An enhanced detection system against routing attacks in mobile ad-hoc network

Prasad, Mahendra; Tripathi, Sachin; Dahal, Keshav

Published in:
Wireless Networks

DOI:
10.1007/s11276-022-02913-1

Published: 15/02/2022

Document Version
Peer reviewed version

Prasad, M., Tripathi, S., & Dahal, K. (2022). An enhanced detection system against routing attacks in mobile ad-hoc network. *Wireless Networks*.

Noname manuscript No.
(will be inserted by the editor)

An enhanced detection system against routing attacks in mobile ad-hoc network

Mahendra Prasad · Sachin Tripathi · Keshav Dahal

Abstract Mobile ad-hoc network is a dynamic wireless network that transfers information through neighbor nodes with a temporary configuration. Due to its dynamic nature, it is exposed to attacks and intrusions. Routing disruption attack is the main problem of this network where intermediate nodes act maliciously. An encryption-based security mechanism is a first-line defense system that is efficient. It is still not compatible with the mobile ad-hoc network environment. Malicious nodes can drop encrypted data packets in this network. The lightweight technique analyzes a few parameters that consume few resources and provide comparatively low detection rates. However, an intrusion detection system is a reliable second-line security mechanism. In this paper, we have proposed a detection method that classifies malicious and benign information. The proposed intrusion detection method is based on learning techniques that initially require a dataset to determine mobile nodes' behavior. Subsequently, we perform this work in an order such as mobile ad-hoc network simulation with some malicious nodes, features selection, and data collection using packet captured files. This work is executed through extensive simulations in the NS-3. The proposed method learns the system for information classification, and experimental results that show the proposed method performs better than existing schemes. Moreover, the obtained performance confirms that the suggested feature set is suitable for the intrusion detection system in mobile ad-hoc networks.

Mahendra Prasad
Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, India. E-mail: je.mahendra@gmail.com

Sachin Tripathi
Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, India. E-mail: sachin2781@iitism.ac.in

Keshav Dahal
School of Computing, Engineering and Physical Sciences, University of the West of Scotland, Paisley, UK. E-mail: Keshav.Dahal@uws.ac.uk

Keywords Intrusion detection system · Mobile ad-hoc network · Blackhole attack · Wormhole attack · Classification mechanism

1 Introduction

A mobile ad-hoc network (MANET) is an easily installable and temporary network. It is composed of many mobile nodes, and an infrastructure-less network whose random mobility frequently changes the network topology. These nodes have a radio range, and they communicate over wireless link [1, 2, 3]. Due to the node's limited radio range, it fails to transfer data to more than one hop nodes. Then, it transmits a data packet through the message relay. In MANET, a routing table has possible paths that select the best specific route from source to destination, and it requires legitimate support of nodes in the communication path. In recent years, the ad-hoc network has preserved worldwide applications. This network is mainly employed in military services [4], traffic control, rescue operations [2], and others. One of the main applications of this network is in military services [4], where information security is more important. An army unit consisting of infantry squads for battlefields and search operations. Each infantry squad has a wireless mobile device to transfer information to the destination. Sometimes, it is also used for military search operations that need to function in dense population areas. There are many devices and intruders in the wireless range. The proposed method detects malicious behavior information that disrupts MANETs and misuse information.

The MANET characteristics such as self-structuring, mobility of nodes, without central monitoring, and message relay [2, 3]. It is more vulnerable to attacks that effective defense mechanism is not publicly available or designed. Many types of attacks harm network resources, and an attacker can be either internal or external. One of them, a routing disruption attack, is a Denial of Service (DoS) attack [5] of the network layer. It uses the vulnerability of insecure routing protocol. A malicious node advertises itself as a part of the destination route and acts maliciously. We have considered two routing disruption attacks in this proposed detection method, such as blackhole and wormhole attacks. They affect the route selection process and routing table, while the routing table also continuously updates due to the dynamic nature of active nodes. The cryptographic or key management-based techniques are first-line defense mechanisms that work efficiently; however, these methods are not compatible with the MANETs environment [6, 7]. Blackhole attack drops the packets [8], and the wormhole attack tunnels the packets [9]; whenever they also drop or tunnel the encrypted packets. These attacks are not easy to handle using cryptography techniques. Therefore, we have applied machine learning techniques to mitigate these attacks. This method is as lightweight technique in resource consumption and obtained a better detection rate than deep learning mechanism [3], M-DelPHI [10], DAWA [11], and lightweight techniques.

An Intrusion Detection System (IDS) detects malicious behavior's nodes that learn or computes nodes' behavior from the training dataset [2, 12, 13]. However, it is not easy to apply in MANETs due to the limited memory and energy capacities of mobile nodes. Therefore, we have collected significant samples and formed lightweight datasets. There are two main categories of IDS, namely the misuse and anomaly detection system. The misuse detection system detects only those signatures are present in the database, whereas the anomaly detection system detects those samples deviate from the baseline [13]. The primary purpose of IDS to increase the detection rate and decrease the false alarm rate; when the system detects malicious information [1, 2, 3], then send an alert to the network administrator. In the IDS dataset, the data collection to real-world-enterprise networks is not an easy task. Many IDS datasets are publicly available, which are generated through testbeds or simulated [14, 15]. Existing traditional wired IDSs are executed on KDDcup'99 (65%), DARPA (13%), NSL-KDD (12%), ISCX (2%), UCI (4%), UNSW-NB'15 (2%), and GNOME (2%) using fuzzy based machine learning techniques [15]. There is still no dataset available for MANETs. Therefore, we have simulated IDS datasets for MANET (IDS-MANET) in Network Simulator (NS-3). Data generation, feature selection, data collection, and classification into normal and malicious are necessary steps to execute IDS. Experimental results show the proposed method performs better than existing methods of intrusion detections in MANETs. The main contribution of our work is enumerated below.

1. We have simulated two routing disruption attacks in the MANET environment, namely blackhole and wormhole attack in NS-3, and generated packet captured (*.pcap) files for further steps.
2. A subset of significant features increases classification accuracy. In this work, we have analyzed 20 features and collected data for the system as the training set. This work is executed on different datasets, which differ in their size and characteristics.
3. This work has been executed on different classifiers such as Naive Bayes, Bayes Net, Radial Basis Function (RBF) Network, Multi-Layer Perceptron (MLP), Random Forest, and compared their performances. Finally, we provide the performance comparison of these classification methods to existing approaches.

The rest of this paper is arranged as follows. Section 2 provides detail of existing works. Section 3 describes the attacking nature of blackhole and wormhole attacks, while Section 4 introduces machine learning techniques and their working principles. We provide detailed descriptions of the proposed method in Section 5. Section 6 describes simulation details, experimental results, and performance comparisons to existing techniques. We conclude the proposed work in Section 7.

2 Related work

The IDS is an active monitoring system that generates an alert when it finds abnormal behavior of nodes. This section presents a literature review of IDSs in MANETs; we have found some Machine Learning (ML) algorithm-based IDSs and analyzed these works.

Table 1: Comparison of related works

Work	Simulator	Attack	ML	Limitation
Feng et al. [3]	NS-2	DoS	yes	System adopted 24 features of KDD'99 dataset. Deep learning model has achieved approx 98.5% detection rate.
Alappatt et al. [6]	NS-2	Blackhole, Greayhole	no	Cluster heads as additional nodes that store keys of corresponding members. Node mobility affect key exchange.
Qazi et al. [10]	NS-2	Wormhole	no	Above 90% detection rate and false positive rate almost 20%.
Jamali et al. [11]	NS-2	Wormhole	yes	Low detection rate.
Assia et al. [16]	Java	Blackhole	no	Attack identifies based on acknowledgment packets.
Pragya et al. [17]	NS-2	Collusion	no	Threshold-based collusion detection that allows 30% packets drop.
Panos et al. [18]	NS-3	Blackhole	no	Blackhole intensity is based on SQN where malicious node generates high-value fake source SQN.
Geetha et al. [19]	MatLab	Wormhole	no	Node behavior identifies based on the consumption of energy and resource utilization.
Kaur et al. [20]	NS-2	Wormhole	no	Delay based detection.
Sankara et al. [21]	NS-2	Wormhole	yes	Data interpretation risk is not considered.
Arthur et al. [22]	NS-2	Blackhole	yes	Small training and test sets.
Subba et al. [23]	NS-2	Blackhole	yes	Front-runner nodes consume more energy.
Elwahsh et al. [24]	*C#*	multiple	yes	Algorithm suggests only better classification method executed on KDD'99 dataset.
Islabudeen et al. [25]	NS-3	multiple	yes	Designed for MANET and tested on KDD'99 dataset.

