







Research Article

Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature

Md Ibrahim Talukdar ¹, Rosilah Hassan ², Md Sharif Hossen ¹, Khaleel Ahmad ³,
Faizan Qamar ² and Amjed Sid Ahmed ⁴

¹Department of Information and Communication Technology (ICT), Comilla University, Cumilla, Bangladesh

²Centre for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM),
43600 UKM Bangi, Selangor, Malaysia

³Department of Computer Science and Information Technology, Maulana Azad National Urdu University, Hyderabad, India

⁴Computing Department, Engineering Faculty, Global College of Engineering and Technology, Oman

Correspondence should be addressed to Md Sharif Hossen; mshossen@cou.ac.bd, Khaleel Ahmad; khaleelahmad@manuu.edu.in, and Faizan Qamar; faizanqamar@ukm.edu.my

Received 24 November 2020; Revised 3 January 2021; Accepted 13 February 2021; Published 2 March 2021

Academic Editor: Ihsan Ali

Copyright © 2021 Md Ibrahim Talukdar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In mobile ad hoc networks (MANETs), mobile devices connect with other devices wirelessly, where there is no central administration. They are prone to different types of attacks such as the black hole, insider, gray hole, wormhole, faulty node, and packet drop, which considerably interrupt to perform secure communication. This paper has implemented the denial-of-service attacks like black hole attacks on general-purpose ad hoc on-demand distance vector (AODV) protocol. It uses three approaches: normal AODV, black hole AODV (BH_AODV), and detected black hole AODV (D_BH_AODV), wherein we observe that black holes acutely degrade the performance of networks. We have detected the black hole attacks within the networks using two techniques: (1) intrusion detection system (IDS) and (2) encryption technique (digital signature) with the concept of prevention. Moreover, normal AODV, BH_AODV, and D_BH_AODV protocols are investigated for various quality of service (QoS) parameters, i.e., packet delivery ratio (PDR), delay, and overhead with varying the number of nodes, packet sizes, and simulation times. The NS2 software has been used as a simulation tool to simulate existing network topologies, but it does not contain any mechanism to simulate malicious protocols by itself; therefore, we have developed and implemented a D_BH_AODV routing protocol. The outcomes show that the proposed D_BH_AODV approach for the PDR value delivers around 40 to 50% for varying nodes and packets. In contrast, the delay decreases from 300 to 100 ms and 150 to 50 ms with an increase in the number of nodes and packets, respectively. Furthermore, the overhead changes from 1 to 3 for various nodes and packet values. The outcome of this research proves that the black hole attack degrades the overall performance of the network, while the D_BH_AODV enhances the QoS performance since it detects the black hole nodes and avoids them to establish the communication between nodes.

1. Introduction

Wireless sensor network (WSN) is an interesting research nowadays in the field of communication. The improvement of tiny-structured, resource-constraint, cost-effective sensors is getting simpler. Also, they seem to be able to perceive the parameters of the environment, accumulate relevant data from the area, and convey information to the users. The

Internet of Things (IoT) represents a major and significant component for the 4.0 industrial revolution, and its implementation requires extensive research to ensure that it will operate appropriately [1]. Wireless networks are classified as infrastructure-based networks with a central access point and ad hoc with no access point. Mobile ad hoc network (MANET) is a dynamic network without fixed infrastructure due to its wireless nature that can be deployed as multihop

packet networks. It is a wireless network and has a dynamic topology due to its mobility nature [2]. Also, there is no fixed infrastructure, and each node can act as a source, a destination, or a bridge to forward information packets for the nodes that are out of the transmission range [3–5]. These nodes or devices can have different speeds, transmission ranges, data rates, and packet sizes. Some unique characteristics of MANET are autonomous, dynamic topology, multihop, etc. [6]. These networks are also constrained to transmission ranges, packet losses, security, QoS, etc. Moreover, routing is a fundamental requirement to establish a basic communication among various nodes.

MANET protocols can be described as reactive, proactive, and hybrid in general [7]. The primary function of routing in MANETs is to establish routes among different mobile nodes that satisfy QoS requirements such as bandwidth and end-to-end delay and can be able to operate within the limited energy constraints [8, 9]. There are various kinds of MANET protocols including AODV, dynamic source routing (DSR), destination sequenced distance vector (DSDV), reverse-AODV (RAODV), ad hoc on-demand multipath distance vector (AOMDV), and temporarily ordered routing algorithm (TORA) [10]. The general-purpose AODV is chosen for black hole simulation because it outperforms other reactive routing protocols under important QoS parameters [11, 12]. In fact, the AODV and DSR protocols are two of the most on-demand protocols used in MANETs [13]. Moreover, it combines both DSR and DSDV routing protocols and gets the advantages of both of them [14, 15]. The AODV [16] is a reactive routing protocol that follows route discovery and route maintenance mechanisms and guarantees a loop-free routing by using sequence numbers.

The infrastructureless architecture makes MANETs to numerous attacks [17] such as denial-of-service (DoS) attacks, which create the worst impact on energy consumption [18]. An approach in [19] was focusing on designing an energy-efficient cluster-based on queen-bee (QB) algorithm for wireless sensor networks. This algorithm's high rate results in premature convergence that improves the capability of finding the optimum value of the local minimum. It considers normal and strong mutation, so the diversity of children will be higher and premature divergence can be neglected. The outcome proves that the proposed QB algorithm delivers better results than the genetic algorithm (GA) in terms of energy efficiency that ultimately helps increase the network's lifetime. The authors in [20] proposed a new hierarchical clustering algorithm (HCAL) and corresponded protocol for large-scale MANETs (LMANET). The idea is to utilize the combined weight matrix of both table-driven and on-demand routing in order to locate a dominant set of nodes. The interlink between the LMANET has been established by using the node's relative degree and link expiration time. The results have been evaluated in terms of delay, total rounds of cluster head, cluster head time, overhead, and PDR. The outcome of the proposed HCAL protocol outperforms. They are compared with various routing approaches such as dynamic Doppler velocity clustering, signal characteristic-based clustering, dynamic link duration clustering, and mobility-based clustering algorithms.

The black hole is one of the fatal attacks which acts like a hole that destroys all data packets by itself [21]. The malicious nodes also interrupt the route discovery that causes network packets to be absorbed by the attacker. In route discovery of AODV, the intermediate nodes are liable for finding a correct route to the destination by sending "hello" packets to the neighbors. Whereas in AODV, malicious nodes instantly respond to the source with a false route reply as if it has a correct route to the destination instead of forwarding discovery packets to neighboring nodes [22]. Consequently, the source node immediately forwards its data packets to the destination node through the malicious node, presuming it is an actual route. As a result, the network is affected by a black hole attack where malicious nodes are knowingly misbehaving and damaging the node interface. In general, nodes in the network will restlessly be trying to find a path for the destination, which makes the node consume its resources and lose packets [23].

