International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1015-1028
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Mobile Ad Hoc Network Security: An Anomaly Detection Approach Using Support Vector Machine for Black-Hole Attack Detection

Ashraf Abdelhamid Abdallah[1], Mahmoud S. El Sayed Abdallah[2], Heba Aslan[1], Marianne A. Azer[1,3], Young-Im Cho[4*], Mohamed S. Abdallah[5,6]

[1] Faculty of Information Technology and Computer Science, Nile University, Giza 12588, Egypt
[2] School of Computer Science, University College Dublin, Belfield, Dublin D04 V1w8, Ireland
[3] National Telecommunications Institute, Cairo 3650108, Egypt
[4] Department of Computer Engineering, Gachon University, Seongnam 13415, Korea
[5] Informatics Department, Electronics Research Institute (ERI), Cairo 11843, Egypt
[6] AI Lab, DeltaX Co., Ltd., Seoul 04522, Korea

Corresponding Author Email: yicho@gachon.ac.kr

https://doi.org/10.18280/ijsse.140401

Received: 17 April 2024
Revised: 22 June 2024
Accepted: 9 July 2024
Available online: 30 August 2024

Keywords:
ad hoc networks, blackhole attacks, MANETs, routing protocols, support vector machine, SVM

ABSTRACT

In the contemporary environment, mobile ad hoc networks (MANETs) have become necessary. They are absolutely vital in a variety of situations, where setting up a network quickly is required; however, this is infeasible due to low resources. Ad hoc networks have many applications: education, on the front lines of battle, rescue missions, etc. These networks are distinguished by high mobility and constrained computing, storage, and energy capabilities. The main aim of this research is to create a method for identifying blackhole attacks through anomaly detection techniques utilizing Support Vector Machines (SVM). Our detection system looks at node activity to scan network traffic for irregularities. In blackhole scenarios, the attackers exhibit distinct behavioral characteristics that distinguish them from other nodes. This can be efficiently detected by the proposed SVM-based detection system. The proposed detection system is designed to analyze network traffic and identify anomalies by examining node behaviors. Specifically, in the context of blackhole threats, it distinguishes the attackers from normal nodes based on behavioral characteristics. Using this approach, the system effectively detects blackhole attacks. The results demonstrate a very high level of accuracy in detecting blackhole attacks, confirming its efficacy in ensuring the security of mobile ad hoc networks (MANETs) by identifying and isolating malicious nodes. This solution is particularly valuable in scenarios like military operations and disaster management where a reliable communication system is crucial. Furthermore, the proposed detection method, ADS-SVM, was compared to two other methods (J48 classifier and NB classifier) from different researchers. The results indicate that ADS-SVM outperforms the other methods with a detection accuracy of 99.96%, surpassing the 99.2% achieved by J48 classifier and the 96.5% achieved by NB classifier. The results indicate that ADS-SVM is a highly efficient approach for identifying blackhole attacks in MANETs, potentially offering superior accuracy compared to other related methods.

1. INTRODUCTION

Wireless networks can be categorized into the following categories: infrastructure-based networks and infrastructure-less networks [1]. In infrastructure networks, administrators set up wireless equipment so that it may connect to fixed base hardware and get services like security, storage, and routing. In contrast, infrastructure-less networks, such as mobile ad hoc networks (MANETs), have no fixed base infrastructure; instead, nodes in them are self-configured and rely on one another. MANETs are preconfigured to run independently and can be built without the assistance of administrators or traditional base infrastructure. In other words, each node performs a range of functions [2].

Due to these limitations, MANETs face several unique difficulties that set them apart from traditional infrastructure networks. The difficulties with security and routing are two important considerations when developing MANETs [3]. Regarding security issues, MANETs typically lack the essential equipment to undertake security operations utilizing tools like firewalls, routers, IDS, IPS, and other similar devices. Nodes need a routing function in order to efficiently communicate with one another, which presents routing issues. The primary objective of the routing function is to ensure that messages from the sender follow the shortest path to their destination. Traditional infrastructure-based routing protocols are ineffective in MANETs for several reasons. Lack the infrastructure necessary to support routers, which prevents

these networks from performing routing functions is one of these reasons. Instead, almost every network node fulfills this function. Consequently, new and improved routing protocols were developed specifically for MANETs.

Proactive (table driven) and reactive (on demand) routing protocols are the two main categories of MANETs [4, 5]. A table-driven protocol automatically updates routing information whenever a change takes place. The on-demand routing system, in contrast, only obtains routing information when it is necessary [6]. A prominent on-demand routing protocol is the Ad hoc On-Demand Distance Vector (AODV). It outperforms other on-demand routing technologies [7, 8]. However, due to constraints in terms of lack of infrastructure, physical security, and limited resources, MANETs are open to a number of attacks. One of these threats is the blackhole attack which is an important exploit that significantly influences network performance. In this attack, the shortest path to the target is through the node of the attacker who drops the packets it has received. It consequently has a big impact on the network delivery ratio.

Over the past two decades, researchers began developing specialized techniques for anomaly detection in MANETs. Initial methods employed statistical and machine learning algorithms to identify deviations from normal behavior, which could indicate security threats such as intrusions or attacks. These early approaches primarily focused on individual node behavior but soon expanded to consider network-wide patterns, leveraging the collaborative nature of MANETs. Advances in computational power and machine learning have significantly influenced anomaly detection techniques in MANETs. However, anomaly detection in MANETs remains an active area of research. Challenges such as resource constraints, high false positive rates, and the need for real-time detection continue to drive innovation. As MANETs become more prevalent in critical applications, the importance of effective anomaly detection mechanisms will only increase, ensuring these networks remain secure and reliable.

The following is the paper's main contribution:

• Classifying the blackhole attack mitigation categories and identifying the pros and cons of each to help network administrators, researchers, and security professionals in making informed decisions when selecting the most appropriate blackhole attack mitigation approach for their specific MANET scenarios.

• Making a dataset for OMNET++'s analysis of blackhole attacks, which will allow us to closely investigate the behavior of the research nodes and traffic during an attack.

• Creating a method for detecting malicious nodes.

The subsequent sections of this paper are structured as follows: The background information on MANETs is presented in Section 2. Relevant studies and initiatives conducted by other researchers in this field are examined in Section 3. The methodology of our proposed solution is outlined in Section 4. Finally, Section 5 concludes with suggestions for future work.

2. BACKGROUND

There are many ways that mobile ad hoc networks differ from traditional networks. This section discusses MANETs' characteristics, security concerns, routing protocols, and common attacks.

2.1 MANETs characteristics

MANETs possesses several distinctive features which support their varied applications. In the following, we present these features:

• Lack of infrastructure: MANETs are described as networks without any infrastructure. They are hence efficient in terms of time and money. They are easily and reasonably established at low cost [9]. They are, however, also more susceptible to threats compared to traditional networks.

• Distributed management: Many functions are distributed across the nodes due to the lack of centralized control. This has an impact on network structure, node authentication, and data security [10].

• Cooperativeness: Instead of the client-server architecture that is typically utilized in traditional networks, MANETs use peer-to-peer architecture. To fill the gaps left by the MANETs' lack of infrastructure, nodes should cooperate to provide security and centralized management services. This partnership seeks to boost node confidence.

• Multi-hop routing: routing is performed by nodes themselves. When sending a message, a node utilizes neighboring nodes as intermediate hops to reach its destination [11]. Multi-hop routing is the name of this procedure.

• Dynamic topology: Nodes can enter and exit the network at any time and without notice as MANETs do not have perimeter barriers. Furthermore, since there is no centralized supervision, networks can develop independently spontaneously [12, 13].

• Decentralized architecture: Each node within a network operates independently, capable of joining or leaving the network autonomously due to self-configuration. Additionally, nodes have the liberty to either forward or discard data packets, even those intended for them [13].

• Limited resources: Nodes in MANETs have minimal power and processing capabilities due to their reliance on batteries and lesser processing units. The primary issue associated with a limited power source is the increased susceptibility of MANET nodes to Denial of Service (DoS) attacks [14]. In this case, the attacker bombards nodes with additional packets to deplete their batteries.

Table 1 provides an overview of the key characteristics, advantages, and challenges associated with MANETs. Understanding these aspects is crucial for anyone considering the deployment of MANETs in various applications, from emergency response operations to military communication and beyond. The table aims to highlight the unique features that make MANETs a versatile and valuable networking solution, while also acknowledging the potential hurdles that need to be addressed in their implementation.

