Int. J. Advanced Networking and Applications
Volume: 17, Issue: 03, Pages : 6944-6953 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17307


# Black Hole Attack Detection using Advanced Intrusion Detection Approaches Integrated with Machine Learning

R.Sivaranjani[1] , Dr R.Shankar[2], Dr S.Duraisamy[3]

Department of Computer Science, chikkanna Govt Arts College, Tirupur
Email: sranjani146@gmail.com
Department of Computer Science, chikkanna Govt Arts College, Tirupur
Email: shankarcgac@gmail.com
Department of Computer Science, chikkanna Govt Arts College, Tirupur
Email: sdsamy.s@gmail.com

----------**ABSTRACT**----------
Mobile Ad hoc Networks (MANETs) are dynamic and self-organizing. Yet, the decentralized and changing nature provides the possibility of Black Hole Attacks (BHA) because of the establishment of incorrectly announced ideal routes to intersect and discard data packets by malicious nodes. The conventional security solutions including cryptographic protocols and rule-based Intrusion Detection Systems (IDSs) are poor solutions to such environments. The authors of this paper have come up with two new machine-learning-based IDSs: Behaviour-Based Anomaly Detection using Machine Learning (BBAD-ML) and the Enhanced Random Forest Intrusion Detection System (ERF-IDS) to deal with this issue. The former BBAD-ML identifies behavioural anomalies associated with BHAs by studying both the historical and real-time node behaviour while RFIDS improves the ability to detect BHAs based on ensemble learning and optimized feature selection, which decreases computational overhead. The paper outlines the main contributions, which consist of the design of BBAD-ML and ERF-IDS to identify BHAs accurately; the inclusion of feature optimization and a comparative analysis of both detection models within the simulated MANETs. From experimental results, BBAD-ML has achieved 94.10% accuracy, while ERF-IDS achieved 97.45% accuracy along with a 3.2% false positive rate and only 100 ms detection time. The results demonstrate that the two models provide scalable, efficient and robust solutions to detect BHAs, thereby making MANET security significantly stronger.

**Keywords - Black hole attack, Intrusion detection, Machine learning, Mobile Ad hoc Networks, Security.**

Date of Submission: July 29, 2025 Date of Acceptance: September 05, 2025

## I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are unstructured wireless networks which are most often used in military, disaster management situations and in Internet of Things (IoT) systems. These are dynamic and highly mobile, which offers a sense of agility and at the same time makes these prone to serious security vulnerability like the Black Hole Attack (BHA). In BHAs, rogue nodes unload the legitimate nodes to route data through these and drop the packets causing serious performance radiation. Because of its decentralization, it is difficult to detect BHAs. Traditional Intrusion Detection Systems (IDSs) and cryptographic models are inappropriate since these are not flexible and require immense processing power. Use of machine learning techniques [1] have been implemented but lack accuracy and are inefficient in a dynamic environment. Lightweight anomaly detection [2] is limited in terms of scalability whilst deep learning [3] models are not applicable in real-time MANETs because of the high training requirements. Support Vector Machines (SVMs) [4] and the Hybrid approaches [5], [6] are also investigated [7], but are haunted with management problems, redundancy or too many false positives. Other methods like gravitational search [9], Classification Algorithm 4.5 (C4.5) as well as Classification and Regression Trees (CART) [10] failed to deliver efficient results in the dynamic nature of routing in MANETs.

To overcome these shortcomings, this paper has outlined two novel models that use Machine Learning (ML): Behavior-Based Anomaly Detection using ML (BBAD-ML) and Random Forest Intrusion Detection System (RFIDS). Both the BAD-ML and RFIDS analyze node behaviour (historical and real-time), but BAD-ML lacks predefined signatures. In contrast, RFIDS uses ensemble learning to improve on the accuracy and reduce redundancy through feature selection. The two are lightweight, adaptive and apt to real-time MANET deployment.

The works by the same researchers have three contributions: (1) it introduces BBAD-ML and RFIDS as the solutions to detect BHA in MANETs; (2) through ensemble learning and feature selection, it proves the

accuracy of RFIDS in detection and its efficiency; and (3) it proves that both models attain high accuracy and low overhead in real-time through simulations. A comparison analysis underlines the accuracy-resource consumption tradeoff to indicate the deployment options. Organization: Section 2 gives a review of related work, Section 3 describes the proposed methods of detection and classification, Section 4 gives some results and discussion. Section 5 concludes the paper.

## II. RELATED WORKS

John et al. (2024) [12] presented cluster-based WSN architecture of DoS attack detection by integrating clustering with ensemble ML (Random Forest, Gradient Boosting) and feature selection to enhance the accuracy, decrease the false positives, and conserve energy.Venkatasubramanian et al. (2022) [13] proposed a deep learning model using the Cat Swarm Optimization (CSO) and Particle Swarm Optimization (PSO) system in an effort to optimize hyperparameters and sufficiently improve their ability to detect black hole and gray hole attacks in MANET with higher accuracy yet at a higher cost-computationally.Kushwah & Ranga (2021) [14] presented a hybrid DDoS possession in cloud-based computing using an ELM, which had enhanced DDoS detection accuracy, and did not slow down because of their rapid capabilities. The model is exhibiting higher accuracy in detection and lesser falsely alarms than classical classifiers, however, there is still significant scaling costs involved.Recently, Nagalakshmi et al., (2021) [15] used ML classification models (Decision Tree (DT), SVM, Random Forest (RF)) to identify a black hole attack in wireless ad hoc networks. Routing metrics were used to enhance detection precision and flexibility of feature extraction.Li et al. (2024) [16] proposed a CNN-BHO hybrid IDS of IoT, in which CNN learns hierarchical features of traffic and BHO optimises its detection. The collaborative architecture improved the modularity, up scalability and precision with small false positive rates.

