electronics

MDPI

Article

A Lightweight Anomaly Detection System for Black Hole Attack

Ashraf Abdelhamid [1], Mahmoud Said Elsayed [2,*], Anca D. Jurcut [2] and Marianne A. Azer [3]

[1] School of Information Technology and Computer Science, Nile University, Cairo 11511, Egypt
[2] School of Computer Science, University College Dublin, D04V1W8 Dublin, Ireland
[3] National Telecommunication Institute, Nasr City 11765, Egypt
* Correspondence: mahmoud.abdallah@ucdconnect.ie

Abstract: Mobile ad hoc networks (MANETs) are now key in today's new world. They are critically needed in many situations when it is crucial to form a network on the fly while not having the luxury of time or resources to configure devices, build infrastructure, or even have human interventions. Ad hoc networks have many applications. For instance, they can be used in battlefields, education, rescue missions, and many other applications. Such networks are characterized by high mobility, low resources of power, storage, and processing. They are infrastructure-less; this means that they don't use infrastructure equipment for communication. These networks rely instead on each other for routing and communication. MANETs use a hopping mechanism where each node in a network finds another node within its communication range and use it as a hop for delivering the message through another node and so on. In standard networks, there is dedicated equipment for specific functions such as routers, servers, firewalls, etc., while in ad hoc networks, every node performs multiple functions. For example, the routing function is performed by nodes. Hence, they are more vulnerable to attacks than standard networks. The main goal of this paper is to propose a solution for detecting black hole attacks using anomaly detection based on a support vector machine (SVM). This detection system aims at analyzing the traffic of the network and identifying anomalies by checking node behaviors. In the case of black hole attacks, the attacking nodes have some behavioral characteristics that are different from normal nodes. These characteristics can be effectively detected using our lightweight detection system. To experiment with the effectiveness of this solution, an OMNET++ simulator is used to generate traffic under a black hole attack. The traffic is then classified into malicious and non-malicious based on which the malicious node is identified. The results of the proposed solution showed very high accuracy in detecting black hole attacks.

Keywords: ad hoc networks; anomaly detection; attacks; blackhole; MANETs; network security; routing protocols; support vector machine (SVM)

check for updates

Citation: Abdelhamid, A.; Elsayed, M.S.; Jurcut, A.D.; Azer, M.A. A Lightweight Anomaly Detection System for Black Hole Attack. *Electronics* **2023**, *12*, 1294. https://doi.org/10.3390/electronics12061294

Academic Editor: Hamid Reza Karimi

Received: 26 November 2022
Revised: 16 February 2023
Accepted: 19 February 2023
Published: 8 March 2023

1. Introduction

Mobile ad hoc networks (MANETs) can be formed without standard fixed infrastructure or support from administrators [1]; they are rather pre-configured in order to work spontaneously. In general, wireless networks are divided into two main categories: infrastructure and infrastructure-less. In Infrastructure networks, the wireless devices are configured by administrators to be connected to fixed-base equipment to provide them with multiple services, for instance, routing, storage, and security services. In infrastructure-less networks, such as MANETs, nodes are self-configured and do not rely on fixed-base infrastructure; instead, they rely on each other. In other words, every node performs multiple functions [2]. In light of these limitations, MANETs have some challenges that are unique to them compared with traditional infrastructure networks. When establishing MANETs, two important aspects are taken into consideration: security and routing challenges [3]. As for security challenges, MANETs, in general, lack the infrastructure that can perform sophisticated perimeter security functions such as firewalls, border routers, IDS, IPS, etc. When it comes to routing challenges, in order for nodes to communicate with one another, they need a routing function. The routing function is mainly used to ensure that the message from the sender is going the most efficient way (route) to reach its intended destination. The standard traditional infrastructure routing protocols are not effective for MANETs for many reasons. One of them is that MANETs are infrastructure-less networks meaning that the routing function is not performed by dedicated devices such as routers. This function is rather performed by almost every node in the network. That is why new enhanced routing protocols were developed for MANETs.

MANET routing protocols can be divided into two main categories: proactive (table-driven) and reactive (on demand) [4,5]. In table-driven protocols, routing information is maintained regularly whenever any change takes place, while in on-demand routing protocols, routing information is collected only when needed [6]. One of the well-known on-demand routing protocols is the ad hoc on-demand distance vector (AODV). It shows better performance among other on-demand routing protocols [7]. However, due to its limitations, MANETs are exposed to multiple attacks. One of these attacks is the black hole attack. The blackhole attack is a major attack that affects the network performance dramatically [8]. In this attack, the attacker's node acts as the shortest path to the destination, then drops the packets it receives; hence, it heavily affects the network delivery ration.

The main contributions of this paper are as follows:

- Reviewing and categorizing the different approaches and comparing the different techniques used to mitigate the black hole attacks in MANETs.
- Developing a dataset for studying the black hole attacks using OMNET++ in order to thoroughly analyze the traffic in order to effectively study node behavior in the presence of an attack.
- Developing a lightweight detection system for identifying malicious nodes.

The remainder of this paper is organized as follows: Section 2 provides a background on mobile ad hoc networks, their applications, characteristics, and challenges. Section 3 reviews the related work and efforts undertaken by other researchers in this topic. In Section 4, the methodology of our proposed solution is explained. Section 5 concludes the paper and provides suggestions for future work.

2. Background

Mobile ad hoc networks have unique characteristics and in general are different from networks, especially when it comes to security. In this section, we discuss MANETs applications, security challenges and common attacks.

2.1. MANET Characteristics

MANETs have many special characteristics that help in their unique applications. Their characteristics are as follows:

- Lack of infrastructure: MANETs are featured as infrastructure-less networks. This makes them efficient in terms of time and cost. They can be formed at very low cost and on the fly [9]. At the same time, it makes them more vulnerable to attacks than standard networks.
- Distributed management: Due to the lack of centralized management and control, these functions are distributed across the nodes. Hence, the node security, network topology, authentication of new nodes, and data security are all affected [10].
- Cooperativeness: Unlike standard networks that use client-server architecture, MANETs are peer-to-peer architecture. In order for MANETs to be effective, all nodes should cooperate by providing the functions that are left unattended due to the lack of infrastructure security and centralized management. This cooperation aims at building confidence among nodes.
- Multi-hop routing: One of the functions that are fulfilled by nodes themselves is routing. In order for a node to send a message to another node, it uses adjacent nodes as hops to reach out to the destination [11]. This is what is called multi-hop routing.

- Dynamic topology: As there are perimeter boundaries for MANETs, nodes move in and out of the network unpredictably at any time. Furthermore, there is no centralized management, so networks themselves can be formed autonomously at any time [12,13].
- Decentralized architecture: All the nodes in the network are independent. They are self-configured and do not require any support to join or leave the network. They are autonomous in taking such decisions. They are also free to forward or drop data packets even if they are not supposed to do so [13].
- Limited resources: Nodes in MANETs are characterized by low resources of power and processing as they run on batteries and have less powerful processing units. The key issue of a limited power supply is that it makes MANET nodes more targeted by denial-of-service attacks [14]. The attacker, in this case, sends additional packets to nodes in order to consume their batteries.

2.2. MANET Security Challenges

MANETs are more vulnerable than standard wired networks due to their limited resources as well as physical security, dynamic topology, and lack of perimeter security. They are more prone to attacks from inside and outside the network. MANET attacks can be divided into two main categories: passive attacks and active attacks [15].

