

---

# Journal of Informatics and Web Engineering

Vol. 4 No. 2 (June 2026)

eISSN: 2821-370X

---

## Detecting Black Hole Attack using Support Vector Machine with XGBoosting in Mobile Ad-Hoc Networks

Anhar Al Madani<sup>1</sup>, Saima Anwar Lashari<sup>2</sup>, Sana Salah Uddin<sup>3</sup>, Abdullah Khan<sup>4, 5\*</sup>, Muhammad Nouman Atta<sup>6</sup>, Dzati Athiar Ramli<sup>7</sup>

<sup>1,2</sup>College of Computing and Informatics, Saudi Electronic University, Riyadh, Kingdom of Saudi Arabia

<sup>3,4,6</sup>Institute of Computer Science and Information Technology, University of Agriculture Peshawar, Pakistan

<sup>5,7</sup>Intelligent Biometrics Group (IBG), School of Electrical and Electronic Engineering, USM Engineering Campus, University Sains Malaysia, 14300 Nibong Tebal, Pulau Pinang, Malaysia

\*corresponding author: (abdullah\_khan@aup.edu.pk; ORCID:0000-0003-1718-7038)

**Abstract** - Mobile Ad-Hoc Networks (MANET) is a type of ad-hoc networks which use less infrastructure, that means the nodes in this network forward the messages without the need of infrastructure such as routers, switches etc. One of the most used attacks that can affect MANET performance is the black hole attack. This attack leads to dropping the packets that means these packets will never arrive and it will decrease the delivery ratio for the packets. This attack is a real problem as the sender is not informed that the data has not reached the intended receiver. The main goal of this study is to propose a solution for detecting black hole attacks using Extreme Gradient Boosting (XGBoost) based on a Support Vector Machine (SVM), the system for detection seeks to examine network traffic and spot anomalies by examining node activities. Attacking nodes in black hole situations exhibit specific behavioural traits that set them apart from other nodes, the traffic under a black hole attack is created using an Network Simulator-2(NS-2) simulator to test the effectiveness of this strategy, and the malicious node is then identified based on the classification of the traffic into malicious and non-malicious. The results of the proposed technique outperformed the existing machine learning techniques such as Neural Network (NN), SVM, k-Nearest Neighbors (KNN), Decision Tree (DT), Logistic Regression (LR), Random Forest (RF), AdaBoost-SVM in terms of accuracy score as it achieved 98.67% as well as other classification performance measures (Precision, Recall, and F-measure).

**Keywords**— Mobile Ad-Hoc Networks, Black-Hole Attack, XGBoost, Support Vector Machine, Ad-hoc Network, Network Simulator-2

*Received: 30 January 2025; Accepted: 1 April 2025; Published: 16 June 2025*

*This is an open access article under the [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.*



## 1. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) are decentralized wireless systems where mobile nodes communicate without relying on a central base station. Each node functions as both a host and a router, making security a critical concern due to the lack of centralized control [1], [2]. One of the most dangerous attacks in the network, is the black hole attack when a malicious network node intentionally discards or consumes all incoming packets, essentially causing a black hole in the network [3], [4]. This type of attack, especially when it comes to wireless ad-hoc and sensor networks, can have substantial effects on the network's performance and dependability [5]. The main motivation behind this study is to enhance the performance of detecting the black hole attack based on machine learning [6], [7] black hole attacks in a network can be more accurately detected with the help of ensemble methods and machine learning [8]. A huge dataset of network traffic can be used to train machines learning algorithms to find trends and anomalies connected to black hole attacks [9]. Once taught, these algorithms are highly accurate in analysing real-time network data and spotting possible black hole assaults [10].

Supervised learning algorithms, such as SVM [11], [12], RF [13], and NN [14] have proven effective in detecting black hole attacks. These algorithms can be trained on labelled datasets to identify patterns indicative of malicious behaviour, making them valuable tools for enhancing network security. A labelled dataset of network traffic that contains both regular and black hole attack traffic can be used to train these algorithms, based on characteristics of the traffic, including packet size, source and destination addresses, and protocol type. This algorithm teaches to categorize incoming traffic into one of these two groups. Machine learning method called boosting combines several weak models to get a strong model. The fundamental principle of boosting is to train a series of weak models iteratively, each of which concentrates on the data points that the preceding models have misclassified, with the expectation that the combination of these models will result in a more accurate forecast [15]. Boosting can be used to iteratively train a classifier, like a SVM on misclassified data, effectively giving more weight to misclassified instances and improving the accuracy of the classifier over time. This improves the performance of a single detection algorithm [16].

A set of mobile devices [17], is called MANET, which communicate with less Central Processing Unit (CPU) processing and the characterization of low power storage, through wireless medium, and memory starvation. Different attacks can affect the MANET such as Man in the Middle attack, synchronization flooding attack and spatially black hole attack. The black hole attack can cause serious dangers [4] as this attack drops the traffic headed to a specific destination, that the data packets were not delivered to the destination through it without informing the source node. The lack of network infrastructure services restricts wireless security, thus it must increase the security [18]. Meanwhile, different ensemble methods such as bagging, stacking, and boosting have been used to address black hole attack. Researchers have emphasizes that include boosting ensemble methods will enhance the classification performance of the machine learning and the accuracy, the author explained in the current study that using an adaptive boosting with SVM as a classifier has better accuracy results than using machine learning as a classifier [16]. However, there are more powerful boosting methods such as gradient boosting and extreme gradient boosting. The more robust the method is used, the more accurate and better the results. To send and receive messages in MANET the routing protocols such as ad-hoc on-demand multipath distance vector routing protocol (AOMDV) need to be used. The type of protocol depends on some specific requirement such as energy efficiency and scalability. The researcher has emphasized that using the extension of Low Energy Adaptive Clustering Hierarchical routing protocol (LEACH) can provide better results in the network lifetime [19]. This study focuses on overcoming the unbalanced dataset using XGBoost is a highly optimized implementation of the gradient boosting algorithm that is designed to be both fast and accurate. It has many features that make it well-suited for handling unbalanced datasets, such as the ability to assign different weights to different classes and the ability to handle missing data, Therefore this study focuses on exploring the detection of black hole attack using XGBoost and SVM as a classifier including an extension AOMDV protocol also it will focus on different parameters such as accuracy, TP, FP, Precision, Recall, and F-measure. The main contribution of this paper as given as below:

- To design the MANET that contains wireless links and nodes and simulates the black hole attack.
- To implement the Support vector machine as a classifier to find the dropped packets then use XGBoosting to predict the bad node number.
- To evaluate the proposed technique in terms of accuracy, F1 score, precision score, and recall score, and compared with the existing techniques such as RF classifier, DT Classifier, and Ada boosting-SVM.

The remainder of this work is broken into the following sections. Section 2 discusses the literature Review. Section 3 provides details of the proposed methodology. Section 4 discusses the results of realistic scenario-based studies. Section 5 presents the conclusion and future work.

