REPUBLIC OF TURKEY

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Information Technologies

INTELLIGENT SECURITY SYSTEM FOR MOBILE ADHOC NETWORKS BASED ON MACHINE LEARNING

Marwa KHALIFA

Master of Science

Supervisor

Prof. Osman Nuri UCAN

Istanbul, 2022

INTELLIGENT SECURITY SYSTEM FOR MOBILE ADHOC NETWORKS BASED ON MACHINE LEARNING

Marwa KHALIFA

Information Technologies

Master of Science

ALTINBAŞ UNIVERSITY

2022

The thesis titled " INTELLIGENT SECURITY SYSTEM FOR MOBILE ADHOC NETWORKS BASED ON MACHINE LEARNI " prepared MARWA KHALIFA and submitted on 9/10/2022 has been **accepted unanimously** for the degree of Master of Science in Information Technologies

Prof. Dr. Osman Nuri UÇAN

Supervisor

Thesis Defense Jury Members:

Prof. Dr. Osman Nuri UÇAN	Faculty of Engineering and Architecture, Altinbas University	_____
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Faculty of Engineering and Architecture, Altinbas University	_____
Prof. Dr. Hasan Hüseyin Balık	School of Computer Engineering, Yıldız Teknik Universty	_____

I hereby declare that this thesis meets all format and submission requirements of a master thesis

Submission date of the thesis to the Graduate Education Institute: ___/___/___

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Marwa KHALIFA

Signature

DEDICATION

I dedicate this research to everyone who supports me.To the souls of my mother, father, and mother-in-law To my beloved husband, Ahmed Qasim To my two precious angels, Yamen and Taleen To all my sisters and brothers To all of my friends.

ACKNOWLEDGEMENTS

Thanks to Dr. Osman Nuri UCAN, my research supervisor at the Turkish University of Altnbaş, I was able to carry out my project. With great pleasure, I would like to convey my sincere thanks to my co-advisor, Dr. Khattab M. Ali Alheeti, who has supported me greatly in my research and for his enormous efforts in leading me to this project. In addition, I would like to express my gratitude to my close friends, Hanaa Khudher and Shahad Mahdi, for their support and guidance.

ABSTRACT

INTELLIGENT SECURITY SYSTEM FOR MOBILE ADHOC NETWORKS BASED ON MACHINE LEARNING

Khalifa, Marwa,

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Prof. Dr. Osman nuri UCAN

Date: 01/2022

Pages: 81

Mobile Ad-hoc Networks (MANET) provide a service through network applications in one way or another. In many diverse fields, such as tactical networks used in military communications and environmental applications, the network is used as business networks such as Personal Area Network (PAN). They are used in educational environments such as schools and linked to Internet networks to expand coverage. Because of the multiple characteristics of MANET, including high-level mobility, node decentralization, physical insecurity, etc. MANET networks are susceptible to a variety of possible threats active or passive. MANET units (devices) are surveilled using detection technology to differentiate between ordinary and harmful actions. Therefore, Classification was accomplished utilize artificial intelligence with unsupervised Machine Learning (ML) approaches, which comprise the Random Forest (RF), Support Vector Machine (SVM), and Naïve-Bayes (NB) algorithms. Depending on a training samples in the feature space. The suggested Intrusion Detection System (IDS) is composed of the following basic stages: the traffic generation stage, the network simulation stage, the data collection. Five steps just for pre-processing a data set, the training stage, and the testing stage. We generated the dataset using Network Simulator-2 (NS2). The proposed system tested with dataset extracted from the trace file of network simulator. performance metrics are calculated: Confusing Matrix, Accuracy

rate, Error rate, Precision, Recall, F1. Besides determining each algorithm's training and testing duration. The findings revealed that the suggested system yielded promising outcomes, the accuracy rate of the R.F. algorithms reached 100%, SVM =99.18%, and NB =94.33%. Using trial and error feature selection improves the system and reduces training and testing time complexity. High levels of detection capacities and performance metrics have been evaluated by comparing and analyzing the results.

Keywords: Ad-hoc Mobile Networks, Intrusion Detection System, Network Simulator, Machine Learning.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

MANET	:	MOBILE AD- HOC NETWORK
ML	:	MACHINE LEARNING
IDS	:	INTRUSION DETECTION SYSTEM
RF	:	RANDOM FOREST
SVM	:	SUPPORT VECTOR MACHINE
NB	:	NAÏVE BAYES
SMOTE	:	SYNTHETIC MINORITY OVERSAMPLING TECHNIQUES
DOS	:	DENIAL-OF-SERVICE
NS-2	:	NETWORK SIMULATOR-2
TP	:	TRUE POSITIVE
TN	:	TRUE NEGATIVE
FN	:	FALSE NEGATIVE
FP	:	FALSE POSITIVE
DSDV	:	DISTANCE SEQUENCED DISTANCE VECTOR ROUTING PROTOCOL
OLSR	:	OPTIMIZED LINK STATE ROUTING
DSR	:	DYNAMIC SOURCE ROUTING
AODV	:	AD HOC ON-DEMAND DISTANCE VECTOR
NAM	:	NETWORK ANIMATOR

1. INTRODUCTION AND LITERATURE REVIEW

1.1 MOBILE ADHOC NETWORK

MANET is made up of wirelessly devices that are attached (node or hub). It could be a mobile phone, a laptop, or any other device connecting wirelessly to other devices. That means that the MANET structure is always changing, indicating that new nodes can be added or other nodes can break away from the network, and so on without restriction, where the nodes move freely and arbitrarily.

When it comes to the self-configuration and decentralization of a MANET network that is made up of a network of nodes responsible for the formation and discovery of new nodes and acting as a router, they interact with each other. MANET is cost-effective since it connects locations where a stable infrastructure cannot be established. It is possible to link MANET network to internet or even other networks. allowing them to communicate across longer distances[1][2]. Figure1.1 shows MANET network.

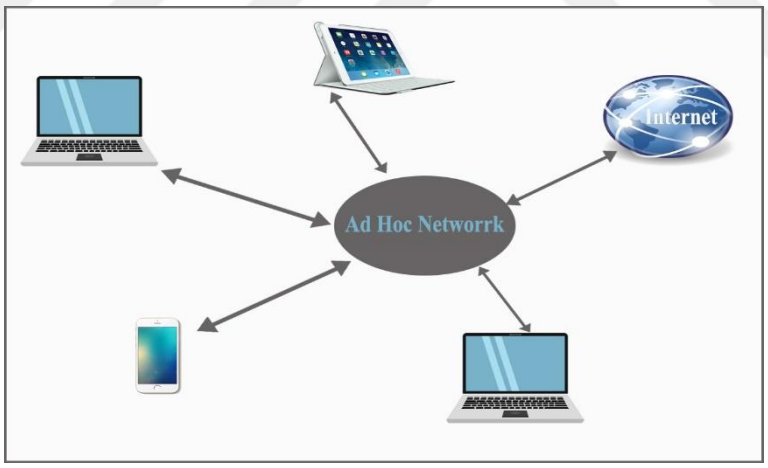


Figure 1.1: MANET Network

Wireless communication connections can be set up between nodes that are in the same broadcast spread. There is a chance the links will be broken. Every node can be powered by one or more radio interfaces, each with a different transmitting capacity and operating at different radio frequencies.

1.2 MOTIVATION

Considering MANET networks can be utilised in a number of important ways in a different fields, like,tactical networks used in military communications, and specific networks such as home

applications and environmental applications such as monitoring weather activities and the body area network. MANET, sometimes known as a Personal Area Network (PAN), is operated as a home's or companies network., similar to electronic commerce and vehicle services. Furthermore, it is often used in emergencies such as their utilize in catastrophic events such as tremors, cyclones, and so on. Additionally, it is utilized in civil and commercial settings. It is also used in schools and online education for educational purposes. It has also been used to expand Internet network coverage[3].Therefore, this thesis seeks to develop a protection system capable of monitoring assaults through the use of ML approach in order to backup network security that is susceptible to a variety of active and passive attacks.

1.3 RELATED WORKS

Several researchers are improving MANET networks' security. Studies on this topic have been given in this section. The following are summaries of some of these studies:

Almomani and et al. (2021) Compare a variety of ML models to determine which one is the most effective at identifying attacks. The UNSW-NB15 data - set is utilized in the evaluation of ML models. The system is evaluated using standard assessment metrics. According to the results, The RF exceeds many algorithms in high accuracy (87%), F1, and sensitivity[4].

M. A. Saranya and et al. (2020) describe and discuss a study of systems that apply machine learning to analyze intrusions. It makes use of KDD'99 Cup data -set used in this analysis. Their performance was evaluated to test classification and regression tree approaches, this study used the LDA, CART, and RF. algorithms. In terms of accuracy, the R.F. algorithm outperforms the LDA, CART algorithms by 99.81%[5].

K. Sakthidasan Sankaran and et al. (2021) described a machine learning strategy based on recurrent reward (R.R.) that they call stable neighbor selection (SNS). Neighbors are rewarded depending on their contact qualities once the nodes are pre-classified in the suggested neighbor option. The projected reward is recursively reviewed throughout the transmission to select the most efficient path nodes. Classifications of nodes that have been made. To get to the desired area, each hop level has been checked. if everyone agrees on raising anomaly detection ratio and reducing delay, the network's delivery ratio will improve[6].

Liyange S. R. & Jinarajadasa G. M. (2020) presented Critical evaluations of machine learning (ML) and other methods for enhancing MANET confidence were offered by the researchers. According to the researchers, ML is superior to other processes and appears to be suited for use in ad hoc networks since it is adaptive and can predict the network's newly connected node. In comparison to the other methods, Q-Learning provides the most accurate results[7].

Node misconduct in ad-hoc networks may be detected with the help of machine learning, and Kanthimathi and Jhansi Rani Prathuri(2020) presented a comparison between the support vector machine (SVM) and the back-propagation neuron in order to attain a safety ratio in these networks. An evaluation of the network's ability to detect malicious nodes (BPNN) found that BPNN technology is more efficient than SVM technology in this regard[8].

Li and et al.(2019) presented for enhancing MANET routing efficiency, implemented diagnosing anomalies with provenance and verification (DAPV approach). DAPV is reliable When it comes to discovery, directly and indirectly, routing opponents. DAPV uses peer archives and Merkle-based hashing Trees to find the secure and Reliable neighbourhood. This is superior to the average discovery process in terms of time and indirect costs[9].

Cai and et al.(2019) presented Evolutionary self-cooperative trust (ESCT) in MANETs to reduce routing dispersion. This safe routing scheme simulates user interference and predicts the path of reliable nodes on various levels. The scheme's dependable feature ,its unflappable resistance to established assaults. at each stage of attack detection, decision-making is new. This scheme produces a dependable network result that can be calculated. Energy consumption, lag, and packet distribution rate are all factors to consider[10].

Vaseer and et al (2019) introduced a node activity & response for the categorization approach., the technique is flexible enough to operate against assaults like (DOS). Attacks can be calculated based on how nodes react to their neighbors, assuring packet delivery. The lag ratio and package delivery were used to demonstrate the algorithm's performance[11].

Zhang and et al. (2019) For increased adaptability and dissemination, they used connectivity resources and used a recommendation-based confidence assessment for the MANET scenario. The confidence model's adaptive essence is evaluated based on packet transmission rate, energy reservation, range, knowledge, and node integrity. The assailant's effect is reduced by the

confidence model, which enhances single-to-one metrics validation. This aids in the verification of the node's consistency; following transmissions are based on a medium level of confidence. By appropriately analyzing the nodes' confidence, we may help boost the detection rate[12].

Veerraju Gampala et al. (2021) The goal in their research was to look into the Mobile ad - hoc requirements. Networks specifying and configuring infrastructure for the use of enhanced systems that can promote contact among healthcare bodies and emergency physicians throughout shipboard activities. The job tests on multiple levels. Our investigation focused on finding whether the commercial off-the-shelf radios (COTS) MANET will enable interactions between medical staff in the ship-to-ship ambience in emergencies through augmented Reality equipment[13].

Arush S.Sharma and Dongsoo S.kim(2021)They described a mobile ad hoc routing method that relies on wireless routing paths to save energy, adopts the social behaviours of ant colonies to provide decent, strong routing paths from source to destination and addresses challenges such as restricted Bandwidth, battery life, memory, and so on. The individual impact factor was examined to address these obstacles. This algorithm was matched to AODV, which is a way to route traffic. Correspond factors like efficiency, latency, packet drop, and internet lifetime., and so on. the proposed algorithm was found to be 49 percent of the network's lifetime in terms of performance measures[14].

MohanPatsariya & Anand Rajavat(2021) presents these verification techniques and the effect of different factors on the node, where the node is examined upon entry to the node and the influence of factors such as movement patterns, store management, and energy consumption method. Factors NCAODV performs better than AODV[15].

Mechtri and et al. (2018) Designed a system called(MASID-R-SA) in response to threats to avoid attacks where In the path from source to destination, the suspicious node is reported in the preceding and following nodes , aim to provide a more dependable and safe route, and the number of false alerts in the network decreases despite the nature of MANET networks that operate individually as They are distinguished by the enormous list of possible attacks that they are by attempting to regulate the rate of Error Detection This technique improves package transportation while minimizing waits[16].

Zhang and et .al. (2019) proposed a system that would manage reputation. this system handles malicious attacks and enhances network performance. It consists of gathering trust data and calculating its values. They proposed a novel approach of obtaining confidence for enhancing trust in data collection capacity. Due to the subjective and recommendation trust, they have designed a model for a node reputation value calculation. The results showed the high efficiency of this model[17].

Sakthidasan and et al.(2019) The optimized affinity propagation-based routing protocol applied The study describes a clustering-based routing strategy for wireless networks with time-ticklish WSNs. This method uses less energy and It employs clustering and routing techniques to optimize the performance. Various criteria are used to assess the validity of the provided technique, and the offered solution outperforms current approaches significantly.[18].

Li Jiang et al.(2020) An Ad Hoc network topology control model is proposed in Their research paper. An Ad Hoc network is setting up using the associated network model, with the main goals of topology control in mind. Topology control-related factors are synthetically calculated, and the main topology control protocol is developed using OPNET. The network analysis and simulation techniques validate the algorithm's efficiency, reduce the network's power consumption, improve end-to-end data transmission, and achieve well the mobile Ad Hoc network's reliability. It enhances mobile predictive capabilities and ensures network availability and business efficiency[19].

Daniil S. Meitis and et.al. (2020) The BATS code is discussed in this article, as well as its execution by ns-3 simulation, the overview for decoding efficiency, & a rationale for its application in FANET are all discussed. From the user's perspective, BATS is a type of technology that blends binary linear network software development and waterfalls.. In the case of unreliable connections, BATS seems to be very effective. Disaster preparedness, prevention, and response using a drone network are one of the potential applications[20].