Active attacks are the ones in which the attacker tries to modify or distort the data being transmitted into the network. There are many examples of active attacks, such as black hole attacks, which are the focus of this paper, routing table overflow, impersonation, rushing attacks, denial-of-service attacks, Byzantine attacks, packet replication, and distributed denial-of-service attacks.

Passive attacks are the ones in which the attacker tries to get authorized access to eavesdrop on the data [6]. Some of the examples of passive attacks are eavesdropping, traffic analysis, and location disclosure. In this section, some the MANET challenges are explained as follows:

- Lack of perimeter security: As MANETs are infrastructure-less, there are no defined boundaries for their nodes. Furthermore, any node can join or leave the network freely, which makes the topology dynamic and challenging. When a malicious node reaches the range of the network, it can impersonate a legitimate node and start an attack.
- Limited physical security: MANETs are formed on the fly anywhere and at any time. There is no physical security to protect the core service, such as keeping the network backbone in a secure data center in traditional networks.
- Lack of centralized control: In MANETs, there is no centralized system to provide essential security requirements, such as identification, authentication, and authorization as well as other security services, such as firewalls, network access controls, etc. This makes MANETs more challenging in terms of security than standard networks.
- Dynamic topology: MANET nodes are free to move in and out of a networks; hence, the connectivity between nodes in MANETs can change anytime because nodes can move freely. The same also applies to networks. Some networks can move and merge into other network. This can change the routing information rapidly all the time.
- Scalability: MANETs consist of large number of nodes that can grow and shrink according to different situations. This makes MANETs very efficient yet challenging due to the security requirements of identifying and authenticating new nodes.
- Quality of Service: Different data types have different requirements. For instance, media streaming and live transmission require a higher bandwidth and stability. In such cases, the avoidance of latency and data loss needs to be guaranteed through QOS policies and algorithms.
    - ○ Resource limitations: Nodes in MANETs have limited resources in terms of batteries, processing, and storage. This is a source of two potential issues: first, the nodes can be equipped with sophisticated end protection due to limited processing capability; second, is being targeted by some attacks to drain batteries.

○ Security: Due to the various vulnerabilities stemming from the lack of physical recourse, limited resources, absence of infrastructure, and dynamic topologies, MANETs possess more security challenges than traditional networks.

2.3. MANET Routing Protocols

Routing protocols are the methods or rules that define how nodes will communicate with each other. The key function of a routing protocol is to find the best way a message can take from a sender to reach the destination [16]. Generally, there are three common categories of routing protocol as depicted in Figure 1 proactive, reactive, and hybrid [17].

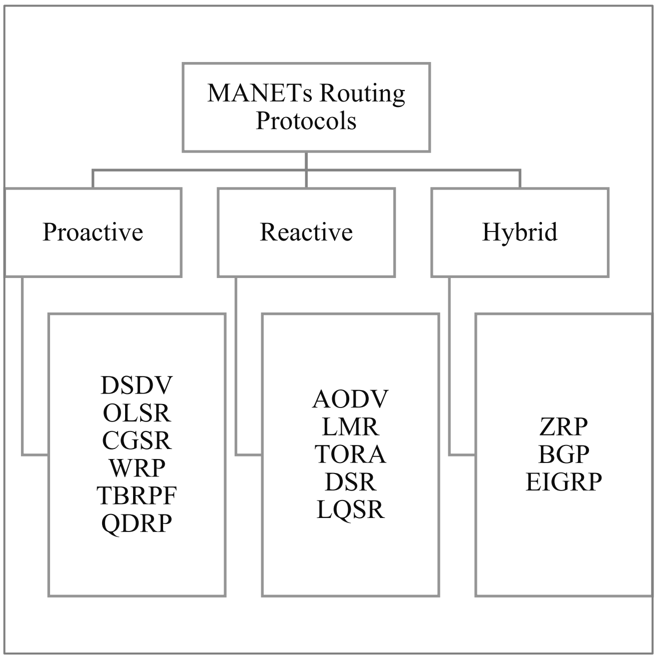

Figure 1. Classification of MANET routing protocols.

In proactive routing protocols, each node keeps a table of all the possible routes, and in case of any change in the network (i.e., a node moves in or out of the network), the table is updated at a predefined interval. That is why it is called a table-driven protocol. Proactive protocols aim mainly at efficiency. The nodes react effectively with changes, and they are ready every time to send data efficiently. The key issue is the overhead on the network to update changes at a fixed interval.

In reactive protocols, when a change takes place in the network, nothing happens unless a data exchange starts and discovers the change. Then, the update takes place; that is why it is called an on-demand routing protocol [4]. These protocols do not put a heavy overload on the network proactive routing protocol as it does not update regularly regardless of the need. That is why there is a latency every time during data exchange in case of having a change in the network. To solve the previous two issues, hybrid protocols were developed. In such a type, a mix of both algorithms is adopted. For instance, a proactive routing protocol is performed with close nodes so that routing tables are updated without creating a heavy overhead. At the same time, a reactive protocol algorithm is adopted for remote nodes to decrease the time taken to discover the routes with remote nodes.

2.4. Black Hole Attack

A black hole attack exploits the way the AODV routing protocol works. In the AODV routing protocol, every node in the network maintains a routing table in which it keeps all the information about the most efficient routes to particular destinations. When a node tries to send a packet to another node, it first checks whether or not it has the information needed in its own routing table. If it doesn't find it or if the required route is not active anymore, it initiates a discovery process. In this case, the node broadcasts a route request (RReq) to all its neighbors. If the receiving node is the destination node, it then sends back a route reply (RRep) containing the most updated sequence number, the broadcast ID, and hop count [18]. If not, it checks its own routing table to see if it has any routing entries to the destination, and it then compares the routing destination sequence. If the sequence number is less or equal to the one it has, then it sends out an RReq to its neighbors. If the sequence number if higher, then it means that it is a fresh route, and it updates its own table with it and sends back an RRep to the one it sent the RReq to [19]. A blackhole attack happens when a malicious node injects itself into a network and then claims that it has the shortest path to the destination [20]. Figure 2 shows an illustration of this process. Node "S" wants to reach node "D", so it sends out "RReq to the adjacent nodes. Node "M" injects itself and replies rapidly claiming that it has the best route. Once communications start, node "M" drops all the information sent through it.

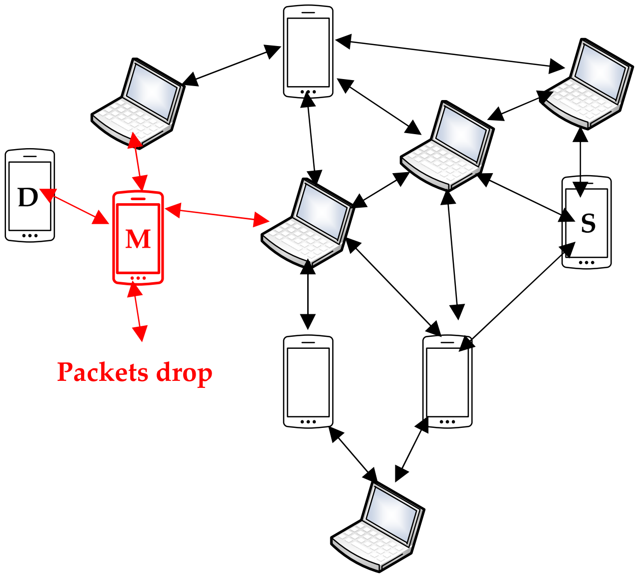

Figure 2. Malicious node (M) drops packets in a black hole attack.