2.2 MANETs security challenges

MANETs exhibit higher vulnerability compared to traditional networks due to factors such as limited resource availability, absence of perimeter security, lack of physical security, and unpredictable topology. This heightened vulnerability extends to both internal and external threats. The primary forms of attacks on MANETs include active and passive attacks [15].

Active attacks involve perpetrators attempting to modify or falsify information within the network. Examples of active attacks include impersonation, routing table overflows, rush

attacks, Byzantine attacks, denial-of-service attacks, packet replication attacks, blackhole attacks, and distributed denial-of-service attacks. The main paper's focus is to study the blackhole attack.

When an attacker conducts a passive attack, they attempt to acquire access to the system in order to intercept data [6]. Passive attacks include traffic analysis, eavesdropping, and location disclosure. Subsequently, we present the challenges affecting MANETs' security:

• Lack of perimeter security: MANETs lack the necessary infrastructure; hence it is difficult to specify the boundaries between their nodes. Moreover, the network's topology becomes complex and dynamic, as any node can enter or exit the network freely. This dynamic nature creates opportunities for rogue nodes to infiltrate the network's coverage area and masquerade as legitimate nodes, potentially launching attacks.

• Weak physical security: MANETs can be established at any time or location, unlike traditional networks, where the network backbone is typically secured within a data center. In contrast, MANETs lack physical protection for safeguarding the core services.

• Absence of centralized control: In addition to other security services like firewall, network access control, etc., MANETs lack a centralized system to provide identification, authentication, and permission. This makes MANETs more difficult to secure than regular networks.

• Dynamic topology: The connectivity between nodes in a MANET can vary at any time as MANET nodes are free to enter and quit networks. For networks, the same is true. A few networks have the ability to relocate and connect to others. This might alter the routing information continuously.

• Scalability: MANETs consist of a significant number of nodes that can expand, or contract based on various conditions. While MANETs are effective, their security is challenging, particularly concerning the need to identify and authente new nodes.

• Quality of Service: There are numerous standards available for handling various data types. For applications such as media streaming and live transmission, which demand higher bandwidth and stability, it is crucial to implement Quality of Service (QoS) policies and algorithms to mitigate delays and data loss effectively.

• Resource restrictions: Processing, storage, and battery capacity are constrained on MANET nodes. Two serious issues could result from this: nodes cannot have sophisticated endpoint protection due to their low computational capability, and they could be the focus of several attacks that seek to exhaust batteries.

• Security: Due to several vulnerabilities caused by the absence of infrastructure, limited resources, a lack of physical resources, and changing technological methods, MANETs are more vulnerable to security threats than traditional networks.

Table 1. MANETs characteristics, advantages, and challenges

Characteristic	Description	Advantages	Disadvantages
Dynamic Topology	Self-organizing and self-configuring.	- Suitable for temporary or emergency deployments.	- Frequent topology changes and increased overhead.
	No need for a fixed infrastructure.	- Enhanced reliability and robustness.	- Routing and maintenance overhead.
		- No single point of failure.	- Coordination and resource sharing challenges.
Decentralization	No single point of failure.	- Enhanced reliability and robustness.	- Limited scalability for large networks.
	Enhanced reliability and robustness.	- Complex management and security.	
Flexibility	Easy to deploy in remote or ad hoc scenarios.	- Reduced infrastructure costs.	- Limited data storage and processing capabilities.
	Suitable for military, disaster recovery, and sensor networks.	- Less reliance on fixed base stations.	- Power consumption in mobile devices.
Low Infrastructure	Reduced infrastructure costs.	- Enhanced fault tolerance.	- Energy constraints may limit network lifetime.
	Less reliance on fixed base stations.	- Suitable for both small and large networks.	- Limited battery capacity in mobile devices.
Self-Healing	Automatic network recovery after node failures.	- Better power management for mobile devices.	- Delay in network recovery due to routing recalculations.
	Enhanced fault tolerance.	- Energy-aware routing protocols.	- May require additional network maintenance.
Multi-hop Communication	Extends the network's reach.	- Extends the network's reach.	- Increased latency due to multiple hops.
	Enables communication in remote or inaccessible areas.	- Enables communication in remote or inaccessible areas.	- Higher potential for congestion.
Energy Efficiency	Better power management for mobile devices.	- Reduced infrastructure costs.	- Energy constraints may limit network lifetime.
	Energy-aware routing protocols.	- Better power management for mobile devices.	- Limited battery capacity in mobile devices.
Scalability	Suitable for both small and large networks.	- Suitable for temporary or emergency deployments.	- Scalability challenges with increased network size.
	Adaptable to diverse application requirements.	- Adaptable to diverse application requirements.	- Overhead and complexity in large-scale deployments.

Table 2. Security challenges in MANETs

Challenge	Description	Effect on MANETs Security
Node Mobility	Frequent movement of nodes within the network.	- Increased vulnerability to attacks due to changing network topology. - Difficulties in maintaining secure connections.
Limited Resources	Mobile devices often have constrained resources such as processing power and battery life.	- Limited capacity for complex security measures. - Increased vulnerability to resource-intensive attacks.
Dynamic Topology	MANETs exhibit dynamic and self-organizing topologies.	- Rapid changes in network structure can challenge the effectiveness of security mechanisms.
Lack of Infrastructure	MANETs operate without a fixed infrastructure.	- Absence of centralized security controls, leading to difficulties in intrusion detection and prevention.
Routing Protocol Vulnerabilities	Vulnerabilities in routing protocols can be exploited for attacks.	- Attacks on routing can disrupt communication and compromise network integrity.
Limited Bandwidth	MANETs often have limited available bandwidth.	- Encryption and security overhead can significantly impact available bandwidth.
Heterogeneous Devices	MANETs consist of diverse devices with varying security capabilities.	- Compatibility and integration challenges for security solutions.
Malicious Nodes	The presence of malicious nodes that actively participate in attacks.	- Threats such as Sybil attacks, blackhole attacks, and data injection attacks can compromise network trust.
Secure Key Management	Establishing and managing secure keys for encryption and authentication.	- Difficulty in maintaining robust key management due to the dynamic nature of MANETs.
Intrusion Detection	Detecting and responding to security breaches.	- Challenges in accurately identifying attacks due to dynamic topology and limited infrastructure.

Table 3. Comparison between routing protocols in MANETs

Routing Protocol Type	Description	Examples of Routing Protocols	Advantages	Disadvantages	Suitable Type of Network
Proactive (Table-Driven)	Maintains up-to-date routing information with regular updates.	- Optimized Link State Routing (OLSR) - Destination-Sequenced Distance Vector (DSDV)	- Low latency for route establishment. - Supports real-time communication.	- High control overhead due to constant updates. - Inefficient for large, highly dynamic networks. - Consumes more power and bandwidth.	Small to Medium-sized Networks
Reactive (On-Demand)	Establishes routes only when needed, based on specific requests.	- Ad Hoc On-Demand Distance Vector (AODV) - Dynamic Source Routing (DSR)	- Reduced control overhead in idle periods. - More efficient for larger, highly dynamic networks.	- Longer route setup time. - Increased latency for initial communication. - May incur route discovery overhead for each new communication session.	Medium to Large-sized Networks
Hybrid (Zone-Based)	Combines features of both proactive and reactive protocols.	- Zone Routing Protocol (ZRP) - Temporally Ordered Routing Algorithm (TORA)	- Balances control overhead and route setup time. - Suitable for medium to large-sized networks with moderate dynamics.	- More complex to implement and manage. - Limited scalability for very large networks. - May still exhibit some control overhead.	Medium-sized Networks with Moderate Dynamics

Table 2 presents a comprehensive overview of the security challenges, providing the description of each challenge, and its potential impact on MANETs' security. By identifying and addressing these challenges, network administrators and security professionals can develop robust strategies to enhance the security of MANETs in various scenarios, from military and emergency response operations to Internet of Things (IoT) deployments.

2.3 MANETs routing protocols

The primary objective of the routing protocols is to determine the most effective route for a message to take from the originator to the destination [16]. Routing protocols are often categorized into reactive, proactive and hybrid [17].

n proactive routing protocols, each node maintains a table containing all potential routes, which is regularly updated whenever there is a change in the network (for instance, when a node enters or leaves the network). For this reason, it is regarded as a table-driven protocol. Effectiveness is the key objective of proactive procedure. The nodes demonstrate good adaptability to changes and consistently ensure efficient data transmission. The main concern lies in the network overhead generated by frequent updates to accommodate these changes.