Jamali et al. [11] proposed three parameters: residual energy, the distance between source to destination, and hop-count based fuzzy logic system. They showed that the detection rate is decreased when the misbehaving node ratio increases; however, the detection rate is increased when the simulation time is increased. Alappatt [6] hybridized the key exchange method of Diffie-Hellman and elliptic curve cryptography (HDHECC) using clustering nodes of MANET. This method provides centralized keys of corresponding members at the cluster

head that store all public keys. The cluster head as an additional node that acts as a router. Due to the dynamic nature of mobile nodes, these may frequently change their clusters. Then, these face the problem in key management and increase the overhead of cluster heads. Assia et al. [16] have assumed as the system generates one ack packet when non-attack for m hop route, while m-1 ack packets generate in case of attacks. In this system, each node maintains two tables named as TrustTable and PostTable. These tables storage requirements are about 6 KBytes of TrustTable and 125 KBytes of PostTable for 1000 nodes when 100 message transfer simultaneously. They have shown a better detection rate, and their system presented no storage constraint. Sankara et al. [21] analyzed seven features and suggested a detection method for wormhole attacks. They used RTT based threshold and applied Modified Secure AODV.

Pragya et al. [17] proposed threshold-based collusion attack detection. They compute the threshold as difference of sent packets and received packets by nodes. Their system allows packet loss by 30% as a normal node. Qazi et al. [10] computed Multi-rate Delay Per Hop Indication (M-DelPHI) such as processing time, queuing, channel access delay, and neighbor monitoring for wormhole attack detection. Their method performs better than DelPHI approach. Panos et al. [18] provided a new attack parameter as blackhole intensity, which quantified by a sequence number (SQN). They utilized a dynamic threshold cumulative sum to detect changes in the AODV sequence number's normal behavior. As their assumption, the malicious node generates and transmits an RREQ message, including an arbitrary high-value of fake source SQN. Geetha et al. [19] discussed malicious nodes are more active and consume higher energy when exchanging routing information. They assumed as faster communication requires security and developed a secure routing protocol. Kaur et al. [20] proposed a wormhole attack detection method that detects attack by computing end to end maximum delay between two nodes in the communication range. The source node decides the maximum delay of the threshold between two legitimate nodes.

Arthur et al. [22] designed an anomaly detection scheme for multi-cast communication based on distributed cross-layer. Their method extracts 75 features from two different collection modes that are 52 attributes from the routing layer and 23 from the MAC layer. They conclude 70% packet drops in the routing layer and remaining 30% packet drops due to retransmissions. Subba et al. [23] proposed a hybrid IDS based on cluster leader election. It comprises a threshold-based lightweight IDS and heavyweight IDS. Their results show that it maintains high performance and reduces IDS traffic; whenever cluster leaders consume more energy. Feng et al. [3] proposed a deep learning model and adopted 24 features of the KDD'99 dataset to detect attacks. Their method collect 196,000 XSS (160,000 normal and 36,000 attack) samples and 292,490 SQL (204,542 normal and 87,948 attack) samples for training the model. Conclusively, they reported that their method achieved approx 98.5% detection rate, 99.8% precision, and 99.8% accuracy. Elwahsh et al. [24] designed a hybrid framework to detect unknown attacks and utilized self-organized features maps and Genetic Algorithms (GA). They defined neu-

trosophic conditional variables and validated their experimental results on the KDD'99 dataset. Islabudeen et al [25] proposed Smart Approach for Intrusion Detection and Prevention System (SA-IDPS) and analyzed seven features of packets for intrusion detection. They used BOAT with ANN to enhance results and validated performance on the KDD'99 dataset.

We have extended detection schemes [8, 9] with many changes such as compress the datasets, machine learning techniques, reduce self signal from the dataset, different numbers of normal and malicious nodes, etc. Table 1 shows the related works that detect blackhole, wormhole, and other attacks in MANETs. Many are lightweight techniques that analyzed few network parameters such as acknowledgments, hop-counts, sequence number, message transfer mode, message counts, etc. These are not powerful enough to detect blackhole and wormhole attacks. A few works have applied the ML technique, which shown lower detection rates. There is still no unique method that generates datasets and efficiently applies ML techniques in MANETs to detect blackhole and wormhole attacks.

3 Problem definition

Routing disruption attacks affect the route selection and data transmission process in the network. Malicious nodes easily enter into a wireless network and attract routing packets during route creation by false information. These nodes advertise themself as a part of the destination and route reply through the reverse path to the sender node. Attacker nodes are dynamic that mainly modify hop count, sequence number and also send acknowledgment packets. Figure 1 shows the attacking nature of malicious node (M) in the network.

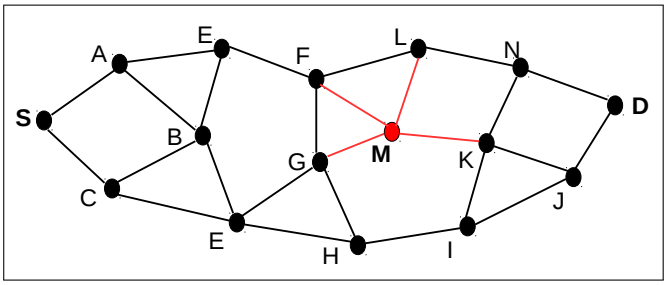


Fig. 1: MANET structure

The MANET contains a source (S) and destination (D) with many normal nodes. This network has many legitimate routes as SAEFLND, SCEHIJD, and others; whenever a malicious node attracts route request packets and replies, that deviates path selection towards malicious information. The sender node selects the shortest path as SAEFMD or SCEGMD, which does not exist.

A malicious node receives the packets and also sends false acknowledgment packets. Two or more malicious nodes can create a tunnel where data packets enter at one end and replay at another end. We have worked with two routing disruption attacks, which are the following.

3.1 Blackhole attack

A malicious node advertises itself having a valid route to the destination node by violating a routing property; then, it drops received packets without forwarding them [8]. A reactive protocol Ad-hoc On-demand Distance Vector (AODV), provides an on-demand route in MANETs. This routing protocol broadcast Route REQuest (RREQ) from a source node to a destination node containing information such as destination sequence number, a destination address, hop count, neighbors of the node, and their tables accordingly. This process iterates until RREQ reaches the destination node; then, it proceeds backward and reestablishes the reverse route send back Route REPly (RREP) to the sender node [16]. Finally, the source node receives more RREPs, and it chooses the best possible path as min hop count and max sequence number. The malicious node activities as blackhole attack are summarized below.

1. When a malicious node receives RREQ; then, it considers destination node information. It is set to the spoof destination address and prepares RREP.
2. The malicious node sends prepared RREP through the intermediate nodes or actual route.
3. When intermediate nodes receive RREP; then, it relays in the network and sends it to the source node through the reverse path.
4. The source node updates its routing table and uses received RREPs as min hop count and max sequence number.
5. Malicious nodes exploit or drop data [18], when they receive.

In this process, malicious nodes deviate to the source node; they spoof the destination address relatively smaller hop count and a higher sequence number. Hence, the malicious path is more probable to assigns routes by the source node.

