of packet loss for every node involved in the routing process. The monitoring of the packet drop value involves the computation of the ratio of forwarded to dropped packets for every node. If the ratio of forwarded packets to the total transmitted packets to a node is lower than the ratio of dropped packets to the total of dropped and forwarded packets, it suggests intentional packet drops by the node. This indicates a potential malicious behavior. This two-pronged evaluation strategy contributes to the heightened accuracy of the intrusion detection system. The ATOM IDS conducts a cross-correlation between nodes identified for intentional packet drops and those identified as suspicious via the RREP COUNT procedure to detect malicious behavior. If a node surpasses the RREP COUNT threshold and has a notably high packet drop value, it is labeled as malicious. Subsequently, nodes identified as malicious are prevented from participating in any route discovery-related operations. The ATOM's performance has been assessed with the conventional AODV in the context of PDR, Overhead, Throughput, and Packet Loss. The proposed scheme demonstrates superior performance compared to AODV across the aforementioned metrics. Notably, the researchers limit their comparison to only the standard AODV.

In [56], SRMAD-AODV introduced to identify and counter black hole and grayhole attacks during the data transfer phase. The whole network undergoes the CDS method to generate small sets of dominating nodes by selecting nodes with sufficient energy and confidence scores as the ADS set.

Regular transmission of status packets occurs among ADS set nodes to assess suspected nodes based on throughput, delay, routing overhead, and PDR to form a blacklist. This blacklist is then transmitted to the source node in order to validate suspected nodes and excludes them from the routing path during data transmission. Upon receiving the blacklist, the origin node transmits a data packet to the target node and waits for an ACK to confirm the acceptance and the absence of suspected nodes along the route. In case a source node receives a false ACK or no ACK, a nonce is combined with the ACK packet to ensure its validity and origin from the target node. If the ACK is genuine, the source node continues data packet transmission; otherwise, it removes blacklist nodes from the routing table and notifies other nodes of the updated routing table. The origin node requires time to authenticate the received ACK, ensuring its authenticity, and this verification process may introduce delays to the communication. The performance assessment of SRMAD-AODV is compared against established schemes namely ACIDS, SRD-AODV, DPBHA, IAODV, and ITIM, in terms of Throughput, E2E delay, and PDR. The findings point out that the suggested mechanism surpasses the effectiveness of the aforementioned schemes. Finally, Table 5 summarizes the comparison of the schemes discussed in the references from 43 to 56 discussed in Section 4.3.

**SURVEY ARTICLE**

Table 5 Summarized Comparison of Miscellaneous Techniques

| Scheme | Detection Type | Year | Defect |
|---|---|---|---|
| TBBT-AODV | Cooperative & Single detection | 2018 | The proposed scheme adds extra overhead to the original AODV |
| NTN Authentication protocol | Cooperative & Single detection | 2016 | The scheme could increase the E2E delay. Unfortunately, the authors do not provide performance evaluations. |
| SAODV | Single detection | 2017 | Cooperative malicious nodes could break the scheme by giving wrong opinion about the neighboring nodes. |
| AODV-Based Routing Protocol | Cooperative & Single detection | 2016 | The original AODV surpasses the introduced scheme in terms of PDR. |
| Secure AODV | Single detection | 2015 | Two or more malicious node could easily break the scheme. The scheme would decrease the network performance in absence of attack. |
| Enhanced AODV | Single detection | 2018 | The article lacks performance evaluation or outcomes to assess the efficiency of the suggested approach. |
| SAODV | Cooperative & Single detection | 2009 | Using hop-by-hop technique would increase the end-to-end delay. |
| Certificateless Signature Scheme | Single detection | 2022 | Unable to prevent cooperative black hole and could shorten the lifetime of the network. |
| SWBAODV | Cooperative & Single detection | 2021 | The original AODV outperforms SWBAODV in absence of attack. |
| LDAS | Cooperative & Single detection | 2023 | Used to only detect the attackers but not to prevent them. |
| RTRG | Cooperative & Single detection | 2022 | High performance node that responds fast would be considered as an attacking node. |
| DHMD | Cooperative & Single detection | 2023 | No comparison with the recently existing schemes. |
| ATOM | Cooperative & Single detection | 2021 | No comparison with the recently developed schemes. |
| SRMAD-AODV | Cooperative & Single detection | 2022 | The verification process at the origin node could introduce delay to the communication. |

## 5. CONCLUSION

The nature of MANETs make it prone to network layer attacks. The paper conducted a survey for one of the most popular attacks in MANET. Specifically, the black hole attacks on the AODV routing protocol and its variations. The survey discussed the latest published articles that proposed new schemes to secure AODV against the black hole attack. The paper categorized the proposed articles into three categories based on their solution techniques. The underlying research discussed in detail how every scheme works and the obstacles that might hinder its effectiveness. As history has demonstrated, attackers continuously develop novel methods to breach computer systems and networks to harm them. In light of this, it is crucial to implement protection mechanisms that can learn from experiences and leverage existing knowledge to identify and thwart new intrusions. Accordingly, exploring the potential of such mechanisms for inferring and detecting novel attacks is a promising area for future research.