Sayan Majumder and et al. (2019) The A.D. (Absolute Deviation) statistical method was proposed for wormhole attack prevention. The utilization of absolute deviation covariance and correlation enables for the rapid discovery of wormhole attacks. There are no additional requirements for running the proposed methodology. Wormhole attackers construct a bogus tube from source to

destination. When the first course is taken, a lot of time is spent. Thus,, the time spent preventing wormhole attackers from entering the network must be carefully measured. The whole variance strategy yields superior results, according to simulations. The Absolute Deviation Correlation Coefficient, as opposed to AODV, is frequently used to locate wormholes[21].

Usman Zeb and et al. (2020) Their paper's goal is to offer a recommended model for a variety of move ranges employing MANET routing protocols like (DSDV), (DSR), as well as (AODV). The simulation criterion chosen for examination using NS-2.35 are End-to-End lateness, throughput, and (PDR) utilized energy NS-2.35. The results could be utilized to improve the efficiency of transmitting capacity[22].

Kavitha and et al. (2017) The main problem of connection loss within the mobile ad hoc network dynamic topology was presented. As a result, they suggested an Instant Route Migration protocol in this article, which includes constructing an immediate path that takes into account path distance and hops count. They introduced a partial topology conscious mechanism to quickly find the shortest route with the support of this process, packets to the target can be easily rerouted in the event of a connection failure, as cache maintenance is current at every node. According to the gathered data, the suggested model gives optimal efficiency, less end-to-end latency, and immediate route migration when compared to methods that already exist[23].

Li Jiang and et al. (2020) a MANET is a network independent structure that supports multi-hop communication and is made up of a community of cluster heads equipped with wireless transceivers. Supporting mobile prediction and improving Qos learning algorithm in ad hoc network has become a pertinent study subject as the size of network applications grows. algorithm for Qos active path detection and management based on mobile prediction is proposed based on MAODV. The optimization algorithm will minimize routing overhead and increase data transfer success rates, according to simulation results[24].

Bo Cui and et al. (2018) Mobile devices can now catch all types of media and interact wirelessly with an increasing number of network technology. Local content owners distribute their content for a variety of reasons. They develop and a modern decentralized P2P system called (HRSS) to enable effective data exchange among mobile devices in MANETs to fix the challenge of information share among foreigners in a limited and clustered environment[25].

1.4 PROBLEM STATEMENT

Ad hoc mobile networks faces many problems due to the independence of the nodes, which in turn can expose the network to internal and external attacks, whether passive or active, where the danger lies in the possibility of stealing information or leaving the network out of service. Due to the difficulty in manage nodes; it is hard to detect potentially hazardous nodes in MANET., and difficulties are facing the network Such as routing packets, packet delivery ratio, power shortage, losses when the link between nodes fails.

1.5 THESIS OBJECTIVES

The purpose of the present study is to design and implement a security system for ad hoc networks using machine learning techniques, whereby many learning approaches are conducted to enhance orientation as soon as possible in MANET networks using multiple algorithms of machine learning. A plan must be offered in order to present the main goal of our research. Pursue the sub-objectives indicated below:

i. Studying of MANET networks security; the challenges they faced, requirements, and most types of potential both passive and active assault affecting the network's various tiers network.

ii. Study the requirements of IDS and the challenges facing MANET networks to achieve the security system.

iii. To implement the security system for MANET networks using more than one of the ML algorithms: RF, SVM and NaiveBayes, comparison between their performance and selection of the most appropriate.

iv. Eexplain types and taxonomy of data packet routing operations.

v. Training and testing of algorithms using a data set that we generated using NS2.

1.6 MAIN CONTRIBUTIONS

This work presents contributions:

i. Suggesting and styling an IDS to discover intrusion as well as potential threats especially (black hole attack) in MANET networks.

ii. Improves network performance by detecting abnormal nodes using the machine learning techniques R.F., SVM, NB.

iii. With the help of NS2, we enable to create a dataset for using in training / testing process.

iv. Processes of selection of the attributes to enhance computation time as well as accuracy rate by selecting feature by trial and error method.

1.7 THESIS STRUCTURE

Five chapters make up this research:

Chapter one is : [introduction] to the entire research: adding to this chapter, the insides of individual chapters of this thesis are briefly reviewed.
Chapter two: [Background Information] presents the background of ad-hoc network technology.

Chapter three: [The Proposed System] explains the steps of the suggested system and the techniques used. A whole description of the suggested system is given.
Chapter four: [Results and Discussion] contain the outcomes of the tests that implemented to estimate system performance. The results of experimental examinations are discussed.

Chapter five: [Conclusions and Future Works] conclude the thesis and explore directions for future work.

2. THEORETICAL BACKGROUND

Even though the MANET is proving to be a success, it is a tool that can be used in several applications. Securing it may be a difficult task in some places. Because of the MANET design of wireless mobile communication, as opposed to static wired networks, it is less secure in data and physical protection. In addition, security technologies designed for static wired networks are difficult to apply to MANET wireless networks[3].

This chapter explores the history of MANET as well as network applications for many fields., and the security system in terms of the challenges facing their application and the requirements for security to create a strong security system in addition to the types of passive and active attacks that attack the different MANET layers. We explained the intrusion detection system used in MANET networks to keep tabs on network activity and identify suspicious behaviour nodes, the basic units of this system challenges facing the system, its requirements, and finally, the machine learning techniques used in MANET were. We explained the types of ML used in our security system: RF, SVM, NB, then Explained the concept of routing protocols and their types. It is worth noting that the type of routing protocol that was used in our system is DSR.

2.1 HISTORY OF MANET

The first model was introduced in 1972. It was known as PRNET at the time (Packet Radio Networks). MANET networks have their origins in the 1970s DoD1 research. When the Department of Defense-funded the packet radio network (PRNET) for military usage along with ALOHA (Area Locations for Hazardous Weather) and CSMA (Medium Sense Carrier Access), two methods to access control. PRNET has been used testable to supply networking application functionality as a medium and type of remote routing. It was in the 1980s that the second generation of MANET networks developed when the SURAN was launched (Survivable Adaptive Radio Networks) software improved and introduced MANET systems That is, in a location where there is no technology network is supplied it. This effort enhanced the efficiency of transmitters by making them simpler, less costly, and more sensitive to cyber threats. With the introduction of notebook computers and other feasible communication devices in the 1990s, the notion of

trade MANET networks was born. Many other research conventions suggested the concept of a series of mobile nodes at a similar time. Much work has been performed on ad hoc criteria since the mid-1990s.Wireless local area networks are the most well-known wireless network WLANs [26]

2.2 MANET APPLICATIONS

MANET finds its application in the Military field, Sensor devices networks, Commercial field, medical services, Personal Area Networks(PAN) [27], Private networks to cover emergency disasters, applications for trade, housing[28][29]. The basic MANET strategies are developed for military purposes. Locally, MANET networks may be connected with multimedia networks via a computer for sharing information with persons in a classroom or a meeting; In the future, PAN is technically a promising application area for MANET.

2.3 SECURITY OF ADHOC NETWORK

Because of MANET's flaws, it confronts some obstacles regarding information transfer. As a result of the nature of wireless transmission. MANET security is challenging to achieve with wireless connections, limited physical security, autonomous behavior, transit, and dispersed infrastructure [28]. We discovered flaws in the MANET network, and they do not have safety restrictions like wired networks. In an attack, the wired network makes it difficult to access the media because it must pass through the protective layer and the network gateway, which is not the case with MANET. If the node's Bandwidth is detected [29], the attack is simple because MANET does not have any security limits[27]. Wired networks may readily access an electric power supply when it comes to energy. The energy supply in MANET is limited, and the nodes sometimes take over the energy source [29]. Because decentralized administration makes it impossible to identify the attack, dynamically ensure data traffic, and restrict its transmission, MANET is managed in a decentralized way, which causes problems with connection reliability [25]. The general assumption of MANETs is that the nodes are cooperative and do not hurt one another. A potential hacker can become a critical router element by refusing to follow the procedure criteria and disrupting the entire network [30].

Figure 2. security of MANET networks is depicted as a diagram, with sections based on challenges, requirements of security, as well as various kinds of attacks, both active and passive.

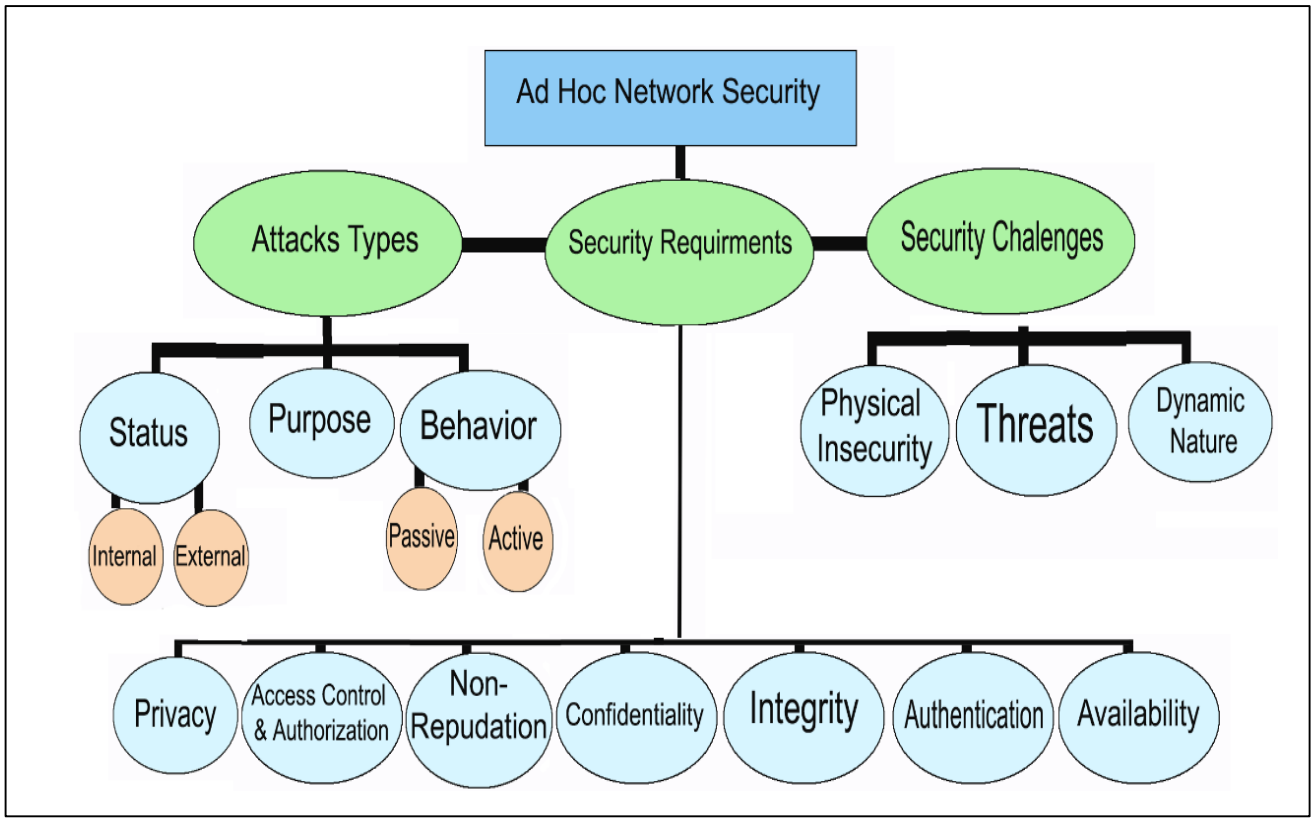


Figure 2.1: Adhoc Network Security[30]

2.3.1 The Challenges to Security

The nature of mobile ad hoc networks presented numerous security concerns that could be considered when developing security standards. These difficulties can be summed up as follows[31][32][33]:

i. Threats: Wireless communication is vulnerable to both passive and violent attacks. Data leaks, nodes, and text alterations are all possible hazards. All of these attacks must have a plan in place.

ii. Physical Protection: Harmful node Because of the design of nodes, assaults are hard to detect. Separated, poorly protected, and difficult to monitor, allowing an adversary to break into the network and kidnap nodes.

iii. Dynamic nature: Because mobile ad hoc networks are dynamic, with nodes joining and leaving at any time, safety procedures with predefined structures do not match the dynamic network structure, necessitating the use of a distributed safety framework.

2.3.2 Requirements of Security (The Goals):

i. Availability: Ensures that the service is accessible even in the face of threats. Mechanisms must be able to work with a lot of dangers, such as Active Interference such as DoS attacks and energy attacks. Node malfeasance and starvation[33].

ii. Authentication: is primarily concerned with achieving protection in networks in general, and MANET networks in particular, because each new node in MANET networks must be authenticated in order to communicate only with trusted nodes; this is advantageous for authentication because it allows for differentiation between the damaging node and the original node, thereby achieving network information and communication security [34].

iii. Integrity: ensures that no user messes with or manipulates data passing via the network. The consumer who receives the data must then verify that the contents and sender are not the work of a network hacker or malware[35].

iv. Confidentiality: ensures that only the intended node has access to information. There are no nodes; only a source and recipient exist. The node can read the details. That is accomplished through the use of data encryption technologies.

v. Non-repudiation: This refers to the fact that data transferred cannot be refuted by either the sender or the recipient.

vi. Control of access and authorization: The client or the authorized node must freely access data and resources without being restricted in any way. It also points out that no user is permitted to receive data or resources outside their designated responsibility scope.

vii. Privacy policy: Any data related to a single node only, such as node identification, keys, organic metrics, and position, is referred as privacy data.

2.3.3 Types of Attacks

There are a variety of MANET attacks according to [36]:

i. Status: MANET network threats might occur on the inside or outside, referring to either a node attack from within the network that is difficult to detect or an external node attack.

ii. Behavior: The type of attack determines the attacker's response, which is characterized as passive or active. The passive attacks do not cause network harm, but they undertake illegal surveillance and do not change the data transit stream. The network is unaffected by passive attacks. In the case of active attacks, the network is slowed, the infrastructure is harmed, and data transmission pathways are altered.

iii. Purpose: The attackers' goals vary; some assaults, such as DoS, Seeks to compromise the service's integrity and network availability; others, such as data privacy and integrity attacks, aim to gather confidential information such as network topology and data sent and received.

Other threats include eavesdropping and data distortion, and routing and redirect attacks. Refusal of service and service termination[37].

2.4 ATTACKS ON DIFFERENT LAYERS OF MANET

MANET networks protocol package is structured into layers. We'll go over the types of passive or active attacks that could be used against these tiers in MANET [38]. The network may be attacked with an active or passive security attack or both types.

2.4.1 The Attacks of the Physical Layer

On the hardware level, an assault on this layer requires support from technology sources. Therefore, it does not matter if the attacker has high technical abilities. We give a list of these assaults here:

i. Eavesdropping attacks: is a passive attack. The malicious node reads and listens to the messages between network nodes and intercepts data transmission between approved nodes[39]. This attack is difficult to detect because it does not cause damage, but in the future, network resources will be targeted with significant information, like passwords, hidden keys, or eavesdropped website data[30].

ii. Active Interference: It is a (DOS) that This messes with the wireless channel in some way. The attack results differ according to the period of the attack and the procedure used[40]. The attacker may also respond to messages and distort them.

iii. Jamming attacks: In such an attack, the malicious node tracks the sending process between the transmitting and receiving nodes to determine the receiving node frequency and then sends signals to the same frequency to prevent messages from being received[41].