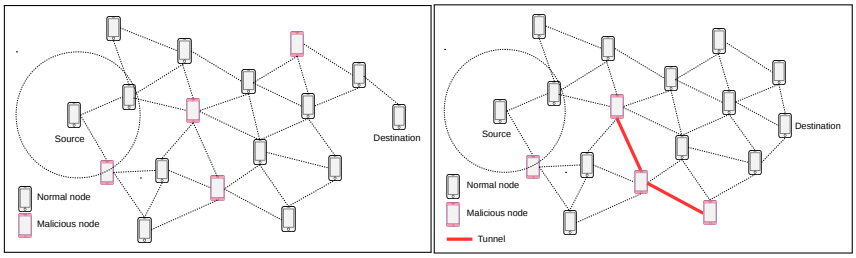
3.2 Wormhole attack

A wormhole attack is the most dominant MANETs security threat that can not immune to traditional security mechanisms. This attack performs whenever the network provides authenticity and confidentiality. In many models, a high-speed communication medium or directional antenna use for tunneling from one malicious node to another malicious node [11, 19]. However, the deployed network has the same functional nodes with the same radio range. In these attacks, a malicious AODV protocol defines attack behaviors for malicious nodes, and AODV protocol for normal nodes [20]. Two attackers in the network

try to maintain their locations strategically. They capture the RREQ packets and send RREP to the sender with min hop count [9, 10] and max sequence numbers. A malicious node attracts data packets and tunnels them other-end. This attack is dangerous for MANETs that disrupt the routing table and attract data packets by false information. The malicious node activities as a wormhole attack are summarized below.

1. When the malicious node receives RREQ; then, it includes false information of the destination by modifies hop count and sequence numbers.
2. Malicious node prepares RREP and sends it through intermediate nodes.
3. Then, intermediate nodes send received RREPs to the sender through a reverse path.
4. The source node updates the routing table and decides the data packet path based on the received RREPs or the routing table.
5. When the malicious node received data packets tunnel them, then replay at other-end [10, 11]. These packets may exploit by malicious nodes or move into the tunnel loop.

In this process, malicious nodes can disrupt routing tables, exploit data packets, misuse information, and move data packets into a loop route. They create a tunnel whenever another malicious node in the radio range. When the other malicious node is not in the radio range, it behaves as a blackhole attack.



(a) Blackhole attack (b) Wormhole attack

Fig. 2: Representation of attacks in the network

Fig. 2 represents the nature of attacks in the network as blackhole and wormhole attacks. It comprises malicious and normal nodes with their bidirectional communications. The node communicates to nodes (or neighbor nodes) that are in the radio range. Malicious nodes are in the Fig. 2a behave as blackhole attack. These nodes capture maximum data packets by spoofing routing packets and drop them. We have observed that minimum malicious nodes captured maximum routing and data packets. However, malicious nodes that behave as a wormhole attack create a tunnel. These malicious nodes (in Fig. 2b) tunnel the data packets and replay at other ends without addressing

them-self as a part of the path [9]. When multiple malicious nodes are not in the range; then, it does not create a tunnel, only dropping the data packets.

4 Classification mechanisms

4.1 Naive Bayes

A naive Bayes classifier is a probabilistic approach [26] that predicts network packet behavior. It also works for an unknown sample and predicts the most probable output. This classifier considers the discrete value of available X = $\{X_1, X_2, X_3, ..., X_m\}$ attributes and finite set C = {normal, malicious} behaviors of network packets.

$$P(c|x_1, x_2, ..., x_m) = P(x_1, x_2, ..., x_m|c)P(c) = P(c)\prod_{j=1}^{m} P(x_j|c), \tag{1}$$

where $x_i \in X_j$ and $c \in C$, Eq. 1 computes probabilities of classes that attributes are conditionally independent. It observes the sample probabilities, where the conjunction of the product of the probability of each attribute.

4.2 Bayes Net

The Bayesian network creates a Directed Acyclic Graph (DAG), G=(V, E), where $V = \{X_1, X_2, ..., X_m\}$ is a set of attributes as vertices and directed edges E between vertices [26]. It is also called Tree Augmented Naive Bayes (TANB) classifier.

$$I(X_i, X_j|C) = \sum_{x_i \in X_i} \sum_{x_j \in X_j} \sum_{c \in C} P(x_i, x_j, c) \log_2 \frac{P(x_i, x_j|c)}{P(x_i|c)P(x_j|c)}. \tag{2}$$

Eq. 2 computes edge weight between each possible attributes (X_i, X_j). The Maximum Weight Spanning Tree (MWST) method selects and assigns the direction of edges.

$$P(X_1, X_2, \ldots, X_m) = \prod_{j=1}^{m} P(X_j|Pa_j), \tag{3}$$

where Pa_j denotes the parent set of X_j and $P(X_j|Pa_j)$ is conditional distribution of attribute X_j. Eq. 3 computes the conditional probability of attributes which can learn by maximum estimation.

Bayesian network classifier is the supervised mode of training method, where each attribute is conditionally dependent on the class or label. Fig. 3 shows the attribute set {packet size, duration, header length, flag, hop count,

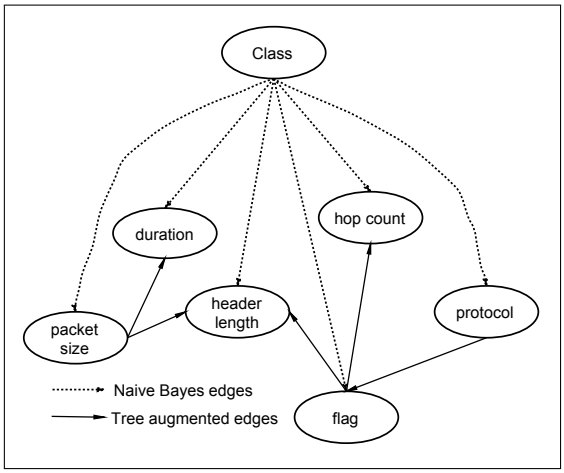


Fig. 3: Bayesian Network

protocol}, and edges between attributes. Naive Bayes edges are directed dotted line edges between class and attribute, and tree augmented edges are solid line edges between attributes that form MWST. It shows the conditionally dependent attribute among attributes.

4.3 Radial Basis Function Neural Network

Radial Basis Function (RBF) neural network consists of three-layer, namely input, hidden, and output layer. We provide input vector x=$\{x_1, x_2, ..., x_m\}$ to input layer, where m is a number of attributes. In this model, the hidden layer maps the input layer to high dimensional data with RBF, where the Gauss basis function is adopted as RBF [27].

$$h(x) = exp\Big(- \frac{(x-\mu)^2}{2\sigma^2}\Big), \tag{4}$$

$$f(x) = \sum_{j=1}^{m} w_j h_j(x), \tag{5}$$

where, $\sigma > 0$, $x \in X$ is input, μ is the mean of inputs, σ is standard deviation, and w denotes weight vector.

Fig. 4 shows the computational model for information processing of RBF network, where Eq. 4 is computed on hidden layer and Eq. 5 is computed on output layer.

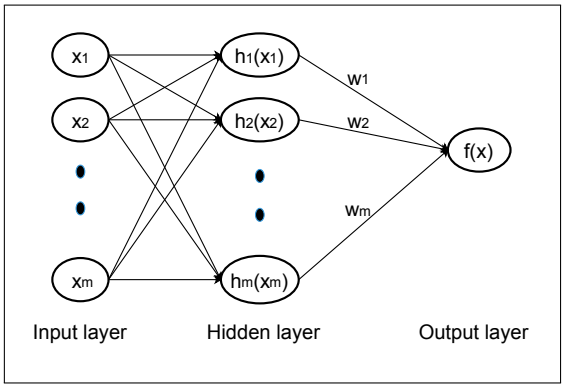


Fig. 4: RBF Network

4.4 Multilayer Perceptron

A multilayer artificial neural network is an interconnected group of artificial neurons that provides a computational model [28]. In this study, we have also considered a multilayer perceptron for predicting packet behavior in MANET, which consists of interconnected neurons as input layer and an output layer with a single hidden layer. The MLP is flexible regarding noisy data and able to generalize patterns from the training set for intrusion detection [29].