A blackhole attack is one of the active attacks [21] when all the data passing by the malicious node are dropped. In such an attack, the malicious node broadcasts false information to its adjacent nodes that it has the shortest paths to the destination requests by the other nodes. The black hole attack affects the performance of the network, especially the throughput and the packet delivery ratio. There are two types of black holes, single and cooperative. A single attack happens when only one node is malicious. A cooperative attack happens when there is more than one malicious node in the same network, and they drop the packets together, which is more complex than a single black hole attack.

3. Related Work

Black hole attacks receive remarkable attention by many researchers as ad hoc networks gain more and more popularity and application in many fields. The common proposed solutions can be classified into four main approaches, as shown in Figure 3 as well as a comparison between the different methodologies as shown in Table 1.

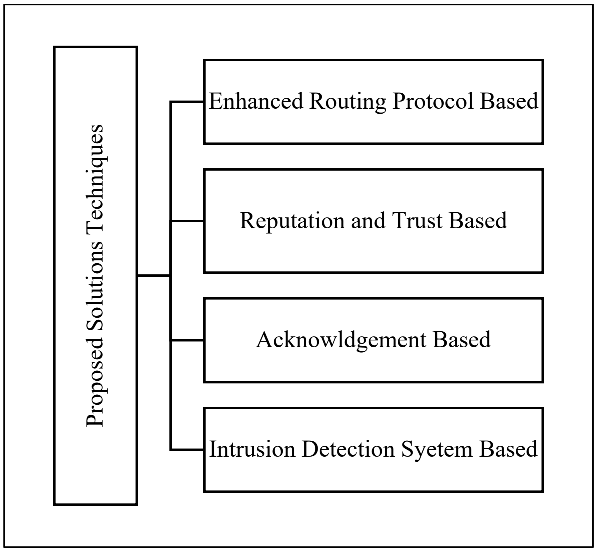
Proposed Solutions Techniques
Enhanced Routing Protocol Based
Reputation and Trust Based
Acknowldgement Based
Intrusion Detection Syetem Based

Figure 3. Classification of the mitigation techniques proposed by other researchers.

3.1. Enhanced Routing-Based Protocol

In this mitigation approach, the solution proposed by different researchers is adding some enhancements to the current protocols so that they become more capable of recognizing and stopping black hole attacks.

An enhanced routing protocol (MBDP-AODV) was proposed in [20]. This enhanced protocol uses some statistical features, such as standard deviation and mean. In normal conditions, the figures should grow in a reasonable manner. However, when there is an attack, the figures grow rapidly in a suspicious way. The proposed solution has three phases. The first phase is dynamic threshold calculation and suspicion. In this phase, a threshold value is calculated by the source node for the sequence number of the destination. The second phase is detection, where the suspect packet is detected, and the malicious node ID is sent out to all nodes in the network. The third phase is prevention, where the malicious node is prevented from participating in the network.

The authors in [7] proposed a technique that can discover black hole nodes by setting bait timers in all nodes. This baiting timer is set to a random number. When the baiting timer reaches the set time, it launches broadcasts with fake ID. The black hole is setup to reply to all requests regardless of their nature, so they reply to those baiting fake requests. Accordingly, the sending node discovers the black hole node and maintains it in a certain table. When the true requests are launched, malicious nodes are disregarded according to the information maintained in the malicious node table.

The authors in [22] suggested modifying the existing AODV protocol by adding a neighbor credit table to each node in the network. Whenever a data packet is sent from a neighbor or forwarded by a neighbor, the neighbor is assumed as a genuine node, and its credit value is increased in the table. Even the genuine node, when not participating, gets poor credit values. Then, when a node wants to use the neighbor node for transmitting a message, it first checks the value of the table. If the neighbor node does not have enough credit, then it is not trusted, and another hop should be used.

The key advantages of this technique are that it can detect the blackhole nodes during the route discovery phase rather than the data transmission phase and has the ability to detect and isolate smart black hole attacks. The drawbacks, on the other hand, are that it increases the overhead due to sending additional packets for the sake of identifying malicious nodes. This also leads to high network traffic.

3.2. Reputation- and Trust-Based System

A reputation system is a system that collects, analyzes, and distributes information about node behavior based on their previous interactions.

It was proposed in [23] that a selfish node can be removed from the network using selfish node removal; using a reputation model (SNRRM), the selfish node, according to the author, is detected using the node's current energy level and its communication ratio. If both the sender (S) and distention (D) fall under the communication range, only the (S) reputation value is checked. If (S) and (D) do not fall under the same communication range, then (S) sends a control packet to its neighbors and waits for replies. Then, the communication ratio is computed through the sent requests and received replies.

In [24], the authors proposed a node activity-based trust and reputation estimation (NA-TRE) solution in order to monitor the activities of the node, assess the status of the activities as normal (N) or malicious (M), and compute the trust and reputation estimation. According to the author, there are three states of nodes: a normal state (NS), where nodes provide the best efforts in cooperation and following routing requirements; a resource limitation state (RS), where nodes are not cooperating much due to low power consumption, being out of the communication range, or high congestion, etc.; and a malicious state (MS), where nodes disrupt the network by initiating the denial of service, path creation, packet delays, or other malicious activities that impact the network. Prediction is performed based on a "Semi-Markov probability decision process" to proactively distinguish different states.

In [25], the authors proposed a reputation and trust system against black hole attacks. This is based on the trust among nodes. In this case, if node A trusts B, then B can trust A. Likewise, if A trusts C and C trusts B, then A can trust B. To perform this solution, every node in the network is equipped with a reputation table. The table maintains data about the behavior of the neighbor node. The behavior is quantified and maintained. Therefore, after sending a message from the source to the destination, an acknowledgment should be sent from the destination confirming receipt of the message. This acknowledgment is sent back to all other nodes. The same way, in the case of a message not being received, then the trusted table is updated negatively.

Based trust is similar to the reputation system where every node has a register of the other nodes based on their interactions. However, in based trust, while the node is forwarding a packet, it checks the trust values of the adjacent nodes and based on this, it chooses the higher trust value.

Node activity-based trust and reputation estimation (NA-TRE) was proposed by [26] in order to ensure both the security and quality of service based on the trust in the node carrying the data, taking into account activity changes, packet forwarding, or dropping. The key advantage of this technique is that it detects the blackhole node during route discovery phase rather than during data transmission phase, with the ability to detect and isolate smart black hole attacks. The main drawback of is that it increases the overhead due to sending additional packets for the sake of identifying malicious nodes. This also leads to high network traffic.

The key advantages of this technique are that the reputation system is not only classifying nodes into good or bad but also providing more information about how cooperative the nodes are, and it provides the node trust values when packets are forwarded and supports QOS. The main drawbacks are that it is a reactive system and takes decisions based on historical data, its reputation tables can be falsified, and it is vulnerable to denial-of-service attacks.

3.3. *Acknowledgment-Based Approach*

An acknowledgement-based approach aims at mitigating the black hole attacks using a mechanism of creating acknowledgment packets through source or intermediate nodes. The acknowledgment packets are sent prior to the route determination. The nodes that refrain from replying are either selfish nodes, nodes with insufficient energy, or malicious nodes.