This paper has implemented black hole attacks on general-purpose AODV protocol with three approaches: normal AODV, black hole AODV (BH_AODV), and detected black hole AODV (D_BH_AODV), wherein we observe that black holes acutely degrade the performance of networks. Hence, we have detected the attackers within the networks using two techniques, i.e., IDS and digital signature encryption technique with the concept of prevention. The IDS detects malicious nodes through the modification of AODV that requires a time stamp, and the digital signature detects malicious nodes through key comparisons. The results have been investigated for various QoS parameters, such as PDR, delay, and overhead with varying the number of nodes, packet sizes, and simulation times.

The rest of the paper is structured as follows. Section 2 includes the related works. In Section 3, we discuss the various issues related to MANET security. Section 4 illustrates the black hole attack and its implementation in AODV. Section 5 explains simulation tools and environment settings. Section 6 represents the black hole attack detection elaborately in AODV using IDS and digital signature. Finally, the conclusion and future remarks are shown in Sections 7 and 8, respectively.

2. Related Works

The ad hoc networks have various application areas in real-world wireless communication scenarios, including sensor networks, military fields, personal area network (PAN), and Bluetooth [24, 25]. Hence, MANET becomes an important research area to establish reliable communication among nodes in an adverse environment [26]. However, these networks fall into various security problems. In recent years, numerous methods but not limited to cryptographic techniques, modification of protocols, IDS, etc. [27, 28] have been suggested by many researchers to improve MANET security. More specifically, the authors in [29] proposed a neuro-fuzzy technique related to IDS for MANETs. The authors of [30] introduced the IDS to detect and identify attackers through the fuzzy technique. The authors in [31] proposed an enhanced trust detection algorithm to improve the detection

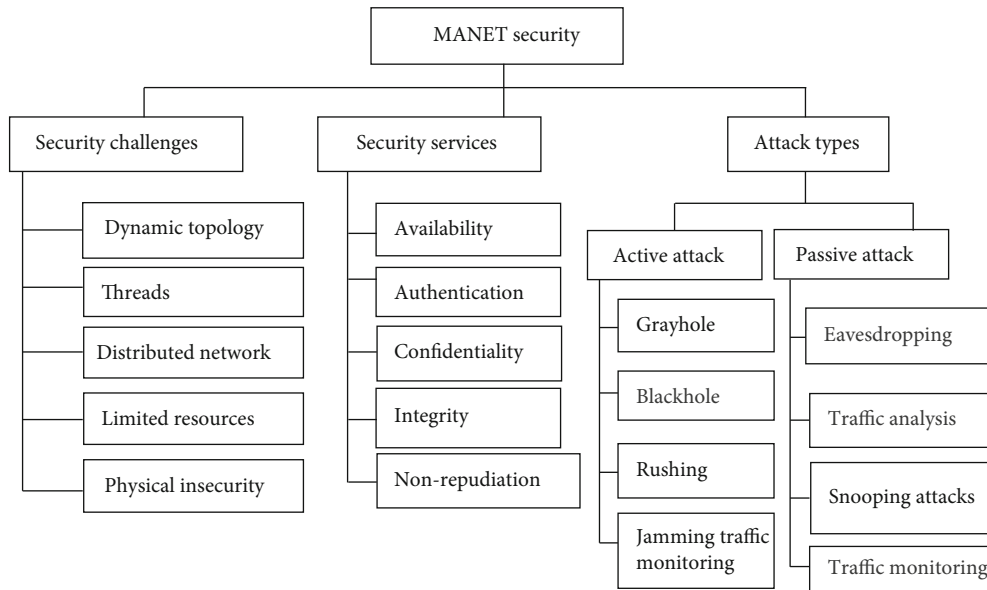


FIGURE 1: Security issues in MANET.

and prevention probability of black hole attackers in MANETs. This method skips the black hole nodes in MANETs, increases the network throughput, and reduces the packet loss as well as the power consumption in the presence of malicious black hole nodes. Another approach in [32] proposed an efficient detection approach that shows low overhead to the network. This approach enhances the delivery ratio by 45.6% for dense networks and 41% for sparse networks. Besides, it improves the dropped packet by 75% for dense networks and 63% for sparse networks. An approach in [33] proposed the honeypot-based security solution which uses cross-layer security to ensure better packet delivery with minimum packet dropped and decrease end to end delay and network load. Similarly, the authors [34] proposed a new protocol based on a dynamic destination sequence number threshold value, which detects and prevents black hole nodes with a better performance than the black hole attack. Another research in [35] proposed lightweight mathematical-based concepts with less computational complexity to detect the hostile nodes and obstruct the black hole nodes in MANETs. Moreover, there are various approaches [36, 37] that improved MANET's security issues.

3. Security Issues in MANET

The security issues in MANETs are highly challenging due to no predefined boundary, adversary inside the networks, no centralized control, and limited energy resource. MANETs are affected by numerous types of threats and attacks. Various attacks but not limited to the black hole, impersonation, wormhole, eavesdropping, man-in-the-middle attack, gray hole, etc. badly interrupt routing mechanism and degrade the execution of ad hoc networks [38, 39]. These attackers are either active attacks or passive attacks [40]. Among these attackers, the black hole attack is one of the fatal attacks that has been considered in this research. Basically, there are two techniques to protect against attacks in MANETs, namely,

proactive and reactive [41]. The proactive approach tries to prevent attackers from launching attacks in the initial stage through numerous cryptographic methods, whereas the reactive method follows the empirical process and responds accordingly to detect security threats. A complete security solution integrates both approaches and includes three sections, i.e., detection, prevention, and reaction. Various mitigation and prevention security approaches such as availability, confidentiality, authorization, authentication, integrity, nonrepudiation, and anonymity might be ensured to establish secure routing [42]. Figure 1 shows the security issues in MANET.

4. Black Hole Attack Implementation in AODV

The AODV protocol used in MANET suffers from a black hole attack wherein an attacker consumes the network traffic and falls all data packets [43, 44]. A black hole is an active attack wherein a malicious node awaits neighboring nodes to forward route request (RREQ) messages. When the malicious node accepts an RREQ message, it instantly sends the route reply (RREP) message of false copy to the sender with the maximum sequence number before other nodes send an actual true one. Therefore, the sender of RREQ presumes that route discovery is accomplished and begins to transmit packets to the malicious node. The black hole attack scenario is explained in Figure 2. Let nodes S , D , and B be the source, destination, and malicious node, respectively. Initially, source node S broadcasts the RREQ message for destination node D to establish a path for communication; however, the malicious node B instantly responds to source node S with a false RREP message exhibiting that it has the maximum sequence number of destination node D , though it is coming from destination node D . Presuming that the destination node D is just behind malicious node B with the single-hop count, source node S refuses the newly received RREP packets come from intermediary node N or M . The

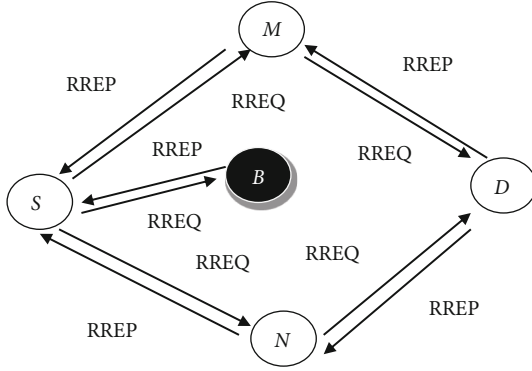


FIGURE 2: Black hole attack scenario.

source node S then begins to send out packets to the malicious node B and presumes that these packets will definitely reach destination node D ; however, in actuality, malicious node B will fall packets and it stops forwarding any packet to any other nodes. The network operation is badly interrupted since the black hole malicious node B consumes all the packets.