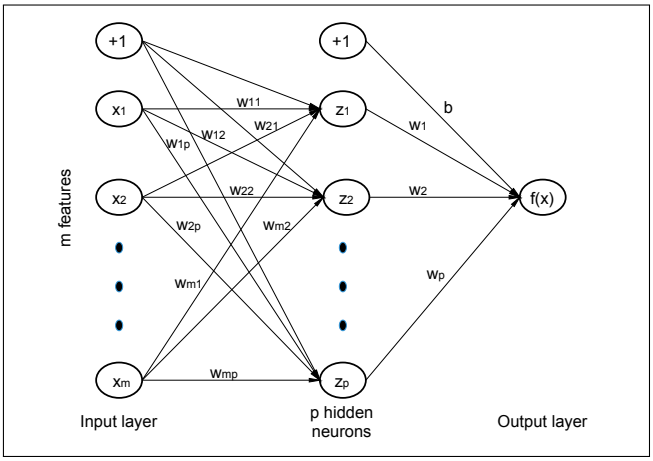


Fig. 5: Multi-layer Neural Network with single hidden layer

Fig. 5 shows a neuron model that x input signal received by input layer neurons. These inputs are weighted and summed together by the next layer

neurons. Finally, the threshold is treated as extra connection weight, and it is applied as an activation function at the output layer of this neuron model.

$$y = \sum_{j=1} w_j x_j + b, \tag{6}$$

where, w denotes the weight vectors, x is the input vector, and b is biased. The MLP is used as a classifier, the number of attributes as the number of inputs, and hidden neurons are computed using input and output neurons. This network provides outputs equal to the number of classes.

4.5 Random Forest

Random forest tree is also a popular classification technique that is a supervised learning algorithm. It creates decision trees on randomly selected data and provides a prediction of each tree, where the system selects the best decision by a majority of results [30].

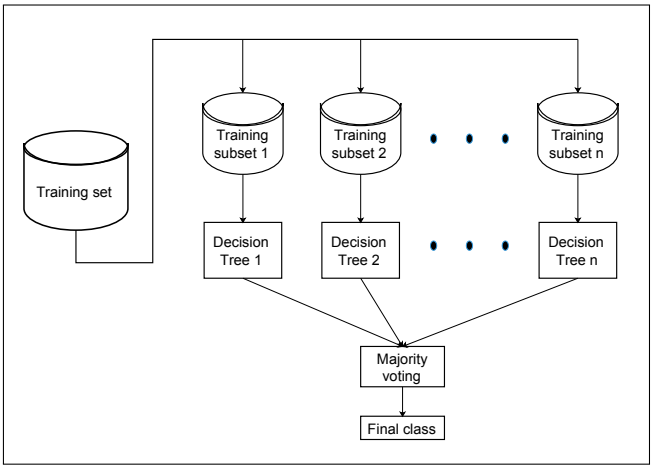


Fig. 6: Random Forest

Fig. 6 is the diagrammatic representation of a random forest method. Initially, it selects random samples as a training subset from a given dataset. Subsequently, this method constructs a decision tree for each training subset and predicts each decision tree's prediction result. Then, the next step performs voting for each predicted outcome. Finally, this selects the prediction result with the most votes as the final prediction. It has various applications such as recommendation systems, network packet behavior classification, feature selection, fraud detection, and disease prediction.

5 Proposed method

An IDS is a fast responding system that sends a warning when it finds any abnormality. This work applies classification techniques that classifies behaviors of received packets as normal or abnormal. The previous Section 4 describes detail procedures of classification techniques such as Naive Bayes, Bayesian Network, RBF, MLP, and Random Forest.

Algorithm 1 Malicious behavior detection

Input: nodes initial data
Output: confusion_matrix

input data
simulate attack in MANET.
each node capture *.pcap file.
export *.pcap data
select essential features.
store data into the database and label them.
apply classification methods (in Section 4) to analyze packet behavior.
store outcome into the confusion matrix $C_{m,m}$.
if $testpacket\_behavior = predicated\_behavior$ **then**
    increment $C_{r,r}$
else
    increment $C_{r,t}$
end if
return $C_{m,m}$

Algorithm 1 defines the classification model in MANET, which starts with input the node information as nodes initial position, number of normal and malicious nodes, node movement, radio range, etc. We simulate attacks in the MANET environment and capture *.pcap files at every node. Then, export packet data and analyzed them. The subsequent step selects a feature set that contains basic and derived features. After that, we store data into the database and label them based on transferring identification specifications. This work applies ML techniques to detect attack behaviors on the generated dataset in MANET environments. The working principles of classification mechanisms on the generated dataset are enumerated below in steps.

1. Initially, we generate the dataset to train learning algorithms, which detail the data generation process in Section 6.1. It also contains the extracted features (in Table 3). We have computed the efforts of feature generation and labeling efforts of datasets. In this work, we have generated eight different datasets (in Table 4) on different parameters and variations of nodes.
2. Data normalization is the foremost step for transferring string data into numeric data, and each feature data value scale into a proportionate range. We have applied the label encoding method to transfer symbolic values to distinct numeric values and normalized them into 0 to 1.

3. This step divides the dataset into training and testing sets. We have used the 10-cross validation method. It repeatedly trains and tests the whole sample into ten rounds.
4. The next step applies ML techniques, namely Naive Bayes, Bayesian network, RBF, MLP, and Random Forest, to detect malicious activities that detail working principles are described in Section 4.
5. Finally, it stores the outcome of classification mechanisms into confusion matrix and analyzes their results.

The malicious behavior detection model deploys at the node of the ad-hoc network that monitors neighbor nodes. When the node receives packet information from neighbor nodes, then analyzed data of both types (basic and derived) features, and classification method predicts the behavior of received data. Whenever the new node enters into the network; then, neighbors receive only basic features information. The proposed method is also suitable for computing the necessary information and predicting similar behavior to complete details. The MANET includes mobile nodes such as smartphones, laptops, tablets, cameras, sensors, and other network devices. When mobile nodes have insufficient memory space (i.e., sensors), we can deploy the classification model as agent-based intrusion detection (IDS nodes) [31] and the plug-and-play method [3]. In the first approach, some nodes work as agent-based intrusion detection that has sufficient memory space. These nodes (or IDS nodes) strategically maintain them-self in the network. In the plug-and-play approach, the classification model trains and transfers the function values or input weights. Nodes need memory space only for a test sample, calculative functions, and input weights. This approach consumes less memory space.

6 Experiments

6.1 Data preparation

The proposed method aims to learn the system using a generated training set; then, the node analyzes receiving packets in the system. These training sets are lightweight that consume less memory space and better computational complexities. We have tested the performance of the system's 10-fold cross-validation method. This approach simulates attacks in NS-3, where some nodes accommodate attack and data collection behaviors as a training set.

We have simulated blackhole and wormhole attacks and applied the proposed approach to detect packets behavior, which simulation parameters are shown in Table 2.

Fig. 7 shows the process of attack simulation and data collection in the database. Firstly, we define malicious and normal nodes in a MANET environment, where malicious nodes behave as attackers in a network that accommodates the attack's behaviors. Subsequently, the system gathers *.pcap files at every node and export data for feature selection. Then, it selects a set of

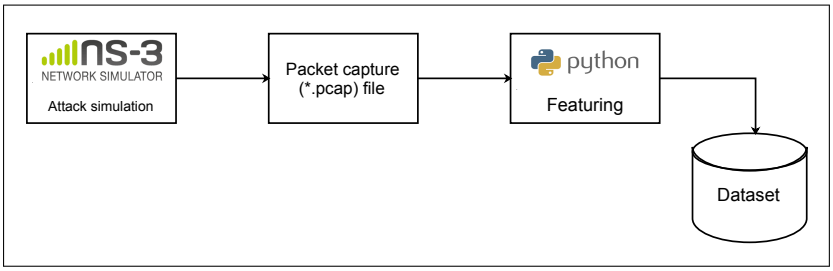


Fig. 7: Data preparation process

Table 2: Simulation parameters

Parameter	Values
Network Simulator	NS-3.25
Routing protocol	AODV
Channel	Wireless
Simulation area	1000x1000 $meter^2$
Number of nodes	20/30/40/50
Network topology	IEEE 802.11
Addressing mode	IPV4
Simulation time	100 seconds
Range of node	250 meters
Mobility of node	Random way point
Speed of node	2 m/s

features that is a combination of basic and derived features. Finally, we store the collected data in the database.