2.4.2 The Attacks on MAC Layer (Link Layer)

MAC layer is vulnerable to several denials of service attacks. These attacks have a general impact on the network.[42] such as energy exhaustion and lack of detection of routing paths, or breaking of the connecting node. The attacks are listed below:

i. Selfish Misbehavior: The egoist node may not damage other nodes. In this kind of onslaught, in addition to reducing the network's efficiency through rejection to participate in the protocols routing, projection, and not sending packets. The primary aim is to save its own communications battery. The result is network latency and bottleneck results.

ii. Malicious misbehavior: malicious nodes deliberately harm other nodes and weaken network efficiency in these kinds of attacks, integrity attacks, DoS assaults and deceptive

network attacks fall into this category, and as the node density in contact increases, so does the intensity of the attacks.

iii. The analysis of traffic attack: In this attempt, the attacker obtains data like node position, network architecture, node position, source, and destination data by examining traffic style in the network.

2.4.3 Network Layer's Attacks

This layer's rules allow hop-by-hop connectivity in which each node takes route decisions Therefore, this layer can be easily attacked by Unauthorized nodes[30]. There can be many attacks. However, we have compiled a list of some of the more well-known assaults here.

i. Attack of a wormhole: A malicious node establishes a pipe or wormhole (digital link) with another malicious node in this attack. This attack is very risky since all information and other paths must pass through the wormhole. Protocols fail the capacity to discern this form of attack, so a security system should secure protocols with the preventive ability[43].

ii. Black-hole Attack: the node that is behaving abnormally impersonates a legitimate node in the path of routing. It is programmed to send a phony response using the shortest route. When the node is in the routing direction, it will either use or route the packages to accomplish their goals.[44] [45] describe a method for detecting and eliminating attacks from black holes.

iii. Sinkhole Attack: its most dangerous attack, in which an attacker node tries to pass all packets to its neighbors in an opportunistic manner. Other disadvantages include reducing the number of hops and increasing packet sequence counts; however, some nodes may notice that a safe shortest route passes through the fraudulent node in this route.

iv. Attack of rushing: Upon request routing protocols target rushing assaults. These attacks were exposed to route discovery. When The penetrate node A routing demand message from source point, It inundates the connection with messages before any other node receiving a certain route request packet can respond [38]. This attack is vulnerable to Upon request routing protocols such as DSDV and others that suppress redundancy during route discovery.

v. Replay Attack: Due to the constantly changing structure in MANET, the attacking node in this type of attack gets set up and controls messages between the authorized nodes and the message store, then the malicious node returns the messages until the routing process is disabled.

vi. Attack on Link Spoofing: Fake control messages are used by a malicious node to deceive others into thinking they are from a legitimate node.

vii. Attack of Sybil: A malignant node pretends to be a large number of other nodes in this attack by generating false names. Sybil is the name given to such fictitious identities that appear to be several nodes. These Sybil either create their personalities or Impersonate those of approved nodes.

2.4.4 Attacks on Transportation Layer

Since the transport layer is more secure than the network layer; so, it is less susceptible to attacks., and the following assaults are listed here:

i. Hijacking of a Session: The beginning portion of a meeting that is inherently risky or poorly guarded is hijacked. When the intruder pretends to be the targeted node's IP address, DoS attack is launched against the system as soon as the correct sequence number is discovered Hackers are looking for passcodes, ID numbers, and hidden keys in order to get access to it information system.

ii. SYN Flooding: Attackers who use this kind of DOS assault, launch a huge number of incomplete TCP connections at once. That never fulfill the handshaking operation to begin full communication. As a result, as per the concept of a DOS attack, this assault often Depleted network resources while performing no beneficial operation.

2.4.5 Attacks on The Application Layer

This layer's protocols are more susceptible to attack-like (DOS) attacks. Web, SMTP, and FTP procedures are all supported by this layer of services and information.

i. Attack via Malicious Code: Users' devices and software would be affected by this form of assault. Viruses, worms, spyware, Trojan Horses, and other malware threats.

ii. Repudiation attack: In this assault, the framework or implementation loses govern of tracking or logging the user's activities, enabling malicious exploitation. Incorrect information is documented in the log file. Often protection protocols implemented at multiple levels are insufficient. As a consequence, a firewall at the application layer is needed to prevent malicious behavior. Table 2.1 illustrates the sort of attacks that can be expected. MANET networks are exposed in different layers and clarifies the types of According upon that attacker's illegal actions. we note a large number of active attacks on the network layer, where this layer is exposed to the most types of active attacks.

Table 2.1: Types of Layer Attacks

Layers	Types of attackers	Active behavior	Passive behavior
Physical	Eavesdropping		✓
	Active Interference	✓	
	Jamming	✓	
MAC	Selfish Misbehavior	✓	
	Malicious Misbehavior	✓	
	The analysis of traffic		✓
Network	Wormhole	✓	
	Black hole	✓	
	Sinkhole	✓	
	Rushing	✓	
	Replay	✓	
	Attack on link spoofing	✓	
	Attack of Sybil	✓	
Transport	Hijacking of a Session	✓	
	SYN Flooding		✓
Application	Attack via Malicious Code	✓	
	Repudiation Attack	✓	

2.5 AN INTRUSION DETECTION SYSTEM (IDS)

By breaching the network's first line of defense, which comprises dependable approval, security, remote entry, and safe transportation, security assaults may infiltrate networks, rendering them insecure. (IDS) is quietly stationed next to first layer of protection. Trying to detect and prevent threats before they have a possibility to do significant damage [46]. " A comprehensive system that tracks actions in networked computers; performs examination of inconsistencies that may have occurred to violate the protection rules of the system, unlawful connectivity from either a harmful or allowed element is classified " .According to the IDS definition which is programmed to automatically analyze attempts to violate the security, reliability, or authenticity of a system[47]. The following are the main responsibilities of IDS:

i. It analyze network traffic.

ii. Discovering unsafe activity in networked devices.

iii. Starting the alert, if any undesirable activity is observed.

That MANET study have helped build a security solution that includes data collection, pre-processing, Classification of network nodes behavior. Achieving good results according to the performance measures used.

2.5.1 The Basic Module of IDS

i. Data Collection: This module is in charge of gathering audit data from the device that is being tracked.

ii. Data Preprocessing: One or more separate preprocessors create this module. This service module aims to quantify and convert audit data into a structure that is compatible with the following module.

iii. Intrusion Recognition: This unit is in control of detecting suspicious activity by the intrusion model's instructions.

iv. Intrusion Model: The security admin provides this module, which includes behaviour samples of previously identified intrusions. This module also includes guidelines for matching newly received examined data to profiles. It can also extract information about unusual behaviour from examined data and update them appropriately.

v. Reporting and Response: If the intruder detecting module detects an intrusion, this module is in charge of raising the alert[48].

2.5.2 MANET's IDS Challenges

Many of the hurdles IDS encounters in MANET will be presented. These should be taken into account when ad hoc network IDS development, The following are the major obstacles [49]:

i. Inadequate central management: Mobility is supported by MANET. As a result, it is preferable to create collaborative and distributive IDS when there isn't any center server in several situations.

ii. Topological Change: regular topological change requires using IDS with scalable frameworks.

iii. Lack of clearly defined bounds: MANET networks are subject to unconstrained assault because they absence obviously identified limitations.

iv. Various protocols: Changes in network design need the development of innovative protocols. That protocols may open the door to additional complex threats. As a result, the IDS must demonstrate usability to assimilation these protocols and the ability to respond to recently discovered attacks.

v. Restricted Bandwidth: Ad hoc networks only have a specific amount of Bandwidth. as a result of this obstacle, MANET limits the source of power available to its nodes. As a result, IDS must utilize method of computing with a small overhead.

vi. Limited Energy Resources: MANET restricts energy resources for its nodes. As a result, IDS should employ a low-computing technique.

vii. Support for encryption: IDS must support encryption so that data is not easily exposed if agents take over or are hacked.

2.5.3 The IDS Requirements in MANET

For the implementation of the IDS system in MANET, there are specific requirements that can be summarized as follows:

i. IDS Reliability: The IDS has to be dependable. To run in the background without the need for user intervention or supervision.

ii. Accept fault: It must manage and accept fault when a machine crash. It should not be necessary to rebuild the framework any time the system is relaunched.

iii. Self- surveillance: In addition to network surveillance, IDS can control itself for matters such as sabotage and other vulnerabilities.

iv. Overhead costs: IDS should have as few overhead costs as possible on the device or networks when checking for normal activity.

v. Template Adoption: Various systems utilize multiple usage patterns. As a result, the IDS should also efficiently adjust to new styles.

vi. Flexible scalability: if new apps are added to the system, IDS must be capable of adapting its behaviour in reply to environmental conditions.

vii. Hard to deceive: IDS must be hard to deceive and distinguish legal and illegal modification.

2.6 APPROACHES OF MACHINE LEARNING (ML)

ML is a pattern detection technology based on artificial intelligence. Its goal is to educate machines on how to perform specified tasks on their own. Machine learning in intrusion detection combines knowledge and experience from accessible data to teach the system how to cluster or classify new unknown data. Machine learning techniques are classified into two groups. The first is supervised machine learning approaches, which are the most extensively utilized; they are simple to implement and comprehend. It is akin to using flashcards to teach a toddler. They train algorithms using samples with labels, and the algorithms learn based on the relationship between the samples and the labels. The second class is unsupervised machine learning approaches, which differ from the first in that there are no labels and the algorithms understand data features by presenting them with large amounts of data and some guidance[50].

In the proposed system, RF, NB, and SVM within supervised type were used to classify our data generated by ns2. Figure 2.2 explains the types of ML.

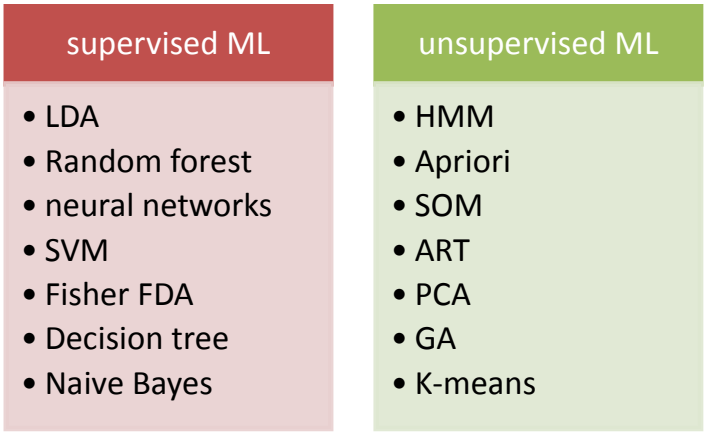


Figure 2.2: Types of ML

There are numerous uses for ML, such as recognition of graphics and voice, as well as automated language interpretation., online fraud detection, email spam and malware filtering [51], self-driving cars [52], biomedical[53], etc. In this thesis, we used RF, SVM, and NB to train and test the proposed security system. Following lines describes the used ML techniques in this thesis:

i. Random Forest: Breiman introduced the supervised classification method., in which a forest is constructed from a group of trees in analyzing a new entry. One of the outcomes is its relevance in selecting several options for each tree, and it was discovered through experimental research that this algorithm is the most accurate in terms of prediction accuracy[54].

ii. Naïve Bayes: is one of the most common artificial intelligence techniques. the premise of feature independence supports its effectiveness. indicates it's able to make predictions for many classifications simultaneously. The Bayes Concept supports it. Probability classifiers are models which analyze multiple categories. The conditional likelihood is used to make the decision. Instead of a single algorithm, this paradigm employs a group of algorithms that having a similar idea. Each feature is supposed to provide an equivalent and distinct ratio to the result in this paradigm. The model has a notable benefit than other models in that it requires relatively minimal training data. [55].

iii. Support Vector Machine: It is a ML analysis method including associated learning methods that assists in examining behaviours for segmentation or regression operations in order to increase forecasting efficiency and eliminate unnecessary input. It is a categorization method that uses binary values. The primary objective of SVM include to create an ideal capable of discriminating between two linearly class labels [56].

2.7 ROUTING PROTOCOL IN MANET

Routing is the activity of determining the most efficient path for transferring data from source and destination nodes. Because MANET is changeable architecture, the wired routing protocol does

not perform well. Routing is usually accomplished using the current MANET routing protocols. Structural considerations, frequency limits error-prone shared broadcast radio stations, secret and revealed terminal problems, and resource limitations all decrease the performance of routing algorithms[57]. The evaluation of a MANET routing protocol is based on characteristics including as:

i. Upkeep of dynamic topology.
ii. Power control that is efficient.
iii. Routing time is reduced.
iv. Effective utilization of existing Bandwidth.
v. Broken routes are quickly reconfigured.
vi. Synchronization of Time.
vii. Communication that is safe.

Recurrent changes in network topology have a significant impact on network efficiency as the routing path can be interrupted due to the movement of intermediate or peripheral nodes, increasing routing consumption and time to recover the interrupted path.

In some instances, a new algorithm or updated algorithms are required for successful routing. A routing algorithm's implementation focuses on one or more of The most common ways for classifying MANET routing systems. It is based on how mobile nodes get and keep track of routing information [57].

2.7.1 Taxonomy of MANET Routing Protocol

The most common way for classifying MANET routing systems. It's based on how mobile nodes get and keep track of routing information. Routing protocols are classified into three main

categories: proactive, reactive, and hybrid routing protocols. This classification demonstrated in Figure 2.3.

