A Multistage Support Vector Machine Based Intrusion Detection System in MANET

Arvin Pourghassem

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Master of Technology
in
Information Technology

Eastern Mediterranean University
February 2022
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Ali Hakan Ulusoy
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Technology in Information Technology.

Assoc. Prof. Dr. Nazife Dimililer
Director, School of Computing and Technology

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Technology in Information Technology.

Prof. Dr. Ahmet Rizaner
Supervisor

Examining Committee

1. Prof. Dr. Ahmet Rizaner
2. Prof. Dr. Ali Hakan Ulusoy
3. Asst. Prof. Dr. Kamil Yurtkan

ABSTRACT

Mobile Ad Hoc Networks (MANETs) have been applied in many different fields in recent years. Although MANETs are highly vulnerable to malicious behavior, complete security is complicated to achieve. Due to the insufficiency of prevention techniques, the Intrusion Detection System (IDS), which monitors system activity and detects intrusions, is generally used with other security measures. Denial of Service (DoS) type attacks such as flooding, blackhole, and grayhole attacks are acute types of network intrusion that aim to make computer/network resources unavailable to legitimate users.

Intrusion Detection (ID) is a security management system that serves as an alarm mechanism for any computer network such as MANET. It detects the incoming security threats to a network and then issues an alarm message to an entity to take needed actions against the intrusion. An IDS gathers and examines information from numerous areas within a computer or a network to identify possible security breaches, including intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

The goal of this study is to develop a multistage ID technique for detecting flooding, blackhole, and gray-hole intrusions using Support Vector Machines (SVM). The SVM mechanism supports binary classification and separating data points into two classes. Hence, in this research SVM approach is used for classifying and detecting multiple attacks after breaking down the multiclassification problem into numerous binary classification problems.

Keywords: Mobile Ad-hoc network, Support Vector Machine, On-demand Distance Vector, black hole, grayhole, flooding

ÖZ

Mobil Ad Hoc Ağlar (MANET'ler) son yıllarda birçok farklı alanda uygulanmaktadır. MANET'ler kötü niyetli davranışlara karşı oldukça savunmasız olsa da, tam güvenliğin sağlanması karmaşıktır. Önleme tekniklerinin yetersizliği nedeniyle, sistem etkinliğini izleyen ve izinsiz girişleri tespit eden Saldırı Tespit Sistemi (IDS) genellikle diğer güvenlik önlemleri ile birlikte kullanılmaktadır. Flooding, kara delik ve gri delik saldırıları gibi Hizmet Reddi (DoS) türü saldırılar, bilgisayar/ağ kaynaklarını meşru kullanıcılar için kullanılamaz hale getirmeyi amaçlayan akut ağ saldırı türleridir.

İzinsiz Giriş Tespiti (ID), MANET gibi herhangi bir bilgisayar ağı için alarm mekanizması görevi gören bir güvenlik yönetim sistemidir. Bir ağa gelen güvenlik tehditlerini algılar ve ardından izinsiz girişe karşı gerekli önlemleri alması için bir varlığa bir alarm mesajı gönderir. Bir IDS, izinsiz girişler (kuruluş dışından saldırılar) ve kötüye kullanım (kuruluş içinden saldırılar) dahil olmak üzere olası güvenlik ihlallerini belirlemek için bir bilgisayar veya ağ içindeki çeşitli alanlardan bilgi toplar ve analiz eder.

Bu araştırmanın amacı, flooding, kara delik ve gri delik saldırılarını tespit etmek için Destek Vektör Makinelerine (DVM) dayalı çok aşamalı bir kimlik mekanizması tasarlamaktır. SVM mekanizması, ikili sınıflandırmayı ve veri noktalarını iki sınıfa ayırmayı destekler. Bu nedenle, bu araştırmada, çoklu sınıflandırma problemini çok sayıda ikili sınıflandırma problemine böldükten sonra çoklu saldırıları sınıflandırmak ve tespit etmek için DVM yaklaşımı kullanılmıştır.

Anahtar Kelimeler: Mobil Geçici ağ, Destek Vektör Makinesi, İsteğe Bağlı Mesafe Vektörü, kara delik, gri delik, flooding

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	Ad hoc On-Demand Distance Vector Routing
AOMDV	Ad hoc On-Demand Multipath Distance Vector
CBR	Constant Bit Rate
DSR	Dynamic Source Routing
DOS	Denial of service
FN	False Negatives
FP	False Positives
IDS	Intrusion Detection System
IP	Internet Protocol address
MANET	Mobile Ad-hoc Network
NS2	Network Simulator 2
RREP	Respiratory-Related Evoked Potential
RREQ	Route Request Packet
SVM	Support Vector Machine
TCP	Transmission Control Protocol
TN	True Negative
TP	True Positive
UDP	User Datagram Protocol

Chapter1

INTRODUCTION

Due to the increasing use of computers today, network security has become increasingly critical. Because new types of attacks are always targeting users, it is crucial to inform them as soon as anything malicious activity occurs on the network. A system that can detect and respond to attacks quickly is needed to protect the data being transferred on the network since the threat becomes increasingly severe day by day. Protecting assets against intrusion is important whether transferring confidential, private, public, or business assets over the internet. Network security relies heavily on Intrusion Detection Systems (IDSs), which are a hot topic of research nowadays.