In [27], the authors proposed an enhanced routing protocol ad hoc on-demand multipath secure routing (AOMSR) based on acknowledgment. According to this routing protocol, a source node needs to keep multiple paths from the source to the destination based on the maximum delay in receiving the data.

The authors of [28] proposed an extension of the acknowledgment-based approach taking into account the selection of the energy-efficient intermediate nodes that are non-congested for communication, session key agreements, a counter base end to end the cycle of acknowledgment, and the authentication of Ack packets by message digest.

The advantage of this technique is that it has the ability to differentiate between the malicious nodes and the selfish nodes and those with insufficient energy, while its drawback is the increasing network load due to congesting the network with additional acknowledgment packets.

3.4. Intrusion Detection-Based System

An intrusion detection system works as an alarm system. When discovering an attack, it issues a warning to the system [29]. The IDS system contains an audit register for keeping all the data for analysis and provides an output based on which decisions are taken.

The solution proposed by the authors in [30] was IDS (DPAA-AODV). This protocol works in two phases: an online phase and offline phase. During the offline phase, one of the ReliefF models is used in order to find a reliable feature of the black hole detection dataset (BDD). The aim of this is to make the selection more accurate. In the online mode, the learnt features from the previous mode are selected. If the results show that the threshold was exceeded, then it might be a malicious node.

In [31], host-based IDS was used where information regarding normal behavior nodes was collected. They used the GloMoSim simulator to simulate the normal malicious behavior of nodes. Then, a machine learning tool (Weka 3.7.11) was used to apply the feature selection, which led to identifying the malicious node. This was achieved by applying six features: the number of RREQ sent, the number of RReps forwarded, the number of high destination sequence numbers, the number of low count of hops to destination, the number of nodes acting as the source, and the number of nodes acting as the destination.

In [32], an IDS was proposed in order to identify malicious nodes. A three-step mechanism for analyzing the solution was applied; the steps are network simulation, data collection, model training, and data testing. The simulation was performed through NS2 for 25 nodes. Then, a CSV was collected from the output for use in the analysis. Afterwards, four algorithms were used for model training and testing: the support vector machine, random forest classifier, decision tree classifier, and logistic regression.

The authors in [18] proposed a solution in two phases: the feature selection phase and the modified AODV phase. In the first phase, the features of the black hole are identified based on the behavior of the nodes, for instance, based how the nodes handle RReps and RREQ. In the second phase, the AODV protocol is enhanced through putting the learnt data in each and every node in order to be able to detect any black hole node and then avoid it while transmitting data.

In [23], an enhanced routing protocol SAODV was proposed. This was supposed to be a securer version of the AODV routing protocol. This enhanced routing protocol is designed specifically for securing MANETs from black hole attacks. It has a similarity with the AODV routing protocol as they both have a discovery process for nodes to know the best route. However, in SAODV, a verification process is added. This verification process tests the adjacent node by exchanging random numbers. This process is initiated every time the adjacent node replies with an RRep in order to ensure that the adjacent node is trusted.

In [33], an IDS which relies on classifiers such as decision trees, KNNs, SVMs, and neural networks was proposed. A decision tree involves nodes and edges together with leaves. This works by simply generating rules. Following these rules, the classification of records is sorted into various classes; the classes decided are malicious and non-malicious. The KNN works by saving the training data taking into consideration the distance metric of other nodes, then relating the classes to which the dataset belongs to. SVM is mainly used for pattern detection problems and can also be used for classification. Finally, a neural network is used for processing and training the records.

Table 1. Mitigation techniques used by other researchers to tackle black hole attacks.

Mitigation Approach	Description	Technique	Ref.	Advantages	Disadvantages	Simulator	Routing Protocol
Acknowledgment-based	An acknowledgement-based approach aims to mitigate black hole attacks using a mechanism of creating acknowledgment packets through source or intermediate nodes. The acknowledgment packets are sent prior to the route determination. The nodes that refrain from replying are either selfish nodes, nodes with insufficient energy, or malicious nodes.	Ack.-based	[32]	Have the ability to differentiate between malicious nodes and selfish nodes and nodes with insufficient energy.	Increases network load due to congesting the network with additional acknowledgment packets.	NS2	AODV
		Counter acknowledgment-based	[34]				
Intrusion detection system-based	An intrusion detection system works as an alarm system. When discovering an attack, it issues a warning to the system. The IDS system contains an audit register for keeping all the data for analysis and provides an output based on which decisions are taken.	ReliefF classification algorithm	[23]	The classification algorithm is not only used for black hole attacks but is also effective in detecting grey hole attacks.	Nodes have to be in a promiscuous mode which is not acceptable to the nodes. The system itself can be attacked.	NS2.35	AODV
		Feature selection for black hole	[24]	Anomaly-based has high accuracy in discovering black hole attacks.		GloMoSim 2.03	
		Machine learning algorithm	[25]	Random forest classifier provided high accuracy and detection rates.		NS2	
		Anomaly-based IDS	[26]	Anomaly-based shows high accuracy in discovering black hole attacks.		NS-2.35	
Enhanced routing protocol	Enhances current protocols so that they become more capable of recognizing and stopping black hole attacks.	Dynamic threshold	[20]	Detects the blackhole node during route discovery phase rather than data transmission phase. Ability to detect and isolate smart black hole attacks.	Increases overhead due to sending additional packets for the sake of identifying malicious nodes. This also leads to high network traffic.	NS-2.35	AODV
		Timer-based baited technique	[7]			NS-2.35	
		Classification algorithm	[18]			GloMoSim	
		Neighbor credit value	[22]			NS2	
Reputation- and trust-based	A reputation system is a system that collects, analyzes, and distributes information about nodes behavior based on their previous interactions. Based trust is similar to the reputation system where every node has a register of the other nodes based on their interactions. However, in based trust, while the node is forwarding a packet, it checks the trust values of the adjacent nodes, and based on this, it chooses the higher trust value.	Black hole protected	[27]			NS2	AODV
		Selfishness detect-and-isolate (SDI)	[28]			NS-2.35	
		Lightweight reputation-based	[29]			Java	OLSR
		Trust- and reputation-based	[30]			GloMoSim	AODV
		Collaborative computing trust model	[31]			Java	

The advantages of this technique are that the classification algorithm is not only used for black hole attacks but is also effective also in detecting grey hole attacks. The anomaly-based approach shows high accuracy in discovering black hole attacks. The random forest classifier provides high accuracy and detection rates. The drawbacks, on the other hand, are that nodes have to be in a promiscuous mode which is not acceptable to nodes, and the system itself can be attacked.

4. Methodology

The methodology used in this paper is based on four steps depicted in Figure 4. The first step is generating the data that will be used for machine learning analysis. This is performed through an OMNET++ simulator in order to generate traffic data that is very similar to a real traffic while having a black hole attack. Then, the generated data are collected in a certain format that can be further analyzed later on. There are some common features or characteristics of the traffic records that are collected. These behaviors are analyzed via a support vector machine (SVM) in order to classify the traffic into normal and malicious traffic. Based on this analysis, malicious nodes can be identified and blocked.