## REFERENCES

[1] Kaur, J. Kaur and N. Kansal, ""D-EPAR: Distance–Efficient Power Aware Routing Protocol for MANETs"," 2nd International Conference on Next Generation Computing Technologies, 2016.

[2] M. A. Ryan, S. Nouh, T. M. Salem and A. M. Naguib, ""EDA-AODV: Energy and Distance Aware "AODV" Routing Protocol"," International Journal of Computer Networks and Applications (IJCNA), vol. 5, no. 5, pp. 61 - 69, 2018.

**SURVEY ARTICLE**

[3] A. Lee, C. G.Laviña, J. Caballero and I. Ra, "Performance Analysis of Ad-Hoc Routing Protocols Based on Selective Forwarding Node Algorithms," in IEEE conference, CO. U.S.A, 2013.
[4] S. K.S. and S. S., "Performance evaluation of routing in MANETs based on QoS parameters," International Journal of Modern Computer Science and Applications (IJMCSA), Vols. Volume No.-4, no. Issue No.-1, pp. pp. 49-54, 2016.
[5] S. K. Sharma and S. Sharma, "Improvement over AODV Considering QoS Support in Mobile Ad-hoc Networks," International Journal of Computer Networks and Applications (IJCNA), vol. 4, no. 2, 2017.
[6] J. and H. N., "Efficient Routing Protocol (DSDV) for Mobile Ad Hoc Network," nternational Journal of Soft Computing and Engineering (IJSCE), vol. 3, 2013.
[7] V. Jayanthi and R. R. Ravi, "Energy Efficient Neighbor Coverage Protocol for Reducing Rebroadcast in MANET," Science Direct, vol. 47, pp. 417-423, 2015.
[8] S. K. Sarkar, T. G. Basavaraju and C. Puttamadappa, Ad Hoc Mobile Wireless Networks. Principle, Protocols and Applications, Florida: Taylor & Francis Group, 2008.
[9] P. Mittal, S. Batra and D. C. K. Nagpal, "Implementation of Novel Protocol for Cordination of Nodes in Manet," International Journal of Computer Networks and Applications (IJCNA), vol. 2, no. 2, 2015.
[10] J. Loo, J. L. Mauri and J. , Mobile Ad Hoc Networks Current Status and Future Trends, Florida: Tylor and Francis Group, 2012.
[11] A. N. Thakare and M. M. Y. Joshi, "Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks," IJCA Special Issue on MANETs, vol. 4, p. 211–218, 2010.
[12] J. S. Shaik, Simulation-Based Comparative Study of Routing, Sweden , Karlskrona, 2014.
[13] -h. Lee, J. -h. Oh and J. -i. Jung, "An Enhanced Selective Forwarding Scheme for Real-Time Applications in MANETs," in 2011 International Conference on Information Science and Applications, Jeju, Korea (South), 2011.
[14] N. G. Patel and M. A. Dadhaniya, "A Survey on Detecting Black Hole Attack in MANETs," IJSRD - International Journal for Scientific Research & Development, vol. 1, no. 10, 2014.
[15] A. M. El-Semary and M. M. Abdel-Azim, "New Trends in Secure Routing Protocols for Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 9, no. 5, 2013.
[16] M. koravand, "A Comprehensive Study on Defense Against Network Layer Attacks in Mobile Ad hoc Networks," International Journal of Computer Science and Information Security (IJCSIS), vol. 14, no. 10, pp. 766-773, 2016.
[17] J. Sen, M. G. Chandra, S. G. Harihara, H. Reddy and P. Balamuralidhar, "A mechanism for detection of gray hole attack in mobile Ad Hoc networks," in 6th International Conference on Information, Communications & Signal Processing, Singapore, 2007.
[18] J. Rahman, F. Ahmed and S. Rashid, "An Analysis on Security Threats of Black-Hole and Jellyfish Attacks in Mobile Ad-Hoc Network using HTTP Traffic," International Journal of Research and Engineering, vol. 6, no. 2, pp. 575 - 579, 2019.
[19] A. Bhattercharjee and S. Paul., "A Review on some aspects of Black Hole Attack in MANET," International Journal of Engineering Trends and Technology (IJETT), vol. 10, pp. 396-401, 2014.
[20] F.-H. Tseng, L.-D. Chou and H.-C. Chao, "A survey of black hole attacks in wireless mobile," Hum. Cent. Comput. Inf. Sci., vol. 1, no. 4, 2011.