When a change occurs in the network, reactive protocols do not react until data exchange begins and notices the change. These protocols are also called on-demand routing protocol since the route table update happens after a request [4]. Therefore, the network overhead is minimized. On the other hand, these protocols suffer from latency every time data is exchanged while there is a change. Hybrid protocols were created to address the first two problems. These types of protocols leverage a blend of algorithms. For instance, a proactive routing protocol collaborates with nearby nodes to update routing tables efficiently, minimizing overhead. Moreover, a reactive protocol approach is employed for distant

nodes to expedite the route discovery process with them. The main drawback of hybrid protocols is that they are more complex than proactive or reactive. This complexity appears in both implementation and maintenance. It is also not scalable like reactive or proactive.

Table 3 provides a comparison of proactive, reactive, and hybrid routing protocols in MANETs, considering their descriptions, examples, advantages, disadvantages, and the types of networks they are most suitable for. The choice of routing protocol depends on specific network characteristics and application requirements.

2.4 Blackhole attack

The blackhole attack exploits vulnerabilities in the AODV routing protocol. Within the AODV routing protocol framework, each node in the network maintains a routing table containing information about the most efficient routes to specific destinations. Before forwarding a packet to another node, a node checks its routing table to ascertain if it contains the requisite information. If the information is not found or the desired route is unavailable, the node initiates a discovery process by broadcasting a route request (RReq) to all its neighboring nodes. Upon receiving the RReq, if the node is the destination node, it responds with a Route Reply (RRep), containing hop count, broadcast ID, and the most recent sequence number [18]. If not, the node compares the destination sequence number with its own routing database and, if necessary, issues an RReq to its neighbors to update its table and respond with an RRep to the originating node. A new route with a higher sequence number is used for the update [19]. A blackhole attack occurs when a rogue node infiltrates the network and falsely claims to possess the shortest path to the target [20]. Figure 1 illustrates this process. For instance, node "S" seeks to reach node "D" and broadcasts an "RREQ" to adjacent nodes. Node "M" promptly responds by falsely claiming to have the optimal route. However, any data transmitted through node "M" is discarded once communication begins.

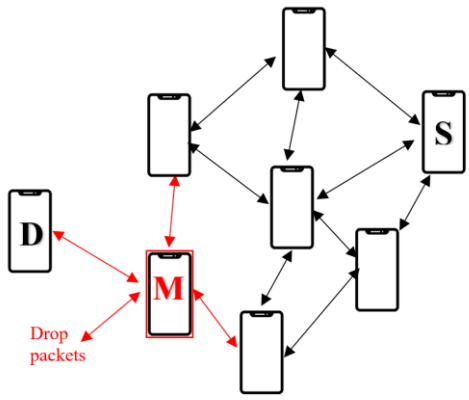

Figure 1. Malicious node (M) drops packets in a blackhole attack

An ongoing attack known as the blackhole attack involves the malicious node dropping all data passing through it [21]. In this attack, the malicious node disseminates false information to its neighboring nodes, falsely asserting to possess the shortest routes to destinations requested by other nodes. Blackhole attack has an impact on the network's throughput and packet delivery ratio in particular. Blackholes come in two varieties: single and cooperative. In case the number of malicious nodes is one, a single incident occurs. It is further sophisticated and deadly than a single blackhole attack when multiple hostile nodes in the same network discard packets simultaneously.

3. RELATED WORK

Blackhole attacks have drawn the attention of many researchers since ad hoc networks are growing and employed in a range of industries. The most popular solutions can be categorized into four groups, as illustrated in Figure 2.

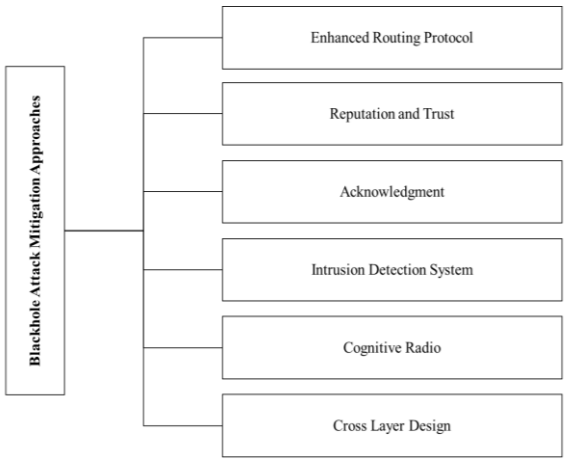

Figure 2. Classification of the blackhole attack mitigation techniques

3.1 Enhanced routing protocol based

he foundation of this solution lies in the concept that bolstering and fortifying the current routing protocols can enhance their ability to accurately identify and thwart blackhole attacks in MANETs. The rationale behind this approach is that the core routing protocols used in MANETs, such as AODV and DSR, have inherent vulnerabilities that can be exploited by blackhole attackers. By implementing modifications and extensions to these protocols, researchers aim to develop more secure and resilient routing mechanisms that can detect and mitigate the blackhole threat.

In the study of Sarao [20], the MBDP-AODV (Multipath and Backup Path Discovery in Ad Hoc On-demand Distance Vector) enhanced routing protocol was proposed. The mean and standard deviation are two statistical concepts that are used in this improved methodology. When there is an attack, the statistics, however, curiously spike suddenly. The suggested treatment consists of three steps. Suspicion and dynamic threshold calculation come first. At this stage, the source node establishes a threshold value for the destination's sequence number. In the subsequent phase, known as detection, the system identifies the suspicious packet and disseminates the ID of the malicious node to all network nodes. Subsequently, in the prevention phase, measures are implemented to restrict the rogue node from further interaction with the network.

Mezher et al. [7] offered a technique for locating blackhole nodes that involved installing bait timers in each node. The baiting timer is programmed with a random number. Fake ID broadcasts begin to run when the baiting timer reaches the predetermined time. The blackhole will respond to all inquiries, regardless of their nature. They answer those deceptive

questions that are used as bait. The sending node finds and keeps track of the blackhole node in a particular table as a result. When the genuine requests are sent out in line with the information stored in the malicious nodes table, malicious nodes are disregarded.

Ponnusamy [22] proposed modifying the current AODV protocol by incorporating Neighbor Credit Table into each network node. When a neighbor sends or forwards a data packet, the neighbor is believed to be a legitimate node, and the table's credit value is enhanced. Even the authentic node receives subpar credit values when not participating. When a node wants to transmit a message using a neighboring node, it first validates the value of the table. A different hop should be chosen if the neighbor node is untrusted or lacks sufficient credit.

The key advantages of this approach are its ability to recognize and isolate smart blackhole attacks as well as its power to recognize blackhole nodes while route seeking rather than data transmission. The drawbacks, on the other hand, include increased overhead brought on by the requirement to send additional packets in order to identify rogue nodes. Another effect is the increase of network traffic.

3.2 Reputation and trust based

The reputation and trust-based approach to mitigating blackhole attacks in mobile ad-hoc networks (MANETs) relies on the development and implementation of robust reputation systems. These systems gather, analyze, and share information about the behavior and activities of individual nodes based on their past interactions within the network.

The underlying principle of this mitigation technique is that by maintaining a comprehensive reputation profile for each node, the network can identify and isolate those nodes that exhibit malicious or untrustworthy behavior, such as participating in blackhole attacks. The reputation system operates by:

Monitoring node behavior: The network continuously monitors the actions and performance of each node, collecting data on factors like packet forwarding, route establishment, and responsiveness to requests.

Reputation score calculation: Based on the observed behavior, the reputation system assigns a quantitative score to each node, reflecting its trustworthiness and reliability within the network.

Reputation information sharing: The reputation scores are shared among nodes, allowing them to make informed decisions about which nodes to trust and which to avoid when establishing communication routes.

Reputation-based routing: The routing protocols are modified to incorporate the reputation scores as a key criterion for selecting the most trustworthy paths, effectively excluding nodes with low reputation scores from participating in the routing process.