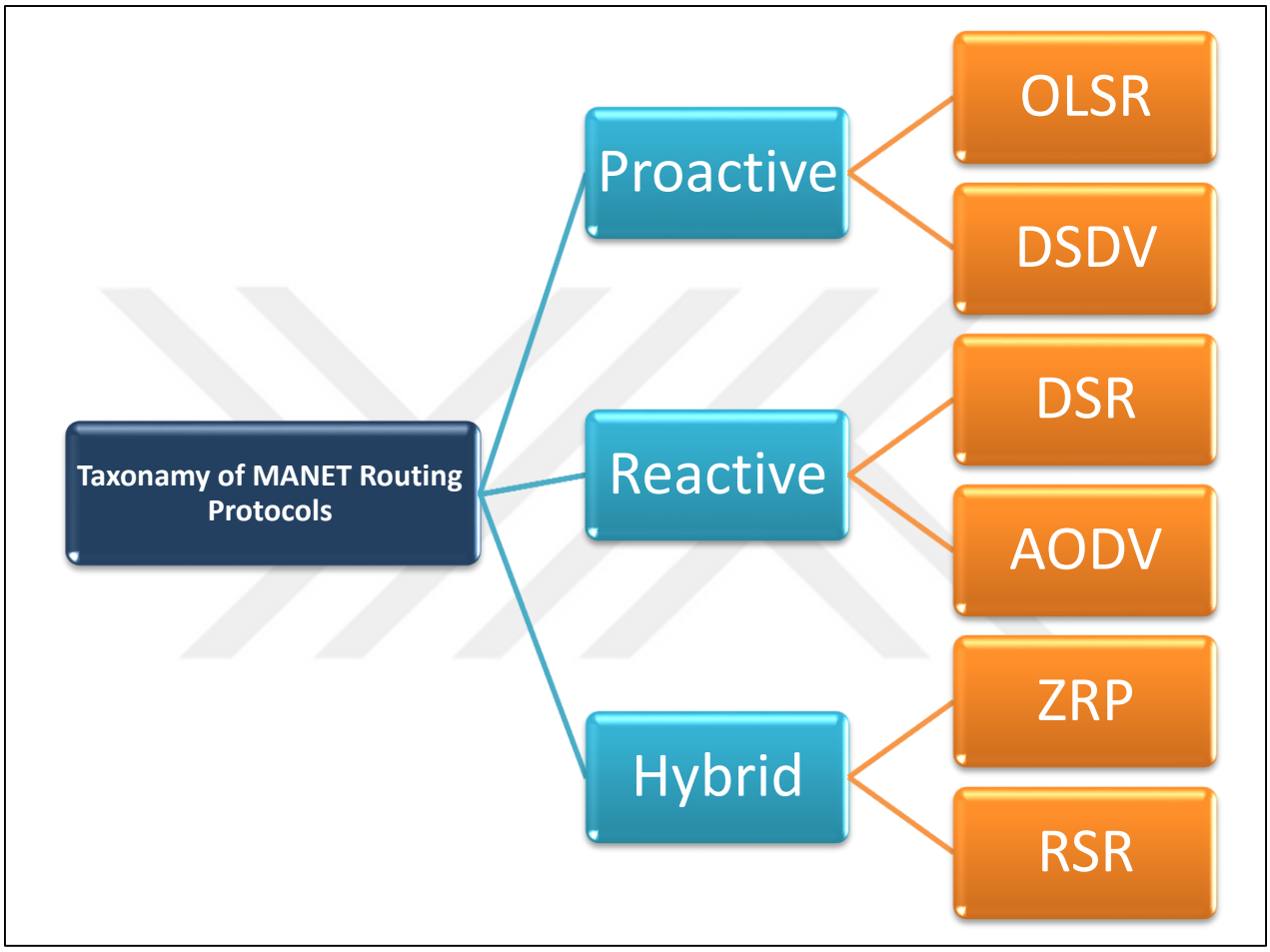


Figure 2.3: Protocol based on topology

i. proactive routing protocols: sometimes referred to as (Table Driven or Source routing) The updated model of the Internet Link State technique. Using the proactive routing technique [7]. Every single node inside the routing tables of the network is kept up to date with latest updates. In the absence of specific communication demand, background routing data can be obtained. which is a typical characteristic of proactive routing systems. When node X wants to transmit data to node Y; X must look for Y in a routing table. that was previously constructed (and stored on node A). Low Bandwidth, alternate path support, and surveillance are just a few of the benefits of the proactive algorithm, which is particularly

useful for applications that require real-time interactions and QoS assurances. However, because of the overhead produced, this strategy has the disadvantage of inefficient Bandwidth and power use. (OLSR)[58],(DSDV) are proactive routing Protocols an example of proactive routing protocols.

Distance Sequenced Distance Vector Routing Protocol (DSDV): Because it's proactive, nodes in their entirety create a table for the routing process. which determines the loop-free paths and solves the problem of counting infinity through serial numbers. Where the sequence numbers are increased by nodes whenever a change occurs due to the addition or removal of new nodes, it updates the routing table instantly; the routing information sequence numbers are preserved for each node. If routing is broken or the link path to the node is broken, an odd number sequence is declared, and that there is no routing path through this node. Routing Complete and periodic dumps are two different kinds of scheduling upgrades that might be attended. DSDV Suggested for use in dedicated multi-hop mobile networks[59][60][61].

Optimized Link State Routing (OLSR) an efficient way from (LSR). Only MPR hubs send data packets, which results in effective control message flooding and reduced control message duplication. Employing Broadcast message(Hello), OLSR discovers two hops for neighbor data for every node.[62]. this missive is used by a connection point(nodes). to connect with its neighbors to disseminate information about its connections. When the node gets a missive from nearest node, it examines the packets to see if the Its IP address is contained. If there is no information for the related record, a new one is produced.

ii. Reactive routing protocols: The Internet Link State Distance Vector algorithm has been updated to become the reactive routing protocol[63]. The reactive routing protocol distinguishes itself by its path identification and upkeep features. Route discovery is made up of two parts: a route demand and a route response which change from protocol to protocol. Nodes don't know how to contact each other when they need, and the route discovery process is activated.

If node A requests that data be sent to node B, the route finding procedure is started by publishing to every node to look for node B. When B accepts this signal, it answer to the

invitation for a connection to source A. forms this kind of protocols are (DSR) [64] ,(AODV) [65].

Dynamic Source Routing (DSR): is a simplified representation of a reactive protocol because it accomplishes two basic functions: path generation & maintenance it. which involves establishing routes, and route maintenance, which involves maintaining the routes generated. DSR prefers to utilize source routing rather than information from intermediary nodes[66]. Like AODV, DSR uses two control packets (R-REQ) and (R-REP). In these packets, the sender includes the whole routing path. Sending data from one node to another requires first tests to see if a path is available and if so, it utilizes that path for the transfer If the route is not reachable, the network is flooded with RREQ packets. If a source node obtains path to the destination, its promptly transmits an RREQ to the origin node.

The message is transferred to the packet; the packet is rebroadcast, in cases where the source node fails to provide a track to the intended goal, until a route to the goal is found, this process is repeated. The destination would then continue to provide RREP. Route maintenance is another procedure. Every node for this procedure must Check whether a message was received or not; if it was not received, a path failure will occur. The packet's sender node is informed of the fault. The source node uses backup routes to re-deliver the message. The path discovery method is resumed if alternative routes are not available.[67][68]. We will use the DSR routing protocol in our proposed system as it will come in the next chapter.

Ad hoc On-Demand Distance Vector (AODV):is a reactive routing method in which nodes produce a record for the surrounding node's state inside the routing table. Where the table aids in determining the path to the nodes to which request packets should be sent. (R-REQUST) that contain messages and information, including messages and information, including the serial number, to avoid the routing protocol from the AODV loop problem, Nodes in the routing table have their own row in AODV, which stores information about each one and deletes the row if it is not used and other nodes are alerted by RERR Which contains messages and information, including the serial number, to avoid the routing protocol from the AODV loop problem, where AODV keeps a row of information for every routing table node and deletes the row, RERR packets inform other nodes if it is not

utilized. the destination node is created (R-REQUST) where it is broadcast Packets to nodes and from there to neighboring nodes within the network and so on until they reach the required node, the output of which is returned to the source node via the same direction in reverse, creating R-REPLY messages. [68].

iii. Hybrid routing: to reap the benefits of both proactive and reactive strategies, connecting the two way at varying levels of hierarchy. As a result, hierarchical design is used because these techniques necessitate the use of an identifying system. As a result, management overhead is reduced. An Examples of this type the Zone Routing Protocol (ZRP)[69].

The strengths and weaknesses of the different types of routing protocols MANET networks are Table 2.2 shows the information.

Table 2.2: Positive and Negative Points in Routing MANET Protocols

Protocols	Positive points	Negative points
OLSR	possibility for using the extension of link quality	High overheads and route loops are available
DSDV	Fewer overhead and loop avoidance	needs big Bandwidth and larger overhead
AODV	Increasing the Bandwidth of the network	Discovery delay in route, and greater Bandwidth
DSR	Suitable for networks with a big area	Problems of Scaling
ZRP	Enhance global route query and response efficiency	Radius is a major element

3. DESIGN AND IMPLEMENTATION

This thesis aims to create a security system to detect intrusion in the MANET networks, especially the black hole attack. This chapter reviews the suggested intrusion detection system will be designed and implemented in stages. First, we created the data set using Network Simulator 2, where we created a mobility model to create a simulation environment to produce normal and abnormal behavior. After the data was generated, we extracted the features and then pre-processed them with processing operations such as Encoding, Uniform distribution, Data scaling, SMOTE, and Split data set into two groups, training testing set. The data was trained using three supervised machine learning algorithms. The basic resources needed to develop and implement the proposed IDS system are listed below:

iv. A network simulator 2: utilized to create a trace file, with the data set extracted from that trace file being used to test the suggested system.

v. The proposed system's training step employs the Python programming language.

vi. MANET security system training and testing are based on RF, SVM, and NB algorithms, which are efficient and effective with a low error rate.

3.1 NETWORK SIMULATOR-2 (NS-2)

Occurrence simulator ns-2 is an open-source event-driven simulator for computer networks. research. Since its establishment in 1989, it has piqued the interest of government, academics, and industries. For years, ns-2 has been expanding and being investigated. It now includes modules for various network components, including transport layer protocol, routing, and applications Use a simple computer language to evaluate and set up networks, as well as examine the results of ns-2. Itis now a commonly used open-source network simulator[70]. In ns-2, Tool Command Language

(TCL) is utilized to improve simulation efficiency. TCL scripting files are used to determine the path of node movement and communication behavior.

Furthermore, Trace files and NAM files generated as the simulation's output., both of which are supplied using a TCL script file. John Oosterhout invented the TCL programming language. It enables programmers to construct projects more quickly. TCL is a free, extensible programming language with a graphical user interface (NAM). Researchers utilize ns-2 since it offers features that aid them in their work, such as being efficient, open-source, having a large library, and being widely used in research[71].

3.2 THE PROPOSED IDS

Despite all the strong conventional security methods previously used, the attackers can initiate their malignant behaviors, so for achieving the security specifications in MANET networks, we presented an IDS based on verification and reliability to detect the attacks by their activities such as dropping packets. RF Algorithm, SVM Algorithm, Naïve based Algorithm are machine learning methods that we used:

Table 3.1: Algorithm of Implementation

Algorithm (3.1): The Implement of machine learning algorithms (RF, SVM, NB)
***Input*:** Training and Testing data sets
***Output*:** Normal or Malignant nodes
The First Step: Creating simulation parameters. The Second Step: Generating random mobility and traffic model. Third Step: Creating a list of attributes from the trace file. Forth Step: Data sets are pre-processed: a. Encoding stage: Convert symbolic Features to numeric values. b. Uniform distribution stage. c. Data scaling (standardization). d. The Synthetic Minority Oversampling Technique (SMOTE) stage. e. Split data set into two groups: training set and testing set. Fifth Step: Features selection phase. Sixth Step: The training dataset. Seventh Step: The Testing data set. Eighth Step 7: Results of classification.

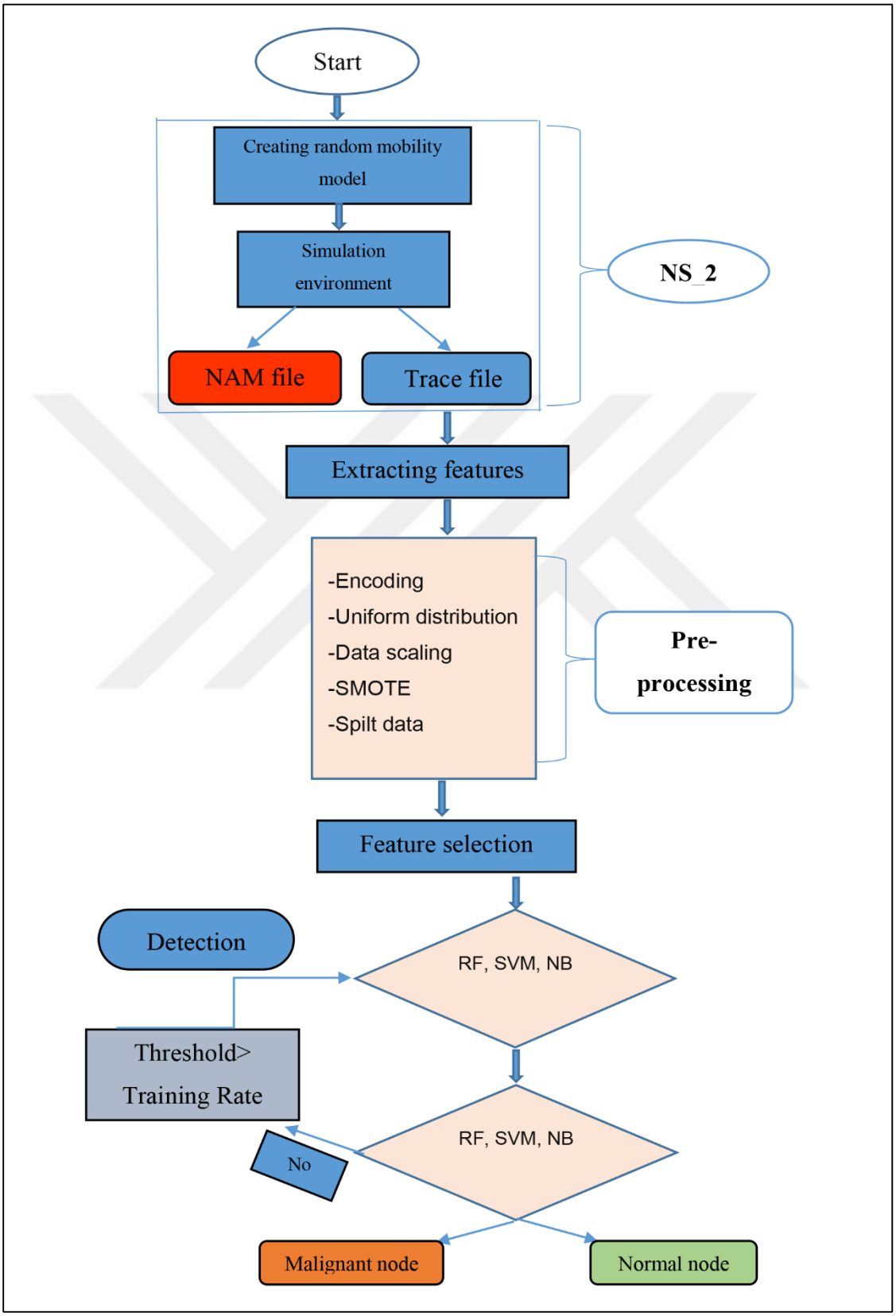


Figure 3.1: The Proposed IDS

3.2.1 Stage 1: Initial Parameters and Environment for Simulating

ns-2 is being utilized to establish network connectivity. and construct a mobility system. One of the system's evaluation processes is creating abnormal/black hole behavior. That is a crucial element to consider while evaluating the proposed system's efficiency. As a result, the DSR routing protocol is used in this suggested system. At the network layer of the simulator, the DSR routing protocol files are updated to produce dropping/malicious behavior. The suggested method should distinguish malicious nodes from the remainder of the network's nodes by detecting any abnormal behavior. The initial settings of ns-2 are thought to be especially important.