[21] U. Singh, M. Samvatsar, A. Sharma and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, 2016.
[22] 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. 95197-95211, 2019.
[23] P. Gupta, P. Goel, P. Varshney and N. Tyagi, "Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET," Smart Innovations in Communication and Computational Sciences. Advances in Intelligent Systems and Computing, vol. 851, 2018.
[24] S. Singh, A. Mishra and U. Singh, "Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm," in Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, 2016.
[25] J. Thakker, J. Desai and L. Ragha, "Avoidance of co-operative black hole attack in AODV in MANET," in International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016.
[26] A. Yamini, J. Stephy, S. Kannan and V. Ravi, "Improving routing disruption attack detection in MANETs using efficient trust establishment," Transactions on Emerging Telecommunications Technologies , 2022.
[27] N. Choudhary and L. Tharani, "Preventing Black Hole Attack in AODV using timer-based detection mechanism," in International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, 2015.
[28] M. B. M. Kamel, I. Alameri and A. N. Onaizah, "STAODV: A secure and trust based approach to mitigate blackhole attack on AODV based MANET," in IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2017.
[29] S. Shahabi, M. Ghazvini and M. Bakhtiarian , "A modified algorithm to improve security and performance of AODV protocol against black hole attack," Wireless Netw, p. 1505–1511, 2016.
[30] J. RYU and S. KIM, "Reputation-Based Opportunistic Routing Protocol Using Q-Learning for MANET Attacked by Malicious Nodes," IEEE Access, vol. 11, pp. 47701-47711, 2023.
[31] K. V. Anand and G. A. Thangaraja, "A Competent Intelligence Modeling for Trust-Based Security Scheme in Mobile Ad Hoc Network," International Journal of Computer Networks and Applications (IJCNA), vol. 9, no. 6, pp. 736-745, 2022.
[32] S. Kurian and L. Ramasamy, "Securing Service Discovery from Denial of Service Attack in Mobile Ad Hoc Network (MANET)," International Journal of Computer Networks and Applications (IJCNA), vol. 8, no. 5, pp. 619-633, 2021.
[33] M. Shukla and B. K. Joshi, "An Effective Scheme to Mitigate Blackhole Attack in Mobile Ad Hoc Networks," Lecture Notes in Electrical Engineering, Springer, vol. 869, 2022.
[34] S. Shafi, S. Mounika and S. Velliangiri, "Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET," Procedia Computer Science, vol. 218, pp. 2309-2318, 2023.
[35] A. Kumari, S. Dutta and S. Chakraborty, "Detection and Prevention of Black Hole Attack in MANET using Node Credibility and Andrews Plot," Research Square, 2023.
[36] V. Dani, P. Kokate and J. Umre, "STABA: Secure Trust Based Approach for Black-Hole Attack Detection," Applications of Artificial Intelligence and Machine Learning. Lecture Notes in Electrical Engineering.Springer, Singapore, vol. 925, 2022.
[37] G. Farahani, "Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks," Security and Communication Networks, 2021.
[38] S. V. Vasantha and A. Damodaram, "Bulwark AODV against Black hole and Gray hole attacks in MANET," in IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 2015.
[39] S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," in 8th International Electrical Engineering Congress (iEECON), Chiang Mai, Thailand, 2020.
[40] A. Ram, J. Kulshrestha and V. Gupta, "Secure Routing-Based AODV to Prevent Network from Black Hole Attack in MANET," in Proceedings of 6th International Conference on Recent Trends in Computing. Lecture Notes in Networks and Systems, Singapore, 2021.