According to Malik and Sharma [23], the Selfish Node Removal using Reputation Model (SNRRM) can be used to remove selfish nodes from a network. The author asserts that the current energy level and communication rate of a node serve as indicators of its selfish behavior. When both sender (S) and distention (D) are inside the communication range, only the sender's reputation value is considered. If (S) and (D) have different communication ranges, (S) transmits a control packet to its neighbors and waits for replies. Requests sent and replies returned are then used to compute the communication ratio.

Shao et al. [24] proposed a Node Activity-based Trust and Reputation Estimation (NATRE) approach. This method is designed to monitor node activity, distinguishing between legitimate (N) and malicious (M) behavior, while also providing estimates of reputation and trust. As per the author's assertion, three separate stares characterize the nodes: Resource Limitation State (RLS), Normal State (NS), and Malicious State (MS). In NS, nodes make every effort to cooperate and follow routing specifications. In RLS, the nodes seldom cooperate due to low power consumption, intense traffic, lack of connectivity, etc. In MS, the nodes disturb the network by launching DoS attacks, establishing new pathways, delaying packets, or participating in other malicious behaviors that have an impact on the network. A "Semi-Markov probability decision procedure" is used for prediction in order to proactively separate several situations.

The authors made a recommendation for a reputation and trust mechanism against blackhole attacks [25]. This relies on the mutual trust between nodes. For instance, if node (A) trusts node (B), then (B) can reciprocally trust (A). Similarly, if (B) trusts (C) and (C) trusts (A), then (B) also trusts (C). So that (A) can believe (B). In order to implement this method, a reputation table is installed on each node in the network. The table contains information about how the neighbor node behaves. The behavior is tracked and measured. As a result, after a message is sent from a source to a destination, the destination must confirm that it has received the message. An acknowledgement is sent to each node, which is then returned. The trusted table is modified negatively in the same way if a message is not received.

In a reputation-based trust system, each node keeps a record of other nodes according to their interactions, similar to a reputation system. However, in based trust, the node examines the trust values of the neighboring nodes and selects the greater trust value based on those results.

To ensure quality of service and security by accounting for changes in activity, packet forwarding, or dropping, Garg and Bawa [26] introduced the Node Activity-based Trust and Reputation estimate (NATRE). The main benefit of this method is that the blackhole node is found before data transmission ever begins, during route discovery, being able to recognize and contain sophisticated blackhole attacks. Its key disadvantage is that by sending extra packets to identify rogue nodes, the overhead is increased. High network traffic is another result of this.

This approach offers significant advantages as the reputation system not only classifies nodes as either good or bad but also provides additional insights into the level of cooperation exhibited by each node. Additionally, it offers node trust value during packet forwarding and additionally supports QoS. Reputation is reactive and makes decisions based on previous data, which has several problems, including the ability to falsify reputation tables and its susceptibility to denial-of-service attacks.

3.3 Acknowledgment based

To address the challenges posed by blackhole attacks in MANETs, the acknowledgment-based approach employs a multi-layered system that leverages the exchange of acknowledgment packets across the source and intermediate nodes. This technique aims to identify and isolate malicious or uncooperative nodes that may be participating in blackhole

attacks.

The key aspects of the acknowledgment-based mitigation approach are as follows:

Acknowledgment packet exchange: Before determining the route for data transmission, the source node or intermediate nodes will initiate the exchange of acknowledgment packets with the neighboring nodes. These acknowledgment packets serve as a means of verifying the responsiveness and reliability of the nodes along the potential communication path.

Node behavior monitoring: The acknowledgment packet exchange allows the network to monitor the behavior of individual nodes. Nodes that fail to respond to the acknowledgment requests or exhibit delays in their responses are flagged as potentially untrustworthy or malicious.

Selective route establishment: Based on the acknowledgment information gathered, the routing protocols are modified to selectively establish communication paths, prioritizing the nodes that have demonstrated reliable and cooperative behavior through their timely acknowledgment responses.

Blackhole node identification: By analyzing the acknowledgment packet exchange patterns, the network can effectively identify nodes that are purposefully not responding or exhibiting suspicious behavior, potentially indicating their involvement in blackhole attacks.

Malicious node isolation: Once a node is identified as a potential blackhole attacker, the network can take appropriate actions to isolate and exclude it from participating in the routing process, thereby mitigating the impact of the blackhole attack.

Chen et al. [27] proposed Ad hoc On-demand Multipath Secure Routing (AOMSR), an enhanced routing system based on acknowledgement. This routing system requires the source node to establish multiple paths from the source to the destination, considering the maximum delay in data reception. Alongside session key agreements, a counter-based end-to-end acknowledgment cycle, and authentication of Ack packets via message digest, Kaur and Kumar [28] suggested an enhancement to the acknowledgment-based approach. This enhancement involves selecting intermediate nodes that are both energy-efficient and uncongested for communication. This method has the advantage of being able to distinguish between selfish and insufficiently energetic nodes from malicious nodes. The network load will increase as a result of the additional acknowledgement packets, which is a disadvantage.

3.4 Intrusion detection system based

To strengthen the defense against blackhole attacks in MANETs, researchers have developed intrusion detection system (IDS) based mitigation approaches. These IDS-based techniques leverage specialized monitoring and alerting mechanisms to identify and respond to suspicious activities that may indicate the presence of blackhole attacks [29].

The key components and functionality of the IDS-based mitigation approach are as follows:

Monitoring and data collection: The IDS system continuously monitors the network traffic and node behavior, collecting relevant data and metrics that can be used to detect anomalies or potential threats.

Anomaly detection: The IDS utilizes a blend of behavior-based and signature-based detection methods to detect anomalies in network activity patterns. These anomalies may be indicative of blackhole attacks or other malicious behaviors.

Alerting and notification: When the IDS detects suspicious activities or potential blackhole attacks, it triggers an alert system to notify the network administrators or other nodes about the identified threat.

Audit log maintenance: The IDS maintains a comprehensive audit log, recording the details of all monitored network events and detected anomalies. This audit data is crucial for subsequent analysis, forensics, and decision-making processes.

Mitigation and response: Based on the IDS alerts and the analysis of the audit data, the network can initiate appropriate mitigation actions, such as isolating the suspected blackhole nodes, rerouting traffic away from the compromised areas, or implementing additional security measures to address the identified vulnerability.

The authors' recommended treatment was IDS in the study of Patil and Kulkarni [30]. DPAA-AODV (Delay-Based Predictive Adaptive Acknowledgment Ad Hoc On-demand Distance Vector) protocol has two operating modes: online and offline. The offline mode is utilized to identify a dependable feature within the Blackhole Detection Dataset (BDD). In the online mode, features learned from the previous mode are utilized. If the results indicate that the threshold has been surpassed, it suggests the presence of a malicious node.

In the study of Rathod and Sharma [31], a host-based IDS was employed to gather data on the normal activities of nodes. The GloMoSim simulator was utilized to replicate common malicious node behaviors. Subsequently, a rogue node was pinpointed through feature selection employing a machine learning technique (Weka 3.7.11). Six features were employed for this purpose: the count of provided RREQs, the count of forwarded RREPs, the count of high destination sequence numbers, the count of low hop counts to destinations, the count of source nodes, and the count of destination nodes.

An IDS was suggested by Ibrahim and Abdulazeez [32] to help find the rogue nodes. The answer was analyzed using a three-step process that included data collecting, network simulation, model training, and data testing. For 25 nodes, NS2 was used for the simulation. Subsequently, a CSV (Comma-Separated Values) file was extracted from the output for analysis. After this, four algorithms—support vector machine, random forest classifier, decision tree classifier, and logistic regression—were employed for model training and testing.

Verma and Kumar [18] suggested a two-phased solution. The improved AODV phase and the features selection phase. The characteristics of a blackhole are initially determined based on node behavior, such as how nodes respond to RREP and RREQ. The AODV protocol is improved in the second phase by incorporating the learned data into each and every node, enabling it to identify any blackhole nodes and avoid them when transferring data.

In the study of Malik and Sharma [23], an enhanced routing protocol named SAODV (Secure Ad hoc On-Demand Distance Vector) was introduced, aiming to provide a more secure alternative to the AODV routing protocol. The objective of this enhanced routing protocol is to safeguard MANETs against blackhole attacks. It is comparable to the AODV routing system in that both use a discovery process to let nodes know which route is the best. However, a verification procedure is included in SAODV. By exchanging random numbers, this verification mechanism puts the neighboring node to the test. Every time the adjacent node responds with

RREP, this process is started to make sure the node can be trusted.