Table 3.2: Initial Parameters of ns-2

Parameters	Values
Node count	25 Nodes
Timeframe for Simulation	200s
Structure	1000 x 1000 (m)
Traffic type	Constant Bit Rate (CBR)
Size of packet	512
Routing Protocol type	Dynamic Source Routing (DSR)
Length of the Queue	50 packets
Radio Propagation Model	Two Ray Ground
MAC	IEEE 802..11
Interface queue type	Priority Queue
network interface type	Wireless

3.2.2 Stage 2: Creating a Model for Mobility and Traffic

NS-2 utilized to generate normal and black hole behavior in this system. This simulation is comprised of 2 files: (NAM) file and a trace file (the text of data). In ns-2, the C++ language and Tool Command Language (TCL) are utilized to improve simulation performance. TCL code files are used to specify the path of node movement and communication behavior. Additionally, the simulation's output requires a trace file as well as a NAM file, both of which are defined using a TCL code file. Figure 3.2 shows the connectivity environment of ad hoc network nodes using the NAM file from ns-2.

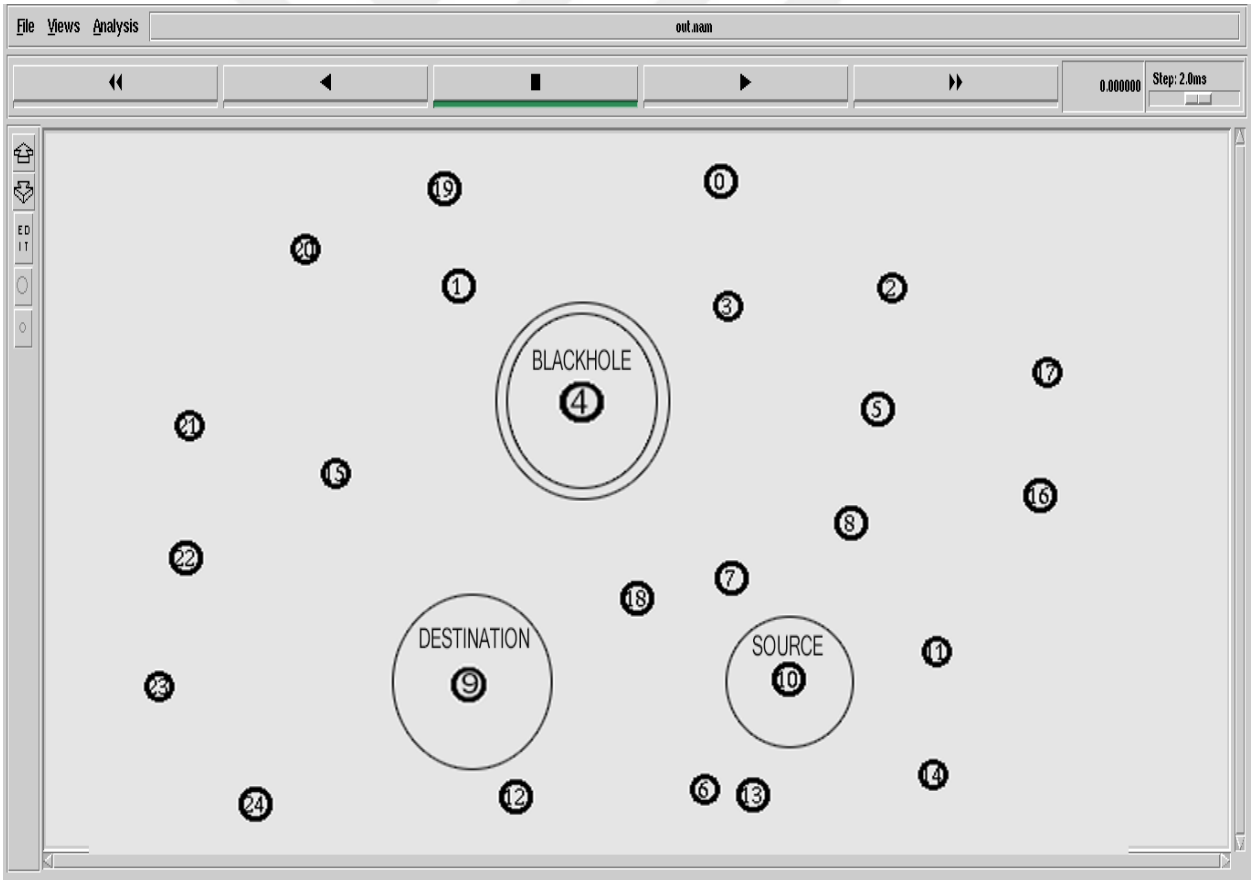


Figure 3.2: Simulation in The ns-2 NAM (Screenshot)

3.2.2.1 The Dataset Source

The NAM and trace file (text) files are the two files that make up the output of the ns-2 simulation. NAM is employed to describe the environment of MANET network, the retrieved The dataset is predicated on the ns-2 trace file. The created dataset is used in this thesis for phases of training and testing for the suggested method. In other words, a dataset is generated from the simulator's trace file, Figure 3.3 show part of trace file (Dataset). the dataset information obtained from the DSR trace file is divided into three sections:

i. essential information

ii. DSR information

iii. Internet Protocol (IP) information.

Table 3.3: The Retrieved Features That Describe All Node Events

Essential information	DSR information	Internet Protocol (IP) information
label, Number of Nods Period level of Trace MAC for Source Node and Destination Nodes Size of Payload and Kind ID for Packet Delay Time Internet Protocol for Packet and Ethernet	The hop counts number The IP of the source The IP of the destination The sequence number ID for Broadcast	The IP source address IP destination address The time life The next-hop address

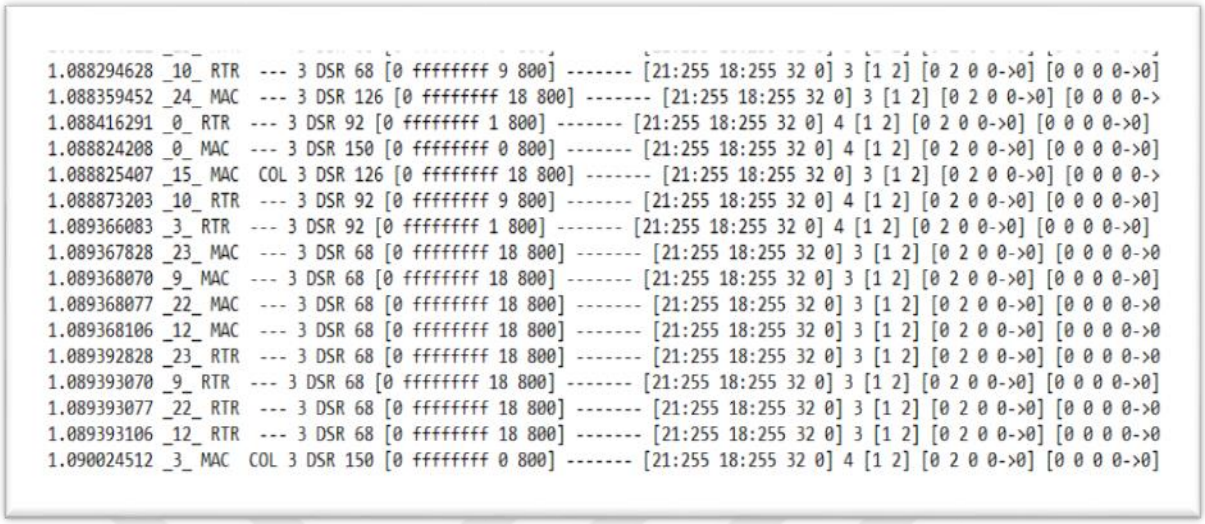


Figure 3.3: Part of Dataset (Screenshot)

To acquire a better grasp of the dataset that has been obtained, the following is an example of a connection record[72]:

s 1.006250852 _21_ MAC --- 1 DSR 90 [0 ffffffff 15 800] ------- [21:255 18:255 32 0] 1 [1 1] [0 1 0 0->0] [0 0 0 0->0]

i. Event: s" represent (send); D" represent (Drop); r" represent (receive); f means (forward).

ii. Level of trace is at "MAC" layer of network

iii. Flag: ---

iv. Node "_21_" sends (i.e., "s") at specific time "1.006250852" s.

v. ID packet is "21", contains a payload type is "DSR", and size of packet is "90" bytes. and the ID of this paket is "1"

vi. The source MAC address is (0) and the destination MAC address is "ffffffff

vii. IP packet over an Ethernet is "800".

viii. "255" is the port address for source and destination.

ix. IP source address is "21" and IP destination addresses is "18".

x. "32" is total time to live while "0" is address for the next hop.

xi. 1 [1 1] [0 1 0 0->0] [0 0 0 0->0] DSR detail:

1:num_addrs

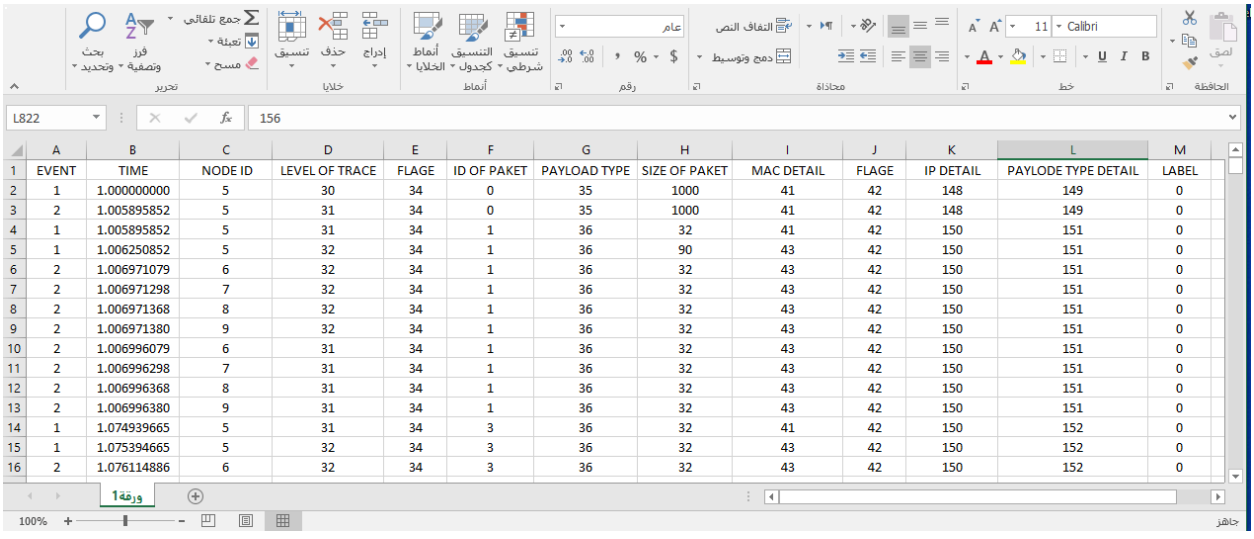
[1 1]: route-requst option where the second 1 is labeled for sequence number

[0 1 0 0->0]: route-replay option

[0 0 0 0->0]: this is show the rout error.

3.2.3 Stage 3: Extraction Features from Trace File

The behavior of nodes is examined in the trace file generated by ns-2 in analyzing their reliability. whether it is standard Black hole behavior. However, because these attributes serve as the foundation for the most of the operation., here is how the ns-2 trace file values are obtained is very important for the suggested system, an excel table was used to collect Thirteen distinct characteristics., these features as shown in Figure 3.4



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	EVENT	TIME	NODE ID	LEVEL OF TRACE	FLAGE	ID OF PAKET	PAYLOAD TYPE	SIZE OF PAKET	MAC DETAIL	FLAGE	IP DETAIL	PAYLODE TYPE DETAIL	LABEL
2	1	1.000000000	5	30	34	0	35	1000	41	42	148	149	0
3	2	1.005895852	5	31	34	0	35	1000	41	42	148	149	0
4	1	1.005895852	5	31	34	1	36	32	41	42	150	151	0
5	1	1.006250852	5	32	34	1	36	90	43	42	150	151	0
6	2	1.006971079	6	32	34	1	36	32	43	42	150	151	0
7	2	1.006971298	7	32	34	1	36	32	43	42	150	151	0
8	2	1.006971368	8	32	34	1	36	32	43	42	150	151	0
9	2	1.006971380	9	32	34	1	36	32	43	42	150	151	0
10	2	1.006996079	6	31	34	1	36	32	43	42	150	151	0
11	2	1.006996298	7	31	34	1	36	32	43	42	150	151	0
12	2	1.006996368	8	31	34	1	36	32	43	42	150	151	0
13	2	1.006996380	9	31	34	1	36	32	43	42	150	151	0
14	1	1.074939665	5	31	34	3	36	32	41	42	150	152	0
15	1	1.075394665	5	32	34	3	36	32	43	42	150	152	0
16	2	1.076114886	6	32	34	3	36	32	43	42	150	152	0

Figure 3.4: The Features Extracted From Trace File (Screenshot)

Figure 3.4 illustrates thirteen attributes were collected from the dataset and included in this study; they are as follows: Event, Time, Node ID, Flage1, Packet ID, Payload Type, Packet Size, MAC detail, Flage2, IP Detail as well as Label.

3.2.4 Stage 4: Pre-processing Phase of The Extracting Features

The retrieved features of the trace file must be used to generate training and testing datasets in this stage; An excel table was used to collect Thirteen distinctive features, these features, on the other hand, are formed of letters, symbols, and numbers. Because machine learning only works with numbers, Pre-processing entails the following steps:

i. Encoding phase Since RF, SVM, and NB are technologies that perform using numbers, an encoding process tries to convert both alphabet letters or symbol into numeric.

ii. Uniform distribution phase: Since the data set for the modeling provided only limited an overall count of events (rows). This procedure is being employed to acquire a total of 10,000 rows of data.

iii. Standerd scaling: The numerical features focused on the mean with a unit standard deviation.

iv. Data balancing: by using Synthetic Minority Oversampling Technique (SMOTE). SMOTE utilized to increase the rate of the category with the lowest number(abnormal) category, as a result, acquire more balanced data, resulting in more accurate results.

v. Start dividing the data is divided into two portions, with 67 percentages being used for the training phase with 33 percent being utilized for the test phase.

3.2.5 Stage 5: Select of Features

The data set may contain erroneous or unnecessary information. since this data might limit the performance of the proposed study, the purpose of minimizing features is to simplify the task of

reducing the elapsed time, by selecting the features to improve the classification model. Neglecting features whose deletion does not affect the workflow of the system and lessen the complexity of time[73] In our security system, the selection of 7 types of features that we named was tested to find the best sample that was deleted and achieved better results for Every one of the techniques we used for classification There are RF, SVM and NB. we take the random method based on the trial-error principle of selecting from the data set.

First sample=selected feature(event).

Second sample= selected feature(flag1)

Third sample= selected feature(node_id)

Forth sample= selected feature(payload_type_detail)

Fifth sample= selected feature(size_of_packet)

Sixth sample= selected feature(MAC_detail)

Seventh sample= selected features (level_of_trace + MAC_detail).