The crucial question is that “Which node becomes a malicious node from the nodes?”. One must design the attacking nodes since no node automatically acts as an attacker. In this research, we have designed black hole nodes by modifying the pair of *aodv.h* and *aodv.cc* files. The ns-2.35 simulator has been used in the study to design a network structure and to diminish the black hole node. According to the nodes’ trust value, we design a node to identify that either is an attacker or not. A node may have high, medium, or low trust values (as Boolean values). We can make fewer trust value nodes as a malicious node. In this study, we have designed a black hole attack within AODV by using the five steps:

5. Simulation Tools and Environment Settings

This study utilized a discrete event simulator “NS2” to evaluate the MANET protocols. A tool named “cbrgen” under “~ns/indep-utils/cmu-scen-gen” is used to find random traffic among the nodes using transmission control protocol (TCP) or constant bit rate (CBR) connection. Moreover, “setdest” under “~ns/indep-utils/cmu-scen-gen/setdest/” is used for generating the traces of nodes by random movement with the velocity of the node to any location (not fixed) within the considered wireless region. Node’s mobility is distributed in a random waypoint [45] fashion which can manually create traffic connections and node mobility for a small network. The wireless network environment is constructed using moving nodes. The CBR traffic patterns with specified simulation area, channel, time, etc. are used to design networks. Here, we have considered the random waypoint [46] as the mobility model, which adds the concept of pause time to the random walk model [47]. Table 1 shows the general simulation parameter. We have fixed the number of nodes equal to 60 when we vary the packet sizes, i.e., 512, 1000, 1800, and 2100 bytes. In contrast, we have fixed the packet size = 1000 when we change the number of mobile nodes,

i.e., 20, 60, 80, and 100. Moreover, we have performed the simulations four times and then take the average results in order to calculate the packet delivery ratio, average delay or latency, and overhead ratio.

We choose AODV protocol with a specified simulation area, omnidirectional antenna, random waypoint mobility model, and CBR connection, and transmitted and received power to design the black hole attack. Then, a black hole is designed inside the class files and TCL scripts with few nodes. The TCL scripts are run with the commands “*ns blackhole_nodes.tcl*” where “blackhole_nodes” is the script’s name and *.tcl* is an extension. These scripts will generate two files, namely, *nam* (*.nam*) and trace (*.tr*) files. It has then analyzed the trace files through AWK scripts, which will provide performance value such as PDR, delay, and overhead. Also, we plot the performance using xgraph. Here, *nam* is used for analyzing network simulation traces and practical packet traces. After running a *nam* file for 30 nodes, we can see the node positions and definitions according to declaration where node 16 is defined as an attacker, nodes 2, 8, 13, and 15 are defined as the source, and nodes 0, 6, 7, and 14 are defined as the destination. Here, the attacker is positioned in the middle of the network to succeed in a black hole attack. Multiple sources and destinations are linked through mesh topology while designing networks.

Figure 3 shows the network animator (*nam*) screen for the TCL of black holes. These TCL scripts generate trace (*.tr*) files that can be analyzed through AWK scripts or xgraph. After evaluating the trace files using AWK scripts, simulation results are collected and plotted into graphs. These graphs or xgraphs carefully exhibit the comparison among protocols.

The network’s scalability means that with the growth of the number of nodes in the network, the algorithm maintains the same outcome for different network sizes. With the increase of the number of mobile nodes, the network size increases; hence, the proposed D_BH_AODV algorithm justifies the higher delivery, lower delay, and lower overhead. At present, only 100 nodes are used with 2100 bytes in the present scenario but can be extended for more number of nodes and packets in the future.

6. Black Hole Attack Detection and Simulation Analysis

This section has been divided into subheadings, where the black hole attack detection in AODV is using IDS and digital signature. It provides a concise and precise description of the experimental results and their interpretation, and the experimental conclusions are drawn.

According to the number of attacker nodes, the black hole attacks can be split into two types: (1) single black hole node and (2) cooperative black hole nodes. In a single black hole node, there is only one attacker exists in the network. On the contrary, a cooperative black hole node occupies multiple attackers in the network. In this paper, the black hole attacker has been identified in two ways: (1) IDS [48] or modification of the AODV protocol technique with a single attacker and (2) encryption technique such as digital

Step 1: Variable (attacker) declaration
 We declare a variable malicious as Boolean within the code *aodv.cc*, and *aodv.h*, firstly modifying the code in *aodv.h* file as below:
 Boolean malicious; // or BH

Step 2: Variable (attacker) initialization
 We initialize the attacker variable as a false within the constructor of *aodv.cc*.

Step 3: The normal node is a black_hole (BH), what's happening to the malicious or attacker node value inside some block of code in *aodv.cc*
 file command () function if (argc ==2)
 add some lines of code and replace it as the below code
 if (strcasecmp (argv[1], "black_hole") == 0)
 {
 attacker = true;
 return TCL_OK;
 }

Step 4: The attacker node is true what will be?
 if (attacker == true) {
 printf ("Packets are dropped index of node and number of packets %d is as %d \n",
 index, t_count++);
 drop (p,DROP_RTR_ROUTE_LOOP); //dropped all packet based on this function
 }
 After this completion of work, open the command prompt and go to the ~ns-2.35/
 then finally run the make command
 \$ make
 If there are no mistakes in the above technique of packets dropped, your compilation and execution will be successful.

Step 5: Finally, we go running Tool Command Language (TCL) file with AODV protocol, with Attacker (BH) modified code and normal code, then comparing total experimental outcomes.
 \$ ns AODV.tcl

ALGORITHM 1

TABLE 1: General simulation parameters for black hole evaluation.

Parameters	Values
Protocol	AODV
Modified routing protocols	BH_AODV, D_BH_AODV
Mobility mode	Two-ray ground
Antenna	Omni antenna
Channel	Wireless channel
Simulation time	160 sec
Mobility model	Random waypoint
Simulation area	1100 × 750
Traffic	CBR
Packet size	1000 bytes
Variation of packets	512, 1000, 1800, 2100 bytes
MAC	MAC/802-11
Mobile nodes	60
Variation of nodes	20, 60, 80, 100
Mobility speed	6 m/s
Data rates	0.1 mbps
Performance metrics	PDR, delay, overhead
Simulator	NS 2.35

signature with cooperative black hole node. The following subsections discuss first detecting single black hole attackers using IDS and then detecting multiple attackers using a digital signature.

6.1. IDS and Digital Signature. Intrusion detection system (IDS) detects unwanted activities and security violations to systems [49]. The goal of IDS is to automate the intrusion detection that tries to interrupt the availability, integrity, or confidentiality. Different types of IDS, including signature-based IDS, anomaly-based IDS, and hybrid IDS, are introduced to improve MANET security [50]. At first, IDS detects the black hole nodes and tracks its route, and then it informs the sender node about the malicious node by transmitting a high sequence number so that the sender node does not use that path and does not send any message to that node and searches for a new route to establish a successful secure communication between two nodes [51].