An IDS employing classifiers like decision trees, KNN, SVM, and neural networks was introduced [33]. A decision tree comprises nodes, edges, and leaves, functioning by generating rules to categorize records into different classes, distinguishing between harmful and non-malicious ones. Training data are stored with consideration for the distance metric of other nodes, and connections are established based on the dataset's classes. SVM is primarily employed for pattern recognition tasks, although it can also serve for classification purposes. Finally, the records undergo processing and training utilizing neural networks. This method offers several advantages, including the effectiveness of the classification algorithm in detecting grayhole and blackhole attacks, the high accuracy of the anomaly-based classifier in identifying blackhole attacks, the random forest classifier's high accuracy and detection rate, and the anomaly-based classifier's accuracy in identifying blackhole attacks. On the other hand, the disadvantages include the fact that nodes must be in a promiscuous state, which is unacceptable to nodes.

3.5 Cognitive radio networks based

Cognitive radio technology is applied to MANETs to enhance security through spectrum sensing, identifying malicious nodes and mitigating blackhole attacks. Khan and Javaid [34] propose a recent approach that mitigates cooperative blackhole attacks using spectrum sensing in cognitive radio networks. This technique leverages cognitive radio technology to identify and respond to malicious nodes, enhancing the security of MANETs [35].

In another study [36], the authors explored spectrum allocation to protect cognitive radio ad hoc networks against malicious users. Their approach focuses on dynamic spectrum access and spectrum allocation strategies to secure MA-ETs, mitigating blackhole attacks and similar threats.

Additionally, Jain and Sharma [37] introduced a novel security framework that combines cognitive radio technology with dynamic spectrum access in cognitive radio ad hoc networks. This approach enhances the security of MANETs by mitigating blackhole attacks and other threats through dynamic spectrum management.

3.6 Cross-layer design based

Cross-layer design strategies integrate information from multiple network layers to detect and mitigate attacks in an integrated manner. In the study of Rabiaa et al. [38], the authors introduced a recent cross-layer trust-based routing and detection mechanism to mitigate cooperative blackhole attacks in MANETs. Their approach combines cross-layer information to identify and respond to attacks effectively, enhancing the security of these networks.

Table 4. Blackhole attack mitigation approaches in MANETs: Categories, descriptions, advantages, and disadvantages

Category	Description	Advantages	Disadvantages
Enhanced Routing Protocol-Based	Strengthen routing protocols with enhanced security mechanisms such as authentication and data integrity to detect and prevent blackhole attacks.	- Improved network security - Data integrity protection - Resilience against blackhole attacks - Compatibility with various routing protocols	- Increased overhead due to security mechanisms - Complex implementation and key management - May not protect against all types of attacks
Reputation and Trust-Based	Evaluate node trustworthiness based on behavior and interactions, isolating or excluding nodes with low reputations to mitigate blackhole attacks.	- Effective in identifying malicious nodes - Isolation of nodes with low reputations - Promotes cooperation and trust in the network	- Vulnerable to reputation manipulation by attackers - Potential false reputation-based exclusion - Impact on network performance due to reputation updates
Acknowledgment -Based	Employ acknowledgment-based schemes to enhance the detection and mitigation of blackhole attacks by monitoring node behaviors and responses.	- Real-time detection and response - Identifies various types of attacks - Scalable and adaptable to evolving threats	- False positives can impact network performance -Resource-intensive, consuming network resources - May not prevent attacks if not updated regularly
Intrusion Detection System-Based	Utilize Intrusion Detection Systems (IDS) to continuously monitor network traffic for signs of malicious behavior, providing real-time protection against blackhole attacks.	- Real-time detection and response - Identifies various types of attacks - Scalable and adaptable to evolving threats	- False positives can impact network performance - Resource-intensive, consuming network resources - May not prevent attacks if not updated regularly
Cognitive Radio-Based	Integrate cognitive radio technology to enhance security by applying spectrum sensing to identify malicious nodes and mitigate blackhole attacks.	- Dynamic spectrum access enhances security - Effective against various types of attacks - Improved network resilience	-Requires specialized hardware or cognitive radios - Complexity in integrating cognitive radio technology - Spectrum sensing accuracy can impact detection
Cross-Layer Design-Based	Implement cross-layer design strategies to integrate information from multiple network layers, enhancing security through coordinated responses.	- Enhanced security through cross-layer collaboration - Improved detection and response - Comprehensive protection against various attacks	- Complex to implement and may require protocol modifications - Potential compatibility issues with existing protocols - Resource consumption from cross-layer coordination

Shafi et al. [39] presented a cross-layer approach to mitigate the impact of coordinated blackhole attacks in MANETs. This approach leverages cross-layer information and mechanisms to detect and respond to malicious activities, enhancing the security of MANETs.

A cross-layer approach to blackhole attack detection in wireless ad hoc networks was proposed by Rani et al. [40]. Their approach leverages information from multiple network layers to identify and mitigate attacks effectively, making MANETs more secure.

These recent references represent a range of approaches within each category for mitigating blackhole attacks in MANETs, offering detailed insights into the recent research efforts and advancements. Researchers and network administrators can select the most suitable solution(s) based on their specific network scenarios and requirements to enhance the security and resilience of MANETs.

Table 4 offers an overview of these approaches, categorizing them into distinct strategies. For each category, the table provides a clear description of the approach, highlights its advantages, and acknowledges its limitations. This structured analysis aims to assist network administrators, researchers, and security professionals in making informed decisions when selecting the most appropriate blackhole attack mitigation approach for their specific MANET scenarios. Each category has its unique strengths and weaknesses, and this table serves as a reference for assessing the trade-offs associated with each approach.

4. METHODOLOGY

The proposed solution consists of four steps as shown in Figure 3. The first step is to create the data required for machine learning analysis. This is done by launching a blackhole attack while creating traffic data with the OMNET++ emulator that closely matches actual traffic. This data is subsequently collected in a specific manner to facilitate later analysis. The collected traffic records have a few fundamental qualities in common. Based on these behaviors, SVM analysis is utilized to divide the traffic into malicious and legitimate traffic. Malicious nodes can be located and blocked using this approach.

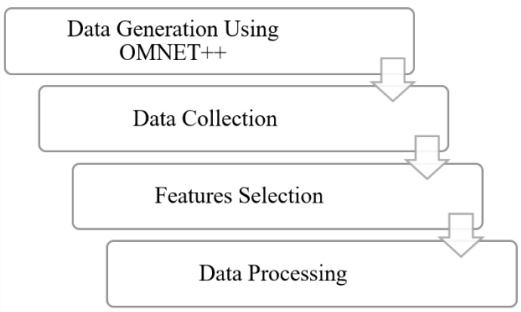

Figure 3. Methodology to mitigate blackhole attack

4.1 Proposed solution

In mobile ad-hoc networks (MANETs), the lack of centralized infrastructure and the inherent collaborative nature of the network operations make nodes heavily reliant on each other to perform various tasks. This interdependence is crucial for the efficient functioning of the MANET. However, it also leaves the network vulnerable to malicious attacks, such as the blackhole attack, where rogue nodes aim to disrupt the normal operations of the network.

To address this challenge, an SVM-based detection system can be implemented to identify and isolate the malicious blackhole nodes within the MANET. The key aspects of this approach are as follows:

Behavioral Characteristics of Blackhole Nodes:

Increased transmission power: Blackhole nodes typically increase their transmission power to respond to the majority of Route Request (RREQ) messages, making it more likely that their malicious responses will be accepted by the source nodes.

Reduced broadcasting: Blackhole nodes often avoid broadcasting RREQ messages and instead prefer to unicast their responses, as this strategy helps them gain control over the communication paths.

Minimal RREQ generation: Blackhole nodes tend to generate very few or no RREQ messages, as they aim to avoid engaging in the legitimate routing process and focus on intercepting and disrupting the data flow.

SVM-based Detection Mechanism:

The SVM algorithm is a robust machine learning technique capable of accurately classifying and identifying malicious blackhole nodes through their unique behavioral traits. The SVM-based detection system is trained on a dataset of normal network behavior and known blackhole attack patterns. This training allows the system to learn the distinctive features that differentiate the blackhole nodes from the legitimate nodes in the MANET.

During the operational phase, the detection system continuously monitors the network traffic and node behavior, extracting the relevant features (such as transmission power, RREQ generation, and unicast/broadcast ratios) and applying the trained SVM model to classify each node as either benign or a potential blackhole attacker.