## 2. LITERATURE REVIEW

The ad-hoc network can be conceptualized as a collection of dispersed wireless nodes that connect via a wireless communication medium without the use of any infrastructure, such as routers, access points, etc. To overcome the infrastructure absence barrier, these nodes must have a specific set of characteristics, such as routing protocol performance, computing power, and transmission range. Despite the strength of ad-hoc applications, topology changes, the mobility node density, network longevity, radio propagation, processing capacity, power consumption, and localization of these sorts of networks restrict their possibilities, Figure 1 shows different types of ad-hoc networks such as MANET [20], Vehicular \_ANET [21], FANE [22], Underwater Vehicle (UWVANET) [23].

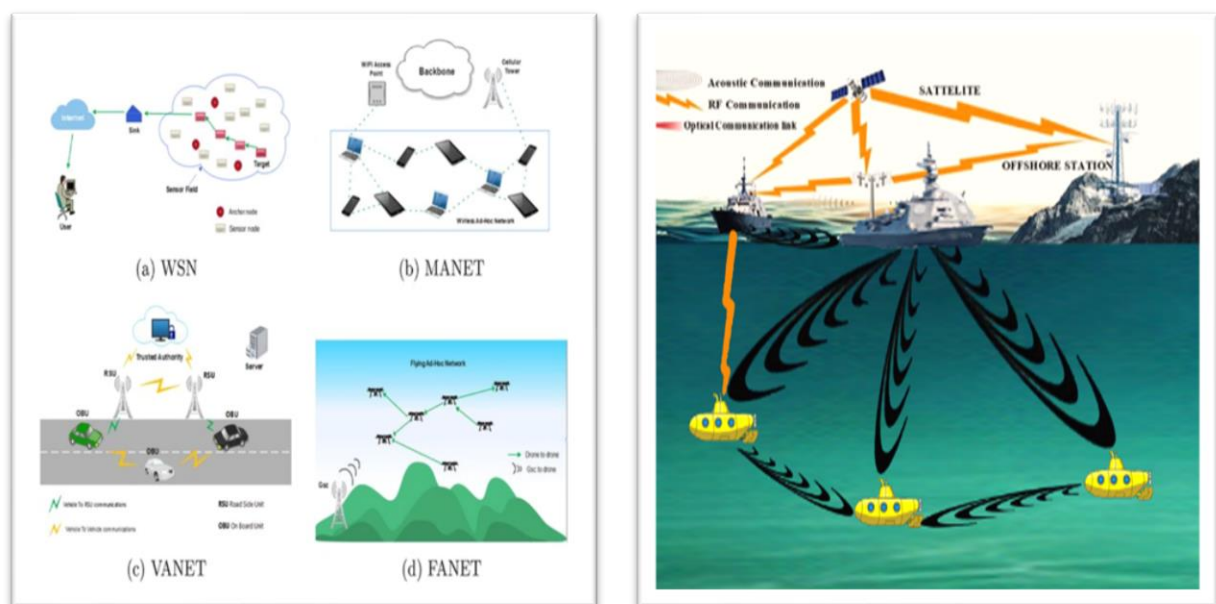


Figure 1. Ad-hoc Network Classification [18]

An unmanned aerial vehicle (UAV) or drone-based ad-hoc network is known as a Flying Ad-Hoc Network (FANET). These drones form a network that wirelessly communicates with one another and can be used for many purposes, including surveillance, search and rescue missions, and environmental monitoring. When conventional communication networks are unavailable or unstable, as is the case in distant places or disaster areas, FANETs can be employed. In a FANET, the drones can serve as relays, transmitting data from one drone to the next until it reaches its target. This enables long-distance communication without the use of infrastructure like cell towers or satellites [24]. Vehicle Ad-Hoc Network (VANET) is a system for vehicle-to-vehicle and vehicle-to-roadside infrastructure communication [21].

Due to its potential to increase traffic efficiency and road safety, VANETs are a fast-developing topic of study. Vehicles in VANETs are fitted with wireless communication equipment that enables them to interact with other vehicles as well as the infrastructure along the roadside. To minimize crashes and optimize routes, vehicles can communicate with one another to exchange information on the flow of traffic, potential hazards on the road, accidents, traffic lights, road signs, and other pertinent [25]. An ad-hoc network called an Underwater Vehicle Ad-Hoc Network (UWVANET) is made for communication between underwater vehicles. Underwater vehicles can connect with other underwater devices like sensors and robots in UWVANET due to communication tools like acoustic modems. The main difference between the other three types of ad-hoc network, and UWVANET is the communication methods

used. Where UWVANET use the Acoustic communication, in which communication depends upon Acoustic signals, which can be thought as dealing with the mechanics of waves in the fluids [18].

A MANET allows mobile devices to communicate with each other using some routing protocols. Each network node can function as both a host and a router, passing data packets to and from other nodes. The network architecture can vary dynamically when the devices move in and out of range or join and leave the network, the gadgets can roam around freely. Because many services include information transmission, security issues have become more important in MANET, and their dynamic nature makes them vulnerable to a variety of assaults. Security in the mobile ad-hoc network is a significant concern because there is no central authority to control the different nodes functioning in the network. Attacks may come from the network or from outside it, there are three types of black hole attacks based on the number of the malicious node quantity and there are two main attacks in Mobile Ad-Hoc Networks MANET, the passive attack and the active attack [6]. It does not interfere with the nodes' ability to communicate, but it does intercept and read packets and chats sent by unauthorized nodes. Radio Frequency spectrum is largely used by mobile nodes in MANETs for communication and broadcast networks. As a result, it is possible to eavesdrop on packets being transmitted and to intercept, copy, store, or analyse data packets [26]. One of the most significant attacks that can harm MANET network is the black hole attack, in the black hole attack data packets are drawn to the malicious node from other nodes in the network by its misleading claim to have the quickest path to the target[5]. The malicious node either drops the data packets to stop them from reaching the target, or it can alter the packets before sending them on. Other nodes may route their packets through the black hole node if it advertises that it has a new path to the target [9]. A black hole attack in MANET refers to a security risk in which a hostile node in the network drops or discards all data packets that it receives from other nodes in the network. To draw traffic to itself, the malicious node presents itself as having the shortest route to the destination [12].

However, it drops the packets it receives rather than passing them on to the following hop as shown in Figure 2. In a MANET, a black hole attack can be divided into the following steps. First by broadcasting bogus Route Request (RREQ) packets, the malicious node claims to have the shortest route to the target node. Second neighbouring nodes change their routing tables to add the malicious node as the next hop to the destination when they get the RREQ packet, then believing that the malicious node is the quickest path to the target, other nodes in the network begin transmitting packets to it. By dropping every packet it receives, the rogue node effectively creates a "black hole" in the network where all communications vanish, as a result, the packets are never sent to the intended node, and node to node communication is interfered with. MANETs are susceptible to a variety of attacks, including black hole attacks that can obstruct node-to-node communication [27].