3.2.6 Stage 6: The Training of dataset

Our presented IDS employs ML techniques RF, SVM, NB, to better classification and minimize false alarm rate. 67% of all pre-processed and divided datasets were used for the training phase for the proposed system.

3.2.7 Stage 7: The Testing of dataset

In this stage, kinds of alerts known as confusion matrixes are employed to evaluate the accuracy rate of classification, and other performance measures involve Precision, Recall, F1, and Time of running.

4. RESULTS AND DISCUSSIONS

The dataset created by NS2 was used to illustrate how ml algorithms RF, SVM, and NB were trained and tested. The performance and efficiency of the proposed system were also measured using various performance measures such as confusion matrix calculation (TP, TN, FP, FN), accuracy rate, error rate, Precision, Recall, F1. Then we will compare the performance of the three algorithms RF, SVM, NB, according to the evaluated results and reach the best algorithm, and then compare the system's performance with other systems for other research.

4.1 THE PERFORMANCE METRICS

Based on the analysis of trace files, the ad hoc network security system was evaluated in various ways. Two factors can be used to evaluate the MANET security system[74]:

i. Accuracy: This section, also known as effectiveness categorization, defines the system's capacity to Differentiate between aggressive and non-behaviors.

ii. Efficiency of System: This resource base that must be assigned to a system are Processor cycles and main memory.

Performance, accuracy, and usability are all factors to consider while evaluating system features. Developers employed metrics to assess the system 's efficiency. The evaluation use a variety of performance indicators based on the dataset collected from the ns-2 trace file. The suggested system is tested using the identification rate and the confusion matrix calculation where four alarms as a performance measure. To calculate the performance of the proposed model, four types of alarms are required, as indicated in Table 4.1

Table 4.1: Confusion Matrix

Actual class	Predicted class	
	Positive (normal)	Negative (malignant)
Positive	TP	FN
Negative	FP	TN

Where True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN).

The following are the formulas that will be used to calculate the measures[75]:

TP: Identifies actions that have been correctly recognized as normal.

FP: regular connection record attacked.

TN: connection attack record classed as an attack.

FN: Assault connections identify as normal

The confusion matrix can be used to derive a variety of values, as shown below:

$$TP\ RATE = (\frac{TP}{(FN+TP)}) * 100\% \ . \quad (4.1)$$

$$TN\ RATE = \left(\frac{TN}{(FP+TN)}\right) * 100\% \ . \quad (4.2)$$

$$FP\ \ RATE = \left(\frac{FP}{(TN+FP)}\right) * 100\%. \quad (4.3)$$

$$FN\ \ RATE = \left(\frac{FN}{(TP+FN)}\right) * 100\%. \quad (4.4)$$

$$ACCURACY\ RATE = \left(\frac{TN+TP}{TP+FP+TN+FN)}\right) * 100\% \quad (4.5)$$

$$PRECISION\ RATE = (\frac{TP}{(TP+FP)}) * 100\% \quad (4.6)$$

$$RECALL\ RATE = \left(\frac{TP}{(TP+FN)}\right) * 100\% \quad (4.7)$$

$$F1\ SCORE\ RATE = \frac{2*PRECISION*RECALL}{(PRECISION*RECALL\ )} * 100\% \quad (4.8)$$

4.2 EXPERIMENTAL RESULTS

The proposed detection system is set up in MANET, and it can distinguish between two types of activities: normal and malignant. The suggested system's performance can be tested using the four alerts (mentioned above) and the detection rate. The same data set is used during the training and testing phases to calculate the TP , TN, FP, FN, and total accuracy rates. Different algorithms such as RF, NB, and SVM and different techniques such as SMOTE and Features selection were used in stages to improve the intrusion detection system.

4.2.1 Analysis of The Primary Results (Without SMOTE)

We trained and tested algorithms RF, SVM, NB, without SMOTE, and we got the results below:

Table 4.2: The Alarm Numbers (without SMOTE)

Alarm type	Random Forest	SVM	Naïve Bayes
TP	185	175	168
TN	3115	3110	3110
FP	0	5	5
FN	0	10	17

Table 4.3: The Alarm Rates (without SMOTE)

Alarm type	Random Forest	SVM	Naïve Bayes
TP	100 %	94.59%	90.81%
TN	100 %	99.83%	99.83%
FP	0%	0.16%	0.0016%
FN	0%	5.40%	9.189%

From Table 4.2 and 4.3, we notice that the values of TN, TP for the RF algorithm were ideal, and the same values for the SVM, NB were high, and it is required that the values of TN, TP be high. As for the values of FP, FN, they are zero for the RF algorithm and small values for the SVM, NB algorithms.

Table 4.4: The Data Classification Result with evaluation (without SMOTE)

Evaluation metrics	RF	SVM	NB
Accuracy	100%	99.544%	99.333%
Error rate	0%	0.454%	0.666%
Precision	100%	97.222%	97.11%
Recall	100%	94.595%	90.81%
F1	100%	95.89%	93.855%

In Table 4.4 the preliminary findings of the data classification algorithms' work showed promising results, as the accuracy rate of the RF algorithm= 100% SVM=99.544%, NB = 99.333%; when observing the data classification, the percentage was the rate of normal data = 94.370% and the rate of attack data = 5.63%, which is considered unbalanced. For this reason, we will apply SMOTE.

4.2.2 Analysis of The Results After Using The SMOTE

We applied (SMOTE) to increase the rate of the abnormal category and thus obtain more balanced data so that the results would be more accurate and realistic. The results obtained after SMOTE will be approved as the main results.

Table 4.5: The Alarm Numbers after Using The SMOTE

Alarm type	Random Forest	SVM	Naïve Bayes
TP	3099	3070	2834
TN	3130	3108	3037
FP	0	22	93
FN	0	29	265

Table 4.6: The Alarm Rates after Using The SMOTE

Alarm type	Random Forest	SVM	Naïve Bayes
TP	100%	99.06%	92.25%
TN	100%	99.29%	97.02%
FP	0%	0.70%	2.97%
FN	0%	0.93%	8.38%

In Tables 4.5 and 4.6, we note that the alarms numbers of RF, SVM, NB with SMOTE; TP, TN for RF algorithm have high values and FN, FP=0; so RF remained perfect and did not change. As for the SVM algorithm TP, TN, FP ratios decreased, and FN ratio increased. For the NB algorithm, TP, FN, FP ratios increased and TN value decreased; thus, balancing data by SMOTE has real positive results for all algorithms.

Table 4.7: The Data Classification Result with evaluation after Using The SMOTE

Evaluation metrics	RF	SVM	NB
Time (second)	0.62	0.95	0.35
Error rate (%)	0	0.818	5.667
Accuracy (%)	100	99.181	94.333
Precision (%)	100	99.288	96.828
Recall (%)	100	99.064	91.61
F1 (%)	100	99.176	94.147

According to Table 4.7, the results of the classifiers after using SMOTE, which balances the two classes of the dataset (normal and abnormal) by increasing the data of the small class (attack class), are presented, and we remark that the results were good. RF with the highest accuracy=100%, error rate=0% precision=100%, recall =100% and F1= 100%. We also got promising results for the SVM and NB algorithms regarding all performance measures.

Table 4.8: The Detection Rates of The System after Using The SMOTE

Detection rates	Random Forest	SVM	Naïve Bayes
Normal	100%	99.06%	92.25%
Abnormal	100%	99.29%	97.02%
Average	100%	99.44%	94.63%

We note the superiority of the RF algorithm, followed by SVM and finally NB.

4.2.3 Analysis Results after Applying Feature Selection

After balancing the dataset by SMOTE, we take the random method based on the trial-error principle of selecting features by deleting one of the features from the data set and showing the results after running the algorithms, reducing features to build the classification model reduces time complexity, just to note that the seventh sample consists of two features together. We will

also compare the performance results of each sample with the balanced data after SMOTE in tables 4.5, 4.6, 4.7, and 4.8.

4.2.3.1 The First Sample Results

The details of selecting the first sample are listed below.

Table 4.9: Alarm Number of The First Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	3099	3099	2692
TN	3130	2943	1998
FP	0	187	1132
FN	0	407	407

Table 4.10: Alarm Rates of The First Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	100%	88.39%	86.86%
TN	100%	94.02%	63.83%
FP	0%	5.97%	36.166
FN	0%	11.60%	13.13%

When selecting the first sample and comparing results with the alarms ratios after balancing data after SMOTE (the main results) in tables 4.5 and 4.6, the RF algorithm ratios do not change; it is perfect for all the alarms ratios. As for the SVM, NB algorithms, notice that the TP, TN ratios decreased and the FP, FN ratios increased.

Table 4.11: The Data Classification Result of Selecting The First Sample

Sample	Metrics	Random Forest	SVM	Naïve Bayes
First Sample	Time (second)	0.31	3.63	0.33
	Error rate (%)	0	3.002	24.707
	Accuracy (%)	100	96.998	75.293
	Precision (%)	100	94.309	70.397
	Recall (%)	100	100	86.867
	F1 (%)	100	97.071	77.77

Now, note that the execution time is less than the time in the main result in table 4.7 with the stability of the ratios of performance measures for the RF algorithm. As for the SVM and NB algorithms; the error rate increased, and thus the accuracy rate decreased.

Table 4.12: The System Detection Rates of Selecting The First Sample

Detection Rates	Random Forest	SVM	Naïve Bayes
Normal	100%	88.39%	86.86%
Abnormal	100%	94.02%	63.83%
Average	100%	91.20%	75.34%

4.2.3.2 The Second Sample Results

The details of selecting the second sample are listed below.

Table 4.13: Alarm Number of The Second Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	3099	3098	2836
TN	3130	3103	3070
FP	0	27	60
FN	0	1	263

Table 4.14: Alarm Rates of The Second Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	100%	99.96%	91.51%
TN	100%	99.13%	98.08%
FP	0%	0.86%	1.91%
FN	0%	0.03%	8.48%

When selecting the second sample; and comparing results with the alarms ratios after balancing data after SMOTE (the main results) in tables 4.5,4.6 for the alarms, the RF algorithm did not change. It is perfect for all alarms ratios. As for the SVM, NB algorithms; slight changes in alarms ratios, increasing and decreasing.

Table 4.15: The Data Classification Result of Selecting The Second Sample

Sample	Metrics	Random Forest	SVM	Naïve Bayes
Second Sample	Time (second)	0.32	0.53	0.33
	Error rate (%)	0	0.45	5.185
	Accuracy (%)	100	99.55	94.815
	Precision (%)	100	99.136	97.928
	Recall (%)	100	99.968	91.513
	F1 (%)	100	99.55	94.612

We noted that the execution time of all algorithms is less than the value of time in the main result in table 4.7 with the stability of the ratios of performance measures for the RF algorithm. The SVM and NB algorithms achieved promising results by increasing the accuracy rates and reducing the error rates.

Table 4.16: The System Detection Rates of Selecting The Second Sample

Detection Rates	Random Forest	SVM	Naïve Bayes
Normal	100%	99.96%	91.51%
Abnormal	100%	99.13%	98.08%
Average	100%	%99.54	94.795

4.2.3.3 The Third Sample Results

The details of selecting the third sample are listed below.

Table 4.17: Alarm Number of The Third Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	3098	3099	2851
TN	3130	3047	3037
FP	0	83	93
FN	1	0	248

Table 4.18: Alarm Rates of The Third Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	99.96%	100%	91.99%
TN	100%	97.34%	97.02%
FP	0%	2.65%	2.97%
FN	0.03%	0%	8.00%

Selecting the third sample and comparing results with the alarms ratios after balancing data with SMOTE in the main results in tables 4.5 and 4.7 for the alarms; The time with RF algorithm was affected, the TP rate decreased, the FN increased, and the FP, TN rates were not affected. As for the SVM algorithm, increased the ratios of TP, FP and decreased the ratios of TN, FN. As for the NB algorithm, the ratios of TN, FP were not affected, and the ratios of TP, FN were decreased.

Table 4.19: The Data Classification Result of Selecting The Third Sample

Sample	Metrics	Random Forest	SVM	Naïve Bayes
Third Sample	Time (second)	0.34	1.21	0.33
	Error rate (%)	0.016	1.332	5.474
	Accuracy (%)	99.984	98.668	94.526
	Precision (%)	100	97.392	96.841
	Recall (%)	99.968	100	91.997
	F1 (%)	99.984	98.679	94.357

In comparison with the main results in table 4.7, we note that the time it takes for all algorithms to run decreased compared to the time without the feature selection, and the accuracy, error, and other ratios varied with a small increase and decrease.

Table 4.20: The System Detection Rates of Selecting The Third Sample

Detection Rates	Random Forest	SVM	Naïve Bayes
Normal	99.96%	100%	91.99%
Abnormal	100%	97.34%	98.08%
Average	99.98%	98.67%	95.03%

4.2.3.4 The Fourth Sample Results

The details of selecting the fourth sample are listed below.

Table 4.21: Alarm Number of The fourth Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	3099	3076	2811
TN	3130	3108	3044
FP	0	22	86
FN	0	23	288

Table 4.22: Alarm Rates of The Fourth Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	100%	99.25%	90.70%
TN	100%	99.29%	97.25%
FP	0%	0.70%	2.74%
FN	0%	0.74%	9.29%

Select the fourth sample and compare results with the alarms ratios after balancing data (the main results) in tables 4.5 and 4.6 for the alarms. We note that the ratios of the RF algorithm were not affected. As for SVM, NB ratios were affected by a slight increase and decrease.

Table 4.23: The Data Classification Result of Selecting The Fourth Sample

Sample	Metrics	Random Forest	SVM	Naïve Bayes
Fourth Sample	Time (second)	0.67	0.92	0.32
	Error rate (%)	0	0.722	6.004
	Accuracy (%)	100	99.278	93.996
	Precision (%)	100	99.29	97.031
	Recall (%)	100	99.258	90.707
	F1 (%)	100	99.274	93.763

We noted that the execution time for the RF algorithm slightly increased while the other accuracy and error ratios remained constant compared to the time without the feature selection. The evaluation metrics rates for the SVM and NB varied slightly increase and decreasing.

Table 4.24: The System Detection Rates of Selecting The Fourth Sample

Detection Rates	Random Forest	SVM	Naïve Bayes
Normal	100%	99.25%	90.70%
Abnormal	100%	99.29%	97.25%
Average	100%	99.27%	93.97%

4.2.3.5 The Fifth Sample Results

The details of selecting the fifth sample are listed below.

Table 4.25: Alarm Number of The Fifth Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	3099	3099	2823
TN	3130	3103	3034
FP	0	27	96
FN	0	0	276

Table 4.26: Alarm Rates of The Fifth Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	100%	100%	91.09%
TN	100%	99.13%	96.93%
FP	0%	0.85%	3.06%
FN	0%	0%	8.90%

When selecting the fifth sample and comparing results with the alarms ratios after SMOTE (the main results) in tables 4.5 and 4.6 for the alarms, the RF algorithm did not change all the alarms ratios, note that the ratios of the RF algorithm were not affected, as for SVM, NB ratios were affected by a slight increase and decrease.