Malicious Node Isolation:

Once a node is identified as a blackhole attacker by the SVM-based detection system, the network can initiate appropriate mitigation actions, such as isolating the suspected node from participating in the routing and data forwarding processes.

This isolation can be achieved by broadcasting alerts to other nodes in the MANET, informing them about the detected blackhole node and advising them to avoid establishing communication paths that involve the malicious node.

The isolation of the blackhole nodes helps to protect the rest of the MANET from the disruptive effects of the blackhole attack, thereby enhancing the overall resilience and security of the network.

4.2 Data generation

With OMNET++ 5.7, it becomes feasible to replicate the behaviors of both benign and malicious nodes. The simulation was conducted with a total of 7 nodes. One of them, known as node1, acted as a transmitter and is immovable. This node is not included in the graphs since it fails to accurately depict the behavior of the mobile nodes, which constitute the central nodes in the simulation. There are two scenarios in this simulation. In the first scenario, all nodes are cooperative and there are no malicious nodes. As a result, every node is operating normally. In the second case, node 6 was set up to behave maliciously while the other nodes go about their normal behavior. A 1 mW radio transmission power setting is

included on all nods.

In this case, the radio transmission power of node 6 was configured to 5 mW. Node 6 can trick its neighbors into thinking that it is the one nearest to them by amplifying its radio transmission power. It receives as many requests as it can as a result. To put it another way, nodes will initially appear as a neighboring node when they search for the best routes and send their RReq, and they will send their RRep as soon as they can. Table 5 summarizes the configuration parameters used to generate the dataset.

Table 5. The parameters 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]	5mW
Transmission Speed	24Mbps
Mobility Speed	25mps
Transport Protocol	UDP

4.3 Data collection

Results were collected under two different assumptions: one that all nodes were cooperative and acting normally, and the other that one node was acting maliciously. The outcomes of the two scenarios were subsequently evaluated using the detection system. The dataset contained the most crucial information from the simulation performed in OMNET++.

The AODV request, the nodes' packet transmission power, and the kind of data transfer (Broadcast vs. Unicast) were all included. Table 6 illustrates the number of normal traffic records, malicious traffic records, and the total records.

Table 6. The number of normal traffic records, malicious traffic records, and the total records

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

4.4 Feature selection

According to Figure 4, there are three factors that influence how blackholes execute attacks. The malicious node's first trait is that it tricks other nodes into thinking it is the one that is closest to them. The second is the frequency of RReq requests from rogue nodes. They prefer to answer as many questions as they can. Not to mention, they almost never transmit and almost never employ unicast.

4.5 Data processing

Eight columns make up the data taken from the OMNET++ simulator. Three of the eight columns will not be used for the analysis and will be discarded as they do not add any information. Five of the eight columns will be used. These are the five values:

• Hops, this column aids the study in two ways. Initially, the node utilized as a hop or responsible for routing is disclosed, along with the transmission direction.

• Transmission type, the transmission power value is presented in this field. It demonstrates two crucial values: Route Reply (Rrep) or Route Request (Rreq). These fields play a critical role in identifying nodes that are not submitting any requests. This is one of the characteristics that, along with others, indicate malicious behavior.

• Node name, the name of the node that sent the data is contained in this field. Each node's identity and the misbehaving node's identification are used.

• Transfer Type, whether it is broadcast or unicast, this field's value represents the transfer type. It is used to display the nodes that are not broadcasting, which is a significant feature. These nodes are the suspicious ones since they are predicted to act inappropriately by other characteristics.

• Transmission power, the transmission power used to convey the data is displayed in this section. It is also crucial to demonstrate whether the power utilized for communication has been altered, as blackhole attacks typically increase the node's power.

Figure 5 depicts the components of our proposed solution.

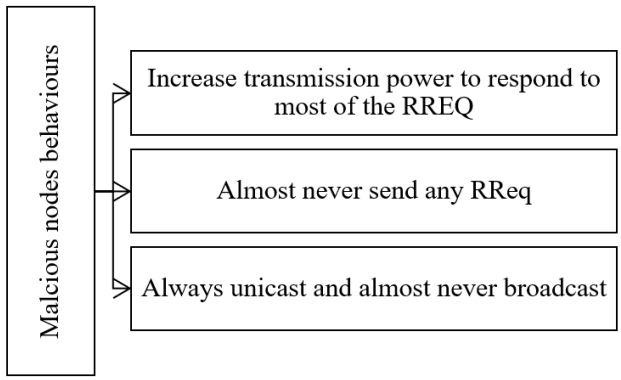

Figure 4. Feature selection based on malicious nodes' behavior

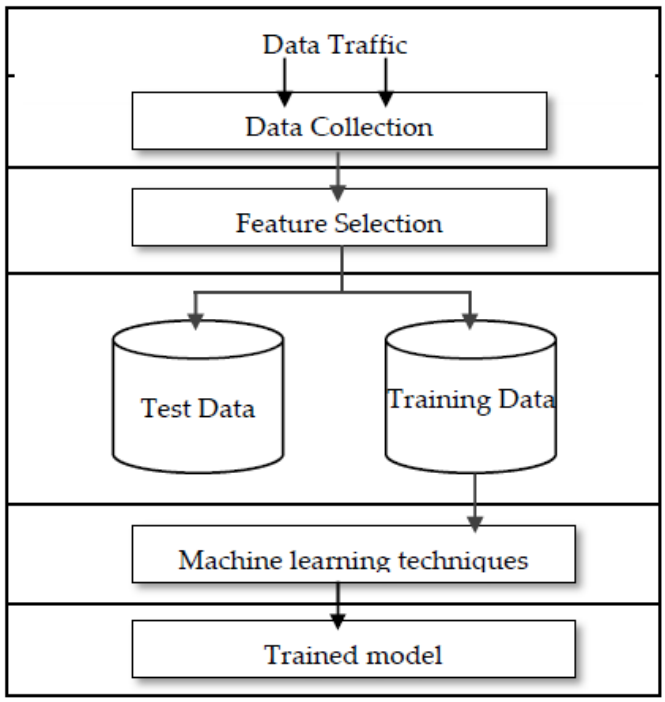

Figure 5. Solution components

4.6 Machine learning using (SVM)

Pattern categorization tasks usually include the use of the well-known machine learning approach, Support Vector Machine (SVM). The model, which is composed of three lines, is shown in Figure 6. The center line serves as the finest classification line. The margin lines are the two additional lines. These lines separate patterns into two classes [34]. This model is used in our system to discriminate between malicious and properly behaving nodes based on the traffic analysis.

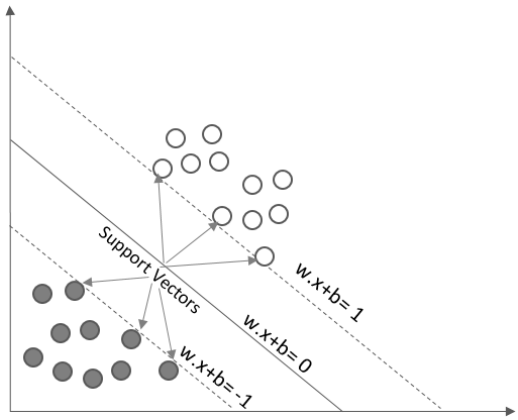

Figure 6. Support vector machine (SVM)

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

Positive class (+1) is the first, and the negative class (-1) is the second. The dataset denotes the sample size with 'n', where it represents the vector characteristic, and 'y' signifies a value of either -1 or +1. While not all traits may be identical, allowing for some variability, they can still be accurately categorized. A specified margin permits acceptable variance. As previously mentioned, the line in the middle is termed the "optimal classification line" since it's where the sum of the weighted vector and bias, as depicted in Eq. (2), equals zero.

$$w.x + b = 0 \quad (2)$$

Two additional lines, each with a certain margin, exist due to variations in vector properties. The optimal classification line, along with the marginal bias, runs parallel to these two lines.

The hyperplane, which is formed by these two marginal lines, is known. According to Eq. (3), the points above the hyperplane are captured as first class.

$$w.x + b \geq 1 \quad (3)$$

As shown in Eq. (4), the points below the hyperplane are also captured as the second class.

$$w.x + b \leq 1 \quad (4)$$

Later, the terms "malicious" and "normal" vectors" are used to describe these two groups.