A digital signature is an encryption technique, in which the nodes that are not verified properly are treated as a black hole and dropped. In our approach, we assign a short signature to all nodes and then each node should be verified to get a message from its neighboring nodes. If the signature is matched, then the routing table is updated; otherwise, all the updates are removed. This information is sent to all nodes in the network. In this research, it is used to verify the black hole attack within AODV. In AODV, a RREQ is forwarded

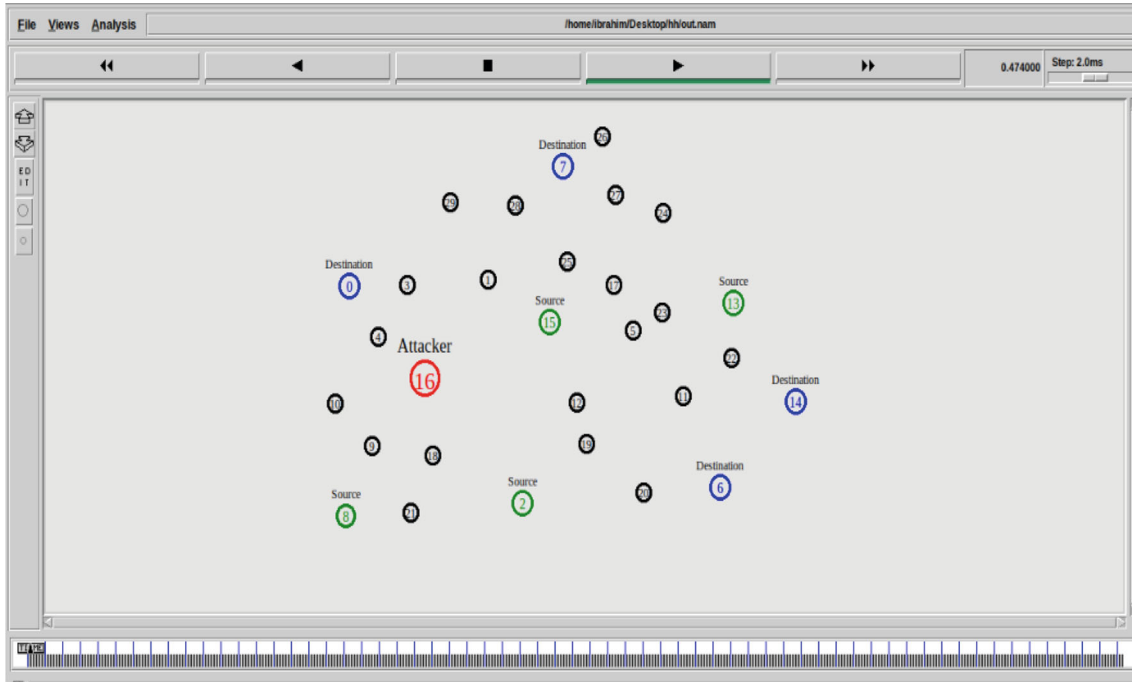


FIGURE 3: The *nam* scenario for black hole simulation.

to the neighboring nodes by the source node until the destination is found. The RREQ packet header retains all the visiting nodes' id while broadcasting RREQ packets to the destination. The destination node containing all of the nodes' id in its header unicasts the reply where each visiting node adds its digital signature. When the receiving node receives the packet compared to the digital signature of the previous node from its database and if the signature is matched, then that node is legitimate; otherwise, that node is considered as an attacker. Whenever an attacker node is detected, that information is broadcast to the neighbors. Hence, in this way, all packets are assigned with a digital signature to prevent the malicious attacks. Digital signature requires much more calculation overhead in signing/decrypting and verifying/encrypting for node activities. In this subsection, we have designed and detected multiple attackers through an encryption standard (digital signature) in which every node has its own key, and the packet transmission has been performed when the key is in a valid state. In this case, both source and destination nodes will exchange the keys before the packet transmission. If the node's key is found to be in a valid state, that node will be considered a trusted node to start a packet transmission. As the attacker node is not aware of the correct key for the transmission, it cannot get any packet from the source node, which ultimately enhances the overall network performance.

6.2. Black Hole Attack Detection Using IDS and Analysis. In this research, a black hole attacker is implemented inside the AODV protocol by modifying AODV using the node's trust value. To mitigate the black hole attacks, a trust-based mechanism has been used to analyze the packets dropped within the time stamp given on TCL code if the black hole is true. The various QoS parameters, such as PDR, delay,

and overhead, have been analyzed through node and packet variations as shown in Figure 4 and Figure 5, respectively. The comparison has been shown among normal AODV, BH_AODV, and D_BH_AODV to investigate protocols' performance.

For node variations (20, 60, 80, and 100), PDR is increasing when the number of nodes is greater than 60 as shown in Figure 4. Moreover, for varying the packet sizes, i.e., 512, 1000, 1800, and 2100, D_BH_AODV outperforms BH_AODV and lags than normal AODV in the case of PDR as shown in Figure 5. In both cases, i.e., for varying the number of nodes and packet sizes, normal AODV shows good delivery. In this research, our consideration is the presence of black hole attacks through communication among nodes in the network. Hence, from both Figures 4 and 5, BH_AODV degrades the delivery of normal AODV for varying the nodes and packet sizes, whereas our proposed D_BH_AODV shows greater delivery than BH_AODV.

It is very often that the delay measurement shows irregularities in performance exhibition. Even small changes in parameters significantly affect the performances. For varying the number of mobile nodes and the packet sizes as shown in Figures 6 and 7, we can see that normal AODV exhibits higher average delay than BH_AODV and D_BH_AODV. However, for both cases, as shown in Figures 6 and 7, it is obvious that D_BH_AODV shows a lower average delay than normal AODV but exhibits a higher delay compared to BH_AODV.

In general, high overhead degrades network performance because the number of packet replication increases to send a successful packet to the destination. Hence, it increases the transmission cost also. So, low overhead is preferable. The black hole attack increases the rate of packet replication. For varying the number of nodes and packet sizes shown in

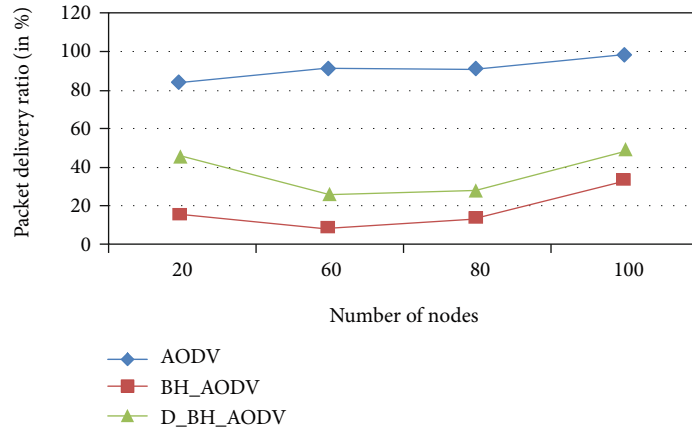


FIGURE 4: PDR with varying nodes.