Table 3 contains a set of selected features, their data types, and generation efforts (Eff). A feature generation effort is computed as a simple inspection from the header file, comparison, and transforming data into other forms [32]. This feature set contains the maximum number of features that generation efforts are small (9 features) whenever medium (8 features), and high (3 features). However, the labeling efforts of the dataset are high that increases the labeling costs. The feature set generation effort and its performance confirm that it is suitable for detection systems. This feature set has twelve basic, and eight derived features are computed from the basic features. Initially, the basic features briefly introduce as duration is a time difference of the received packet. This network uses protocol as AODV, ICMP, etc. The flag shows the status of the message in the binary digit. Packet size and its header length are two different features. Hop count defines the number of intermediate nodes is a member of the path between the current node and destination, and sender to the current node as a request or response condition. Lifetime relates to node energy and message types define as RREQ, RREP, RERR, ACK. Destination sequence numbers show possible destination paths in the routing table that avoid the loop and unreachable destination. The message sequence number is generated by the sender and incremented by each receiver nodes. The sender node transfers the same message to neighbors that have the same stream in-

Table 3: Feature set

S.No.	Feature name	Type	Eff
1	duration	real	medium
2	protocol	string	small
3	packet size	integer	small
4	flag	integer	small
5	header length	integer	small
6	hop count	integer	medium
7	life time	integer	medium
8	message type	string	small
9	destination sequence number	integer	small
10	message sequence number	integer	small
11	stream index	integer	small
12	message transfer mode	binary	small
13	land	integer	medium
14	number of neighbors	integer	medium
15	highest flow	integer	medium
16	average flow	real	high
17	lowest flow	integer	medium
18	average hop count	real	high
19	number of failed connection	integer	medium
20	failed connection rate	real	high
21	label	string	high

dex. Message broadcast and unicast are two main message transfer modes that are represented in the binary digit.

Subsequently, the derived features as land when the sender and originator nodes are the same, different, and unknown represented by three different integer numbers. Many neighbors as several nodes in the radio range of the node. There are three features, such as the highest flow, average flow, and lowest flow show the activeness or dense region nodes by computing their transferring messages. An average hop count can calculate as the total hop count and amount of transferring the node's message. The node maintains a total number of moving messages and message types that also compute the failed connection rate.

Table 4: Dataset details

Dataset	Number of nodes		Number of samples			Memory space
	Normal	Malicious	Normal	Attack	Total	
Blackholeds1	16	4	804	72	876	75.1 KB
Blackholeds2	24	6	1412	123	1535	131.9 KB
Blackholeds3	32	8	7878	1078	8956	800.7 KB
Blackholeds4	40	10	8661	1166	9827	875.6 KB
Wormholeds1	16	4	7631	33141	40772	3.2 MB
Wormholeds2	26	4	17251	60898	78149	6.3 MB
Wormholeds3	36	4	18062	64298	82360	6.9 MB
Wormholeds4	46	4	31565	86509	118074	9.7 MB

We have generated eight datasets or four sets from each attack model that details are shown in Table 4. These datasets have different combinations of malicious and normal nodes. The random movement of nodes made their position unpredictable - a packet signal stores as a sample in the dataset, which the node sends to neighbors. Here, the dense neighbors and packet signal frequency increase the size of the dataset. We exclude self signals, or those signals contain the same sender and destination. Malicious nodes of the wormhole attack are more active compared to blackhole attack. They have generated more signals and shown profound changes in datasets. The last column shows occupied memory space by respective datasets in the range of 75.1 KB to 9.7 MB. The proposed system provides better results on small datasets or similar to large size datasets.

6.2 Performance metrics

The performance of the detection system evaluates using the confusion matrix. It computes statistical parameters and corresponding equations, which are the following.

$$TPR = \frac{TP}{TP + FN}, \tag{7}$$

$$FPR = \frac{FP}{FP + TN}, \tag{8}$$

$$Precision = \frac{TP}{TP + FP}, \tag{9}$$

$$F - measure = \frac{2 * TPR * Precision}{TPR + Precision}, \tag{10}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{11}$$

where, True Positive (TP) and True Negative (TN) are correct predictions of the detection system, while False Positive (FP) and False Negative (FN) are the wrong predictions. TP rate (TPR) is the correct detection rate, and the FP rate (FPR) is the system's incorrect detection rate. The system's high performance determines the higher value of TPR, Precision, F-measure, and a lower amount of FPR. F-measure is the harmonic mean of TPR and precision that evaluates the average performance; accuracy evaluates the overall performance.

Table 5: Statistical parameters of Blackhole dataset

Dataset	Classifier	Class	TP	TN	FP	FN
Blackholeds1	Naive Bayes	normal	699	69	3	105
		attack	69	699	105	3
	Bayes Net	normal	798	55	17	6
		attack	55	798	6	17
	RBF	normal	799	64	8	5
		attack	64	799	5	8
	MLP	normal	804	72	0	0
		attack	72	804	0	0
	Random Forest	normal	804	72	0	0
		attack	72	804	0	0
Blackholeds2	Naive Bayes	normal	1256	110	13	156
		attack	110	1256	156	13
	Bayes Net	normal	1334	105	18	78
		attack	105	1334	78	18
	RBF	normal	1397	57	66	15
		attack	57	1397	15	66
	MLP	normal	1404	104	19	8
		attack	104	1404	8	19
	Random Forest	normal	1407	104	19	5
		attack	104	1407	5	19
Blackholeds3	Naive Bayes	normal	7571	744	334	307
		attack	744	7571	307	334
	Bayes Net	normal	7685	751	327	193
		attack	751	7685	193	327
	RBF	normal	7727	652	426	151
		attack	652	7727	151	426
	MLP	normal	7841	941	137	37
		attack	941	7841	37	137
	Random Forest	normal	7868	977	101	10
		attack	977	7868	10	101
Blackholeds4	Naive Bayes	normal	8010	696	470	651
		attack	696	8010	651	470
	Bayes Net	normal	8062	838	328	599
		attack	838	8062	599	328
	RBF	normal	8248	639	527	413
		attack	639	8248	413	527
	MLP	normal	8462	855	311	199
		attack	855	8462	199	311
	Random Forest	normal	8598	989	177	63
		attack	989	8598	63	177

6.3 Experimental results

This subsection presents the experimental results of the proposed method for attack detection. Table 5 and Table 6 represent statistical parameters of blackhole and wormhole attacks as TP, TN, FP, FN which are computed using confusion matrix. Further, Table 7 represents experimental results as TPR, FPR, Precision, and F-measure. We have executed the proposed system with five classifiers and tabled their results. These tables have shown the comparative results of different classifiers and shown statistical measures that present the classifiers' accurate performance for each sample. The normal category's