Clement Sunder, A. J., & Shanmugam, A. (2020) [17] prototyped a black hole attack detection analysis based on ML classifiers and ICA (Independent Component Analysis) in healthcare WSNs (Wireless Sensor Networks). The approach maintained the patient data integrity and a superior accuracy of detection with minimal latency as compared to single classifiers. The study by Jasim Mohammed et al. (2025) [18] suggested a lightweight ML-based IDS in MANET focusing on response time as a detection indicator. Trained classifications located the malicious delays to enhance performance, precision and flexibility in variable topology. Srinivasan (2021) [19] used honeypot agents supported with deep learning to identify black holes attacks in MANETs. Honeypots were used to collect node behaviors to train. Thereby, the anomaly was detected at the earliest in NS2 simulations with high accuracy. Shameer (2025) [20] proposed an explainable deep learning architecture with XAI and edge computing by detecting black hole attacks on IoT. The balance of accuracy, efficiency and explainability led to the faster and more visible real-time detection.

**TABLE 1: Comparison Table On Black Hole Attacks**

| Authors (Year) | Title | Technique/Method Used | Target Network | Advantages | Limitations |
|---|---|---|---|---|---|
| Talukdar et al. (2021) [21] | Performance improvements of Ad hoc On-Demand Distance Vector (AODV) | IDS and Digital Signature | MANET (AODV) | Improves AODV security, detects malicious routes | Signature overhead, latency issues |
| Kouanou et al. (2024) [22] | ML for intrusion detection | ML Classifiers (SVM, Naïve Bayes (NB)) | Ad-hoc networks | Focuses on wormhole and BHA | Dataset dependency, real-time validation missing |
| Yazdanypoor et al. (2024) [23] | Hybrid detection for black or gray hole | Hybrid Rule-Based and ML | MANET | Dual-attack detection, improved accuracy | Complex integration, higher computation |
| Reshi et al. (2024) [24] | Safeguarding IoT networks | Innovative Defense Algorithm | IoT | Efficient mitigation with low overhead | Lacks scalability validation |

| | | | | | |
|---|---|---|---|---|---|
| Ioulianou et al. (2022) [25] | Trust-based IDS for Routing Protocol for Low-Power and Lossy Networks (RPL) | Trust Metrics and IDS | RPL in IoT | Detects rank and blackhole attacks | Trust metric tuning complexity |
| Ibrahim & Ghanim (2024) [26] | Artificial Intelligence (AI) for blackhole detection. | Comparative AI Models (SVM, Artificial Neural Network (ANN), RF) | MANET | Benchmark study of ML models | Model generalization not validated |
| Shafi & Venkata Ratnam (2023) [27] | Energy-aware MPR for OLSR | ML and Energy-based MPR Selection | OLSR MANET | Energy-efficient secure routing | Needs multi-metric evaluation |

Tejaswini and Adilakshmi (2020) [28] compared the four classifiers such as SVM, RF, DT and K-Nearest Neighbour (KNN) in the detection of BHA. These models are simple and reliable. Hence, it's widely used as benchmark models to others in the future. The research showed limitations in the accuracy over different mobility rates and attack rates, providing information to the enhancement of advanced systems.

2.1 Problem Identification

Black Hole Attacks (BHAs) are very versatile and dynamic security threats that malicious nodes interrupts the routing in NETs. Conventional means such as cryptography and rule-based IDS have the limitation of inefficiency and high cost of computation. Machine learning applied to IDS has potential but is not free of false positives. These constrain the scale in which, IDS is utilized. Thus, there is a need to optimize IDS and make it scalable.

2.2 Proposed solutions

The traditional security solutions like cryptographic model and rule-based IDS are inefficient and computationally expensive in MANETs. Equally, current ML-based IDS methods continue to experience false positives, inability to scale, and inability to adapt to dynamic topologies. Lightweight anomaly detection solutions were not very scaleable, whereas deep learning solutions took heavy training and would not be suitable for real-time use. SVM, RF, and CART hybrid models were moderate in accuracy, and they added redundancy and management problems. Therefore, lightweight, scalable, as well as, adaptive IDS frameworks capable of effectively managing Black Hole Attacks in MANETs are clearly needed.

## III. RESEARCH METHODOLOGIES

The proposed ERF-IDS, used in this study, advocate the implementation of RF classifiers to detect and isolate malicious nodes, raise alerts and provide secure routing updates, offering the defense against black holes on WSNs.

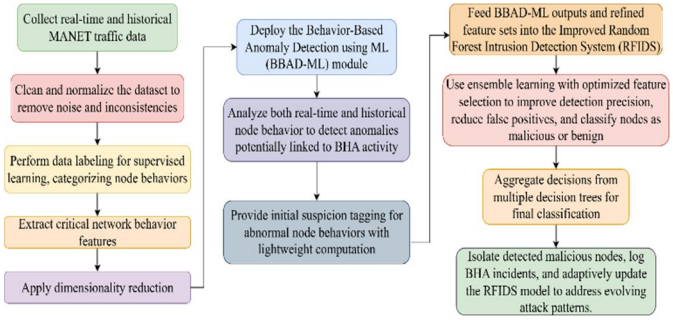


Fig 1: Overall process of black hole detection in MANET

The detection of BHA in MANET is qualitatively shown in Fig.1. The data is pre-processed, features are extracted and the latter are classified by ERF-IDS through ensemble learning. The system identifies BHAs and adapts to the additional information.

3.1 Black Hole Attack

Black Hole Attack take the advantage of faults within the MANET routing protocols to fabricate the most desirable path, make copies of packets and drop these features that devastates the performance of time critical networks. MANETs are susceptible to such attacks until the real-time detection mechanisms such as BBAD-ML are put into use. The presence of one BHA in a MANET is shown in Fig.2.