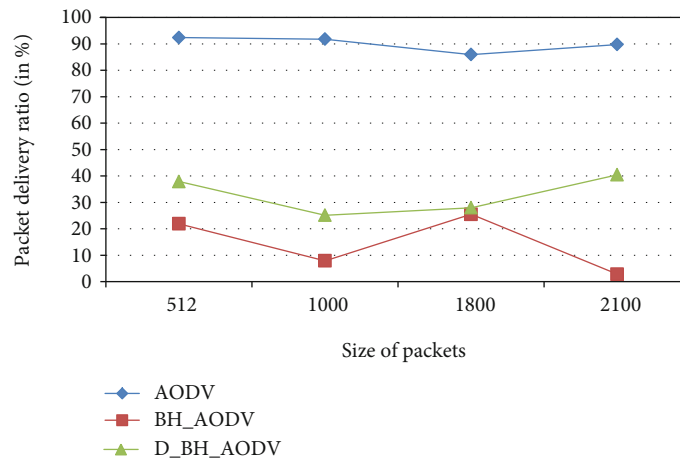


FIGURE 5: PDR with varying packets.

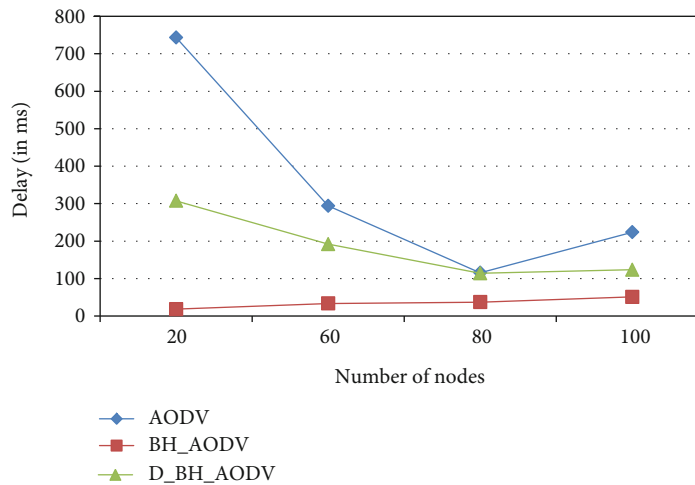


FIGURE 6: Delay with varying nodes.

Figures 8 and 9, normal AODV exhibits lower overhead because we do not consider an attacker node. While BH_AODV receives the packets from neighboring nodes and changes its contents, then, the sender nodes again send their copies. Hence, the BH_AODV results in higher overhead. D_

BH_AODV detects and prevents the black hole nodes from sending copies. So, D_BH_AODV exhibits lower overhead than BH_AODV as shown in Figures 8 and 9.

In this research, the nodes are placed randomly on a specified simulation area and the environment is simulated

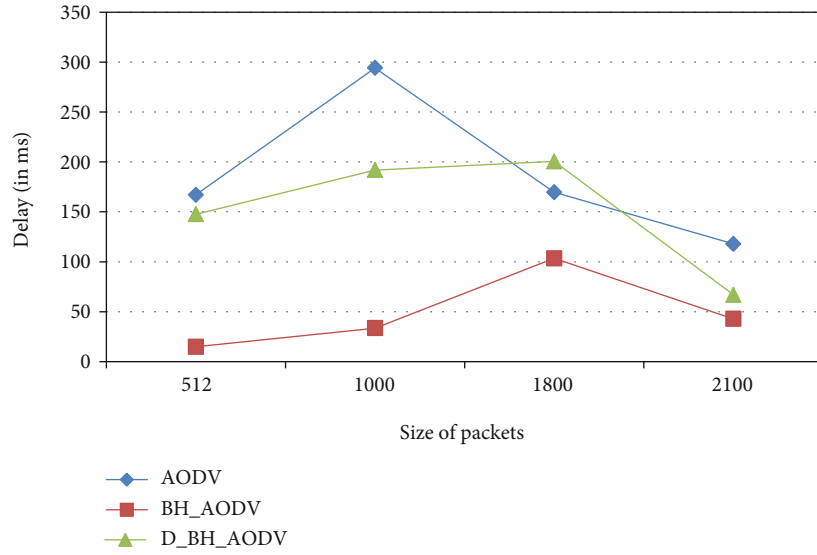


FIGURE 7: Delay with varying packets.

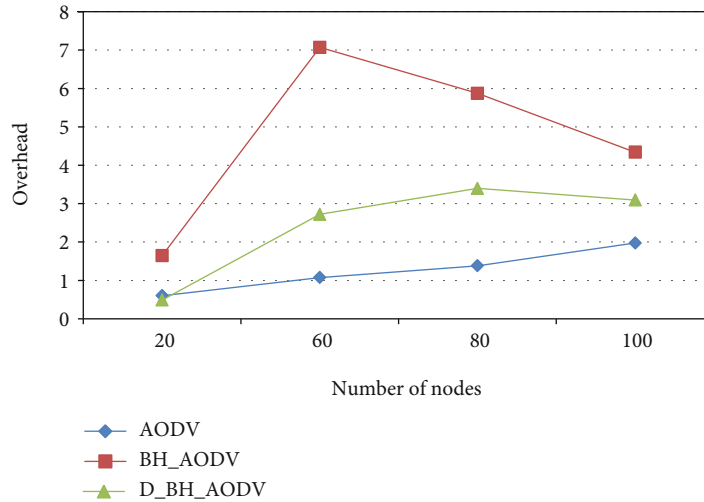


FIGURE 8: Overhead with varying nodes.

through RWP (random waypoint) mobility model. The simulation results depict the state of normal AODV, BH_AODV, and D_BH_AODV for the same network environment. Here, the graphical analyses depict that for varying the number of nodes and packet sizes, the black holes degrade the performance over normal AODV and the D_BH_AODV outperforms BH_AODV in terms of PDR, delay, and overhead ratio. However, in some cases, we cannot find the expected simulation results due to nodes' misbehaving [52]. Misbehaving nodes also known as selfish nodes have full access to the medium that tries to get favored from other nodes but ignoring to forward other node packets can severely reduce the whole network's performance. In this case, the prevention of different attackers is the proper solution to network improvement.

6.3. Black Hole Attack Detection in AODV Using Digital Signature and Analysis. In this section, we will see the com-

parison between the BH_AODV and the D_BH_AODV using xgraph. Here, an effective encryption technique (digital signature) is used to detect black hole attacks. As the previous discussion of generating trace files in Figure 3, the TCL scripts of the BH_AODV and D_BH_AODV are evaluated and xgraphs are plotted to sketch the QoS parameters with respect to the simulation time in second(s). Figures 10, 11, and 12, respectively, show the improved performance of D_BH_AODV over BH_AODV attack in the AODV protocol using xgraph in terms of PDR, average latency or delay, and overhead ratio with varying the simulations times.

For varying the simulation times in seconds as shown in Figure 10, we observe that D_BH_AODV exhibits higher packet delivery ratio compared to the black hole AODV because D_BH_AODV detects the attackers' nodes and does not forward the packets to the black hole attackers' nodes. Hence, it ensures higher delivery (Figure 10) by lowering the packet replications, i.e., lower overhead ratio (Figure 12).