Table 6: Statistical parameters of Wormhole dataset

Dataset	Classifier	Class	TP	TN	FP	FN
Wormholeds1	Naive Bayes	normal	7620	32546	595	11
		attack	32546	7620	11	595
	Bayes Net	normal	7631	32952	189	0
		attack	32952	7631	0	189
	RBF	normal	7513	32907	234	118
		attack	32907	7513	118	234
	MLP	normal	7631	33140	1	0
		attack	33140	7631	0	1
	Random Forest	normal	7631	33141	0	0
		attack	33141	7631	0	0
Wormholeds2	Naive Bayes	normal	17150	59572	1326	101
		attack	59572	17150	101	1326
	Bayes Net	normal	17247	60108	790	4
		attack	60108	17247	4	790
	RBF	normal	16671	59754	1144	580
		attack	59754	16671	580	1144
	MLP	normal	17242	60861	37	9
		attack	60861	17242	9	37
	Random Forest	normal	17246	60879	19	5
		attack	60879	17246	5	19
Wormholeds3	Naive Bayes	normal	18062	63174	1124	0
		attack	63174	18062	0	1124
	Bayes Net	normal	18061	63785	513	1
		attack	63785	18061	1	513
	RBF	normal	17780	63286	1012	282
		attack	63286	17780	282	1012
	MLP	normal	18062	64289	9	0
		attack	64289	18062	0	9
	Random Forest	normal	18062	64295	3	0
		attack	64295	18062	0	3
Wormholeds4	Naive Bayes	normal	31323	84096	2413	242
		attack	84096	31323	242	2413
	Bayes Net	normal	31553	84797	1712	12
		attack	84797	31553	12	1712
	RBF	normal	10045	28982	423	695
		attack	28982	10045	695	423
	MLP	normal	31527	86277	232	38
		attack	86277	31527	38	232
	Random Forest	normal	31541	86433	76	24
		attack	86433	31541	24	76

FP value indicates the number of attack samples that bypasses the detection system whenever FN increases overhead. Therefore, the higher TP and lower FP indicates a better detection system.

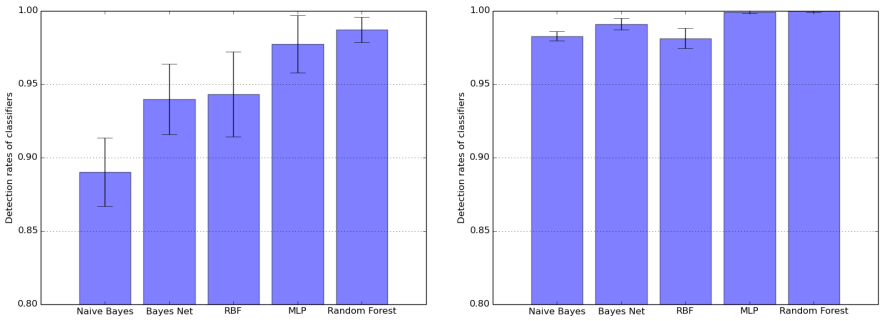
The evaluation finds that the wormhole attack achieves approx full positive detection rate that can not depend on the dataset size. Random forest classifier performs better than other classifiers, whereas MLP also provides similar performance as Random forest. As blackhole attack detection, the system performs better on the small training set that is a favorable sign for the ad-hoc networks. Experimental results have also shown that the MLP and Random Forest classification methods are more suitable to detect attacks or intrusions

Table 7: Comparative results of classifiers and best result is shown in boldface.

Dataset	Classifier	TPR	FPR	Precision	F-measure
Blackholeds1	Naive Bayes	0.877	0.049	0.946	0.928
	Bayes Net	0.974	0.217	0.973	0.973
	RBF	0.985	0.102	0.985	0.985
	MLP	**1.000**	**0.000**	**1.000**	**1.000**
	Random Forest	**1.000**	**0.000**	**1.000**	**1.000**
Blackholeds2	Naive Bayes	0.890	0.106	0.944	0.916
	Bayes Net	0.937	0.139	0.954	0.943
	RBF	0.947	0.494	0.942	0.944
	MLP	0.982	0.143	0.982	0.982
	Random Forest	**0.984**	**0.142**	**0.984**	**0.984**
Blackholeds3	Naive Bayes	0.928	0.277	0.928	0.928
	Bayes Net	0.942	0.270	0.939	0.940
	RBF	0.936	0.350	0.931	0.933
	MLP	0.981	0.112	0.980	0.980
	Random Forest	**0.988**	**0.083**	**0.988**	**0.988**
Blackholeds4	Naive Bayes	0.866	0.364	0.894	0.889
	Bayes Net	0.906	0.256	0.916	0.910
	RBF	0.904	0.404	0.900	0.902
	MLP	0.948	0.238	0.946	0.947
	Random Forest	**0.976**	**0.135**	**0.975**	**0.975**
Wormholeds1	Naive Bayes	0.985	0.005	0.986	0.985
	Bayes Net	0.995	0.001	0.995	0.995
	RBF	0.991	0.014	0.991	0.991
	MLP	**1.000**	**0.000**	**1.000**	**1.000**
	Random Forest	**1.000**	**0.000**	**1.000**	**1.000**
Wormholeds2	Naive Bayes	0.982	0.009	0.983	0.982
	Bayes Net	0.990	0.003	0.990	0.990
	RBF	0.978	0.030	0.978	0.978
	MLP	0.999	0.001	0.999	0.999
	Random Forest	**1.000**	**0.000**	**1.000**	**1.000**
Wormholeds3	Naive Bayes	0.986	0.004	0.987	0.986
	Bayes Net	0.994	0.002	0.994	0.994
	RBF	0.984	0.016	0.985	0.984
	MLP	**1.000**	**0.000**	**1.000**	**1.000**
	Random Forest	**1.000**	**0.000**	**1.000**	**1.000**
Wormholeds4	Naive Bayes	0.978	0.013	0.979	0.978
	Bayes Net	0.985	0.006	0.986	0.986
	RBF	0.972	0.051	0.972	0.972
	MLP	0.998	0.002	0.998	0.998
	Random Forest	**0.999**	**0.001**	**0.999**	**0.999**

in MANETs. These two classifiers have not predicted any false prediction on some datasets, or few samples are falsely predicted. A set of selected features (maximum features) took less effort to generate data and achieve a better detection rate. It is also observed that the feature set captures the maximum activities of nodes in networks. Moreover, the proposed work describes the enhanced mechanism for attack detection in MANET that shows the better detection rates.

Fig. 8 shows the classifier's average detection rates with its deviation. It presents the detection rates of Naive Bayes, Bayes Net, RBF, MLP, and Ran-



(a) Detection of Blackhole attack (b) Detection of Wormhole attack

Fig. 8: Performance of classifiers

dom Forest classifiers of blackhole attack (Fig. 8a) and wormhole attack (Fig. 8b). The proposed classification model evaluates the performance, such as consistency in performance, efficiently detects active malicious node samples, and is suitable for various size datasets. The experimental results show that wormhole attackers are more productive than blackhole attackers. They generate huge signals in a few seconds. Therefore, the wormhole dataset size is larger than the blockhole dataset; whenever the number of normal and malicious nodes is the same, and also the same simulation time. The deviation graph shows the minimum deviation of MLP and Random Forest classifiers. It confirms that these are better than other classifiers. Wormhole attack detection rates have achieved a peak position with a few deviations than blackhole attack.