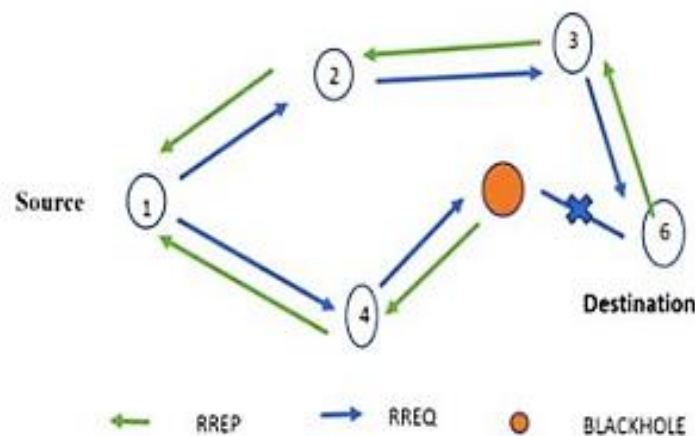


Figure 2. Black Hole Attack [12]

XGBoost is an optimized implementation of gradient boosting that uses a combination of tree-based learners and regularization, parallel processing, to improve performance. XGBoost is a type of boosting algorithm that has been shown to outperform AdaBoost (Adaptive Boosting) in many cases, XGBoost is designed to be highly scalable and can handle large datasets with many features. It also has the efficient implementation of parallel processing, which makes it faster than AdaBoost [15].

Various research studies reviewed focus on various approaches to improving network security, particularly in detecting and mitigating blackhole (BH) attacks using NS-2. [28] proposed the Integrated Cross Interior (ICI) structure, which reduced response time (6.3 ms) and increased throughput (83.5%) but lacked parallelization, affecting performance. Similarly [29] introduced local data exchange for BH attack detection, demonstrating effectiveness with a low false detection rate. Further in [30] implemented an advanced AOMDV protocol with homomorphic encryption, improving packet delivery ratio (PDR) and throughput but suffering from high end-to-end delay. [31] introduced Trust Embedded AODV, ensuring real-time blackhole attack prevention but generating excessive control packets in link failures, reducing QoS. Where else [32] utilized machine learning for BH attack detection but struggled to differentiate attacks from normal network fluctuations. [33] proposed ML-AODV with ANN and SVM, enhancing reliability (44%) and reducing delay (12%), but its performance suffered in urban settings with dynamic node density. Furthermore, [9] introduced NA-DE inspired by dolphin echolocation, enabling early BH attack detection and reducing energy usage but depending on accurate sensory data. Lastly, [34] applied deep learning models for intrusion detection, improving classifier efficacy but requiring high-quality training data for optimal performance. Table 1 presents a comparison of existing black hole attack detection techniques in terms of complexity, computational cost, and scalability.

Table 1. Comparison of Existing Black Hole Attack Detection Techniques in Complexity, Computational Cost, and Scalability

Detection Technique	Complexity	Computational Cost	Scalability
Integrated Cross Interior (ICI) for IDS [28]	Uses secure routing mechanisms and packet prioritization	Minimal routing cost and fast response time (6.3 ms)	Demonstrates high throughput (83.5%) and low overhead
Trust-Based Security [31]	Monitors node behaviour and assigns trust scores	Requires continuous trust evaluation, increasing processing load	Adapts dynamically to network conditions but may struggle in highly mobile scenarios
AODV-BS with Cryptographic Verification [35]	Uses cryptographic verification and threshold evaluation	Encryption and decryption add significant overhead	Protects against internal attacks but require further enhancement for external threats
Adaptive Detection Using Local Data Exchange [29]	Improves sequence number-based detection using local data exchange	Reduces attack success rates with minimal overhead	Performance depends on threshold settings and network size
AOMDV with Homomorphic Encryption [30]	High – Uses encryption-based multipath routing to enhance security	High – Computationally expensive due to encryption overhead	Medium – Improves PDR and throughput but needs further optimization for real-time applications
Machine Learning-Based AODV [33]	High Uses ANN and SVM for trust-based route selection	High Model training, feature selection, and real-time classification increase computational cost	High Optimized routing improves network performance and security
NA-DE (Dolphin Echolocation Model) [9]	High Context-based node acceptance system for early attack detection	Medium Balances security and performance without excessive overhead	High Scales well, effective even with 250 nodes
Smart IDS with Deep Learning [34]	Very High – Uses deep learning models with feature selection and adaptive algorithms	Very High – Requires high processing power but optimizations (AOMA) improve efficiency	High – Deep Supervised Learning Classification (DSLCL) ensures robust scalability

### 3. PROPOSED METHODOLOGY

Figure 3 illustrates the proposed methodology which comprises four phases namely: data generation, SVM, XGBoosting, and evaluation matrix such as accuracy, F1 score, precision score, and recall score.

#### 3.1 Data Generation

The data was generated using the NS-2 simulator, to simulate the normal traffic and the black hole attack in MANET using 33 nodes, and the AOMDV (AD-HOC ON-DEMAND MULTIPATH DISTANCE VECTOR ROUTING PROTOCOL), is an improved of AODV, and The Multipath Routing Protocol AOMDV finds several routes from source to destination. AOMDV offers the same route discovery and route maintenance services as AODV. AOMDV similarly bases its route-finding process on the distance vector notion and uses on-demand route discovery," AOMDV protocol routing tables provide a route list, destination, sequence number, and advertised hop count. The route list includes extra details for each alternative route, such as the next hop, the previous hop, the number of hops, and the timeout.

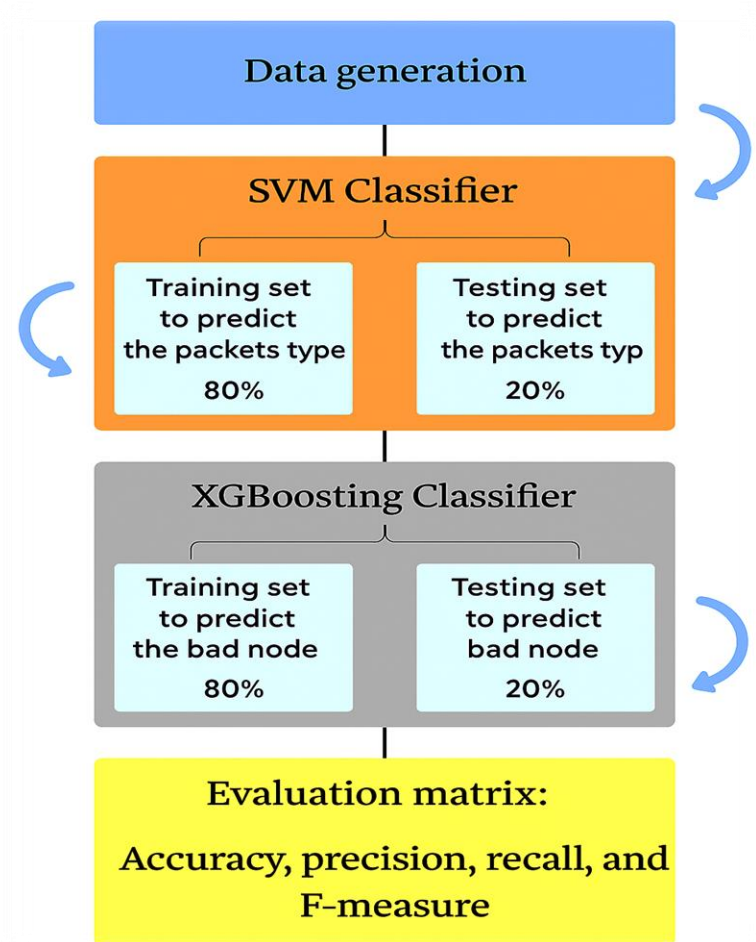


Figure 3. Proposed Methodology

The dataset divided into 80% training dataset and 20% testing dataset, some of the features that can be used to detect black hole attacks include Packet delivery ratio (PDR) and it is a performance metric used to evaluate the quality of service (QoS) provided by a communication network, It measures the percentage of packets that are successfully delivered from a source node to a destination node, relative to the total number of packets sent by the source, also the Packet loss rate (PLR) and it is a performance metric used to measure the percentage of packets that are lost or dropped during transmission between a source and a destination node in a communication network, and packet delay and it is a performance metric that measures the time taken for a packet to travel from the source node to the destination node