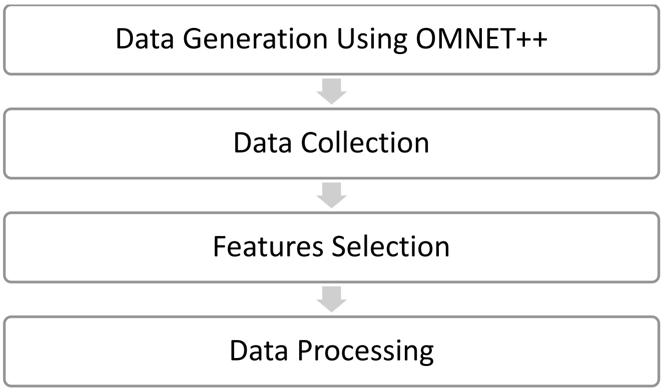

Figure 4. Methodology used in the paper to mitigate a black hole attack.

4.1. Proposed Solution

In MANETs, all nodes should be cooperative. In other words, they should rely on each other to perform the missing functions by the lack of infrastructure. Otherwise, the whole network will not work properly. A blackhole is one of the attacks that targets MANETs to corrupt them. Such attacks can be detected by studying the behavior of those malicious nodes in a network. They have some common behavioral characteristics that can be summarized as follows:

- They increase their transmission power so that they can respond to most of the RREQ.
- They almost never send any RREQ.
- They always unicast and almost never broadcast.

Our solution is to develop a lightweight anomaly detection system (LADS) that can detect malicious nodes based on the behavioral characteristics mentioned above and then label those nodes as malicious in order to isolate them from the network.

4.2. Data Generation

Omnet++ 5.7 is used to simulate both the behavior of normal and malicious nodes. The simulation is performed on 7 nodes as shown in Figure 5. One of them is stationary and functioning as a sender (Node 1). This node is omitted from the graphs as it is not relevant to show the behavior of the mobile nodes, which are the core of the simulation. Two scenarios are performed in this simulation. Scenario one simulates that all nodes are cooperative and no malicious node exists. All the nodes accordingly are behaving normally. In the second scenario, Node 6 is setup as a malicious node, and the rest of nodes continue doing their functions normally. The radio transmission power of all nodes is set to 1 mW.

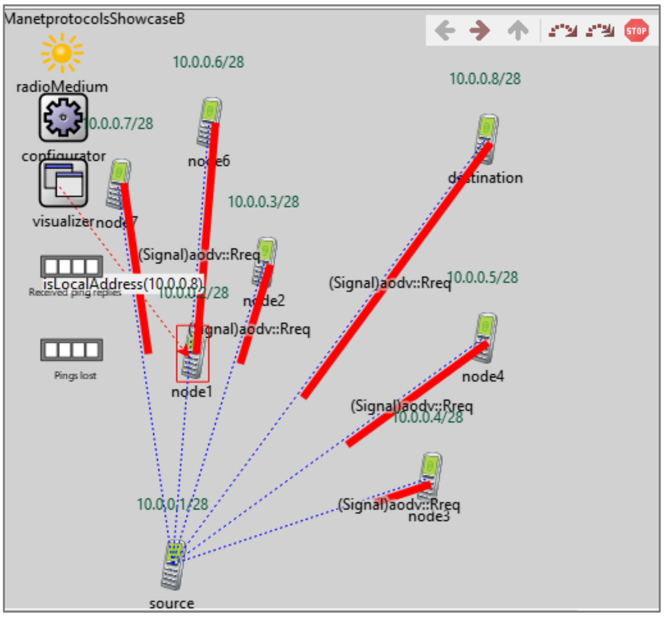

Figure 5. A snapshot from OMNET++ while a node sends packets (RReq) to adjacent nodes.

In this scenario as shown in Table 2, the radio transmission power of Node 6 is set to 5 mW. By increasing its radio transmission power, Node 6 is able to deceive all its neighbors that it is the most adjacent one to them. Accordingly, it receives as many requests as possible. In other words, when a node searches for the best routes and sends a RReq, the attacking node will appear as an adjacent node and will be the first to reply with an RRep as soon as possible.

Table 2. The parameter configuration used to generate the dataset in OMNET++ simulator.

Simulation Environment Parameters	
Simulation used	OMNeT++ 5.7
Number of nodes	7 nodes
Routing protocol	AODV
Total space	400 m
Transmission power (All nodes)	1 mW
Transmission power (Node 6)	5 mW
Transmission speed	24 Mbps
Mobility speed	25 mps
Transport protocol	UDP

4.3. Data Collection

The results were collected from the first scenario as depicted in Table 3, which assumed that all the nodes are cooperative and behaving normally as well as the second scenario, which assumed that one of the nodes acted as a malicious node. The results of the two scenarios were then fed into the detection system for analysis. The dataset contained the most critical data that resulted from the simulation run in OMNET++. It contained the AODV request, the transmission power of the nodes while sending their packets, and the data transfer type (broadcast/unicast).

Table 3. The parameter configuration used to generate the dataset in OMNET++ simulator.

Dataset Generated from OMNET++	
Total number of records	8225
Malicious traffic	2954
Normal traffic	5271

4.4. Feature Selection

As mentioned in Section 5, there are 3 factors featuring the malicious behavior of black holes in this research as depicted in Figure 6. The first feature is that malicious nodes increase their power to deceive the other nodes that it is the most adjacent one to them. The second one is that malicious nodes almost never send any RReqs. Rather, they reply to as many requests as possible. The last but not least feature is that they always unicast and almost never broadcast.

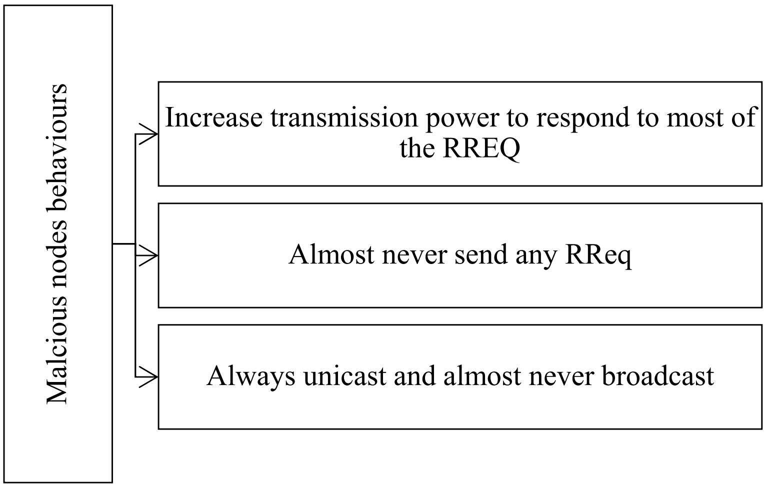
Malcious nodes behaviours
Increase transmission power to respond to most of the RREQ
Almost never send any RReq
Always unicast and almost never broadcast

Figure 6. Feature selection based on malicious node behaviors.

4.5. Data Processing

The data extracted from the OMNET++ simulator consist of eight columns. Five out of the eight columns will be used for analysis, while three of them will be discarded as they will no add value to the analysis. The five values are as below:

- Hops: This column helps the research in two ways. First, it reveals the direction of the transmission as well as the node that is used as a hop, or in other words, the node that performed the routing function.
- Transmission type: This field provides the value of the transmission power. It reveals two important values: whether it is a route request (RReq) or route reply (RRep). This is one of the important fields that is used to identify the nodes that are not sending any RReqs. This is one of the features with other ones that reveal misbehavior.
- Node name: This field contains the node name that transmits the data. It is used to identify each node and recognize the node that misbehaves.
- Transfer type: This field contains the value of the transfer type and whether it is broadcast or unicast. The importance of this is that it is used to show the nodes that are not broadcasting. These nodes are the suspicious ones that are expected with other features to misbehave.
- Transmission power: This field shows the transmission power used to send the data. It is also important to show if there is any manipulation in the power used for communication because usually a black hole attack increases the power of the node.
- The traffic then will be fed into system as shown in Figure 7 where it can be processed and based on the feature selection the malicious nodes can be identified using SVM machine learning algorithm.