Table 4.27: The Data Classification Result of Selecting The Fifth Sample

Sample	Metrics	Random Forest	SVM	Naïve Bayes
Fifth Sample	Time (second)	0.37	1.05	0.32
	Error rate (%)	0	0.818	6.116
	Accuracy (%)	100	99.181	93.883
	Precision (%)	100	99.448	96.477
	Recall (%)	100	98.903	91.029
	F1 (%)	100	99.175	93.674

Note that the execution time for RF, NB algorithms decreased while SVM execution time increased. SVM and NB varied slightly increase and decreasing. Other, the evaluation metrics rates for RF are perfect.

Table 4.28: The System Detection Rates of Selecting The Fifth Sample

Detection Rates	Random Forest	SVM	Naïve Bayes
Normal	100%	100%	90.70%
Abnormal	100%	99.13%	97.25%
Average	100%	99.56%	93.97%

4.2.3.6 The Sixth Sample Results

The details of selecting the sixth sample are listed below.

Table 4.29: Alarm Number of The Sixth Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	3099	3065	2821
TN	3130	3113	3027
FP	0	17	103
FN	0	34	278

Table 4.30: Alarm Rates of The Sixth Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	100%	98.90%	91.02%
TN	100%	99.45%	96.70%
FP	0%	0.54%	3.29%
FN	0%	1.09%	8.97%

When selecting the sixth sample, and comparing results with the alarms ratios after SMOTE in tables 4.29 and 4.30 for the alarms, note that the ratios of the RF algorithm were not affected. As for SVM, NB ratios were affected by a slight increase and decrease.

Table 4.31: The Data Classification Result of Selecting The Sixth Sample

Sample	Metrics	Random Forest	SVM	Naïve Bayes
Sixth Sample	Time (second)	0.42	1	0.32
	Error rate (%)	0	0.433	5.972
	Accuracy (%)	100	99.567	94.028
	Precision (%)	100	99.136	96.711
	Recall (%)	100	100	91.094
	F1 (%)	100	99.566	93.819

Compared with table 4.7, note that the execution time for RF, NB algorithms decreased, while SVM execution time increased, other, the evaluation metrics rates for RF are perfect. SVM and NB varied slightly increase and decreasing.

Table 4.32: The System Detection Rates of Selecting The Sixth Sample

Detection Rates	Random Forest	SVM	Naïve Bayes
Normal	100%	98.90%	91.02%
Abnormal	100%	99.45%	96.70%
Average	100%	99.175	93.86

4.2.3.7 The Seventh Sample Results

The details of selecting the seventh sample are listed below.

Table 4.33: Alarm Number of The Seventh Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	3099	3069	2847
TN	3130	3113	3008
FP	0	17	122
FN	0	30	252

Table 4.34: Alarm Rates of The Seventh Sample

Alarm type	Random Forest	SVM	Naïve Bayes
TP	100%	99.03%	91.86%
TN	100%	99.45%	96.10%
FP	0%	0.54%	3.89%
FN	0%	0.96%	8.13%

When selecting the seventh sample that consists of selecting two features together and comparing results with the alarms ratios after balancing data (after SMOTE) in tables 4.5 and 4.6 for the alarms, we note that the ratios of the RF algorithm were not affected, as for SVM, NB ratios were affected by a slight increase and decrease.

Table 4.35: The Data Classification Result of Selecting The Seventh Sample

Sample	Metrics	Random Forest	SVM	Naïve Bayes
Seventh Sample	Time (second)	0.32	0.44	0.29
	Error rate (%)	0	0.754	6.004
	Accuracy (%)	100	99.245	93.996
	Precision (%)	100	99.449	95.891
	Recall (%)	100	99.032	91.868
	F1 (%)	100	99.24	93.837

Finally, note that the execution time was less than before choosing the seventh sample compared to table 4.7 and the error rate decreased for the RF and SVM algorithms, and it increased slightly for the NB algorithm.

Table 4.36: The System Detection Rates of Selecting The Seventh Sample

Detection Rates	Random Forest	SVM	Naïve Bayes
Normal	100%	99.03%	91.86%
Abnormal	100%	99.45%	96.70%
Average	100%	99.24%	94.28

4.3 COMPARISONS OF EXPERIMENTAL RESULTS

This section compares algorithms results before and after selecting features in terms of accuracy and rate of intrusion detection rate for machine learning algorithms, as well as comparing the results of our proposed system with other researchers. This comparison shows that the proposed security system is a strong security system that aims to secure MANET networks.

4.3.1 Comparison of our Proposed System Results

The comparison of algorithms results before and after selecting features are listed in Table 4.37

Table 4.37: A Comparison Between Accuracy of all samples in Proposed System

	Samples	Models		
		RF	SVM	NB
Accuracy Rates	Before feature selection	100%	99.18%	94.33%
	First sample	100%	96.99%	75.293%
	Second sample	100%	99.55%	94.81%
	Third sample	99.98%	98.66%	94.52%
	Fourth sample	100%	99.27%	93.99%
	Fifth sample	100%	99.18%	93.88%
	Sixth sample	100%	99.56%	94.02%
	Seventh sample	100%	99.24%	93.99%

In Table 4.37 it is obvious that the RF method is often superior, with the highest accuracy rate, which is 100%. The SVM algorithm also recorded the highest accuracy rate when selecting the sixth sample, where the accuracy rate reached 99.56%. As for the NB algorithm recorded the highest accuracy rate when choosing the second sample, where the accuracy rate reached 94.81%.

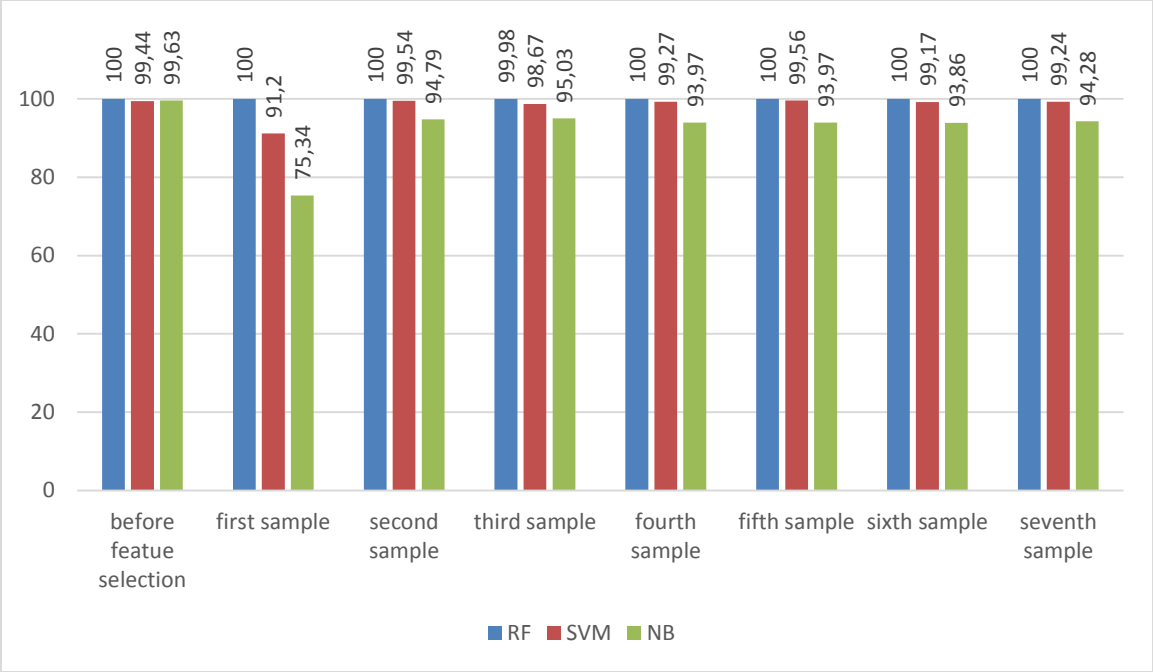


Figure 4.1: The Comparison of Average Detection Rates Among The Algorithms

Figure 4.1 shows the differences in average detection rate between the algorithms RF, SVM, NB.

4.3.2 Comparison of our Proposed System Results with Previous Research Work

Table 4.38 presents the results obtained from comparing the results of our work with other previous works

Table 4.38: A Comparison Results of our Proposed System with Previous Works

Author	Algorithm	Dataset	Accuracy
Our Proposed System	RF	Self-generate using NS-2	100%
Author [4]	RF	UNSW-NB15	87%
Our Proposed System	SVM	Self-generate using NS-2	99.18%
Author [5]	SVM	KDD'99	98.9%
Our Proposed System	NB	Self-generate using NS-2	94.33%
Author [5]	NB	KDD'99	92.7%

According to Table 4.38, the searchers have used RF, SVM, and NB techniques to achieve high accuracy rates in their security systems. Despite this, we can see that the RF, SVM, and NB techniques implemented in our proposed system have the best accuracy rate.

5. CONCLUSIONS, FUTURE WORKS, AND LIMITATIONS

5.1 CONCLUSIONS

Implementing the proposed intrusion detection system on MANET networks has been proven to be a success. This study concludes the following points:

i. In this system, the data generated using the NS 2 simulator was relied upon to suit the environment of the ad hoc networks.

ii. In the training and testing stages, the nodes were classified as normal or malicious using ML approaches such as (NB), (SVM), and (RF). The categorization results revealed a great accomplishment of all algorithms, especially the RF algorithm.

iii. Pre-processing of data is necessary and important, and the proposed system has gone through more than one pre-processing like encoding process: tries to convert both alphabet letters or symbol into numeric, Uniform distribution: it was hard to make a model because there were only a few events in the data set (rows). In this case, this function is being used to get 10000 rows, Standardization, SMOTE, partition the data set. The pre-processing of data obtain numerical and balanced data with normal and attack ratios and in acceptable numbers to give more realistic results for training and testing the used machine learning algorithms.

iv. To assess the efficacy of the proposed system, so here are the most important performance metrics used: the four sorts of alerts defined as a Confusion matrix which are TP rates, TN rates, FP rates, FN rates. As well as accuracy rates error rates, f - score, Precision rates,

recall rates, are also measured. Additionally, the time consumed on training and testing. The accuracy rate for machine learning algorithms using balanced data set as follows: RF=100% &error rate=0%, SVM=99.18% & error rate= 0.81% as well as NB=94.33% & error rate=5.66%.

v. The technique of selecting features from the dataset used in a trial-and-error method has been used, seven samples were chosen at random, and each time we get different results, and this raises the accuracy rate, decreases the percentage for error, and cuts down on time spent on training and testing, and thus increases the efficiency of the system and improves performance.

In comparison to earlier studies, the accuracy and error rate of the suggested system are higher.

5.2 FUTURE WORKS

There are some things that can be done in the future to achieve a better proposed intrusion detection system and thus support the protection of MANET networks:

a. In order to evaluate the proposed system, another data set can be used.

b. Using the proposed system with a different routing protocol such as AODV.

c. Using the proposed system to defend against other kinds of attacks.

d. Reducing the number of collecting features

e. Utilize of other classification approaches, such LDA and KNN, as well as other performance measures, to evaluate the suggested system.

5.3 LIMITATIONS

The dataset is not available specifically for MANETs from websites, such as Kaggle or others

REFERENCES

[1] I. Chlamtac, M. Conti, and J. J. N. Liu, “Mobile ad hoc networking: Imperatives and challenges,” *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, 2003, doi: 10.1016/S1570-8705(03)00013-1.

[2] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, “An overview of mobile ad hoc networks: Applications and challenges,” *J. Commun. Netw.*, vol. 3, no. 3, pp. 60–66, 2004.

[3] R. Datta and N. Marchang, “Chapter 7 - Security for Mobile Ad Hoc Networks,” *books.google.com*2012 „, doi: 10.1016/B978-0-12-415815-3.00007-8.

[4] O. Almomani, M. A. Almaiah, A. Alsaaidah, S. Smadi, A. H. Mohammad, and A. Althunibat, “Machine Learning Classifiers for Network Intrusion Detection System: Comparative Study,” *2021 Int. Conf. Inf. Technol. ICIT 2021 - Proc.*, pp. 440–445, Jul. 2021, doi: 10.1109/ICIT52682.2021.9491770.

[5] M. A. Saranya, T and Sridevi, S and Deisy, C and Chung, Tran Duc and Khan, “Performance analysis of machine learning algorithms in intrusion detection system: A review,” *Procedia Comput. Sci.*, vol. 171, pp. 1251--1260, 2020.

[6] K. S. Sankaran, S. Member, and N. Vasudevan, “Technique for Secure Neighbor Selection in Mobile AD-HOC Networks,” pp. 21735–21745, 2021.

[7] G. M. Jinarajadasa and S. R. Liyange, “A survey on applying machine learning to enhance trust in mobile adhoc networks,” *Proc. - Int. Res. Conf. Smart Comput. Syst. Eng. SCSE 2020*, pp. 195–201, 2020, doi: 10.1109/SCSE49731.2020.9313021.

[8] S. Kanthimathi, J. P.-2020 2nd P. C. On, and U. 2020, “Classification of Misbehaving nodes

in MANETS using Machine Learning Techniques," *ieeexplore.ieee.org*2020 „ Accessed: Apr. 07, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9315311/.

[9] T. Li *et al.*, "DAPV: Diagnosing anomalies in MANETs routing with provenance and verification," *ieeexplore.ieee.org*2019 „ Accessed: Apr. 07, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8660389/.

[10] R. Cai, X. Li, P. C.-I. transactions on Mobile, and U. 2018, "An evolutionary self-cooperative trust scheme against routing disruptions in MANETs," *ieeexplore.ieee.org* , 2019, Accessed: Apr. 07, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8350039/.

[11] G. Vaseer, G. Ghai, D. G.-I. C. Electronics, and U. 2019, "Novel intrusion detection and prevention for mobile ad hoc networks: A single-and multiattack case study," *ieeexplore.ieee.org*2019 „ Accessed: Apr. 08, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8684799/.

[12] D. gan Zhang, J. xin Gao, X. huan Liu, T. Zhang, and D. xin Zhao, "Novel approach of distributed & adaptive trust metrics for MANET," *Wirel. Networks*, 2019, doi: 10.1007/s11276-019-01955-2.

[13] V. Gampala, S. Aurelia, S. Krishna Kishore, and S. K. Mydhili, "Nautical communication relying on mobile Ad-hoc network via augmented reality devices," *Mater. Today Proc.*, Jan. 2021, doi: 10.1016/j.matpr.2020.11.822.

[14] A. S. Sharma and D. S. Kim, "Energy efficient multipath ant colony based routing algorithm

for mobile ad hoc networks," *Ad Hoc Networks*, vol. 113, p. 102396, Mar. 2021, doi: 10.1016/j.adhoc.2020.102396.

[15] M. Patsariya and A. Rajavat, "Node capability-based route selection on mobile ad hoc network," *Mater. Today Proc.*, Feb. 2021, doi: 10.1016/j.matpr.2020.12.210.