in a communication network, these features can be computed from the trace file. Table 2 illustrates the proposed MANET parameter simulation settings.

Table 2. The Proposed MANET Parameter Simulation

Parameter	Value
MAC-Protocol	IEEE 802.11
Model of Antenna	Omni-Directional
The scale of MANET Network	1500m × 1500m
Simulation Time	150 sec
MAC Type	802.11
Traffic	CBR
Routing Protocol	AOMDV
Size Of Packet	1000Bytes/packet
Data Rate	0.1Mbps
Node Placement	Random
Node Movement	Random
Node Velocity	5-20m/s
Pause Time	1 sec
No. of Mobile Nodes	33
No. of Attackers	1
Observation Parameter	Jitter, PDF, End-to-end Delay, Throughput

In this phase data has been generated using NS-2 simulator based on the parameters shown in Table 3, using Ubuntu to set up ns.2 simulator. There are two simulations that have been done using the same parameters to show the different observation parameters as shown in Table 3. Sent packets refer to the number of packets generated by the source node and sent into the network, received packets refer to the number of packets that successfully reach their destination nodes after traversing the network, dropped packets refer to the number of packets that are discarded by the network due to congestion, errors, or other reasons, end-to-end delay refer to the time it takes for a packet to travel from the source node to the destination node. It includes the time spent in transmission, queuing, and processing delays at network nodes, and PDF stands for Probability Density Function. Which is a statistical measure that describes the distribution of a set of values. In NS2, PDF is often used to analyse the distribution of various network performance metrics, such as packet delay or throughput. The total packets dropped from the simulation with the black hole attack is more than the simulation without the black hole attack as shown in Table 3.

Table 3. Comparison of Black Hole and No Black Hole Simulation

	Without Black Hole	With Black Hole
Sent Packets	3129	3455
Received Packets	444	348
Dropped	2685	3107
E2E delay sec	1.47796	2.11703
PDF	14.1898	10.0724

Jitter and throughput are two important characteristics of network performance, as shown in Table 4, Jitter refers to the variation in the delay of network packets as they travel from one point to another. In other words, it is the amount of time difference between the expected arrival time and the actual arrival time of network packets, High levels of jitter can result in choppy or distorted audio and video, throughput, on the other hand, refers to the amount of data that can be transmitted over a network in each period. It is usually measured in bits per second (bps) or bytes per second (Bps). Throughput can be affected by several factors such as network congestion, packet loss, and network latency. High throughput means that more data can be transmitted in a shorter amount of time, which is important for applications that require high bandwidth, such as video streaming, file transfers, and online gaming. Figure 4 gives the details of comparison of Jitter, Throughput Black Hole and No Black Hole Simulation. The pseudocode is depicted in Algorithm 1.



Table 4. Comparison of Jitter, Throughput Black Hole and No Black Hole Simulation

	Without Black hole	With Black Hole
Jitter Sec	0.0279761	0.047282
Throughput Mb/s	0.444	0.348

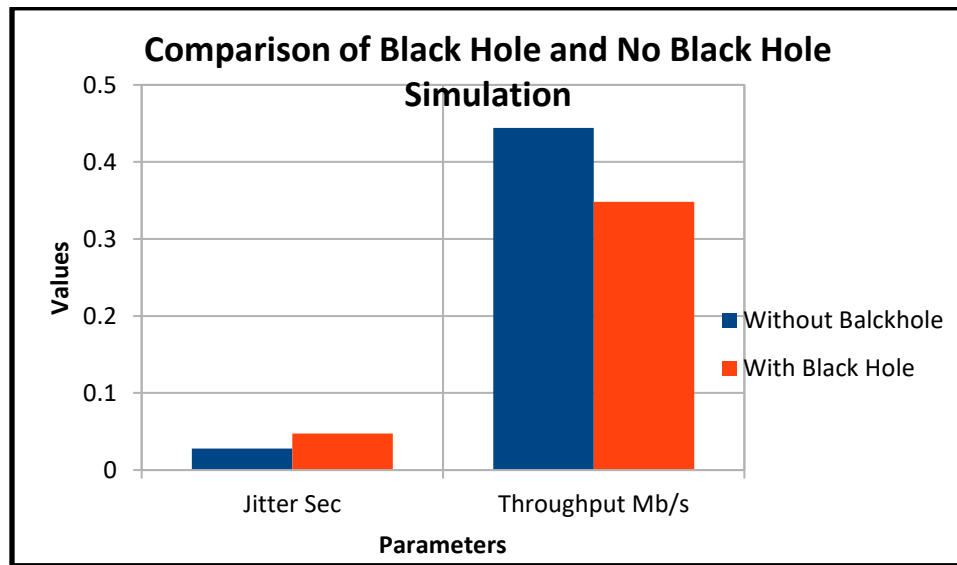


Figure 4. Comparison of Jitter, Throughput Black Hole and No Black Hole Simulation

---

#### Algorithm 1: A Step-by-Step NS-2 Simulator Setup for Black Hole Attack in MANET

---

##### Step 1: Setting Up the NS-2 Simulator Environment

- Install Ubuntu OS as the operating system.
- Install NS-2 simulator by downloading and compiling the NS-2 package.
- Configure the necessary Tcl (Tool Command Language) scripts to define the MANET simulation parameters.

##### Step 2: Defining the Network Parameters

- Define the simulation area as  $1500\text{m} \times 1500\text{m}$  to represent the MANET environment.
- Set the simulation time to 150 seconds to allow enough data collection.
- Specify 33 mobile nodes, where one node acts as an attacker to simulate the black hole attack.
- Use the AOMDV (Ad-Hoc On-Demand Multipath Distance Vector) routing protocol, which maintains multiple paths between source and destination to improve network resilience.
- Configure IEEE 802.11 MAC protocol to handle medium access control.
- Assign random node placement and movement, with velocities ranging from 5 m/s to 20 m/s and a pause time of 1 second to simulate a realistic mobile environment.
- Set the traffic type as Constant Bit Rate (CBR) with 1000 Bytes per packet and a data rate of 0.1 Mbps.