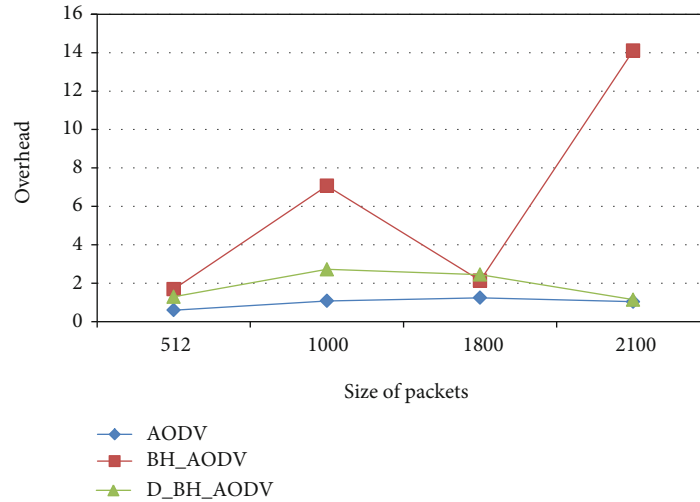


FIGURE 9: Overhead with varying packets.



FIGURE 10: PDR with varying time for black hole and detected black hole attack.

For varying the simulation times in seconds as shown in Figure 11, we observe that the average delay of the BH_AODV is very high compared to the average delay of D_BH_AODV. Therefore, D_BH_AODV significantly improves wireless networks' performance by ensuring higher delivery (Figure 10) and lower delay (Figure 11) compared to the BH_AODV.

As the above discussion of Figure 10, using D_BH_AODV reduces the packet replication and ensures lower overhead as shown in Figure 12 indicated by the green line, while BH_AODV exhibits very high overhead compared to D_BH_AODV because of its uncontrolled attacking behavior.

Figure 10 to Figure 12 illustrate that PDR, delay, and overhead are desirable for D_BH_AODV over BH_AODV because D_BH_AODV ensures a higher delivery ratio, lower delay, and lower overhead ratio compared to BH_AODV. Therefore, we can say that the D_BH_AODV improves the performance over the black hole affected by AODV protocol (BH_AODV) in terms of QoS parameters under consideration.

In a concise discussion, it is clear that the D_BH_AODV routing can detect the black hole nodes and prevent those nodes from participating in further communication. Hence, D_BH_AODV uses IDS and digital signature methods to ensure higher delivery, lower delay, and lower transmission

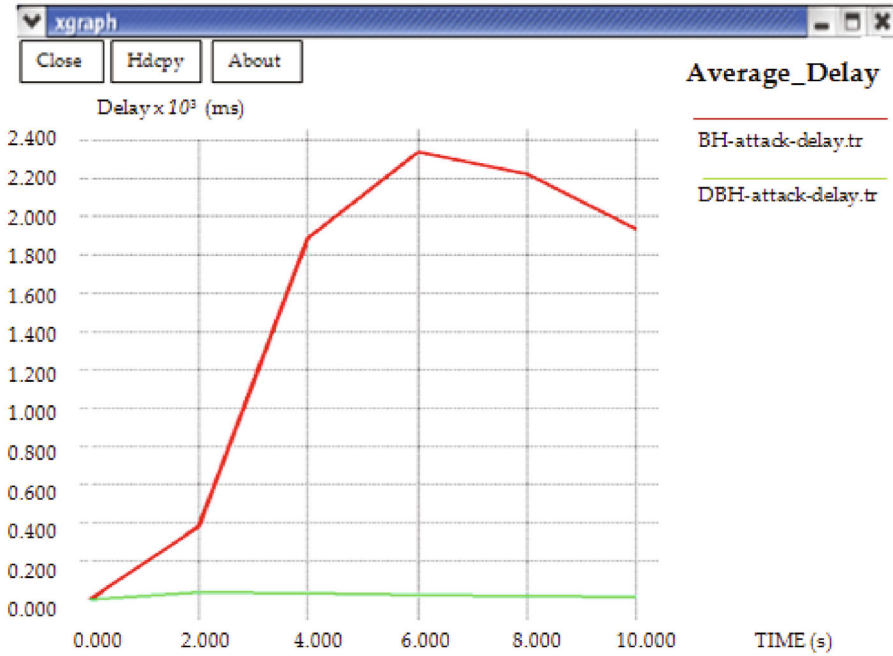


FIGURE 11: Delay with varying time for black hole and detected black hole attack.

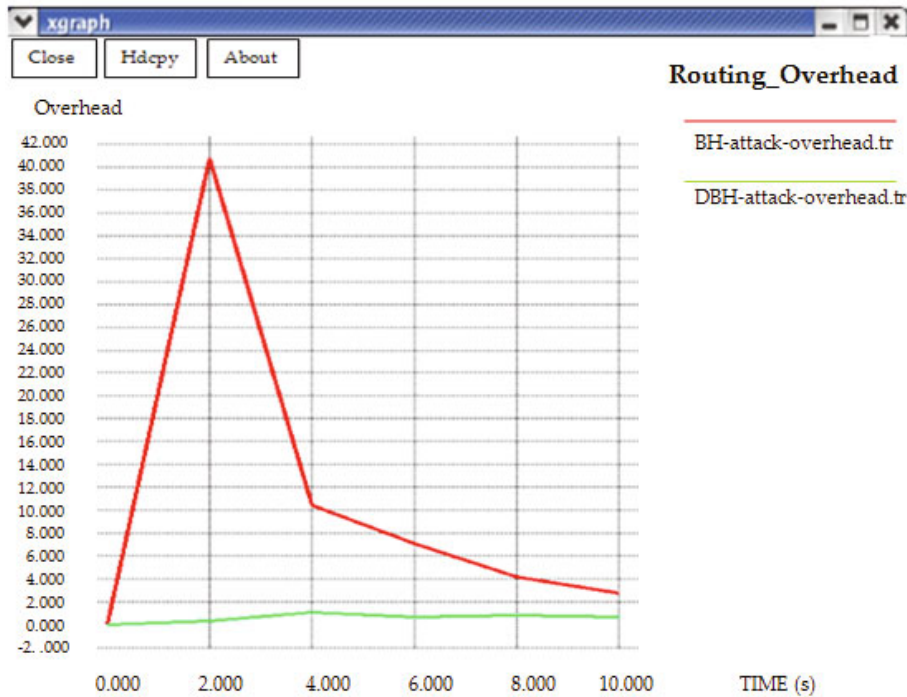


FIGURE 12: Overhead with varying time for black hole and detected black hole attack.

cost (i.e., lower overhead ratio) because D_BH_AODV does not forward/send message copies or packets to an attacker's node. The above investigations (from Figure 4 to Figure 12) exhibit that D_BH_AODV outperforms BH_AODV by ensuring good delivery, lower delay, and lower overhead in case of digital signature and IDS wherein D_BH_AODV shows higher delay than BH_AODV but lower delay than AODV in case of using IDS (as shown in Figures 6 and 7).