The key drawbacks of SVM include its poor performance with large datasets, excessive noise, and feature counts that are greater than the number of trained data samples. As our dataset was small and the features were distinct, these SVM's shortcomings had little effect on the caliber of our work.

5. RESULTS

The simulator was set up to look at interactions between seven nodes. One of the nodes was configured as a rogue node that mimicked a blackhole attack. The simulation was allowed to run for fifteen minutes. The records the system looked at included 29,338 records generated by the simulation. In the end, the algorithm was able to separate the records into two categories: harmful records and useful records. 22,837 of the 29,338 records were labelled as normal, and 6,498 as harmful out of the total. The following three key features provided evidence in favor of this:

- Whether a change is made to the transmission power. The rogue node modifies its transmission power as previously mentioned to look close to the RReq sender.
- Exceptionally increased response to as many requests as feasible.
- Almost never transmits broadcast messages; only ever send unicast.

The machine learning program accurately pinpointed the malicious articles based on their features. The system has demonstrated a high level of accuracy in identifying malicious nodes by analyzing their behaviors using the aforementioned features.

In our example, node 6's radio transmission power is increased to 5 mW while the remaining nodes maintain their default values of 1 mW. The ability to respond to as many requests as possible while sending hardly any routing requests (RReq) is the second characteristic of blackhole attackers. The last factor is that the blackhole attacker hardly ever broadcasts and uses unicast for all its communication. The six nodes of the graph behave normally, as seen in Figure 7. They all communicate by sending standard RReps and RReqs. Each node in the diagram has a relative ratio between the number of RRep and RReq.

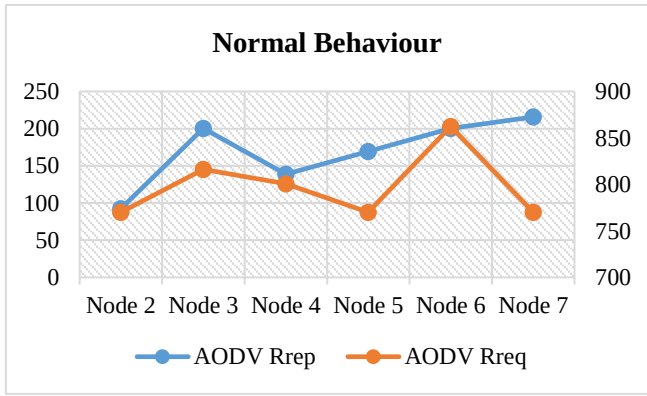

Figure 7. Results of the simulator in the absence of a blackhole attack

The numbers of RRep sent by node 6 to the other nodes are vastly different, as seen in Figure 8. The transmission power of node 6 has been raised to 5 mW, while the other nodes maintain a transmission power of 1 mW, which accounts for this disparity. Moreover, node 6 emits significantly fewer RReqs compared to both the other nodes and those in close proximity to each other.

As illustrated in Figure 9, when we compare the results of our proposed method for detecting blackhole attacks in MANETs, called ADS-SVM, with J48 classifier and NB

classifier using our generated dataset, it becomes evident that ADS-SVM performs superiorly.

ADS-SVM attains an impressive detection accuracy of 99.96%, surpassing the accuracy of the other methods. The J48 classifier achieves a still respectable detection accuracy of 99.2%, though it falls short of ADS-SVM's accuracy. Meanwhile, the NB classifier achieves a lower detection accuracy of 96.5%. These findings indicate that ADS-SVM stands out as a remarkably effective method for detecting blackhole attacks in MANETs and may excel in terms of accuracy when compared to other existing methods.

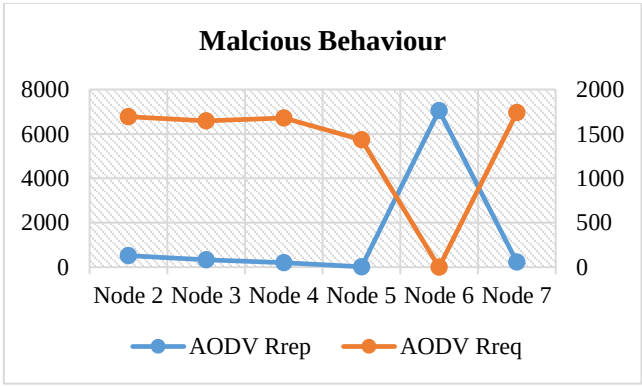

Figure 8. Results of the simulator in the presence of a blackhole attack

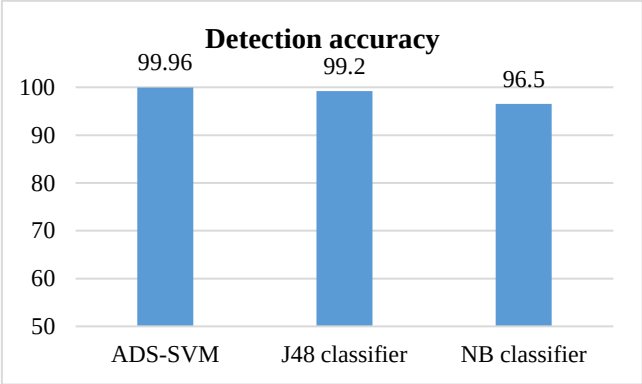

Figure 9. Comparison of the proposed method (ADS-SVM) with J48 classifier and NB classifier

6. CONCLUSIONS AND FUTURE WORK

Without any physical infrastructure, MANETs rely on the cooperation of its nodes to enable both client and router functioning. These networks lack numerous security components and have inadequate resources. As a result, they are more exposed than networks that use conventional infrastructure. We discussed several MANET applications, security concerns, and one of the most common attacks, the blackhole attack, in this study. We looked at, categorized, and compared the solutions recommended in the literature to mitigate blackhole attacks. Then, a suggested strategy for recognizing and averting similar attacks was proposed utilizing machine learning.

In order to completely investigate blackhole attacks, we simulated a malicious node in a MANET network using OMNET++, and we generated a dataset that we used for analysis and looking at the behavior of the malicious node acting as the blackhole attack. Our three main areas of focus for detecting blackhole attacks were transmission power, the volume of answers relative to the other nodes, and the form of communication—broadcast or unicast. These three features were thoroughly examined using machine learning. The simulation in this study comprised only seven nodes, with only one of them acting as the attacker. In future research, a larger network may be established for a more comprehensive analysis, potentially involving multiple attacker nodes. This will make it possible to analyze network data when there are several attacker nodes present and to analyze blackhole attacks in larger networks in greater detail. By accurately recognizing and categorizing potential security threats within network traffic data, the system empowers network administrators to take proactive actions in mitigating possible attacks. This contributes to an overall enhancement in network system security, reducing the likelihood of data breaches or other security incidents. Using our generated dataset, we compare the performance of our proposed method, called ADS-SVM, for detecting blackhole attacks in MANETs with J48 classifier and NB classifier. We find that ADS-SVM performs better. Specifically, ADS-SVM outperforms the other methods with an impressive detection accuracy of 99.96%. Even with its lower detection accuracy of 99.2%, the J48 classifier is still quite good compared to ADS-SVM. The NB classifier, meanwhile, only manages 96.5% detection accuracy. These results suggest that ADS-SVM is an effective approach for identifying blackhole attacks in MANETs and may be more accurate than other approaches currently in use.

ACKNOWLEDGMENT

This paper is supported by Korean Agency for Technology and Standard under Ministry of Trade, Industry and Energy in 2023, project numbers are 1415181638 (Establishment of standardization basis for BCI and AI Interoperability), 1415181629 (Development of International Standard Technologies based on AI Learning and Inference Technologies), and 1415181629 (Development of International Standard Technologies based on AI Model Lightweighting Technologies).

REFERENCES

[1] Ghildiyal, S., Srivastava, D., Mall, S., Sharma, V., Gupta, A., Manish, M., Kumar, S. (2023). Performance optimization of multi-node density using random mobility model in mobile adhoc network. AIP Conference Proceedings, 2771(1): 020059. https://doi.org/10.1063/5.0152315

[2] Qazi, F., Khan, S.A., Hanif, F., Agha, D.E.S. (2024). Efficient routing algorithm towards the security of vehicular AD-hoc network and its applications. International Journal of Wireless Information Networks, 31(1): 12-28. https://doi.org/10.1007/s10776-023-00613-x

[3] Kommineni, K.K., Prasad, A. (2023). A review on privacy and security improvement mechanisms in MANETs. International Journal of Intelligent Systems and Applications in Engineering, 12(2): 90-99.