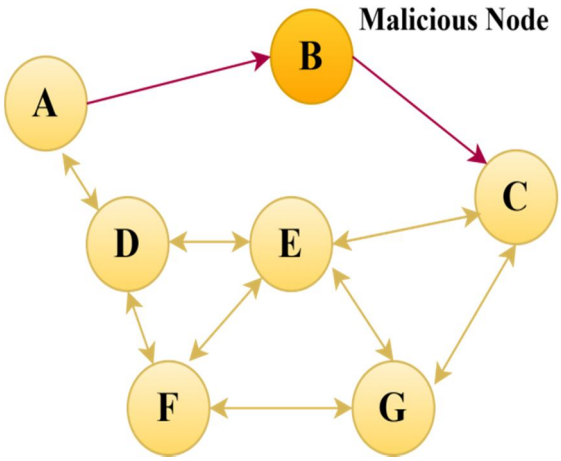


Fig 2: Black Hole Attack

Int. J. Advanced Networking and Applications
Volume: 17, Issue: 03, Pages : 6944-6953 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17307


3.2 Data Gathering and Simulation Set-up Preparation
NS2, an open-source network simulator with the support of wireless protocols and mobility models is utilized to simulate the MANET environment. Simulations are conducted with 20-100 nodes and random waypoint mobility. Constant Bit Rate (CBR), Transmission Control Protocol (TCP) traffic and AODV is used as a routing protocol. In the BHAs, malicious nodes initiate false fake Route Request (RREQ) returns to promote the shortest paths. Each simulation last 900 seconds, creating logs of transmissions, updates of routing and the behaviour of nodes. Then, the logs are parsed to provide the features on packet drops, RREQ anomalies and delivery delays as the dataset to be created.

3.3 Data Preprocessing
The traces of S2 traffic are noisy and also incomplete. Z scores are used to remove outliers, missing values filled by mean or KNN, features scaled on [0,1] Min-Max, and the targets converted to label encoding (0 = normal, 1 = BHA).

$$N_{norm} = \frac{N - N_{min}}{N_{max} - N_{min}} (1)$$

Equation (1) applies Min-Max normalization, where NNN is the original feature, NminN_{min}Nmin and NmaxN_{max}Nmax are its minimum and maximum values, and NnormN_{norm}Nnorm is the normalized result between 0 and 1. This scaling makes all MANET features uniform, reducing bias and improving ML model performance.

3.4 Feature Engineering
This process converts raw simulation data into end features which depict possible BHA operations. To calculate each of the time intervals of all nodes, there are 4 metrics done that are calculated using the cleaned version of traffic logs: (i) Packet Delivery Ratio (PDR) is an effectiveness measure, which spatially and temporally quantifies the data sent and in this particular case, PDR = number of packets successfully received by node $i$ or the number of packets sent by *i*. (ii) Packet Drop Rate (PDRate) is a reliability measure of network and quantifies the percentage of packets that are dropped; (iii) False Packet Rate (FP) represents the percentage of packets that are deceptive or corrupted, which are universally high in malicious nodes and (iv) Route Request Rate (RRR) is the count of RREQ messages, overwhelmingly high when Black Hole Attack is occurring. Time-series behavioural features look at both historical and current anomalies. It is good to note the structure of traffic logs as the team need to restructure it, if the instance is to run the previously captured data. Boruta feature selection is selected to minimize outcome learning and improve model by discarding non-informative and non-duplicative features after benchmarking identified features against randomized shadows and other selected features.

$$PDR(i) = \frac{P_r(i)}{P_t(i)} (2)$$

In the context of this analysis, $P_t(i)$ indicates the total number of packets sent by node *i*. Conversely, $P_r(i)$ is the total number of packets received by node i. So, equation (2) simply captures the ratio of counted packets or the fraction of successfully received packets $PDR(i)$. Low PDR indicates a potential BHA.

$$PDRate\ (i) = \frac{P_d(i)}{P_t(i)} (3)$$

In equation (3), $P_d(i)$ is the total number of packets dropped by node *i*. PDR is the proportion of dropped packets. A high PDR is the indicative of malicious behaviour.

$$FP(i) = \frac{P_f(i)}{P_t(i)} (4)$$

In this, $P_f(i)$ represents the total number of packets forwarded by node *i*. Equation (4) identifies the nodes that have not forwarded the packets. An overall low FP is malicious.

$$RRR(i) = \frac{Accepted\ Route\ Requests}{R_r(i)} (5)$$

In this paper, $R_r(i)$ is the total number route request raised by node *i*, *RRR* is route request response rate in Equation (5). Often, malicious nodes reply too many route requests but then drop packets. The threshold rules are explained to detect the nodes with a high loss rate of packets and low forwarding probability as proximate black hole attackers. The anomaly detection approach detects the deviation of normal behaviour.

If $PDR(i) < T_1$ and $PDRate(i) > T_2$, node $i$ is a potential black hole and $FP(i) < T_3$.Thresholds values $T_1$,$T_2$,$T_3$ are established from the normal behaviour of network A classifiers (SVM, RF). These are learned from the extracted features to classify normal nodes and malicious nodes.

$$F(i) = [PDR(i), PDRate\ (i), FP(i), RRR(i)] (6)$$

Equation (6) forms a feature vector *F(i)* for each node i in the MANET. This feature vector is made up of the important metrics of network behaviour in detecting anomalies. This feature vector help detect suspicious activity by comparing any deviations from the normal traffic flow.

3.5 Black Hole Attack detection and classification using Behavior-Based Anomaly Detection using Machine Learning

The presented BBAD-ML is a system of unsupervised detection of anomalies, but it is a lightweight framework used to detect Black Hole Attacks (BHAs) in the Mobile Ad hoc Networks (MANETs). The framework is engaged in the continuous monitoring of node-level behavioural indicators (the ratio of packets delivered on time, drop rate, the frequency of requesting a route), which remain used to establish the degree of deviation of the values and normal ranges. The system relies on the Isolation Forest algorithm at the heart of its functionality, which is primarily effective for anomaly detection in data that is high-dimensional and highly imbalanced. Unlike the conforming classifiers that learn the structure of normal data, Isolation Forest only learns

Int. J. Advanced Networking and Applications
Volume: 17, Issue: 03, Pages : 6944-6953 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17307


the structure of target data in terms of partitioning between the normal and abnormal features randomly and anomalous loci (such as BHA nodes) generally need fewer splits to be isolated since these tend to have unique and infrequent behaviour. The method also detects a new attack strategy or an evolving attack for which, there are no labelled training data. Finally, real-time and distributed detection is emerging as a key requirement for MANET. The system allows local nodes to assess the own behaviour and that of the neighbouring nodes independently, significantly decreasing the burden on centralized processing units, which leads to better scaling in a largely heterogeneous and dynamic MANET.