**SURVEY ARTICLE**

[41] S. Lu, L. Li, K. -Y. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," in International Conference on Computational Intelligence and Security, Beijing, China, 2009.
[42] 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.
[43] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET," Wireless Netw 25, p. 1685–1695, 2019.
[44] M. Abu Zant and A. Yasin, "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique," Wireless Communications and Mobile Computing, pp. 1-10, 2018.
[45] U. M. K and A. S. Poornima, "Node-to-node authentication protocol to prevent black hole attack in AODV," in International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016.
[46] S. Dhende, S. Musale, S. Shirbahadurkar and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs," in International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2017.
[47] S. R. Deshmukh, P. N. Chatur and N. B. Bhople, "AODV-based secure routing against blackhole attack in MANET," in IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2016.
[48] A. K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks," in International Conference on Pervasive Computing (ICPC), Pune, India, 2015.
[49] Q. M. Yaseen and M. Aldwairi, "An Enhanced AODV Protocol for Avoiding Black Holes in MANET," Procedia Computer Science, vol. 134, pp. 371-376, 2018.
[50] V. Kumar, M. Shanker, A. M. Tripathi, V. Yadav, A. K. Rai, U. Khan and M. Rahul, "Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme," Journal of Scientific & Industrial Research, vol. 81, pp. 1061-1072, 2022.
[51] M. Shukla, B. K. Joshi2 and U. Singh, "Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET," Wireless Personal Communications, p. 503–526, 2021.
[52] A. Abdelhamid , M. S. Elsayed, A. D. Jurcut and M. A. Azer, "A Lightweight Anomaly Detection System for Black Hole Attack," Electronics, vol. 12, no. 6, 2023.
[53] Ahmed, T. Abdelaziz and S. B. Hacene, "Mitigate Black Hole Attack Using the Reply Generation Time In MANET," Turkish Journal of Computer and Mathematics Education, vol. 13, no. 3, pp. 466-487, 2022.
[54] O. M. Olanrewaju, A. A. Abdulwasiu and N. Abdulhafiz, "Enhanced On-demand Distance Vector Routing Protocol to prevent Blackhole Attack in MANET," International Journal of Software Engineering and Computer Systems, vol. 9, no. 1, p. 68 – 75, 2023.
[55] S. Sivanesh and V. R. S. Dhulipala, "Analytical Termination of Malicious Nodes (ATOM): An Intrusion Detection System for Detecting Black Hole attack in Mobile Ad Hoc Networks," Wireless Pers Commun, vol. 124, p. 1511–1524, 2021.
[56] V. Jebaseelan and K. K. Raju, "Protecting MANETs from Black and Gray Hole Attacks Through a Detailed Detection System," International Journal of Intelligent Engineering & Systems (INASS), vol. 15, no. 6, 2022.

Authors

**Mohamed A. Ryan** received his B.Sc. degree and M.S. degree in Systems and Computers Department, Faculty of Engineering, Al-Azhar University in 2012 and 2019 respectively. He studies his PhD. in Al-Azhar University from 2021 to 2023. His research areas are: performance analysis and evaluation of computer networks, Ad-hoc routing protocols and cyber security.

**Sayed A. Nouh** is the professor of computer networks, Computers and Systems Engineering Department at Al Azhar University, Cairo, Egypt. He received his B.Sc. degree in communications engineering and M.Sc. degree in computer engineering form Al Azhar University in 1978 and 1982 respectively. He received his Ph.D. degree in computer engineering from AGH university, Cracov, Poland in 1992. From 2006-2010, he has served as the Egyptian Consultant at African Union, Adds Ababa, Ethiopia. From 2012-2015 he has served as the chairman of Computers and Systems Engineering Department at Al Azhar University.He is the chairman of committee of upgrading the professors and Associate Professors. He is an IEEE member since 1991. He has been involved with research in performance analysis and evaluation of computer networks, Ad-hoc routing protocols, routing and security protocols for wireless sensor neyworks, Mobile Computing and Wireless Networking, Modeling & Computer Simulation techniques, Data Communications Networks.

**Aly M. El-Semary** was born in Egypt in 1969. He received the B.S. degree in Systems and Computer Engineering from Al- Azhar University, Cairo, Egypt in 1992. In addition, He received his M.S. and Ph.D. in network security from Tulsa University, Oklahoma, USA in 2001 and 2004, respectively. In 1998, He awarded a full scholarship from the government of Egypt to study his M.S. and PhD at Tulsa University, Oklahoma, USA Currently, He is the head of Systems and Computer Engineering Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt. He is the author of several journal articles, conference papers, and book chapters. He is a reviewer for several journals and conferences. His current interests include cyber security, wireless and sensor networks, applications of chaotic systems in multimedia encryption, Big Data, and AI.

**How to cite this article:**

Mohamed A. Ryan, Sayed Nouh, Aly M. El-Semary, "A Survey of Current Detection and Prevention Techniques for Black Hole Attack in AODV of MANET", International Journal of Computer Networks and Applications (IJCNA), 10(6), PP: 947-963, 2023, DOI: 10.22247/ijcna/2023/223691.