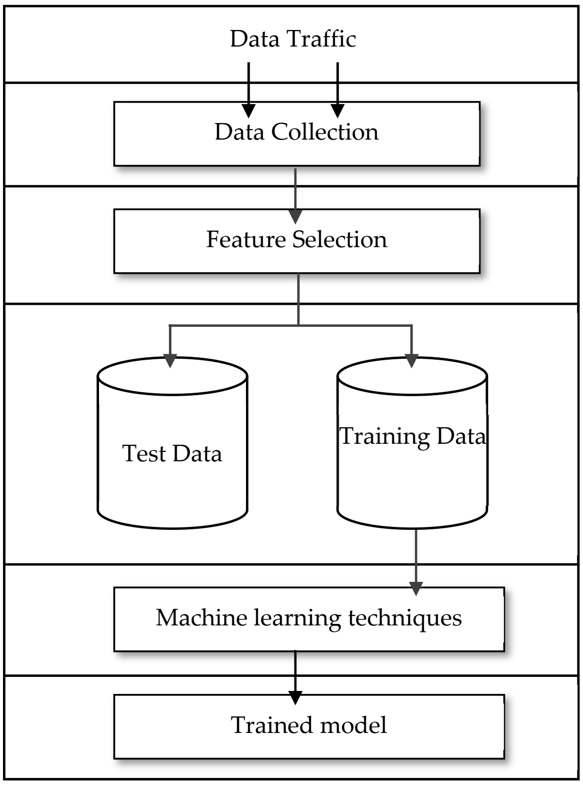

Figure 7. Intrusion detection system methodology.

4.6. *Using Machine Learning (SVM)*

A support vector machine (SVM) is a well-known machine learning algorithm that is widely used for pattern classification problems. As depicted in Figure 8, the model consists of three lines. The line in the middle is called the optimal classification line, and the other two lines are called the lines of the margin. These lines are used to classify patterns into two classes [35–37]. In our case, this model is used for separating the normal behaving nodes from the malicious ones based on the analyzed traffic:

$$D = \{(x_i, y_i)\}_{i=1}^{n}, \tag{1}$$

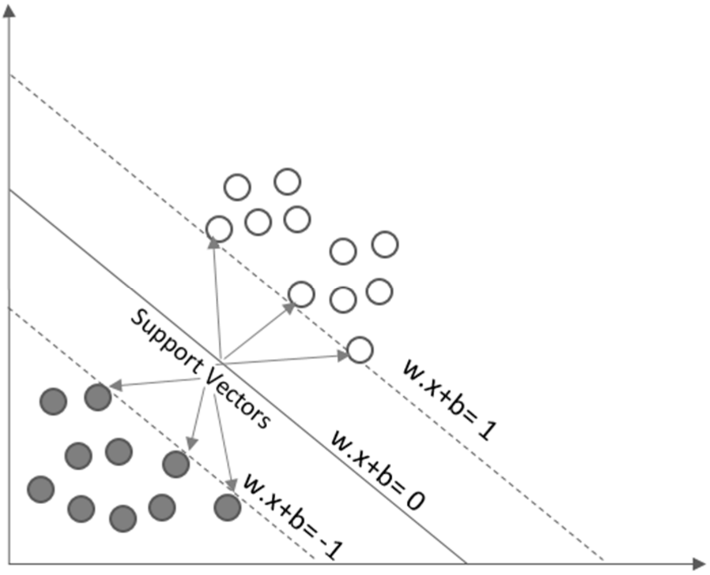

Figure 8. Support vector machine (SVM).

The first class is positive class (+1), and the second class is the negative one (-1). In the collected dataset, n represents the sample size, x_i represents the vector characteristic of i^n, and y_i is the value of -1 or +1. Characteristics cannot be identical, and there is room for some deviation, but they can be accurately classified. There is a margin defined that can give some room for acceptable deviation. As mentioned previously, the line in the middle is called the optimal classification line, where the sum of w (weighted vector) and b (the bias) is equal to zero, as depicted in Equation (2):

$$w.x + b = 0 \tag{2}$$

As the vectors' characteristics are not identical, there are two other lines with some margin. These two lines are parallel to the optimal classification line with the marginal bias.

These two marginal lines form what is called the hyperplane. The points above the hyperplane are captured as the first class, as mentioned in Equation (3):

$$w.x + b \geq 1 \tag{3}$$

Similarly, the points below the hyperplane are captured as the second class, as described in Equation (4):

$$w.x + b \leq 1 \tag{4}$$

These two classes are referred to later on as malicious and normal vectors.

The main disadvantages of a SVM is that it does not perform well with big datasets, when there is too much noise, and when the number of features exceed the number of trained data samples. These drawbacks of a SVM did not impact the quality of our work as our dataset was not very big, and the features were clear.

4.7. Results

The simulator was configured to examine seven nodes interacting with one another. A rogue node that imitated a black hole attack was set up as one of the nodes. Seven minutes were allocated for it. A total of 13,336 records produced by the simulation were among the records the system examined. The algorithm eventually succeeded in categorizing the records into two groups: legitimate records and harmful records. A total of 10,381 of the 13,336 records were classified as normal, while 2954 were classified as malicious. This was supported by the following three main aspects:

- A change in the transmission power. As previously explained, the malicious node changes its transmission power in order to appear adjacent to the RReq sender.
- A remarkable increase in responding to as many RReqs as possible.
- Always sending unicast, and almost never sending broadcast.

In our simulation, the radio transmission power of Node 6 increased to 5 mW, while the rest of the nodes were normally set to the default of 1 mW. The second feature is that the black hole attacker replied to as many requests as possible while keeping almost salient in terms of route requests (RReqs). The last but not least feature is that the black hole attacker almost never broadcast, and all of its communication was in the form of unicast. As shown in Figure 9, the graph shows the normal behavior of six nodes. All of them send both RReqs and RReps in a normal way. In other words, the number of RReqs to the number of RReps is in a relative proportion in all nodes.

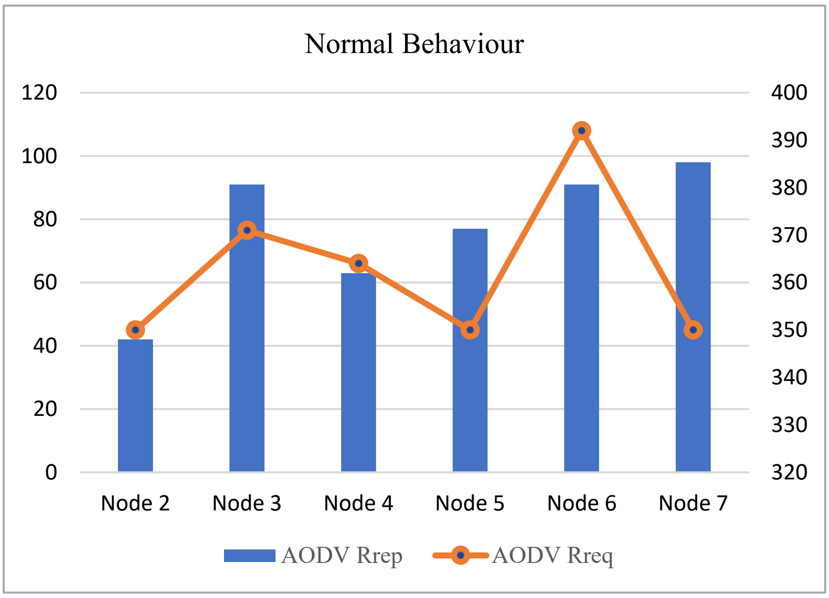

Figure 9. Results of the simulator in the absence of a black hole attack.