Following feature selection such as Packet Delivery Ratio, Drop Rate and Route Request Rate, each node's behaviour has been mapped into a multidimensional feature vector. Isolation Forest is an algorithm that creates an aggregate of binary trees. In each tree, data points are recursively isolated through randomly chosen features and split values. There is a behavioural difference because; an average path length to isolate the malicious or anomalous nodes like BHA usually ends up being shorted than the other nodes because it is closer to the root. An anomaly score is the average length of maximum node isolation path in trees, the shorter path the more probable is that a node is malicious. This provides a scalable and efficient way to detect the BHA node. In a rooted tree, the length of a path from the root node to a leaf node is called the path length of sample $x$ and is denoted by$h(x)$. Anomaly Score is then found as:

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}} \quad (7)$$

Where, $s(x,n)$ is the anomaly score of instance $x$ in an $n$ -sized data, Domain: 0 1. Approaching the value 0.5 - indicates a probable normal behavior. Equation (7) obtains the anomaly score of a specific instance $x$ by computing the ease at which it is isolated within the Isolation Forest. The rationale is, the shorter the average path length, the anomaly score is greater. There is the possibility of abnormal behaviour. c (n) is the average path length of unsuccessful searches in Binary Search Trees and it is approximated as:

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n} \; with \; H(i) \approx In(i) + 0.5772 \quad (8)$$

Where, *H (i)* is the harmonic number, $In(i)$ is the natural logarithm of *i*. γ is Euler-Mascheroni constant which is approximately 0.5772. Scores close to 1 indicate high anomaly (potential BHA), while scores near 0.5 suggest normal behaviour. The provided method operates in almost real-time, dynamically processing behaviour vectors while acknowledging the potential confusion that arise in flagging suspicious nodes. This method allows BBAD-ML to effectively and efficiently perform adaptive anomalous detection within the decentralized MANETs. This is the description of equation (8). It is used to normalize the score allowing for an anomaly score that is comparable across the datasets of various sizes.

In BBAD of MANETs, nodes are represented by behaviour vector, which contains the attributes such as Packet Delivery Ratio, Packet Drop Rate, False Packet Rate and Route Request Rate that characterize the behaviour of the past and ongoing information communication. BBAD-ML model utilizes an isolation forest method trained on normal traffic in order to capture the regular patterns. In the examinations, anomalies such as BHAs are singled out within a small time through the anomaly scores that rely on the length of paths, where high scores classify suspicious nodes. This technique makes it possible to carry out the intrusion detection (in real time) of MANETs in which, very scarce resources are involved.

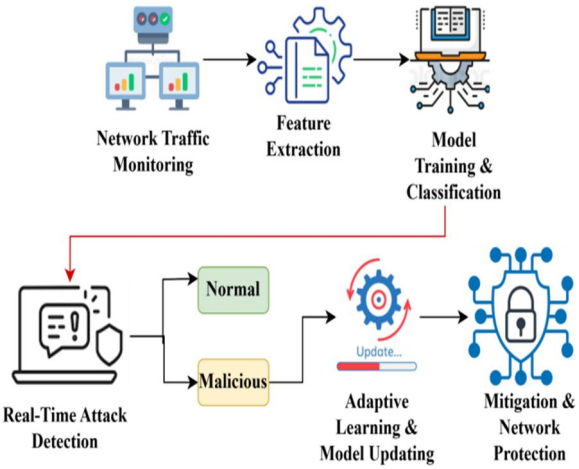


Fig 3: Behavior-Based Anomaly Detection with Machine Learning Pipeline

Fig.3 illustrates the BBAD-ML detection system of BHA under the MANETs. It begins with the process of gathering data. This is followed by preprocessing of the gathered data, followed by the extraction of features and the training of model with labelled data and with the unseen data. Behaviour is categorized as either normal or malicious and the model learns during its lifetime to new attack behaviours, maintaining a higher overall success rate or accuracy as it learns.

| ***Algorithm 1: Behavior-Based Anomaly Detection with Machine Learning (BBAD-ML)*** |
|---|
| Input: Network traffic data, feature set F(i) = [PDR(i), PDRate(i), FP(i), RRR(i)] |
| Begin |
| Step 1: Data Collection |
| Initialize network and capture real-time traffic data. |
| Monitor packet forwarding behavior of each node. |
| Step 2: Feature Extraction |
| For each node i in the network: |
| Compute Packet Delivery Ratio (PDR (i)) |
| Compute Packet Drop Rate (PDRate (i)) |
| Compute False Packets sent (FP (i)) |
| Compute Route Request Rate (RRR (i)) |
| Construct feature vector F (i) = [PDR (i), PDRate (i), FP(i), RRR(i)] |

Int. J. Advanced Networking and Applications
Volume: 17, Issue: 03, Pages : 6944-6953 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17307


Step 3: Model Training
Load labeled dataset (Normal & Malicious nodes).
Train a Random Forest Classifier on feature vectors F(i).
Optimize hyperparameters to improve classification accuracy.
Step 4: Attack Detection & Classification
For each new node i:
Extract real-time feature vector F (i).
Compute classification function C (i) = f (F (i)) using the trained model.
If C (i) predicts "Malicious":
Flag node i is BHAer.
Else:
Mark node i as Normal.
Step 5: Adaptive Learning & Model Update
Periodically update the model with newly detected patterns.
Retrain on newly labeled data to adapt to evolving attack strategies.
Step 6: Mitigation Response
If a node is classified as Malicious:
Isolate the node from the network.
Alert network administrators.
Reconfigure routing paths to avoid BHAers.
End Algorithm
Output: Classification of nodes as Normal or Malicious