6.4 Complexity analysis

The effect of the machine learning techniques in training and testing is analyzed in time and space complexities [13, 33]. We can compute the time complexity and space complexities using equations; where, the number of samples and features measures complexities. The number of comparisons defines time complexity.

$$Time\_Complexity(all\_training) = TT_R * TT_n, \tag{12}$$

where, TT_R is the number of training samples and TT_n is number of test samples. It computes the time complexity of the training set for all test samples.

$$Space\_Complexity = TT_R * nFeatures, \tag{13}$$

Table 8: Comparative complexities

Dataset	TT_R	TT_n	Time complexity	Space complexity	Memory size (in MB)
Blackholeds1	788	88	69344	1760	0.0067
Blackholeds2	1382	153	211446	3060	0.012
Blackholeds3	8060	896	7221760	17920	0.068
Blackholeds4	8844	983	8693652	19660	0.075
Wormholeds1	36695	4077	149605515	81540	0.311
Wormholeds2	70334	7815	549660210	156300	0.596
Wormholeds3	74124	8236	610485264	164720	0.628
Wormholeds4	106267	11807	1254694469	236140	0.901

where, nFeatures represents number of features, Eq. 13 computes the space complexity of the training set.

$$Space\_Complexity(NaiveBayes\_function) = nClass * nFeatures, \quad (14)$$

where, nClass is number of classes or labels in training set, Eq. 14 computes the space complexity of probabilistic functions of Naive Bayes classifier.

$$Space\_Complexity(BayesNet\_function) = nClass * nFeatures + \varphi, \quad (15)$$

where, φ represents the link of nodes (directed Edges); these directed edges are represented using a matrix or linked list. Eq. 15 computes the space complexity of probabilistic functions of the Bayesian Network for a test sample.

$$Space\_Complexity(RandomForest) = nTree * nFeatures + \epsilon, \quad (16)$$

where, nTree is number of tree constructed during the execution and ϵ is an extra space which takes during voting and decision. Eq. 16 computes the space complexity of functional values of features of the Random Forest classifier.

$$Space\_Complexity(NN\_weight) = nHidden * nFeatures + \epsilon, \quad (17)$$

where, nHidden is the number of hidden layer of Neural Network (NN), Eq. 17 computes the space complexity of input weights of Artificial NN.

$$MemorySize(inMB) = \frac{4 * nSamples * nFeatures}{1024^2}, \quad (18)$$

where, nSample is number of samples, Eq. 18 computes the memory size of the dataset. We have assumed that a single (cell) value of the dataset consumes 4-byte memory.

We have applied 10-fold cross validation method; therefore, TT_R (90%) and TT_n (10%). Table 8 presents TT_R, TT_n, Time and space complexities, and memory size (in MB) of training set . Table 9 shows the approx space

Table 9: Complexities of functions or input weights of classifiers

Classifier	Space complexity (approx)
Naive Bayes	2*20 = 40 (Eq. 14), 40*4 (Eq. 18) = 160 byte
Bayes Net	2*20 + 20 = 60 (Eq. 15), 60*4 (Eq. 18) = 240 byte
RBF	1*20 + 2 = 22 (Eq. 17), 22*4 (Eq. 18) = 88 byte
MLP	1*20 + 2 = 22 (Eq. 17), 22*4 (Eq. 18) = 88 byte
Random Forest	5*20 + 5 = 105 (16), 105*4 (18) = 420 byte

complexity of function or input weights of the classifiers that compute using equations. It is computed using nHidden = 1, nFeatures = 20, nClass = 2, φ = nFeatures, nTree = 5, $\epsilon = 2$ (for NN) and $\epsilon = 5$ (for Random Forest). This computation shows the RBF and MLP consumes less memory for function or input weights.

6.5 Performance comparison

The proposed method is different from cryptographic and traditional wired IDSs that is compatible with node mobility. In the cryptographic technique, the main difficulties of key exchange from intermediate nodes when continually changing their positions. Some methods cluster the nodes and store keys of corresponding members at cluster heads, while these heads act as the router for their clusters. When the nodes move into other clusters, then increase the overhead of cluster heads and key management. An attacker can easily modify or provide false acknowledgments; then, acknowledgments based attack prevention techniques [16] may not mitigate attacks. Whenever lightweight methods analyze a few network parameters [10, 11]; therefore, these are not powerful enough to prevent attacks. Some IDSs datasets are publicly available for a wired network whenever there is no such dataset available for MANETs. Therefore, we have generated lightweight datasets for the MANET environment. These have collected data with 20 extracted features and labeled for the supervised mode of training methods. This work simulates routing attacks as blackhole and wormhole that can drop or tunnel the encrypted packets. Most of the existing techniques are executed in NS-2 and others, whenever we have executed the proposed work in NS-3. This work is not used any additional hardware such as directional antennas, timer, and high-speed communication medium. It consumes the minimum network resources and provides better performance than existing methods.

We have analyzed the packet behaviors based on multiple characteristics rather than only acknowledgment signals, energy of packets, delay of packets, round trip time, message sequence number, and hop count. This work has also analyzed the characteristics of MANETs and suggested a significant feature set, which leads to organizing the training set. It overcomes the limitations of detection mechanisms (in Table 1) and increases detection accuracy. In MANET, DAWA is a defending approach using fuzzy logic and an artificial immune system that defends a wormhole attack. DAWA is lightweight IDS

Table 10: Comparative performance

Algorithm	Accuracy (%)	FPR (%)
C4.5 [24]	93.23	1.65
SVM [24]	87.18	3.20
C4.5 + ACO [24]	95.06	0.87
SVM + ACO [24]	90.82	2.42
C4.5 + PSO [24]	95.37	0.72
SVM + PSO [24]	91.57	1.94
EDADT [24]	98.12	0.18
Neutrosophic GA [24]	99.36	**0.09**
SA-IDPS [25]	99.74	0.14
Proposed (MLP-IDS)	**99.83**	0.20

that shows a low detection rate [11]. M-DelPHI detection mechanism achieved 90% TPR and 20% FPR that resists a wormhole attack [10]. The deep learning algorithm [3] is executed on 24 features and achieved 98.5% detection rate. There is no dataset online available for intrusion detection in MANETs. Therefore, many authors validate their works on the KDD'99 dataset [3, 24, 25]. We have also executed the MLP on the KDD'99 dataset and tabled (in Table 10) comparative results. The dataset has been divided into equal training and test sets that are labeled as normal and abnormal. We have shown the comparative results and evaluated the complexities of five classifiers such as Naive Bayes, Bayes Net, RBF, MLP, and Random Forest. These results show better performances and lesser complexities of the MLP. It also achieves a better detection accuracy than existing methods.

6.6 Analysis of variance (ANOVA)

We have evaluated this scheme through a statistical ANOVA test. It is used to test differences between two or more means, and computes test statistic (F value). This test obtains probability (P value) that assume the null hypothesis when the means of different populations are equal [34]. The work assumes five different populations and mathematically defines null hypothesis as H_0: $\mu_1 = \mu_2 = \mu_3 = \mu_4 = \mu_5$. Here, it also defines an alternate hypothesis when at least one mean is different. We have conducted ANOVA with our simulations

Table 11: Data summary of classification mechanisms in terms of F-measure

Methods	Blackhole attack			Wormhole attack		
	Mean	Std. Dev.	Std. Error	Mean	Std. Dev.	Std. Error
Naive Bayes	0.9153	0.0184	0.0092	0.9828	0.0036	0.0018
Bayes Net	0.9415	0.0257	0.0129	0.9913	0.0041	0.0021
RBF	0.9410	0.0343	0.0172	0.9813	0.0081	0.0041
MLP	0.9773	0.0221	0.0110	0.9993	0.0010	0.0005
Random Forest	0.9868	0.0104	0.0052	0.9998	0.0005	0.0003

Table 12: Comparison of statistical values in terms of F-measure for Blackhole attack detection

Source	SS	DF	MS	F value	P value	F critical
Between groups	0.0137	4	0.0034	6.184	0.0038	3.056
Within groups	0.0083	15	0.0006			
Total	0.0220	19				
Note: Sum of square (SS), Degrees of freedom (DF), and Mean square (MS).						

Table 13: Comparison of statistical values in terms of F-measure for Wormhole attack detection

Source	SS	DF	MS	F value	P value	F critical
Between groups	0.0012	4	0.0003	15.9216	0	3.056
Within groups	0.0003	15	0			
Total	0.0015	19				
Note: Sum of square (SS), Degrees of freedom (DF), and Mean square (MS).						

against attack detection with five different techniques outcome on F-measure for both types of attacks. This statistical test confirms the significance of the proposed scheme, that significance level α_{ANOVA} is 0.05, and the results of ANOVA are shown in Tables 11, 12, and 13. These tables visualize the ANOVA test for all performance $Fvalue > Fcritical$ that rejects the null hypothesis. Table 11 shows that all means are different due to this fact $Pvalue < 0.05$.