Figure 10 shows that there is a huge gap between the number of RReps sent by Node 6 to the rest of the nodes. The reason behind this is that the transmission power of Node 6 increased to 5 mW, while the transmission power of the rest of the nodes is 1 mW. In addition, the number of RReqs sent by Node 6 is almost zero, while it is high with the rest of the nodes and close to each other.

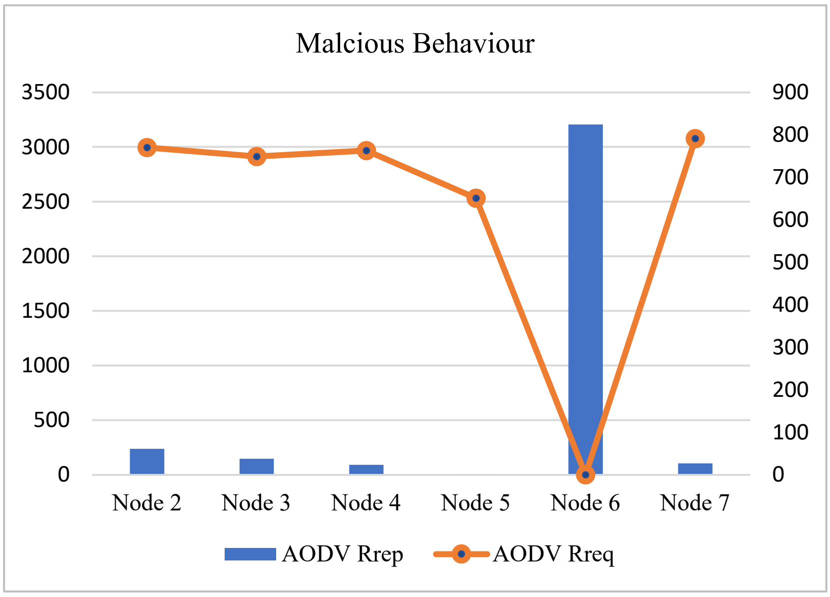

Figure 10. Results of the simulator in the presence of a black hole attack.

The machine learning algorithm identified the malicious records clearly based on the features. The system showed a high accuracy in discovering the malicious nodes through analyzing its behaviors, based on the features mentioned above. The detection accuracy of our solution (LDAS) reached around 99%. When comparing the results of LDAS to other proposed solutions, such as alleviating blackhole identification and prevention (ABIP) that showed a 97% accuracy level and another solution called detection and presentation of a black hole attack (DPBHA), our solution showed a better performance in detecting malicious nodes, as shown in Figure 11.

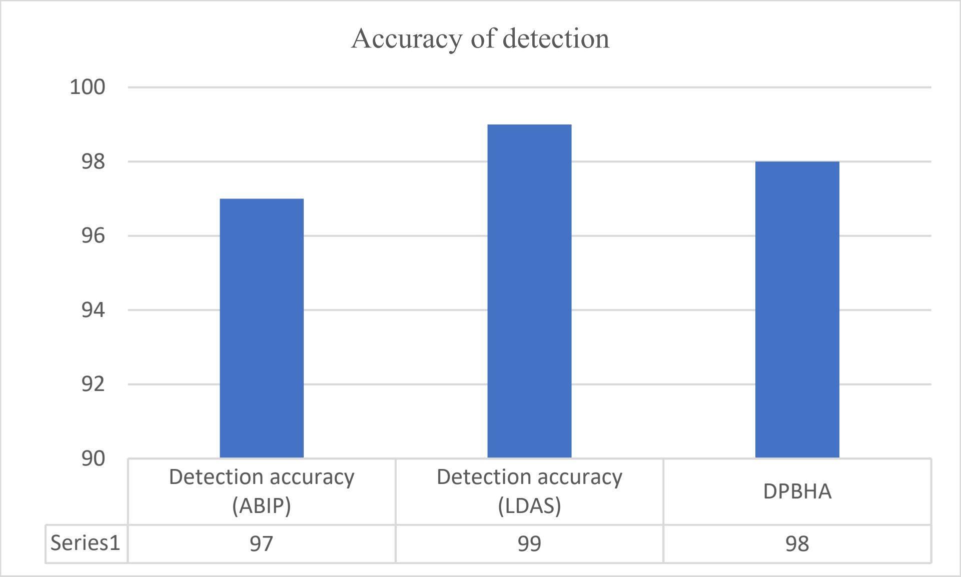

Figure 11. Intrusion detection system methodology.

5. Conclusions and Future Work

MANETs are networks that are infrastructure-less; rather, they depend on cooperation between nodes by providing both features of being clients and routers. Such networks lack resources and many security features. Hence, they are more fragile than standard infrastructure networks. In this paper, we discussed the different applications of MANETs, their security challenges, and one of the most common attacks, which are black hole attacks. We surveyed, categorized, and compared the solutions proposed in the literature to mitigate black hole attacks. Then, a solution for discovering and avoiding such attacks was proposed using machine learning. In order to examine black hole attacks thoroughly, we used OMNET++ to simulate a malicious node in a MANET network and generated a dataset that we used for analysis and to study the behavior or malicious node acting as a black hole attack. We focused on three key features for identifying black hole attacks: transmission power, the number of responses in relation to the rest of nodes, and the communication method (whether it is unicast or broadcast). These three features were thoroughly examined using machine learning. The limitation of this research is that the simulation was performed on seven nodes only, and the attacker was only one node. In the future, a bigger network can be set up for better analysis, and the attackers can be more than one node. This will allow a deeper analysis of black hole attacks in a bigger network as well as a network traffic analysis with the presence of more than one attacking node.