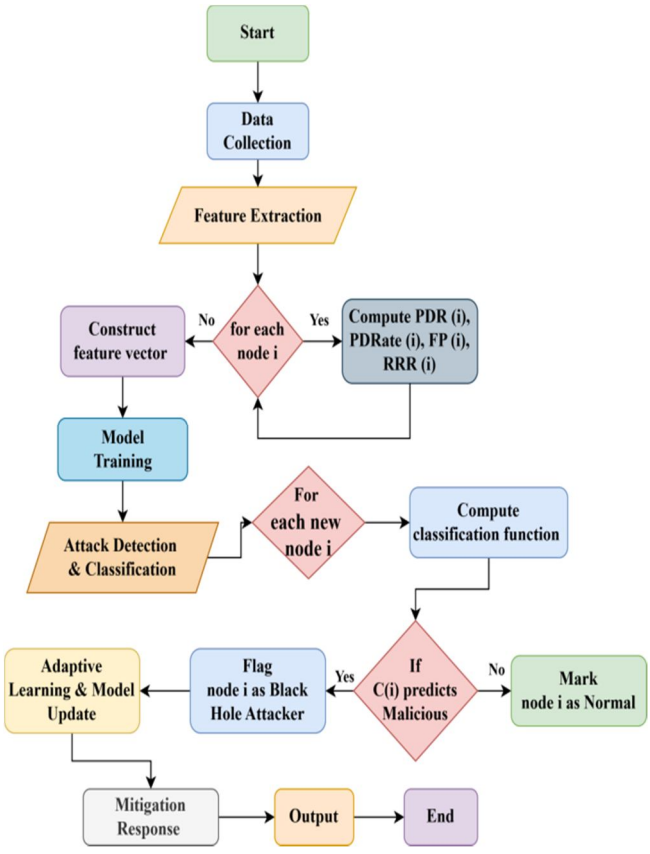


Fig 4: Flow diagram of Behavior-Based Anomaly Detection with Machine Learning

Algorithm 1 and Fig.4 shows the BBAD-ML algorithm identifying and classifying BHAs in MANETs efficiently based on ML.

3.6 Enhanced Random Forest Intrusion Detection System (ERF-IDS)

The ERF-IDS effectively reinforces MANET intrusion detection using RF as a collection of trees. By choosing only the key functions, where the key functions are PDR, PDRlate, FP and RRR, considerably lowers computational load and increases the detection rate. The voting scheme over multiple trees reduces the false alarms and dynamically adapts to any new or evolving patterns in attack. The protocol improves the security of MANET, keeps the consistency of data in these networks as well as stabilizes these because it is well able to detect the normal and malicious nodes.

ERF-IDS creates multiple DTs that all decide which feature is the best classification while utilizing Entropy and Information Gain.

$$H(D) = -\sum_{j=1}^{n} P(C_j)\, log_2\, P(C_j) \quad (9)$$

Equation (9) calculates entropy $H(D)$, where $n$ is the number of classes, $C_j$ is the $j^{th}$ class, and $P(C_j)$ is its probability. It measures dataset impurity—higher values mean more randomness lower values mean more purity. $P(C_j)$ is the likelihood that a node is a member of class $C_j$ (Normal or Malicious). Zero entropy means all the nodes are in one class. High entropy means the nodes are mixed (uncertainty classification). Equation (9) shows that the entropy represents impurity (uncertainty) of dataset. Higher entropy implies that the dataset is more mixed between normal and malicious classes; lower entropy reflects more certainty of classification.

$$IG(D, X) = H(D) - \sum_{v \in X} P(D_v) H(D_v) \quad (10)$$

Equation (10) defines Information Gain ($IG$), where $H(D)$ is the entropy of dataset $D_v$ is the subset for feature value $v$, and $P(D_v)$ is its probability. IG measures the reduction in uncertainty when splitting on feature $X$, higher IG means the feature is more useful for classification.The dataset is split into $D_v$ subsets based on feature $X$. The feature with maximum $IG$ is used to split the DT at node event. The Information Gain (IG) in equation (10) is an indication of a decrease of entropy or impurity as a dataset is separated based on the feature $X$. The bigger the IG is, the more valuable feature to classify:

$$T_k\big(F(i)\big) \rightarrow C_k(i) \forall k \in [1, m] \quad (11)$$

Equation (11) represents the classification mapping, where the transformation function $T_k\big(F(i)\big)$ assigns the feature vector $F(i)$ of instance iii to a class label $C_k(i)$. Here, $k \in [1, m]$denotes the set of possible classes, with mmm being the total number of classes. In simple terms, this equation shows how the trained model maps input features to their corresponding class, like, normal or malicious node.In equation (11), each tree is trained on the distinct random portions of data. The classification output of each tree is either normal or malicious. RFIDS constructs multiple DTs. Each tree $T_k$ produces an independent classification decision$C_k(i)$.

Int. J. Advanced Networking and Applications
Volume: 17, Issue: 03, Pages : 6944-6953 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17307


$$C(i) = arg \max_{c\in\{Normal,malicious\}} \sum_{k=1}^{m} 1(C_k(i) = C) \quad (12)$$

Here, the indicator function 1 addresses whether each individual decision tree *k* predicts the class *C*. The class that has the tallest vote is the outcome. Equation (12) methodology ultimately contributes to lower overfitting and increased accuracy when the multiple DTs are used versus a single DT. Once every tree predicted a classification, ERF-IDS conducted majority voting prediction to determine the outcome.

$$P'(C_j) = \frac{P(C_j)+\lambda\cdot N_{new}}{N+N_{new}} \quad (13)$$

In this, $P'(C_j)$ is the new probability of class $C_j$ (Normal or Malicious), $\lambda$ as learning rate, which is an amount of weight placed on new data. New attack samples are added to the dataset, N is the new number of new attack samples. In equation (13), it is seen that ERF-IDS is continuously being trained by the novel form of attacks to enhance its precision in detection. Key changes in BHA strategies are happening continually and therefore, the model is also retrained using new data.

To evaluate the performance of adaptive learning within the Enhanced Random Forest Intrusion Detection System (ERF-IDS), analyzing the model performance is impacted with and without adaptive updates using equation (14) as the foundation governing adaptive updates.

The model is able to be updated using:

$$M_{t+1} = M_t + \eta \cdot \Delta L(x, y, \theta_t) \quad (14)$$

Equation (14) expresses the model update rule in iterative learning. Here, $M_t$ is the model at iteration t, η is the learning rate that controls the step size, and $\cdot \Delta L(x, y, \theta_t$ ) is the gradient of the loss function $L$ with respect to the parameters $\theta_t$, computed using input $x$ and target $y$. The updated model $M_{t+1}$ is obtained by adjusting the previous model based on this gradient.