##### Step 3: Running the Simulation

- Create a Tcl script that initializes the simulation and defines the routing, mobility, and attack behavior.
  - Introduce a black hole attack by programming an attacker node to drop all received packets instead of forwarding them.
  - Execute the simulation using the NS-2 command-line interface.
-



- 
- d. Collect the output data in an NS-2 trace file, which logs network events such as sent, received, and dropped packets, delays, and throughput.

*Step 4: Dividing the Dataset*

- a. Process the generated dataset and divide it into 80% for training and 20% for testing to evaluate machine learning models.
- b. Extract key performance metrics from the trace file, including:
  - Packet Delivery Ratio (PDR): Measures the percentage of successfully received packets.
  - Packet Loss Rate (PLR): Indicates the proportion of lost packets.
  - End-to-End Delay (E2E): Represents the total delay from source to destination.
  - Jitter: Measures variations in packet arrival times.
  - Throughput: The rate of successfully transmitted data.

*Step 5: Comparing Performance with and Without Black Hole Attack*

- a. Conduct two separate simulations: one with a black hole attack and one without.
- b. Compare the results using Table 3, which shows the significant impact of black hole attacks:
  - Packets Dropped: Increased from 2685 (without attack) to 3107 (with attack).
  - Received Packets: Decreased from 444 to 348, showing a decline in successful data transmission.
  - End-to-End Delay: Increased from 1.47796 sec to 2.11703 sec, indicating slower communication.
  - Packet Delivery Fraction (PDF): Dropped from 14.18% to 10.07%, highlighting the attack's severity.

*Step 6: Analysing Jitter and Throughput Performance*

- a. Compare jitter and throughput using Table 4:
  - Jitter Increased: From 0.0279 sec to 0.0472 sec, leading to unpredictable network delays.
  - Throughput Decreased: From 0.444 Mbps to 0.348 Mbps, reducing the network's efficiency.
- b. Visualize these changes using Figure 4, which clearly shows the degradation in network quality due to the attack.

*Step 7: Conclusion and Future Enhancements*

- a. The simulation results confirm that black hole attacks severely disrupt MANET performance, increasing packet loss and delay while reducing throughput and reliability.
  - b. The use of AOMDV as a multipath routing protocol helps mitigate some negative effects, but additional intrusion detection systems (IDS) and security mechanisms are needed.
  - c. Future enhancements could involve implementing machine learning-based IDS to detect and prevent black hole attacks in real-time.
- 

### 3.2 SVM Classifier

SVM is a popular classification algorithm that attempts to find the best hyperplane that separates the different classes in the data. While SVM and XGBoost have different approaches to solving classification problems. It is possible to use them together in a pipeline to improve the overall performance, a way to use SVM to find the dropped packets, then using XGBoosting classifier to find the bad node as shown in Figure 5.

### 3.3 XGBoosting

XGBoost is a powerful classifier method that can produce highly accurate predictions, XGBoost can be used to find the bad node in the packets that dropped over transmitted in the network as shown in Figure 6.

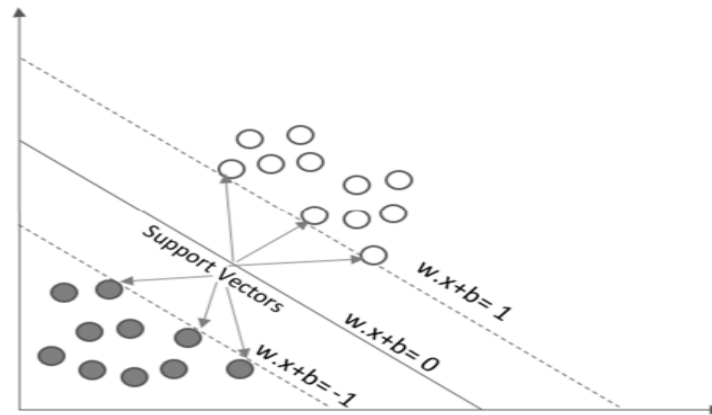


Figure 5. Support Vector Machine

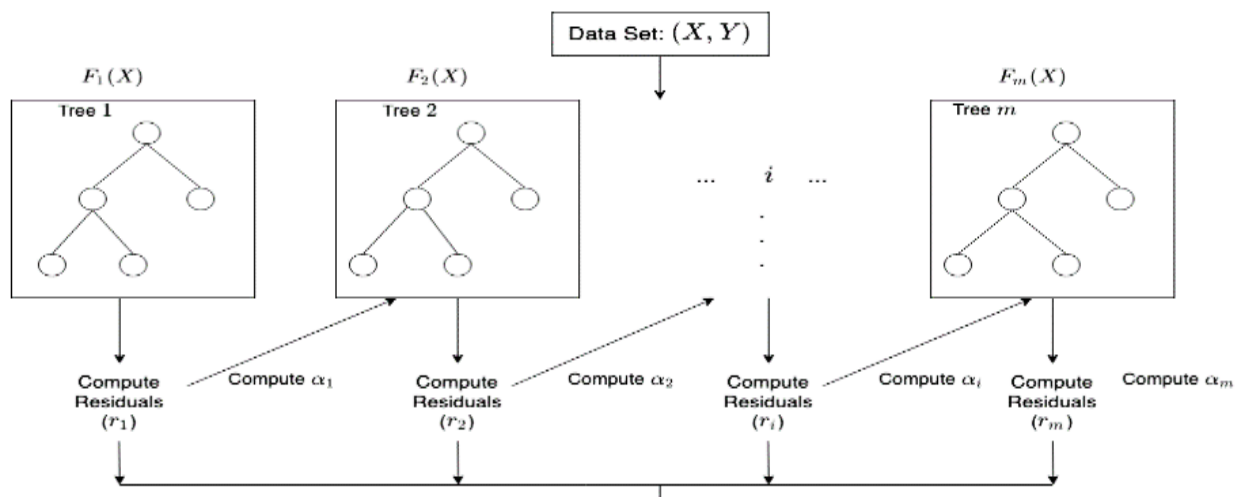


Figure 6. Illustration on How Gradient Tree Boosting Works

### 3.4 Evaluation Metrics

Evaluation metrics are used to measure the performance of machine learning models on a given task. The choice of evaluation metric depends on the specific task and the type of data being used. Evaluate the performance on a test set using appropriate evaluation metrics such as accuracy, precision, recall, and F-measure.

## 4. RESULTS AND DISCUSSION

This section will explain the simulation result of the proposed model used in this paper.

### 4.1 Proposed Technique

Table 5 presents a comparison between AdaBoost-SVM and the proposed XGBoosting-SVM model based on three key performance metrics: precision, recall, and F-measure. The proposed approach achieves a precision of 98%, recall of 98%, and an F-measure of 98%, outperforming AdaBoost-SVM, which records values of 94%, 97%, and 95%, respectively. Precision measures how accurately the model identifies black hole attacks, indicating a lower false positive rate for the proposed model. Recall assesses how well the model detects all possible attacks, and a higher recall means fewer missed detections. The F-measure, which balances precision and recall, confirms the overall reliability of the classification. The superior performance of the XGBoosting-SVM approach can be attributed to its combination of SVM and XGBoosting, where SVM effectively classifies malicious packets, and XGBoosting

identifies black hole nodes with high precision. This hybrid technique significantly improves detection accuracy while reducing false positives, making it a more robust solution than AdaBoost-SVM.