7. Conclusion

MANETs are vulnerable to different attacks that badly affect the wireless networks while establishing a secure routing. In this study, we implement a black hole attack within the AODV protocol by modifying AODV and the trust value of nodes. We detect attackers through a trust mechanism using IDS that requires a time stamp and the encryption technique

using a digital signature. In IDS, we make a graphical comparison among AODV, BH_AODV, and D_BH_AODV. Moreover, in the encryption technique, we make a comparison between BH_AODV and D_BH_AODV black hole AODV. In both cases, the analysis is done in terms of PDR, average delay, and overhead ratio for varying the number of nodes, packets' size, and simulation times. Our investigated results exhibit that under the consideration of AODV routing, the BH_AODV degrades the performance of AODV by lowering the delivery ratio and maximizing the overhead ratio for varying the number of nodes, the size of packets, and the simulation times. It also verifies in both cases, i.e., IDS and digital signature, whereas the D_BH_AODV shows higher delivery and lower overhead compared to the BH_AODV. Although the D_BH_AODV exhibits a higher delay compared to the BH_AODV in case of using IDS, our proposed and implemented D_BH_AODV shows a lower average delay than the original AODV routing for the above variation. In the case of using a digital signature, we observe that the D_BH_AODV routing exhibits a lower delay compared to the BH_AODV. Therefore, the BH_AODV sharply degrades the performance, and the D_BH_AODV improves the networks' overall performance.

8. Future Work

In this network scenario, the variation in the number of nodes is from 20 to 100, whereas the variation of packets is from 512 to 2100 bytes along with the 6m/s of mobility speed. However, the possibility of having a higher number of nodes and packets with higher mobility can likely happen in real-world scenarios; therefore, this work can be extended to explore the scalability of the network. A secure AODV protocol would be established to prevent various attacks such as wormhole and jellyfish within wireless networks through encryption techniques to guarantee a good trade-off among PDR, average delay, overhead ratio, and energy consumption. Also, this research can also lead to other security services and domestic appliances. It can be used to prevent multiple black hole attacks. AODV protocols can also help in various IoT applications by designing different AODV extensions based on numerous criteria, e.g., quality, reliability, energy, security, and routing strategies [53]. For example, an optimized AODV (OAODV) can be designed to ensure low energy consumption of IoT sensors [54]. Also, an energy-aware secure AODV routing can be implemented by using better route maintenance approaches for large networks [55]. Furthermore, advanced AODV approaches such as collaborative black hole attack-AODV routing protocol (CBHA-AODV) [56] can be implemented for real-time IoT-based civil construction application.

Data Availability

The data used to support the findings of this study are available from the first author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

The authors would like to acknowledge the support of the Network Communication Technology (NCT) Research Groups, FTSM, Universiti Kebangsaan Malaysia. This paper is supported under the Dana Impak Perdana UKM (DIP-2018-040) and Fundamental Research Grant Scheme (FRGS/1/2018/TK04/UKM/02/17). The authors also would like to thank the ICT Division of the Bangladesh Government for awarding a research fellowship to Md Ibrahim Talukdar for this research.

References

- [1] I. Mohd Zaki and H. Rosilah, "The implementation of Internet of Things using test bed in the UKMnet environment," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 8, no. 2, pp. 1–17, 2019.
- [2] Z. Ismail and R. Hassan, "A performance study of various mobility speed on AODV routing protocol in homogeneous and heterogeneous MANET," in *the 17th Asia Pacific Conference on Communications*, IEEE, 2011.
- [3] T. Salam and M. S. Hossen, "Performance analysis on homogeneous LEACH and EAMMH protocols in wireless sensor network," *Wireless Personal Communications*, vol. 113, no. 1, pp. 189–222, 2020.
- [4] M. S. Hossen, "DTN routing protocols on two distinct geographical regions in an opportunistic network: an analysis," *Wireless Personal Communications*, vol. 108, no. 2, pp. 839–851, 2019.
- [5] M. Singh, C. Kumar, and P. Nath, "Challenges and protocols for P2P applications in multi-hop wireless networks," in *in 2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 310–316, IEEE, 2018.
- [6] T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, "Heterogeneous ad hoc networks: architectures, advances and challenges," *Ad Hoc Networks*, vol. 55, pp. 143–152, 2017.
- [7] C. S. R. Murthy, *Ad Hoc Wireless Networks: Architectures and Protocols*, Pearson Education India, 2004.
- [8] S. M. Adam and R. Hassan, "Delay aware reactive routing protocols for QoS in MANETs: a review," *Journal of applied research and technology*, vol. 11, no. 6, pp. 844–850, 2013.
- [9] S. Malathy, V. Porkodi, A. Sampathkumar et al., "An optimal network coding based backpressure routing approach for massive IoT network," *Wireless Networks*, vol. 26, no. 5, pp. 3657–3674, 2020.
- [10] H. M. Haglan, S. A. Mostafa, N. Z. M. Safar et al., "Analyzing the impact of the number of nodes on the performance of the routing protocols in MANET environment," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 434–440, 2020.
- [11] S. Yan and Y. Chung, "Improved ad hoc on-demand distance vector routing (AODV) protocol based on blockchain node detection in ad hoc networks," *International Journal of*