Where, $\theta$ of time t is the model parameter and $\theta$ is the learning rate, $\Delta L$(x, y,$\theta_t$) is the gradient of loss with respect to new data computed (x, y). Equation (14) describes a framework that keep the model continuously learning based on new threats and data streams.

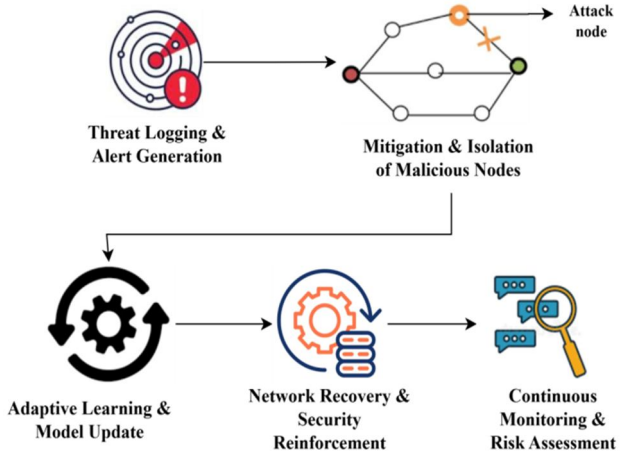


Fig 5: Enhanced Random Forest Intrusion Detection System (RFIDS)

As per Fig.5, BBAD-ML dynamic response after the attack detection is explained, as the threats have been detected, the routes reassessed, the model parameters are updated dynamically and the new attacks patterns analyzed to strengthen the defense.

***Algorithm 2: Enhanced Random Forest Intrusion Detection System (RFIDS)***

Input: Network traffic data (N) with features {PDR, PDRate, FP, RRR}
Begin
Step 1: Data Preprocessing
Extract network traffic features F(i) = {PDR, PDRate, FP, RRR} for each node i.
Normalize feature values to ensure consistency.
Split dataset into training (70%) and testing (30%) sets.
Step 2: Construct Multiple DTs
Initialize Random Forest with M DTs.
For each DT $T_k$ (k = 1 to M):
Select a random subset of training data (Bootstrap Sampling).
Select a random subset of features for node splitting.
Compute Entropy for current dataset:

$$H(D) = -\sum_{j=1}^{n} P(C_j)\log_2 P(C_j)$$

For each feature *X*, calculate Information Gain:

$$IG(D,X) = H(D) - \sum_{v\in X} P(D_v)H(D_v)$$

Choose the feature with the highest IG as the splitting criterion.
Step 3: Classify Nodes Using Majority Voting
For each test instance *F(i)*, get predictions from all DTs:

$$T_k(F(i)) \rightarrow C_k(i)$$

Apply majority voting:

$$C(i) = \arg \max_{c\in\{Normal,malicious\}} \sum_{k=1}^{m} 1(C_k(i) = C)$$

Assign the final class label to node *i*.
Step 4: Adaptive Model Update
Collect new attack patterns and update dataset.
Recalculate probability for each class:

$$P'(C_j) = \frac{P(C_j) + \lambda \cdot N_{new}}{N + N_{new}}$$

Retrain the Random Forest model periodically with new data.
Step 5: Output Results
Display classification results: Normal or Malicious.
Generate security alerts if a BHA is detected.
End Algorithm
Output: Classification of nodes as Normal or Malicious

Int. J. Advanced Networking and Applications
Volume: 17, Issue: 03, Pages : 6944-6953 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17307


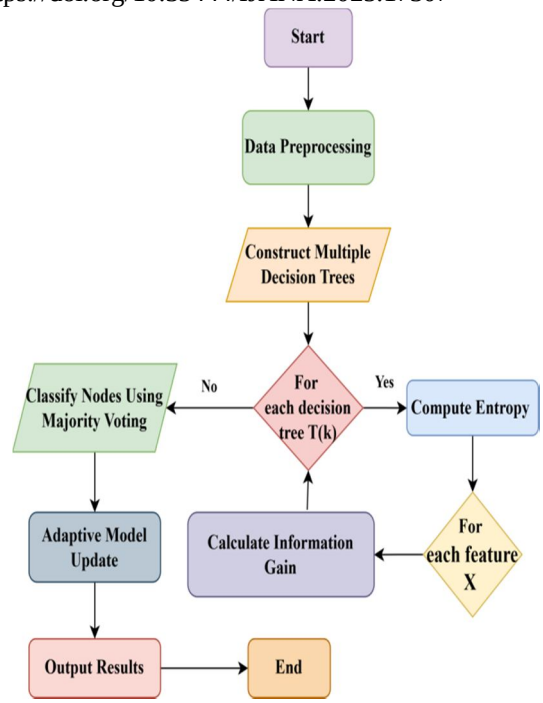

Fig 6: Flow diagram of Enhanced Random Forest Intrusion Detection System

Algorithm 2 and Fig.6 clearly show the Enhancement Random Forest Intrusion Detection System (ERF-IDS).

## IV. RESULTS AND DISCUSSIONS

The proposed ERF-IDS demonstrated 97.45% detection accuracy as well as shorter detection latency of 300 ms versus RF, SVM, k-NN and BBAD-ML. It is implemented in Python with the use of Scikit-learn to be tested against synthetic MANET datasets that are based on PDR, PDRate, FP and RRR to control the conditions to compare black hole attacks and adaptive detection.

**TABLE 2: Simulation Parameters**

| Parameter | Value |
|---|---|
| Number of Nodes | 50, 100, 150 |
| Network Area | 1000 m × 1000 m |
| Mobility Model | Random Waypoint |
| Simulation Time | 1000 seconds |
| Node Speed | 0–20 m/s |
| Pause Time | 5 seconds |
| Traffic Type | CBR (Constant Bit Rate) |
| Packet Size | 512 bytes |
| Transmission Range | 250 meters |
| Routing Protocol | AODV (Ad hoc On-Demand Distance Vector) |
| Attack Model | Black Hole Attack |
| Number of Malicious Nodes | 5, 10, 15 (varied) |
| Attack Behavior | Drops all received data packets, falsely replies with high sequence number |
| Simulation Tool | Python (with Scikit-learn) |

Table 2 is a setup of the simulation with a random waypoint model with 50-150 nodes. Traffic is CBR with AODV routing and BHA simulations are performed by malicious nodes dropping packets and sending the forged replies. The effect of attacks is classified with the use of a Python-Scikit-learn intrusion detection framework.