Table 5. Performance Evaluation of Adaboosting-SVM and the Proposed Technique

Technique	Precision	Recall	F-measure
Adaboosting-SVM	0.94	0.97	0.95
Proposed XGBoosting-SVM	0.98	0.98	0.98

Table 6 provides a broader comparison of machine learning models in detecting black hole attacks, highlighting how different techniques perform in terms of accuracy. Traditional machine learning models such as SVM, RF, DT, and LR as used by Tejaswini & Adilakshmi, demonstrate lower accuracy levels.

Table 6. Performance Evaluation of Proposed Technique with Machine Learning.

Author (s)	Technique(s)	Accuracy
Tejaswini & Adilakshmi [27]	SVM, RF, DT and LR	SVM 82.35%, RFC 88.23%, DT 82.35%, LR 88.23%
Hikala, et al [16]	Adaboost SVM	Accuracy 97%
Abadleh, et al [36]	RF	Accuracy 97.8%
	Proposed SVM with XGBoosting	Accuracy 98.67%

SVM and DT achieve only 82.35% accuracy, while RF and LR perform slightly better at 88.23%. These models struggle because they operate independently and lack ensemble learning mechanisms, making them less effective at distinguishing between normal and malicious nodes. The AdaBoost-SVM model, analysed by Hikala et al., improves upon traditional methods by achieving 97% accuracy, showing the benefits of boosting techniques in enhancing model performance. Similarly, RF, used by Abadleh et al. [36], performs slightly better than AdaBoost-SVM, achieving 97.8% accuracy due to its capability of handling complex decision-making processes. However, both AdaBoost-SVM and RF still fall short compared to the proposed XGBoosting-SVM model. The proposed XGBoosting-SVM model achieves the highest accuracy of 98.67%, surpassing all previous approaches. This superior performance is due to the combination of SVM's ability to identify malicious packets and XGBoosting strong feature selection and classification capabilities, which reduce false positives, improve classification accuracy, and enhance overall model robustness. Additionally, XGBoosting employs parallel processing and regularization techniques, ensuring better performance on large and imbalanced datasets, making it highly scalable for real-world applications.

In Figure 7 the results clearly indicate that XGBoosting with the SVM model achieves the highest accuracy at 98.67%, demonstrating its superior performance over other approaches. This is due to the combination of SVM for detecting malicious packets and XGBoosting for identifying the compromised nodes, which significantly enhances classification accuracy. Among other models, NN (95%) and standard SVM (97.5%) perform well but still fall short of the proposed hybrid model. Traditional machine learning models such as KNN (85%), DT (92.5%), and LR (88.23%) show relatively lower accuracy, indicating their limitations in handling complex network attacks. On the other hand, ensemble learning methods like RF (97.8%) and AdaBoost-SVM (97%) perform better than standalone classifiers, but they still do not match the effectiveness of XGBoosting with SVM. These results highlight those boosting techniques, particularly XGBoost, improve classification performance, making them more suitable for security applications in MANETs. The superior performance of the XGBoosting-SVM approach underscores its potential as a highly reliable and efficient solution for detecting black hole attacks, ensuring enhanced network security and robustness.

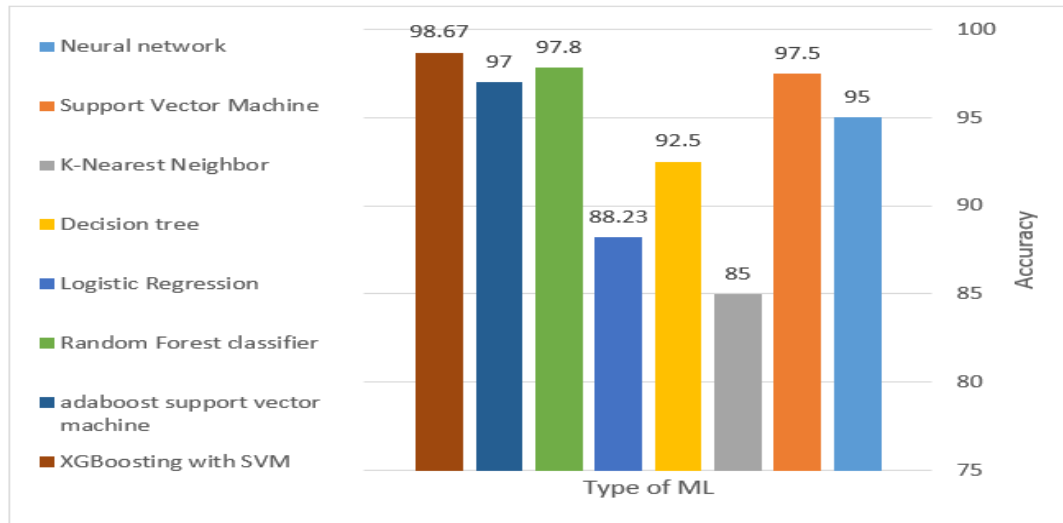


Figure 7. Comparative Analysis in Terms of Accuracy

## 5. CONCLUSION

Hackers are rapidly updating their techniques to carry out wormhole attacks in networks with great professionalism. Therefore, detection and prevention of this attack is a serious challenge and is considered a topic with many variables and requirements. Several machine learning approaches have been used to detect a black hole attack. In this study, SVM technique was implemented to find the packets that drop from the network and then XGBoosting technique was used to find the malicious node that dropped the packets and never delivered them and then compared it with other machine learning techniques using the default values of the hyperlink parameters defined by the Python scikit library package- Learn. As a result, the proposed SVM and XGBoosting technology outperformed other developed machine learning technologies (DT, LR, RF, SVM, and AdaBoost, SVM) in terms of performance metrics. This study was helpful to me in my future studies to continue in this field. In the future, the attack execution time and the number of malicious nodes that drop packets in the network will be increased, increase the time of the simulation will provide more transmission paths in the network and that will help to increase the training data and check if this could provide better attack detection. In this study, one malicious node applied and to increase the complexity of the network and checking the effectiveness of the proposed technique proposed the future study should increase the number of bad nodes.

## ACKNOWLEDGEMENT

The Authors would like to thank the University of Agriculture Peshawar and University and Sains Malaysia for supporting this research.

## FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this manuscript

## AUTHOR CONTRIBUTIONS

Anhar Al Madani: Methodology, Validation, Writing – Original Draft Preparation;  
 Saima Anwar Lashari: Conceptualization & Supervision;  
 Sana Salah Uddin: Literature Review;

Abdullah Khan: Project Administration;  
 Muhammad Nouman Atta: Writing & Review;  
 Dzati Athiar Ramli: Validation & Review.

## CONFLICT OF INTERESTS

The authors have no conflict of interests.

## ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. <https://publicationethics.org/>




## REFERENCES

- [1] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in Dynamic Mobile Ad Hoc Networks MANETs," *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pp. 28–33, Apr. 2019. doi: 10.1109/jeeit.2019.8717449.
- [2] P. Li, H. Wang, G. Tian, and Z. Fan, "A cooperative intrusion detection system for the internet of things using convolutional neural networks and black hole optimization," *Sensors*, vol. 24, no. 15, pp. 4766, Jul. 2024. doi: 10.3390/s24154766.
- [3] M. Yazdanypoor, S. Cirillo, and G. Solimando, "Developing a hybrid detection approach to mitigating black hole and gray hole attacks in mobile ad hoc networks," *Applied Sciences*, vol. 14, no. 17, pp. 7982, Sep. 2024. doi: 10.3390/app14177982.
- [4] W. Ali and S. Z. Ninoria, "An Efficient Algorithm for Black Hole Attacks Detection in VANET," in *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, 2024, vol. 7, pp. 893-898: IEEE. doi: 10.1109/IC3I61595.2024.10828590
- [5] D. A. Rashid and M. B. Mohammed, "Black hole attack detection in wireless sensor networks using hybrid optimization algorithm," *UHD Journal of Science and Technology*, vol. 8, no. 1, pp. 142–150, May 2024. doi: 10.21928/uhdjst.v8n1y2024.pp142-150.
- [6] A. Abdelhamid, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "A lightweight anomaly detection system for black hole attack," *Electronics*, vol. 12, no. 6, pp. 1294, 2023. doi: 10.3390/electronics12061294
- [7] M. Shukla, N. B. K. Joshi, and U. Singh, "A novel machine learning algorithm for MANET Attack: Black hole and gray hole," *Wireless Personal Communications*, vol. 138, no. 1, pp. 41–66, Aug. 2024. doi: 10.1007/s11277-024-11360-4.
- [8] S. M. Hassan, M. M. Mohamad, and F. B. Muchtar, "Advanced Intrusion Detection in MANETs: A survey of machine learning and optimization techniques for mitigating Black/Gray Hole Attacks," *IEEE Access*, pp. 1, Jan. 2024. doi: 10.1109/access.2024.3457682.
- [9] R. Vatambeti, S. V. Mantena, K. V. D. Kiran, S. Chennupalli, and M. V. Gopalachari, "Black hole attack detection using Dolphin Echo-location-based machine learning model in MANET environment," *Computers & Electrical Engineering*, vol. 114, pp. 109094, Jan. 2024. doi: 10.1016/j.compeleceng.2024.109094.
- [10] S. Gurung, and S. Chauhan, "A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability," *Wireless Networks*, vol. 26, no. 3, pp. 1981–2011, Feb. 2019. doi: 10.1007/s11276-019-01966-z.
- [11] A. A. Abdallah, M. S. Abdallah, H. Aslan, M.A. Abdallah, Y.-I. Cho, and M. S. Abdallah, "Enhancing mobile ad hoc network Security: An anomaly detection approach using Support Vector Machine for Black-Hole attack detection," *International Journal of Safety and Security Engineering*, vol. 14, no. 4, pp. 1015–1028, Aug. 2024. doi: 10.18280/ijssse.140401.
- [12] N. Panda, and M. Supriya, "Blackhole attack prediction in wireless sensor networks using support vector machine," in *Lecture notes in electrical engineering*, 2023, pp. 321–331. doi: 10.1007/978-981-19-8865-3\_30.




- [13] T. Nagalakshmi, and R. S. Kumar, "Comparative Analysis of Random Forest and Decision Tree for Gray Hole Attack Detection in Wireless Ad Hoc Networks," in *2024 IEEE International Conference on Smart Power Control and Renewable Energy (ICSPCRE)*, 2024, pp. 1-6: IEEE. doi: 10.1109/ICSPCRE62303.2024.10675140
- [14] S. Khan, M. A. Khan, and N. Alnazzawi, "Artificial Neural Network-Based Mechanism to detect security threats in wireless sensor networks," *Sensors*, vol. 24, no. 5, pp. 1641, Mar. 2024. doi: 10.3390/s24051641.
- [15] M. Alqahtani, A. Gumaiei, H. Mathkour, and M. M. B. Ismail, "A Genetic-Based extreme gradient boosting model for detecting intrusions in wireless sensor networks," *Sensors*, vol. 19, no. 20, pp. 4383, Oct. 2019. doi: 10.3390/s19204383.
- [16] N. A. Hikal, M. Y. Shams, H. Salem, and M. M. Eid, "Detection of black-hole attacks in MANET using adaboost support vector machine," *Journal of Intelligent & Fuzzy Systems*, vol. 41, no. 1, pp. 669–682, Jul. 2021. doi: 10.3233/jifs-202471.
- [17] M. Kumar, and R. Mishra, "An overview of MANET: History, challenges and applications," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 3, no. 1, pp. 121-125, 2012. ISSN : 0976-5166
- [18] A. R. S. A. Ragab, "A new classification for Ad-Hoc network," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 14, no. 14, pp. 214, Aug. 2020. doi: 10.3991/ijim.v14i14.14871.
- [19] H. Kalkha, H. Satori, and K. Satori, "Performance evaluation of AODV and LEACH routing protocol," *Advances in Information Technology: Theory and Application*, vol. 1, no. 1, pp. 112-118, 2016. ISSN 2489-1703
- [20] D. Wijonarko, S. Arifin, M. Faisal, M. N. Pratama, O. N. Priambodo, and E. S. Nugraha, "Mobile Ad-Hoc Network (MANET) Method: Some trends and open issues," *Recent in Engineering Science and Technology*, vol. 3, no. 2, pp. 49–74, Apr. 2025. doi: 10.59511/riestech.v3i2.108.
- [21] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Vehicular Communications*, vol. 28, p. 100310, Oct. 2020. doi: 10.1016/j.vehcom.2020.100310.
- [22] A. Mukherjee, V. Keshary, K. Pandya, N. Dey, and S. C. Satapathy, "Flying Ad hoc Networks: A Comprehensive Survey," in *Advances in intelligent systems and computing*, 2018, pp. 569–580. doi: 10.1007/978-981-10-7563-6\_59.
- [23] E. Wengle, J. Potter, and H. J. Dong, "Underwater Ad-Hoc Networks: A Review," *Authorea Preprints*, 2023. doi: 10.36227/techrxiv.17000266.v1
- [24] S. Lateef, M. Rizwan, and M. A. Hassan, "Security threats in Flying Ad hoc Network (FANET)," in *Studies in computational intelligence*, 2022, pp. 73–96. doi: 10.1007/978-3-030-97113-7\_5.
- [25] M. M. Hamdi, L. Audah, S. A. Rashid, A. H. Mohammed, S. Alani, and A. S. Mustafa, "A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs)," in *2020 international congress on human-computer interaction, optimization and robotic applications (HORA)*, 2020, pp. 1-7: IEEE. doi: 10.1109/HORA49412.2020.9152928
- [26] N. Sivanesan, and K. S. Archana, "A machine learning approach to detect network layer attacks in mobile ad hoc networks," *International Journal of Early Childhood Special Education*, vol. 14, no. 3, 2022.
- [27] K. Tejaswini, and M.Y. Adilakshmi, "Black hole Attack Detection Using Machine Learning Algorithms in MANET-Performance Comparison," *International Journal of Research and Analytical Reviews*, pp. 6047-6051, 2020. doi: 10.1109/ICESC48915.2020.9155770
- [28] J. Vinayagam, Ch. Balaswamy, and K. Soundararajan, "Certain Investigation on MANET Security with Routing and Blackhole Attacks Detection," *Procedia Computer Science*, vol. 165, pp. 196–208, Jan. 2019. doi: 10.1016/j.procs.2020.01.091.
- [29] T. Terai, M. Yoshida, A. G. Ramonet, and T. Noguchi, "Blackhole attack cooperative prevention method in manets," in *2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW)*, 2020, pp. 60-66: IEEE. doi: 10.1109/CANDARW51189.2020.00024
- [30] E. Elmahdi, S.-M. Yoo, and K. Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks," *Journal of Information Security and Applications*, vol. 51, pp. 102425, Jan. 2020. doi: 10.1016/j.jisa.2019.102425.
- [31] E. Lema, G. Esubalew, M. Desalegn, B. Tiwari, and V. Tiwari, "Trust Embedded AODV for securing and Analyzing Blackhole attack in MANET," in *2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)*, 2022, pp. 362-367: IEEE. doi: 10.1109/WIECON-ECE57977.2022.10150765