[4] Sbayti, O., Housni, K., Hanin, M.H., El Makrani, A. (2023). Comparative study of proactive and reactive

routing protocols in vehicular AD-hoc network. International Journal of Electrical & Computer Engineering (2088-8708), 13(5).

[5] Mukti, F.S., Lorenzo, J.E., Zuhdianto, R., Junikhah, A., Soetedjo, A., Krismanto, A.U. (2021). A comprehensive performance evaluation of proactive, reactive and hybrid routing in wireless sensor network for real time monitoring system. In 2021 International Conference on Computer Science and Engineering (IC2SE), Padang, Indonesia, pp. 1-6. https://doi.org/10.1109/IC2SE52832.2021.9791992

[6] Li, X., Wang, Y. (2022). A novel hybrid anomaly detection algorithm for MANETs based on machine learning. Journal of Network and Computer Applications, 2022: 1030.

[7] Mezher, A.E., AbdulRazzaq, A.A., Hassoun, R.K. (2023). A comparison of the performance of the ad hoc on-demand distance vector protocol in the urban and highway environment. Indonesian Journal of Electrical Engineering and Computer Science, 30(3): 1509-1515. https://doi.org/10.11591/ijeecs.v30.i3.pp1509-1515

[8] Ramphull, D., Mungur, A., Armoogum, S., Pudaruth, S. (2021). A review of mobile ad hoc network (MANET) protocols and their applications. In 2021 5th International conference on intelligent computing and control systems (ICICCS), Madurai, India, pp. 204-211. https://doi.org/10.1109/ICICCS51141.2021.9432258

[9] Prasanna, S., Lenka, M.R., Swain, A.R. (2024). A survey on routing protocols for disaster management. SN Computer Science, 5(2): 216. https://doi.org/10.1007/s42979-023-02509-2

[10] Zhang, H., Feng, J., Zhou, B. (2023). An adaptive anomaly detection framework for MANETs using ensemble learning. IEEE Transactions on Mobile Computing, 22(1): 120-132.

[11] Sharma, S., Kaushik, B.K. (2023). A comprehensive review on intrusion detection in MANETs: Trends, challenges, and future directions. Computer Networks, 226: 107406.

[12] Chugh Majumder, S., Bhattacharyya, D., Chakraborty, S. (2024). Mitigation of wormhole attack in MANET using Cryptic-AODV: A modified routing protocol. International Journal of Intelligent Systems and Applications in Engineering, 12(1): 619-627.

[13] Macedo, D.F., Guedes, D., Vieira, L.F., Vieira, M.A., Nogueira, M. (2015). Programmable networks—From software-defined radio to software-defined networking. IEEE Communications Surveys & Tutorials, 17(2): 1102-1125. https://doi.org/10.1109/COMST.2015.2402617

[14] Sivapriya, N., Mohandas, R. (2022). Analysis on essential challenges and attacks on MANET security appraisal. Journal of Algebraic Statistics, 13(3): 2578-2589.

[15] Nawir, M., Amir, A. (2023). Secure AODV protocol against black hole attack in MANETs. IEEE Access, 11: 13456-13468.

[16] Yogarayan, S. (2021). Wireless ad hoc network of MANET, VANET, FANET and SANET: A review. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 13(4): 13-18. https://jtec.utem.edu.my/jtec/article/view/6119.

[17] Kushwaha, P., Mishra, A., Sharma, V. (2022). Detection and mitigation of black hole attack in MANET using machine learning techniques. International Journal of Distributed Sensor Networks, 18(8): 1-12.

[18] Verma, P., Kumar, A. (2022). Secure routing protocol using watchdog mechanism to detect and mitigate black hole attack in MANETs. Ad Hoc Networks, 124: 102667.

[19] Choudhary, R., Yadav, D. (2023). Cooperative bait detection scheme with honeypot to mitigate black hole attack in mobile Ad-hoc networks. Journal of Network and Systems Management, 31(2): 289-308.

[20] Sarao, P. (2022). Performance analysis of MANET under security attacks. Journal of Communications, 17(3): 194-202.

[21] Gupta, N., Sharma, S. (2023). Machine learning-based intrusion detection system to mitigate black hole attack in MANET. Wireless Networks, 35(2): 703-715.

[22] Ponnusamy, M. (2021). Detection of selfish nodes through reputation model in mobile adhoc network-MANET. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9): 2404-2410.

[23] Malik, A., Sharma, V. (2022). Secure AODV protocol using cryptographic techniques to mitigate black hole attack in MANETs. Wireless Personal Communications, 125(4): 2789-2803.

[24] Shao, W., Rajapaksha, P., Wei, Y., Li, D., Crespi, N., Luo, Z. (2023). COVAD: Content-oriented video anomaly detection using a self-attention-based deep learning model. Virtual Reality & Intelligent Hardware, 5(1): 24-41. https://doi.org/10.1016/j.vrih.2022.06.001

[25] Dave, D., Dave, P. (2014). An effective black hole attack detection mechanism using Permutation Based Acknowledgement in MANET. In 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India, pp. 1690-1696. https://doi.org/10.1109/ICACCI.2014.6968417

[26] Garg, N., Bawa, S. (2023). Collaborative approach to detect and mitigate black hole attack in mobile Ad-hoc networks. Wireless Personal Communications, 128(2): 1043-1059.

[27] Chen, X., Liu, Q., Ma, Y. (2022). Context-aware anomaly detection in mobile ad hoc networks: A deep learning perspective. Ad Hoc Networks, 129: 102814.

[28] Kaur, J., Kumar, S. (2022). Mitigating black hole attack in mobile Ad-hoc networks using fuzzy logic. International Journal of Computer Networks and Communications Security, 10(6): 143-151.

[29] Yasin, M.B., Khamayseh, Y.M., AbuJazoh, M. (2016). Feature selection for black hole attacks. Journal of Universal Computer Science, 22(4): 521-536. http://dx.doi.org/10.0416/j.jucs.2016.04.005

[30] Patil, V., Kulkarni, U. (2022). Secure routing protocol for mitigating black hole attack in MANETs. Ad Hoc Networks, 122: 102612.

[31] Rathod, D., Sharma, S. (2023). Reputation-based approach to detect and mitigate black hole attack in MANET. Journal of Network and Computer Applications, 195: 103301.

[32] Ibrahim, I., Abdulazeez, A. (2021). The role of machine learning algorithms for diagnosing diseases. Journal of Applied Science and Technology Trends, 2(1): 10-19. https://doi.org/10.38094/jastt20179

[33] Sharifi, B., Sharifi, M. (2021). Spectrum allocation to protect cognitive radio ad hoc networks against malicious users. Wireless Communications and Mobile

Computing, 2021: 5595204.
[34] Khan, M.A., Javaid, N. (2022). Fuzzy logic-based mechanism to detect and mitigate black hole attack in MANETs. IEEE Transactions on Vehicular Technology, 71(11): 12456-12468.
[35] Singh, A., Kumar, V. (2023). Intrusion detection system to mitigate black hole attack in mobile Ad-hoc networks. Wireless Networks, 29(3): 1021-1035.
[36] Gill, H., Mahajan, R. (2022). Cooperative bait detection scheme to mitigate black hole attack in MANET. Journal of Communications and Networks, 24(6): 567-578.
[37] Jain, S., Sharma, G. (2023). Secure routing protocol for MANET to detect and mitigate black hole attack. IEEE Transactions on Mobile Computing, 22(5): 1789-1801.
[38] Rabiaa, N., Moussa, A.C., Sofiane, B.H. (2023). A cross-layer method for identifying and isolating the blackhole nodes in vehicular ad-hoc networks. Information Security Journal: A Global Perspective, 32(3): 212-226. https://doi.org/10.1080/19393555.2021.2007316
[39] Shafi, S., Mounika, S., Velliangiri, S.J.P.C.S. (2023). Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. Procedia Computer Science, 218: 2309-2318. https://doi.org/10.1016/j.procs.2023.01.206
[40] Rani, P., Kavita, Verma, S., Rawat, D.B., Dash, S. (2022). Mitigation of black hole attacks using firefly and artificial neural network. Neural Computing and Applications, 34(18): 15101-15111. https://doi.org/10.1007/s00521-022-06946-7