4.2 Performance Evaluation

**TABLE 3: Performance Comparison on various BHA detection algorithms**

| Model | Accuracy (%) | Detection Rate (TPR) (%) | Precision (%) | Recall (%) | F1-Score (%) | Execution Time (s) |
|---|---|---|---|---|---|---|
| RF | 95.10 | 93.60 | 92.80 | 93.60 | 93.20 | 0.47 |
| SVM | 91.20 | 89.70 | 90.10 | 89.70 | 89.90 | 0.62 |
| k-NN | 89.85 | 88.20 | 87.70 | 88.20 | 87.95 | 0.39 |
| DT | 90.40 | 89.00 | 88.10 | 89.00 | 88.55 | 0.35 |
| BBAD-ML | 94.10 | 92.75 | 93.20 | 92.75 | 92.97 | 0.33 |
| ERF-IDS | 97.45 | 96.80 | 95.90 | 96.80 | 96.35 | 0.30 |

According to the results presented in table 3, it is visible that ERF-IDS performs the best with 97.45 % accuracy, 96.80% detection rate, and 96.35% F1- score with comparatively lesser execution time. The BBAD-ML (Isolation Forest) method achieves a higher accuracy (94.10%) than the alternative benchmark (89.67% accuracy) despite the fact it does not require labeled attack data, which makes it useful in unknown threats. Traditional models such as RF and SVM are more susceptible and not flexible. It is an indication of the power of behavior-aware metrics using ensemble learning in MANET intrusion detection.

4.3 Adaptive Learning Performance

Adaptive Learning (Sec. 4.3): ERF-IDS adapts as new data becomes available (Eq. 11), thus it learns over time and becomes more accurate. This forms continuous learning that provides vigorous detection across different network conditions

**TABLE 4: Accuracy Improvement Over Time**

| Time Interval | Accuracy (Before) | Accuracy (After Adaptive Learning) |
|---|---|---|
| T1 | 93.10% | 93.10% |
| T2 | 92.60% | 94.20% |
| T3 | 91.70% | 95.30% |
| T4 | 90.85% | 96.00% |
| T5 | 89.90% | 97.45% |

Table 4 demonstrates that accuracy increases using adaptive learning as time goes by. Accuracy remains unchanged at T1 but returns higher at T2, T3 and T5 as the change of trends is adopted by the model, demonstrating the effectiveness of the model in dealing with evolving attacks and improvement in detection.

4.4 Ablation Study

The ablation experiment on RF demonstrates that PDR and FP become mostly decisive features and the rest of considered features, namely, PDRate and RRR only support BHA detection to a lesser degree. This affirmatively proves that it is essential to concentrate on PDR and FP in order to classify the anomalies accurately in MANETs.

**TABLE 5: Ablation Study comparison table**

| Removed Feature | Accuracy (%) | Detection Rate (TPR) (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|---|
| All Features | 97.45 | 96.80 | 95.90 | 96.80 | 96.35 |
| PDR Removed | 91.60 | 90.30 | 89.80 | 90.30 | 90.05 |
| PDRate Removed | 95.20 | 93.90 | 93.00 | 93.90 | 93.45 |
| FP Removed | 92.40 | 91.10 | 90.60 | 91.10 | 90.85 |
| RRR Removed | 96.00 | 94.85 | 94.10 | 94.85 | 94.47 |

Table 5 evidences that the elimination of PDR or FP radically downs the performance, which in turn proves the significant role in identifying BHA, whereas the individual effect of RRR is negligible but it is significant in combination.

4.5 Discussions

ERF-IDS enhance random forest intrusion detection in MANETs to provide the increased black hole threat detection due to the usage of features such as PDR, FP and RRR. Size of its ensemble with tuned hyperparameters, weighted voting, normalization and SMOTE assures of high accuracy, precision, recall and robustness, even in noisy data. Compared to the baseline models, ERF-IDS shows low overhead and high performance, which is appropriate in the case of real-time MANETs. Nonetheless, it is susceptible to attacks when using collaboration, a situation which has to be addressed in the future by incorporating the trust score fusion and online learning to enhance dynamism. It has to be mentioned that SVM are not the components of the proposed IDS framework. These have been listed only in the result section, as benchmark models on which comparison has been made. This guarantee that the efficacy of proposed ERF-IDS is appraised against commonly used conventional classifiers hence confirming its robustness.

## V. CONCLUSION

This paper suggests the BBAD-ML architecture that detects Black Hole Attacks in MANETs and uses ERF-IDS as a critical component of such architecture. PDR, PDRate, FP and RRR are the key features that have been optimised using Boruta and SMOTE and normalisation handle the imbalance and scaling. The hyperparameter optimization results in ERF-IDS beating SVM, KNN, DT and RF in terms of the overall performance, indicating an accuracy of 97.45% and an adaptive increase (T1-T5). BAD-ML is relatively easy to explain, scale and is applied on real-life MANETs. Thus, future efforts are first been on trust analysis, cooperative attack detection and mobility awareness.

## REFERENCES

[1] Pandey, S., & Singh, V. (2020, July). Blackhole attack detection using machine learning approach on MANET. In 2020 international conference on electronics and sustainable communication systems (ICESC) (pp. 797-802). IEEE.

[2] Abdelhamid, A., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). A lightweight anomaly detection system for black hole attack. *Electronics*, *12*(6), 1294.

[3] Bhonsle, M., Sreenivasulu, G., Chaitanya, K., Raghu, D., Surendra, G., Kumar, K. K., ... & Vuppu, V. K. (2025). Enhancing Security in Wireless Mesh Networks: A Deep Learning Approach to Black Hole Attack Detection. *Advance Sustainable Science Engineering and Technology*, *7*(1), 02501010-02501010.