- [32] R. Gotti, A. Polagani, G. S. L. Posina, S. Veerapaneni, and T. Prasanth, "Detection and Analysis of Single Blackhole Node with TCP Connection in MANETs using Machine Learning Algorithms," in *2023 International Conference on Inventive Computation Technologies (ICICT)*, 2023, pp. 1704–1710: IEEE. doi: 10.1109/ICICT57646.2023.10134058
- [33] S. Shafi, S. Mounika, and S. Velliangiri, "Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET," *Procedia Computer Science*, vol. 218, pp. 2309–2318, Jan. 2023. doi: 10.1016/j.procs.2023.01.206.
- [34] M. S. Sheela *et al.*, "Adaptive Marine Predator Optimization Algorithm (AOMA)-Deep Supervised Learning Classification (DSL) Based IDS Framework for MANET Security," *Intelligent and Converged Networks*, vol. 5, no. 1, pp. 1–18, 2024. doi: 10.23919/ICN.2024.0001
- [35] P. R. B, B. R. B, and D. B, "The AODV routing protocol with built-in security to counter blackhole attack in MANET," *Materials Today Proceedings*, vol. 50, pp. 1152–1158, Aug. 2021. doi: 10.1016/j.matpr.2021.08.039.
- [36] A. Abadleh *et al.*, "Mitigating the Effect of Blackhole Attacks in MANAT," *Journal of Engineering Science & Technology Review*, vol. 15, no. 6, 2022. doi: 10.25103/jestr.156.13

## BIOGRAPHIES OF AUTHORS

	<p><b>Saima Anwar Lashari</b> was born in 1985 in the Punjab province of Pakistan. She began her PhD at University Tun Hussein Onn Malaysia (UTHM) in late 2010, specializing in information technology. Under the expert supervision of Professor Dr. Rozati Ibrahim, she embarked on her research journey. Currently, she serves as an assistant professor at the College of Computing and Informatics, Saudi Electronic University, Riyadh, KSA. She has published numerous research articles in areas such as optimization, mathematics, neural networks, data mining, prediction, and deep learning. Her primary research interests include knowledge-based systems, data mining, optimization, prediction, and web mining. She is contactable at s.lashari@seu.edu.sa</p>
	<p><b>Anhar Al Madani</b> is a BS student at Saudi Electronic University, Riyadh, KSA. He began his research journey under the professional supervision of Professor Dr. Saima Anwar Lashari. Currently enrolled in the College of Computing and Informatics at Saudi Electronic University, he has started working in the research fields of prediction and web mining. He is contactable at s.lashari@seu.edu.sa</p>
	<p><b>Abdullah Khan</b> was born on February 6, 1985, in Dir (Lower), KPK province, Pakistan. He completed his BSc degree at Malakand University between 2004 and 2006. In 2006, he pursued an MSc in Computer Science at the University of Science and Technology, Bannu, KPK, Pakistan. At the end of 2010, he enrolled at University Tun Hussein Onn Malaysia (UTHM) to pursue a PhD in Information Technology. Under the professional supervision of Professor Dr. Nazri Mohd. Naw, he embarked on his research journey. Currently, he is an assistant professor at the Institute of Computer Sciences and Information Technology, Faculty of Management and Computer Sciences, at the University of Agriculture, Peshawar, Pakistan. He has published numerous research articles in the fields of optimization, metaheuristics, neural networks, data mining, prediction, and deep learning. His primary research interests include hybrid neural networks, knowledge-based systems, data mining, deep learning, optimization, prediction, and web mining. He is contactable at Abdullah_khan@aup.edu.pk</p>



	<p><b>Muhammad Nouman Atta</b> completed his BSc in Computer Science at the University of Agriculture, Peshawar, Pakistan, from 2016 to 2020. In 2021, he pursued an MS in Computer Science at the same university. Under the professional guidance and supervision of Assistant Professor Dr. Abdullah, he began his research journey. Currently, he is enrolled in a PhD program at the Institute of Computer Sciences and Information Technology, Faculty of Management and Computer Sciences, University of Agriculture, Peshawar, Pakistan. He has published several research articles in the fields of optimization, metaheuristics, neural networks, and deep learning. His primary research interests include hybrid neural networks, knowledge-based systems, data mining, deep learning, optimization, prediction, and web mining. He is contactable at <a href="mailto:mnaaupkp@gmail.com">mnaaupkp@gmail.com</a></p>
	<p><b>Sana Salah Uddin</b> was born in Peshawar, KPK province, Pakistan. She completed her BSc degree at the University of Agriculture, Peshawar, from 2012 to 2016. In 2017, she pursued an MSc in Computer Science at the same university. Currently, she is working as a visiting lecturer at the Institute of Computer Sciences and Information Technology, Faculty of Management and Computer Sciences, University of Agriculture, Peshawar, Pakistan. She has published several research articles in the fields of optimization, methodology, neural networks, data mining, and prediction. Her primary research interests include hybrid neural networks, knowledge-based systems, data mining, prediction, and networking. She is contactable at <a href="mailto:sanabatoor@gmail.com">sanabatoor@gmail.com</a></p>
	<p><b>Dzati Athiar Ramli</b> (Senior Member, IEEE) earned her B.Sc. and M.Sc. degrees in Mathematics from University Sains Malaysia. She later obtained her Ph.D. in Electrical, Electronic, and System Engineering from University Kebangsaan Malaysia. She is currently serving as an Associate Professor and Doctoral Supervisor at University Sains Malaysia. With extensive experience in academia and research, she has made significant contributions to the fields of biometric sensing systems, image processing, computer vision, data fusion, and detection recognition algorithms. Her work focuses on developing innovative solutions for complex computational problems, advancing technological applications in security, healthcare, and intelligent systems. She is contactable at <a href="mailto:dzati@usm.my">dzati@usm.my</a></p>