- Internet, Broadcasting and Communication*, vol. 12, no. 3, pp. 46–55, 2020.
- [12] R. K. Mohapatra, S. Samantaray, A. Sahoo et al., “Performance analysis of reactive routing protocols in MANET under CBR traffic using NS2,” in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 352–356, IEEE, 2018.
 - [13] A. K. Biswas and M. Dasgupta, “AODV-DSR hybrid reactive routing protocol and its generalization for mobile ad-hoc networks,” in *2019 3rd International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, pp. 1–5, IEEE, 2019.
 - [14] V. Sharma, B. Alam, and M. Doja, “An improvement in DSR routing protocol of MANETs using ANFIS,” in *Applications of Artificial Intelligence Techniques in Engineering*, pp. 569–576, Springer, 2019.
 - [15] K. L. Arega, G. Raga, and R. Bareto, “Survey on performance analysis of AODV, DSR and DSDV in MANET,” *Computer Engineering and Intelligent Systems*, vol. 11, no. 3, pp. 23–32, 2020.
 - [16] F. T. AL-Dhief, N. Sabri, M. S. Salim, S. Fouad, and S. A. Aljunid, “MANET routing protocols evaluation: AODV, DSR and DSDV perspective,” in *MATEC Web of Conferences*, vol. 150, p. 06024, EDP Sciences, 2018.
 - [17] A. Kulkarni, R. Bukate, and S. Nanaware, “Study of various attacks and routing protocols in MANETS,” in *2018 International Conference on Information, Communication, Engineering and Technology (ICICET)*, pp. 1–3, IEEE, 2018.
 - [18] A. M. Fahad and R. C. Muniyandi, “Harmony search algorithm to prevent malicious nodes in mobile ad hoc networks (MANETs),” *Information Technology Journal*, vol. 15, no. 3, pp. 84–90, 2016.
 - [19] Z. Pooranian, A. Barati, and A. Movaghar, “Queen-bee algorithm for energy efficient clusters in wireless sensor networks,” *World Academy of Science, Engineering and Technology*, vol. 73, pp. 1080–1083, 2011.
 - [20] S. H. H. Nazhad, M. Shojafar, S. Shamshirband, and M. Conti, “An efficient routing protocol for the QoS support of large-scale MANETs,” *International Journal of Communication Systems*, vol. 31, no. 1, article e3384, 2018.
 - [21] M. S. Pathan, J. He, N. Zhu, Z. Ali, M. Qasim, 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.
 - [22] 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 *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 1278–1282, IEEE, 2017.
 - [23] G. K. Wadhvani, S. K. Khatri, and S. K. Mutto, “Trust framework for attack resilience in MANET using AODV,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 1, pp. 209–220, 2020.
 - [24] S. El Jay and A. Hasbi, “Security in mobile ad hoc networks (MANETs) and WSNs (wireless sensor networks),” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 16, no. 9, p. 118, 2016.
 - [25] M. Y. Thanoun and A. M. Aleesa, “Routing, significant and applications of mobile ad-hoc wireless sensor networks,” *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 2, pp. 850–854, 2020.
 - [26] V. Tilwari, M. D. N. Hindia, K. Dimyati, F. Qamar, and M. S. A. Talip, “Contention window and residual battery aware multipath routing schemes in mobile ad-hoc networks,” *International Journal of Technology*, vol. 10, no. 7, pp. 1376–1384, 2019.
 - [27] V. L. Narayana and C. Bharathi, “Identity based cryptography for mobile ad hoc networks,” *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 5, p. 1173, 2017.
 - [28] M. Rath and B. K. Pattanayak, “Security protocol with IDS framework using mobile agent in robotic MANET,” *International Journal of Information Security and Privacy*, vol. 13, no. 1, pp. 46–58, 2019.
 - [29] A. Chaudhary, V. N. Tiwari, and A. Kumar, “Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks,” *International Journal of Soft Computing and Networking*, vol. 1, no. 1, pp. 17–34, 2016.
 - [30] E. V. Balan, M. K. Priyan, C. Gokulnath, and G. U. Devi, “Fuzzy based intrusion detection systems in MANET,” *Procedia Computer Science*, vol. 50, pp. 109–114, 2015.
 - [31] J. Manoranjini, A. Chandrasekar, and S. Jothi, “Improved QoS and avoidance of black hole attacks in MANET using trust detection framework,” *Automatika*, vol. 60, no. 3, pp. 274–284, 2019.
 - [32] Y. M. Khamayseh, S. A. Aljawarneh, and A. E. Asaad, “Ensuring survivability against black hole attacks in MANETS for preserving energy efficiency,” *Sustainable Computing: Informatics and Systems*, vol. 18, pp. 90–100, 2018.
 - [33] G. Usha, M. R. Babu, and S. S. Kumar, “Dynamic anomaly detection using cross layer security in MANET,” *Computers & Electrical Engineering*, vol. 59, pp. 231–241, 2017.
 - [34] 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.
 - [35] M. Thebiga and R. SujiPramila, “A new mathematical and correlation coefficient based approach to recognize and to obstruct the black hole attacks in MANETs using DSR routing,” *Wireless Personal Communications*, vol. 114, no. 2, pp. 975–993, 2020.
 - [36] S. Kumar, M. Goyal, D. Goyal, and R. C. Poonia, “Routing protocols and security issues in MANET,” in *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)*, pp. 818–824, IEEE, 2017.
 - [37] S. Gurung and S. Chauhan, “Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET,” *Wireless Networks*, vol. 25, no. 3, pp. 975–988, 2019.
 - [38] 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 *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, pp. 1–6, IEEE, 2016.
 - [39] R. K. Singh and P. Nand, “Literature review of routing attacks in MANET,” in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 525–530, IEEE, 2016.
 - [40] S. Shrestha, R. Baidya, B. Giri, and A. Thapa, “Securing black-hole attacks in MANETs using modified sequence number in AODV routing protocol,” in *2020 8th International Electrical Engineering Congress (iEECON)*, pp. 1–4, IEEE, 2020.
 - [41] 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 *in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, IEEE, 2019.
- [42] D. A. F. B. H. INTRUSION, “Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks,” *Journal of Computer Science*, vol. 9, no. 4, pp. 521–525, 2013.
- [43] S. R. Deshmukh, P. Chatur, and N. B. Bhople, “AODV-based secure routing against blackhole attack in MANET,” in *in 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pp. 1960–1964, IEEE, 2016.
- [44] V. Savkare and N. Kazi, “AODV and DSR routing protocol performance comparison in MANET using network simulator (NS2),” *Int. Res. J. Eng. Technol*, vol. 6, no. 9, pp. 7–10, 2019.
- [45] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, “Security challenges and attacks in dynamic mobile ad hoc networks MANETs,” in *in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pp. 28–33, IEEE, 2019.
- [46] R. Skaggs-Schellenberg, N. Wang, and D. Wright, “Performance evaluation and analysis of proactive and reactive MANET protocols at varied speeds,” in *in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 981–985, IEEE, 2020.
- [47] A. Pramanik, B. Choudhury, T. S. Choudhury, W. Arif, and J. Mehedi, “Behavioral study of random waypoint mobility model based energy aware MANET,” in *in 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 624–629, IEEE, 2016.
- [48] R. Thiagarajan and M. Moorthi, “Efficient routing protocols for mobile ad hoc network,” in *in 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, pp. 427–431, IEEE, 2017.
- [49] H. Moudni, M. Er-rouidi, H. Mouncif, and B. E. Hadadi, “Black hole attack detection using fuzzy based intrusion detection systems in MANET,” *Procedia Computer Science*, vol. 151, pp. 1176–1181, 2019.
- [50] Z. Ahmad and A. Bansiya, “Survey on security by using intrusion detection system in MANET,” *A RKDF University Journal of Science and Engineering*, vol. 2, no. 1, pp. 21–25, 2019.
- [51] S. Sivanesh and V. S. Dhulipala, “Accurate and cognitive intrusion detection system (ACIDS): a novel black hole detection mechanism in mobile ad hoc networks,” *Mobile Networks and Applications*, 2020.
- [52] V. Nancy, “A security for MANET interruption recognition & preclusion approaches for network layer attacks,” *International Journal of Applied Engineering Research*, vol. 13, no. 12, pp. 10702–10706, 2018.
- [53] T. K. Saini and S. C. Sharma, “Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept,” *Ad Hoc Networks*, vol. 103, p. 102148, 2020.
- [54] A. Zrelli, H. Khlaifi, and T. Ezzedine, “Performance evaluation of AODV and OAODV for several WSN/IoT applications,” in *in 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–6, IEEE, 2019.
- [55] N. Kamboj and M. Rai, “A new secure ad-hoc on demand distance vector routing protocol to ensure less power consumption in mobile ad-hoc network,” *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 6, pp. 2483–2487, 2020.
- [56] T. A. S. Srinivas and S. M. Manivannan, “Preventing collaborative black hole attack in IoT construction using a CBHA-AODV routing protocol,” *International Journal of Grid and High Performance Computing*, vol. 12, no. 2, pp. 25–46, 2020.