[4] Rahman, F., & Sharma, P. (2025). Designing an Intrusion Detection System to Identify Black Hole Attacks in Wireless Ad-hoc Networks using Support Vector Machines, with a comparison to Decision Trees. *Recent Developments in Microbiology, Biotechnology and Pharmaceutical Sciences*, 281.

[5] Abdallah, A. A., Abdallah, M. S., Aslan, H., Abdallah, M. A. A., Cho, Y. I., & Abdallah, M. S. (2024). Enhancing Mobile Ad Hoc Network Security: An Anomaly Detection Approach Using Support Vector Machine for Black-Hole Attack Detection. *International Journal of Safety & Security Engineering*, *14*(4).

[6] Yazdanypoor, M., Cirillo, S., & Solimando, G. (2024). Developing a Hybrid Detection Approach to Mitigating Black Hole and Gray Hole Attacks in Mobile Ad Hoc Networks. *Applied Sciences*, *14*(17), 7982.

[7] Amalia, A., Pramitarini, Y., Perdana, R. H. Y., Shim, K., & An, B. (2023). A deep-learning-based secure routing protocol to avoid blackhole attacks in VANETs. *Sensors*, *23*(19), 8224.

[8] Sunitha, D., & Latha, P. H. (2025). A secure routing and black hole attack detection system using coot Chimp Optimization Algorithm-based Deep Q

Network in MANET. *Computers & Security*, *148*, 104166.

[9] Dhanaraj, R. K., Jhaveri, R. H., Krishnasamy, L., Srivastava, G., &Maddikunta, P. K. R. (2021). Black-hole attack mitigation in medical sensor networks using the enhanced gravitational search algorithm. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *29*(Suppl 2), 297-315.

[10] Gite, P., Chouhan, K., Krishna, K. M., Nayak, C. K., Soni, M., & Shrivastava, A. (2023). ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4. 5 and CART classifiers. *Materials Today: Proceedings*, *80*, 3769-3776.

[11] Li, P., Wang, H., Tian, G., & Fan, Z. (2024). A cooperative intrusion detection system for the internet of things using convolutional neural networks and black hole optimization. *Sensors*, *24*(15), 4766.

[12] John, A., Isnin, I. F. B., Madni, S. H. H., & Faheem, M. (2024). Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms. *Intelligent Systems with Applications*, *22*, 200381.

[13] Venkatasubramanian, S., Suhasini, A., & Hariprasath, S. (2022). Detection of black and grey hole attacks using hybrid cat with PSO-based deep learning algorithm in MANET. *International Journal of Computer Networks and Applications (IJCNA)*, *9*(6), 724-724.

[14] Kushwah, G. S., & Ranga, V. (2021). Distributed denial of service attack detection in cloud computing using hybridextreme learning machine. *Turkish Journal of Electrical Engineering and Computer Sciences*, *29*(4), 1852-1870.

[15] Nagalakshmi, T. J., Gnanasekar, A. K., Ramkumar, G., &Sabarivani, A. (2021). Machine learning models to detect the blackhole attack in wireless adhoc network. *Materials Today: Proceedings*, *47*, 235-239.

[16] Li, P., Wang, H., Tian, G., & Fan, Z. (2024). A cooperative intrusion detection system for the internet of things using convolutional neural networks and black hole optimization. *Sensors*, *24*(15), 4766.

[17] Clement Sunder, A. J., & Shanmugam, A. (2020). Black hole attack detection in healthcare wireless sensor networks using independent component analysis machine learning technique. *Current Signal Transduction Therapy*, *15*(1), 56-64.

[18] Jasim Mohammed, F., Andalib, A., Azgomi, H., & Sharifi, S. A. (2025). Enhancing the Security of Mobile Ad-hoc Networks: A Black Hole Attack Mitigation Approach Using Response Time and Machine Learning Models. *Journal of Industrial and Systems Engineering*, *17*(1), 204-216.

[19] Srinivasan, V. (2021). Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET. *Ingénierie des Systèmes d Inf.*, *26*(6), 549-557.

[20] Shameer, M. (2025). Secure IoT Networks: A Deep Learning-Based Framework for Detecting Black Hole Attacks in RPL Protocol with Explainable AI and Edge Computing Integration. *EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR*, *46*(1), 146-167.

[21] Talukdar, M. I., Hassan, R., Hossen, M. S., Ahmad, K., Qamar, F., & Ahmed, A. S. (2021). Performance improvements of AODV by black hole attack detection using IDS and digital signature. *Wireless Communications and Mobile Computing*, *2021*(1), 6693316.

[22] Kouanou, A. T., Fonzin, T. F., Zanga, F. M., Mouelas, A. N., Ndenoka, G. N., &Ekonde, M. S. (2024). Machine learning for intrusion detection in ad-hoc networks: wormhole and blackhole attacks case. *Cloud Computing and Data Science*, 62-79.

[23] Yazdanypoor, M., Cirillo, S., & Solimando, G. (2024). Developing a Hybrid Detection Approach to Mitigating Black Hole and Gray Hole Attacks in Mobile Ad Hoc Networks. *Applied Sciences*, *14*(17), 7982.

[24] Reshi, I. A., Sholla, S., & Najar, Z. A. (2024). Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm. *Journal of Engineering Research*, *12*(1), 133-13

[25] Ioulianou, P. P., Vassilakis, V. G., &Shahandashti, S. F. (2022). A trust-based intrusion detection system for RPL networks: Detecting a combination of rank and blackhole attacks. *Journal of Cybersecurity and Privacy*, *2*(1), 124-153.

[26] Ibrahim, Z. B., & Ghanim, M. F. (2024). Leveraging artificial intelligence for blackhole attack detection in MANETs: A comparative study. *Inf. Dyn. Appl*, *3*(4), 245-257.

[27] Shafi, S., & Venkata Ratnam, D. (2023). New energy aware MPR selection for securing OLSR routing scheme under black hole attack: a machine learning approach. *Wireless Personal Communications*, *132*(3), 1917-1931.

[28] Tejaswini, K., & Adilakshmi, M. Y. (2020). Black hole Attack Detection Using Machine Learning Algorithms in MANET–Performance Comparision. *International Journal of Research and Analytical Reviews*, 6047-6051.