Table 11 contains the data summary of the statistical test as Mean, Standard Deviation (Std. Dev.), Standard (Std.) Error of Blackhole and Wormhole attacks detection for five classification mechanisms. It shows the different means for all performance with minimum deviations and errors. Whenever, Tables 12 and 13 show statistical values of the ANOVA test for both routing attack detection mechanisms. We have performed the statistical test on F-measure that is the harmonic mean of Recall and Precision of the system performance; thus, it also confirms the system performance as Recall and Precision.

7 Conclusion

The research work proposed a novel method of intrusion detection in MANETs. It selects a set of significant features that covers the maximum characteristics of nodes in networks. We have simulated two different routing disruption attacks in NS-3 and collected adequate data for the training set. Then, the classification technique classifies receiving packet signals. This work considers the maximum characteristics of networks and provides a higher detection rate than existing algorithms without using any external hardware or network resources.

Overall, the experimental result has shown the best performance of the proposed method to actively detect malicious packets. In this system, we have characterized significant features that increased the detection capacity. The

proposed method can be applied in military services, social area security, search operations, where wireless intruders are more active. This work can inspire researchers from the area of MANET security, wireless network security, or intrusion detection in any wireless network, which can also deal with many challenging tasks. The proposed method's performance encourages us to extend this method using unsupervised learning techniques that remove labeling costs.

References

1. Myria Bouhaddi, Mohammed Said Radjef, and Kamel Adi. An efficient intrusion detection in resource-constrained mobile ad-hoc networks. *Computers & Security*, 76:156–177, 2018.
2. Aikaterini Mitrokotsa and Christos Dimitrakakis. Intrusion detection in manet using classification algorithms: The effects of cost and model selection. *Ad Hoc Networks*, 11(1):226–237, 2013.
3. Fang Feng, Xin Liu, Binbin Yong, Rui Zhou, and Qingguo Zhou. Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. *Ad Hoc Networks*, 84:82–89, 2019.
4. Dimitrios Papakostas, Soheil Eshghi, Dimitrios Katsaros, and Leandros Tassiulas. Energy-aware backbone formation in military multilayer ad hoc networks. *Ad Hoc Networks*, 81:17–44, 2018.
5. G Akilarasu and S Mercy Shalinie. Wormhole-free routing and dos attack defense in wireless mesh networks. *Wireless Networks*, 23(6):1709–1718, 2017.
6. Valanto Alappatt and PM Joe Prathap. Hybrid cryptographic algorithm based key management scheme in manet. *Materials Today: Proceedings*, 2020.
7. Gulshan Kumar, Mritunjay Kumar Rai, and Rahul Saha. Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in wireless sensor networks. *Journal of Network and Computer Applications*, 99:10–16, 2017.
8. Mahendra Prasad, Sachin Tripathi, and Keshav Dahal. Intrusion detection in ad hoc network using machine learning technique. In *International Conference on Big Data, Machine Learning, and Applications*, pages 60–71. Springer, 2019.
9. Mahendra Prasad, Sachin Tripathi, and Keshav Dahal. Wormhole attack detection in ad hoc network using machine learning technique. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–7. IEEE, 2019.
10. Shams Qazi, Raad Raad, Yi Mu, and Willy Susilo. Multirate delphi to secure multirate ad hoc networks against wormhole attacks. *Journal of Information Security and Applications*, 39:31–40, 2018.

11. Shahram Jamali and Reza Fotohi. Dawa: Defending against wormhole attack in manets by using fuzzy logic and artificial immune system. *the Journal of Supercomputing*, 73(12):5173–5196, 2017.
12. Mohammad Wazid and Ashok Kumar Das. A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks. *Wireless Personal Communications*, 94(3):1165–1191, 2017.
13. Mahendra Prasad, Sachin Tripathi, and Keshav Dahal. An efficient feature selection based bayesian and rough set approach for intrusion detection. *Applied Soft Computing*, 87:105980, 2020.
14. Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419, 2020.
15. Mohammad Masdari and Hemn Khezri. A survey and taxonomy of the fuzzy signature-based intrusion detection systems. *Applied Soft Computing*, page 106301, 2020.
16. Assia Hammamouche, Mawloud Omar, Nabil Djebari, and Abdelkamel Tari. Lightweight reputation-based approach against simple and cooperative black-hole attacks for manet. *Journal of information security and applications*, 43:12–20, 2018.
17. Mishra Pragya, KV Arya, and Singh Hardev Pal. Intrusion detection system against colluding misbehavior in manets. *Wireless Personal Communications*, 100(2):491–503, 2018.
18. Christoforos Panos, Chirstoforos Ntantogian, Stefanos Malliaros, and Christos Xenakis. Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. *Computer Networks*, 113:94–110, 2017.
19. SB Geetha and Venkanagouda C Patil. Graph-based energy supportive routing protocol to resist wormhole attack in mobile adhoc network. *Wireless Personal Communications*, 97(1):859–880, 2017.
20. Parvinder Kaur, Dalveer Kaur, and Rajiv Mahajan. Wormhole attack detection technique in mobile ad hoc networks. *Wireless Personal Communications*, 97(2):2939–2950, 2017.
21. S Sankara Narayanan and G Murugaboopathi. Modified secure aodv protocol to prevent wormhole attack in manet. *Concurrency and Computation: Practice and Experience*, 32(4):e5017, 2020.
22. Menaka Pushpa Arthur and Kathiravan Kannan. Cross-layer based multiclass intrusion detection system for secure multicast communication of manet in military networks. *Wireless Networks*, 22(3):1035–1059, 2016.
23. Basant Subba, Santosh Biswas, and Sushanta Karmakar. Intrusion detection in mobile ad-hoc networks: Bayesian game formulation. *Engineering Science and Technology, an International Journal*, 19(2):782–799, 2016.
24. Haitham Elwahsh, Mona Gamal, AA Salama, and Ibrahim M El-Henawy. A novel approach for classifying manets attacks with a neutrosophic intelligent system based on genetic algorithm. *Security and Communication Networks*, 2018, 2018.

25. M Islabudeen and MK Kavitha Devi. A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks. *Wireless Personal Communications*, 112(1):193–224, 2020.
26. V Muralidharan and V Sugumaran. A comparative study of naïve bayes classifier and bayes net classifier for fault diagnosis of monoblock centrifugal pump using wavelet analysis. *Applied Soft Computing*, 12(8):2023–2029, 2012.
27. Haiying Li, Yitang Wang, Xinyue Xu, Lingqiao Qin, and Hanyu Zhang. Short-term passenger flow prediction under passenger flow control using a dynamic radial basis function network. *Applied Soft Computing*, 83:105620, 2019.
28. Nancy Masih, Huma Naz, and Sachin Ahuja. Multilayer perceptron based deep neural network for early detection of coronary heart disease. *Health and Technology*, 11(1):127–138, 2021.
29. Lediona Nishani and Marenglen Biba. Machine learning for intrusion detection in manet: a state-of-the-art survey. *Journal of Intelligent Information Systems*, 46(2):391–407, 2016.
30. A Murugan, S Anu H Nair, and KP Sanal Kumar. Detection of skin cancer using svm, random forest and knn classifiers. *Journal of medical systems*, 43(8):269, 2019.
31. M Mohanapriya and Ilango Krishnamurthi. Modified dsr protocol for detection and removal of selective black hole attack in manet. *Computers & Electrical Engineering*, 40(2):530–538, 2014.
32. Mahendra Prasad, Sachin Tripathi, and Keshav Dahal. Unsupervised feature selection and cluster center initialization based arbitrary shaped clusters for intrusion detection. *Computers & Security*, 99:102062, 2020.
33. Raman Singh, Harish Kumar, and RK Singla. An intrusion detection system using network traffic profiling and online sequential extreme learning machine. *Expert Systems with Applications*, 42(22):8609–8624, 2015.
34. Abhinav Tomar, Kumar Nitesh, and Prasanta K Jana. An efficient scheme for trajectory design of mobile chargers in wireless sensor networks. *Wireless Networks*, 26(2):897–912, 2020.