Author Contributions: Methodology, A.A.; Validation, M.S.E., A.D.J. and M.A.A.; Formal analysis, A.D.J. and M.A.A.; Investigation, M.A.A.; Data curation, A.A.; Writing—original draft, A.A.; Writing—review & editing, M.S.E.; Supervision, A.D.J.; Project administration, M.S.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by the University College Dublin, School of Computer Science.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hassan, M.H.; Jubair, M.A.; Mostafa, S.; Mustapha, A. Mobile ad-hoc network routing protocols of time-critical events for search and rescue missions. *Bull. Electr. Eng. Inform.* **2021**, *10*, 192–199. [CrossRef]
2. Rani, P.; Kavita; Verma, S.; Rawat, D.B.; Dash, S. Mitigation of black hole attacks using firefly and artificial neural network. *Neural Comput. Appl.* **2022**, *34*, 15101–15111. [CrossRef]

3. Prasad, S.K.; Sharma, T. Performance comparison of multipath routing protocols for mobile ad hoc network. *Int. J. Syst. Control Commun.* **2022**, *13*, 82. [CrossRef]
4. Shrivastava, P.K.; Vishwamitra, L. Comparative analysis of proactive and reactive routing protocols in VANET environment. *Meas. Sens.* **2021**, *16*, 100051. [CrossRef]
5. Mukti, F.S.; Lorenzo, J.E.; Zuhdianto, R.; Junikhah, A.; Soetedjo, A.; Krismanto, A.U. A Comprehensive Performance Evaluation of Proactive, Reactive and Hybrid Routing in Wireless Sensor Network for Real Time Monitoring System. In Proceedings of the 2021 International Conference on Computer Science and Engineering (IC2SE), Padang, Indonesia, 16 November 2021; Volume 1, pp. 1–6. [CrossRef]
6. Shantaf, A.M.; Kurnaz, S.; Mohammed, A.H. Performance Evaluation of Three Mobile Ad-hoc Network Routing Protocols in Different Environments. In Proceedings of the 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 26–28 June 2020; pp. 1–6. [CrossRef]
7. Yasin, A.; Abu Zant, M. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 9812135. [CrossRef]
8. Ramphull, D.; Mungur, A.; Armoogum, S.; Pudaruth, S. A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. In Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 6–8 May 2021.
9. Kanellopoulos, D. Congestion control for MANETs: An overview. *ICT Express* **2019**, *5*, 77–83. [CrossRef]
10. Kanellopoulos, D.; Sharma, V.K. Survey on Power-Aware Optimization Solutions for MANETs. *Electronics* **2020**, *9*, 1129. [CrossRef]
11. Anibrika, B.S.K.; Asante, M.; Hayfron-Aquash, B.; Ghann, P. A Survey of Modern Ant Colony Optimization Algorithms for MANET: Routing Challenges, Perpectives and Paradigms. *Int. J. Eng. Res. Technol.* **2020**, *9*, 952–959.
12. Yadav, N.; Chung, U. Secure Routing in MANET: A Review. In Proceedings of the 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 14–16 January 2019.
13. Justin, J.; Alwar, R.; Sundarraj, S. Comprehensive Learning on Characteristics, Applications, Issues and Limitations of Manets. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 2278–3075.
14. Tu, J.; Tian, D.; Wang, Y. An active-routing authentication scheme in MANET. *IEEE Access* **2021**, *9*, 34276–34286. [CrossRef]
15. Sivapriya, N.; Mohandas, R. Analysis on Essential Challenges and Attacks on MANET Security Appraisal. *J. Algebraic Stat.* **2022**, *13*, 2578–2589.
16. Hamdi, M.M.; Audah, L.; Rashid, S.A.; Mohammed, A.H.; Alani, S.; Mustafa, A.S. A Review of Applications, Characteristics and Challenges in Vehicular Ad Hoc Networks (VANETs). In Proceedings of the 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 26–28 June 2020; pp. 1–7. [CrossRef]
17. Yogarayan, S. Wireless Ad Hoc Network of MANET, VANET, FANET and SANET: A Review. *J. Telecommun. Electron. Comput. Eng.* **2021**, *13*, 13–18.
18. Al-Refai, H. An Enhanced AODV Protocol Against Black Hole Attack Based on Classification Algorithm. *Int. J. Open Probl. Compt.* **2020**, *13*. Available online: http://www.ijopcm.org/Vol/2020/2.5.pdf (accessed on 15 February 2023).
19. Tseng, F.-H.; Chiang, H.-P.; Chao, H.-C. Black hole along with other attacks in MANETs: A survey. *J. Inf. Proc. Syst.* **2018**, *14*, 56–78.
20. Gurung, S.; Chauhan, S. A dynamic threshold based approach for mitigating black-hole attack in MANET. *Wirel. Netw.* **2017**, *24*, 2957–2971. [CrossRef]
21. Sarao, P. Performance Analysis of MANET under Security Attacks. *J. Commun.* **2022**, *17*, 2374–4367. [CrossRef]
22. Abirami, K.R.; Sumithra, M.G. Preventing the impact of selfish behavior under MANET using Neighbor Credit Value based AODV routing algorithm. *Sadhana* **2018**, *43*, 60. [CrossRef]
23. El-Semary, A.M.; Diab, H. BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map. *IEEE Access* **2019**, *7*, 95197–95211. [CrossRef]
24. Ponnusamy, M.; Senthilkumar, A.; Manikandan, R. Detection of selfish nodes through reputation model in mobile adhoc network-MANET. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 2404–2410.
25. Hammamouche, A.; Omar, M.; Djebari, N.; Tari, A. Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. *J. Inf. Secur. Appl.* **2018**, *43*, 12–20. [CrossRef]
26. Raghavendar, R.L.; Reddy, C.R.K. Node activity based trust and reputation estimation approach for secure and QoS routing in MANET. *Int. J. Electr. Comput. Eng.* **2019**, *6*, 5340.
27. Dave, D.; Dave, P. An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET. In Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India, 24–27 September 2014; pp. 1690–1696. [CrossRef]
28. Hussain, M.; Duraisamy, B. Preventing Malicious Packet Drops in MANETs by Counter Based Authenticated Acknowledgement. *ISI* **2020**, *25*, 173–181. [CrossRef]
29. Preet, M.P.; Mishra, R.; Agrawal, S. Research Technology Intrusion Detection System For Manet. *Int. J. Eng. Sci. Res. Technol.* **2020**, *6*, 402–406. [CrossRef]
30. Albalas, F.; Yaseen, M.B.; Nassar, A. Detecting black hole attacks in MANET using relieff classification algorithm. *Int. Res. J. Eng. Technol.* **2019**, *22*, 1–6. [CrossRef]
31. Yassein, M.B.; Khamayseh, Y.; AbuJazoh, M. Feature Selection for Black Hole Attacks. *J. Univers. Comput. Sci.* **2016**, *22*, 521–536.

32. Katakam, M.Y.; Adilakshmi, M. Black hole Attack Detection Using Machine Learning Algorithms in MA-NET-Performance Comparision. *Int. Res. J. Eng. Technol.* **2020**, *7*, 6047–6051.
33. Zhang, R.; Meng, X.; Shou, D.; Liang, W. An algorithm for determining data forwarding strategy based on rec-ommended trust value in MANET. *Int. J. Embed. Syst.* **2002**, *12*, 544–553. [CrossRef]
34. Nausheen, A.I.; Upadhyay, A. A Survey on MANETs: Entrusted Security Challenges. *Int. J. Future Gener. Commun. Netw.* **2020**, *13*, 48–58.
35. Ibrahim, I.; Abdulazeez, A. The Role of Machine Learning Algorithms for Diagnosing Diseases. *J. Appl. Sci. Technol. Trends* **2021**, *2*, 10–19. [CrossRef]
36. Kowsigan, M.; Rajeshkumar, J.; Baranidharan, B.; Prasath, N.; Nalini, S.; Venkatachalam, K. A novel intrusion detection system to alleviate the black hole attacks to improve the security and performance of the MANET. *Wirel. Pers. Commun.* **2022**, *127*, 3. [CrossRef]
37. Malik, A.; Khan, M.Z.; Faisal, M.; Khan, F.; Seo, J.T. An efficient dynamic solution for the detection and prevention of black hole attack in vanets. *Sensors* **2022**, *22*, 1897. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.