[16] L. Mechtri, F. D. Tolba, and S. Ghanemi, "An optimized intrusion response system for MANET:: An attack-severity aware approach," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 3, pp. 602–618, May 2018, doi: 10.1007/s12083-017-0573-5.

[17] S. S. Zhang, S. W. Wang, H. Xia, and X. G. Cheng, "An attack-Resistant Reputation Management System for Mobile Ad Hoc Networks," in *Procedia Computer Science*, Jan. 2019, vol. 147, pp. 473–479, doi: 10.1016/j.procs.2019.01.275.

[18] K. Sakthidasan, N. Vasudevan, P. K. G. Diderot, and C. Kadhiravan, "WOAPR: An affinity propagation based clustering and optimal path selection for time-critical wireless sensor networks," *IET Networks*, vol. 8, no. 2, pp. 100–106, Mar. 2019, doi: 10.1049/iet-net.2018.5081.

[19] L. Jiang, S. Q. Ke, and L. Zhang, "Research on key technologies of topology control in mobile predictive ad hoc networks," in *Proceedings - 2020 International Conference on Wireless Communications and Smart Grid, ICWCSG 2020*, Jun. 2020, pp. 190–194, doi: 10.1109/ICWCSG50807.2020.00050.

[20] D. S. Meitis, D. S. Vasiliev, I. Kaisina, and A. Abilov, "Simulation-based Research of BATS Code Applied to Flying Ad-hoc Networks," Mar. 2020, doi: 10.1109/MWENT47943.2020.9067409.

[21] M. A. Sharma, Zakki Ul Rehman, “Security_Aspects_of_MANETs_A_Review.pdf.” 2019.

[22] U. Zeb, W. U. Khan, S. Irfanullah, and A. Salam, “The Impact of Transmission Range on Performance of Mobile Ad-hoc Network Routing Protocols,” Jan. 2020, doi: 10.1109/iCoMET48670.2020.9074090.

[23] R. Kavitha, T and Muthaiah, “Instant Route Migration During Link Failure in Manets,” *Int. J. Mech. Eng. Technol. Vol.*, vol. 8, 2017.

[24] L. Jiang, S. Ke, and H. Wang, “An improved mobile prediction routing algorithm for Ad Hoc Networks,” in *Proceedings - 2020 International Conference on Information Science, Parallel and Distributed Systems, ISPDS 2020*, Aug. 2020, pp. 226–230, doi: 10.1109/ISPDS51347.2020.00053.

[25] B. Cui and Y. Yang, “Hotspot-based Resource Sharing System for Mobile Ad hoc Networks,” in *Proceedings of 2018 IEEE 8th International Conference on Electronics Information and Emergency Communication, ICEIEC 2018*, Sep. 2018, pp. 146–149, doi: 10.1109/ICEIEC.2018.8473566.

[26] V. Goyal and G. Arora, “Review Paper on Security Issues in Mobile Adhoc Networks,” *irjaes.com*2017 ,, doi: 10.31219/osf.io/sxgwq.

[27] A. Mishra and K. M. Nadkarni, “Security in Wireless Ad Hoc Networks,” in *The Handbook of Ad Hoc Wireless Networks*, USA: CRC Press, Inc., 2003, pp. 499–549.

[28] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT urban scenarios,” *IEEE Sens. J.*, vol. 13, no. 10, pp. 3558–3567, 2013, doi: 10.1109/JSEN.2013.2272099.

[29] G. Liu, Z. Yan, and W. Pedrycz, “Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey,” *Journal of Network and Computer Applications*, vol. 105. pp. 105–122, 2018, doi: 10.1016/j.jnca.2018.01.004.

[30] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, “A survey on intrusion detection and prevention in wireless ad-hoc networks,” *J. Syst. Archit.*, vol. 105, no. September 2019, 2020, doi: 10.1016/j.sysarc.2019.101701.

[31] Z. Y.-N. Laboratory, H. U. Of, and U. 2002, “Security in ad hoc networks,” in , Networking Laboratory, Helsinki University of Technology, 2002.

[32] T. Archana, R and Gracy, “Survey on Attacks in MANET,” *Int. J. Adv. Res. Comput. Commun. Eng.*, 2015.

[33] A. Singh, M. Kumar, and S. K. Chauhan, “A model for secure mobile ad hoc network,” *Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017*, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/I2C2.2017.8321841.

[34] G. Archana, R and Theresa, “Survey on Attacks in MANET,” *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, pp. 125--31, 2015.

[35] J. Liu, Yining and Liu, Gao and Cheng, Chi and Xia, Zhe and Shen, “A privacy-preserving health data aggregation scheme,” *KSII Trans. Internet Inf. Syst.*, vol. 10, pp. 3852--3864, 2016.

[36] J. Di Pietro, Roberto and Guarino, Stefano and Verde, Nino Vincenzo and Domingo-Ferrer, “Security in wireless ad-hoc networks--a survey,” *Comput. Commun.*, vol. 51, pp. 1--20, 2014.

[37] B. Swain, Jhum and Pattanayak, Binod Kumar and Pati, "A new approach for DDoS attacks to discriminate the attack level and provide security for DDoS nodes in MANET," *Int. J. Commun. Networks Inf. Secur.*, vol. 9, pp. 450--456, 2017.

[38] A. K. D. A. Singh, "A Review on Security Attacks in Mobile Ad-hoc Networks," *Int. J. Sci. Res.*, vol. 3, no. 5, pp. 1295–1299, 2014, Accessed: Apr. 03, 2021. [Online]. Available: https://pdfs.semanticscholar.org/bb3a/0ea634570cf4511401987eb69f6681e685dd.pdf.

[39] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6. pp. 53–57, Jun. 2004, doi: 10.1145/990680.990707.

[40] Z. Fadlullah, T. Taleb, … M. S. S.-O. N., and U. 2010, "Combating against security attacks against mobile ad hoc networks (MANETs)," 2010. Accessed: Apr. 03, 2021. [Online]. Available: https://books.google.com/books?hl=ar&lr=&id=ZtBnZoijaDcC&oi=fnd&pg=PA173&dq=Z.+Muhammad+,+Fadlullah,+T.+Taleb+,+M.+Schöller+,+Combating+against+security+at-+tacks+against+mobile+ad+hoc+networks+(MANETs),+in:+Security+of+Self-Organizing+Networks,+2010,+pp.

[41] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. Altamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," *2019 IEEE Jordan Int. Jt. Conf. Electr. Eng. Inf. Technol. JEEIT 2019 - Proc.*, pp. 28–33, 2019, doi: 10.1109/JEEIT.2019.8717449.

[42] P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review," 2012. Accessed: Apr. 03, 2021. [Online]. Available:

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.684.767&rep=rep1&type=pdf.

[43] Z. Khan, M. H. Islam, Z. A. Khan, and M. Hasan Islam, "Wormhole attack: A new detection technique," *ieeexplore.ieee.org*2012 „, doi: 10.1109/ICET.2012.6375443.

[44] N. W. Lo and F. L. Liu, "A secure routing protocol to prevent cooperative black hole attack in MANET," in *Lecture Notes in Electrical Engineering*, 2013, vol. 234 LNEE, pp. 59–65, doi: 10.1007/978-1-4614-6747-2_8.

[45] M. Abdel-Azim, … H. S.-I. J. of, and U. 2017, "Black Hole attack Detection using fuzzy based IDS," *search.proquest.com*2017 „, Accessed: Apr. 03, 2021. [Online]. Available: https://search.proquest.com/openview/863702126ebf2774b47d727ffd27165a/1?pq-origsite=gscholar&cbl=52057.

[46] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, "Fuzzy logic based intrusion detection system against black hole attack in mobile ad hoc networks," *Int. J. Commun. Networks Inf. Secur.*, vol. 10, no. 2, pp. 366–373, 2018.

[47] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Comput. Networks*, vol. 31, no. 8, pp. 805–822, Apr. 1999, doi: 10.1016/S1389-1286(98)00017-6.

[48] J. Mchugh, "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 4, pp. 262–294, Nov. 2000, doi: 10.1145/382912.382923.

[49] A. B. Smith, "An examination of an intrusion detection architecture for wireless ad hoc networks," in *Proceedings of the 5th National Colloquium for Information System Security*

Education, 2001, vol. 7, pp. 44–60.

[50] A. K. A. N. A. hahad Mahdi Al-Abrez, Khattab M Ali Alheeti, "Security System of Autonomous Drones Based on Linear Discrimination Analysis," *Int. J. Psychosoc. Rehabil.*, vol. 24, no. 8, pp. 6681–6693, 2020, doi: 10.37200/IJPR/V24I8/PR280691.

[51] "Applications of Machine Learning - Javatpoint." https://www.javatpoint.com/applications-of-machine-learning (accessed Sep. 09, 2021).

[52] N. Abd, K. M. A. Alheeti, and S. S. Al-Rawi, "Intelligent Intrusion Detection System in Internal Communication Systems for Driverless Cars," *Webology*, vol. 17, no. 2, pp. 376–393, 2020, doi: 10.14704/WEB/V17I2/WEB17039.

[53] A. Alzahrani, K. M. A. Alheeti, S. S. Thabit, D. Al_Dosary, and M. S. Al-Ani, "Intelligent Mobile Coronavirus Recognition Centre Based on IEEE 802.15.4," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 16, pp. 4–15, Aug. 2021.

[54] N. Kumar Trivedi, S. Simaiya, S. Kumar Sharma, and U. Kumar Lilhore, "An Efficient Credit Card Fraud Detection Model Based on Machine Learning Methods," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 5, pp. 3414--3424, 2020, [Online]. Available: https://www.researchgate.net/publication/341932015.

[55] S. Khatri, A. Arora, and A. P. Agrawal, "Supervised machine learning algorithms for credit card fraud detection: A comparison," *Proc. Conflu. 2020 - 10th Int. Conf. Cloud Comput. Data Sci. Eng.*, pp. 680–683, Jan. 2020, doi: 10.1109/CONFLUENCE47617.2020.9057851.

[56] SamanehSorournejad, Z. Zojaji, R. E. Atani, and A. H. Monadjemi, "A Survey of Credit

Card Fraud Detection Techniques: Data and Technique Oriented Perspective," Nov. 2016, Accessed: Sep. 29, 2021. [Online]. Available: https://arxiv.org/abs/1611.06439v1.

[57] G. Jisha and P. Samuel, "Coverage based route maintenance in MANET routing protocol," in *International Conference on Intelligent Systems Design and Applications, ISDA*, 2012, pp. 398–403, doi: 10.1109/ISDA.2012.6416571.

[58] T. Clausen *et al.*, "Optimized Link State Routing Protocol (OLSR)." Accessed: Jun. 23, 2021. [Online]. Available: https://hal.inria.fr/inria-00471712.

[59] N. Kumari, S. Gupta, … R. C.-2016 3rd I., and undefined 2016, "New performance analysis of AODV, DSDV and OLSR routing protocol for MANET," *ieeexplore.ieee.org*, Accessed: Jun. 23, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7724222/.

[60] N. Aggarwal, R. Vohra, S. Bahel, S. Chohan, and K. Singh, "Relative analysis of AODV & DSDV routing protocols for MANET based on NS2 MICROWAVE CHARACTERIZATION OF SPINEL FERRITES View project Transport characteristics of various materials at nanometer-scale View project Relative Analysis of AODV & DSDV Routing Protocols for MANET based on NS2," *ieeexplore.ieee.org*, p. 2016, doi: 10.1109/ICEEOT.2016.7755355.

[61] S. El Khediri, A. Kachouri, S. El Khediri, N. Nasri, A. Benfradj, and A. Wei, "Routing Protocols in MANET: Performance Comparison of AODV, DSR and DSDV Protocols Using NS2," *ieeexplore.ieee.org*2014 „, doi: 10.1109/SNCC.2014.6866519.

[62] R. P. Salim and D. Rajesh, "A Study on Down Syndrome Detection based on Artificial Neural Network in Ultra Sonogram Images A Survey: Optimal Node Routing Strategies in

MANET," *ieeexplore.ieee.org*2016 „ doi: 10.1109/SAPIENCE.2016.7684172.

[63] R. Online, M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," 2004. Accessed: Jun. 24, 2021. [Online]. Available: http://ro.uow.edu.au/eispapers/1158.

[64] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4*2007* "„ Accessed: Jun. 24, 2021. [Online]. Available: https://www.hjp.at/doc/rfc/rfc4728.html.

[65] E. C.-R. 3561 and undefined 2003, "Ad hoc on demand distance vector (AODV) routing," *ci.nii.ac.jp*, Accessed: Jun. 24, 2021. [Online]. Available: https://ci.nii.ac.jp/naid/10017112536/.

[66] M. Aashkaar, P. S.-2016 I. C. on, and undefined 2016, "Enhanced energy efficient AODV routing protocol for MANET," *ieeexplore.ieee.org*, Accessed: Jun. 25, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7764376/.

[67] C. Mafirabadza, P. K.-2016 I. C. on, and undefined 2016, "Energy analysis of AODV routing protocol in MANET," *ieeexplore.ieee.org*, Accessed: Jun. 25, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7754327/.

[68] T. Sapna, K. Deshpande, and K. Ravi, "Study on Routing Protocols for MANETs," *Proc. Int. Conf. Comput. Tech. Electron. Mech. Syst. CTEMS 2018*, pp. 322–325, 2018, doi: 10.1109/CTEMS.2018.8769137.

[69] Z. H.-I. I. draft, draft-ietf-manet-zone-zrp-01. txt, and undefined 1998, "The zone routing protocol (ZRP) for ad hoc networks," *ci.nii.ac.jp*, Accessed: Jun. 24, 2021. [Online].

Available: https://ci.nii.ac.jp/naid/10015375654/.

[70] T. Issariyakul and E. Hossain, "Introduction to Network Simulator 2 (NS2)," in *Introduction to Network Simulator NS2*, Springer US, 2009, pp. 1–18.

[71] D. Al-Dosary, K. M. Ali Alheeti, and S. S. Al-Rawi, "ICMetric Security System for Achieving Embedded Devices Security," in *Journal of Physics: Conference Series*, Mar. 2021, vol. 1804, no. 1, p. 12102, doi: 10.1088/1742-6596/1804/1/012102.

[72] H. Univeristy and J. Chen-burger, "C OMPUTER NETWORK A NALYSIS AND," no. August, 2018.

[73] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Comput. Networks*, vol. 174, p. 107247, Jun. 2020, doi: 10.1016/J.COMNET.2020.107247.

[74] G. Kumar, "Evaluation Metrics for Intrusion Detection Systems-A Study," *Int. J. Comput. Sci. Mob. Appl.*, vol. 2, no. October, pp. 11–17, 2014, [Online]. Available: www.ijcsma.com.

[75] K. M. Ali Alheeti and K. McDonald-Maier, "Intelligent intrusion detection in external communication systems for autonomous vehicles," *Sci. Control Eng. AN OPEN ACCESS J.*, vol. 6, no. 1, pp. 48–56, 2018, doi: 10.1080/21642583.2018.1440260.