The literature classifies IDSs into two broad categories: signature-based IDS and anomaly-based IDS. A signature-based IDS identifies attacks based on the attack patterns established in the IDS database from monitored network traffic. It operates similarly to anti-virus software, detecting suspicious activity based on pattern-matching against a supplied database. This technique can reliably and quickly identify assaults but has certain limitations in detecting new or undiscovered harmful activity. In comparison, an anomaly-based IDS is based on estimate and prediction techniques that use a priori profile assaults or network sensor data. These profiles are used to train a machine-learning algorithm on the many types of assaults that require detection and classification. This technique has several advantages in recognizing unknown threats in this scenario. However, machine learning methods' inherent complexity and constraints make it impossible to develop a comprehensive model capable of detecting all probable assaults. The most extensively researched approach in IDS is the anomaly-based technique. The technique may be classified into three broad categories: statistical, knowledge-based, and machine-learning-based strategies [1]. Machine learning techniques may be used to develop effective classifiers for classification and are classified into four broad categories: supervised learning, semi-supervised learning, unsupervised learning, and reinforcement learning. However, this research will focus on implementing supervised machine learning for attack prediction. Several overviews of supervised learning intrusion detection have been published previously [2, 3, 4, 5]. However, the objective of this study is to increase the predictability of intrusion attempts using the multiclass classification issue.

The one-versus-all and one-versus-one strategies are the most often used procedures for decomposing a multiclass problem into numerous binary problems [6]. These techniques are primarily used in a variety of well-known supervised learning algorithms, including Support Vector Machines (SVMs) [7], Neural Networks (NNs) [8], and logistic regression [9]. Although these multiclass classification problems are commonly used in various machine learning methods, they occasionally fail to categorize instances of test assaults [10] accurately. Additionally, how one should approach a multiclass recognition problem remains an open question [11]. Alternatively, a hierarchical classification might be used to divide the multiclass classification issue into a tree [12, 13, 14]. Each parent node is subdivided into two child nodes in this work, and the procedure is repeated until each child node represents a single class.

1.1 Mobile Ad-hoc Network

Mobile Ad Hoc Networks (MANETs) are created by a set of mobile nodes (the host and the router), which can self-organize to interact with one another and the host. All of these devices that are part of networks send packages, and each of their nodes is responsible for making a decision while communicating with other nodes in the network.

Ad hoc networking enables mobile devices to communicate without relying on central infrastructure. However, the lack of centralized infrastructure and the ability of machines to roam arbitrarily creates a variety of issues, including routing and security. The routing problem is examined in this thesis. Numerous ad hoc routing protocols exist, including the Ad hoc On-Demand Distance Vector Routing that provides solutions for routing inside a mobile ad hoc network. However, when communication between mobile devices in an ad hoc network or between a mobile device in an ad hoc network and a fixed device in a fixed network (e.g., the internet) is desired, the ad hoc routing protocols must be adjusted [11, 12].

1.2 Ad Hoc On-Demand Distance Vector Routing

AODV Routing Protocol is based on the idea of meeting demand as soon as it is made available. The number of route broadcast messages is reduced as a result of this since it gives routes on request. A route-finding message is sent to all neighboring nodes when the source node requires a packet to be transferred to the destination. In response to receiving the broadcasted message, the adjacent device replicates the process of sending a data packet to the target until no data is received at the intended destination. Once the route has been formed, all nodes record the route in their route database so that the source node can get acknowledgment of the route. The source node receives a response from that node. Once the source node receives a route-reply from a neighboring node, the source node deletes all route replies received after that. If the network topology changes throughout the simulation, the source node copies the producer and broadcasts the route request message again to ensure that the communication continues in the network after the topology changes. Whenever a link defect is discovered, the nodes on that connection simply send an error message to their neighbor nodes, and the process of selecting a new route begins from the very beginning.

The ad hoc routing protocol AODV is utilized in this thesis to investigate and simulate the link behavior between a MANET and the internet. Network Simulator 2 (NS 2) was used for this purpose [4].

1.3 Security Issues in MANET

MANET is an association of many sensor nodes that operate autonomously over unprotected wireless connections. Individual nodes in the network are free to enter and exit the network without obtaining permission. MANET is a network devoid of infrastructure. The network architecture changes fast due to the mobility of nodes, resource constraints, and bandwidth limitations of wireless media. Because of the nature of nodes, there are a variety of security risks. The Denial-of-Service attack is one of the most prevalent types of assault in MANETs. The MANET do not rely on a fixed infrastructure to function. There is no fixed infrastructure in the Mobile Ad Hoc Networking paradigm, and packets are transported to their destinations using a wireless multi-hop connection, which is not available in traditional networking. Nodes are frequently used not just as hosts but also as routers, returning traffic generated by other Nodes back to the originator. The topology of a MANET can alter because nodes may not be fixed or, on the other hand, they may fail. MANETs must meet high throughput needs while operating across a relatively wide bandwidth.

MANET is disrupted so that nodes are unable to participate in path-finding procedures, hence impairing the network's overall functionality. Numerous methods for effective routing have been discovered. There are several sorts of security threats that can disrupt the operation of a network.

1.4 Denial of Service Attacks

One of the common forms of network intrusion is a DoS attack. It is designed to cause a desired service provided to other normal users to degrade. DoS attacks may be classified into various types of attacks, including blackhole, grayhole, and flooding. Each exploits a unique security flaw in the network and wreaks on variables, including traffic flooding, connection disconnection, access restriction, and system disruption. These first three attacks listed above affect the system's routing behavior by fabricating and changing routing routes.

In contrast to the other approaches, flooding attacks directly target a network member by delivering a large number of bogus data or control packets. User Datagram Protocol (UDP) is a type of data flooding assault wherein a continuous stream of data traffic swamps the chosen target at a greater bit rate and packet size than typical. In addition, UDP lacks flow control since it is a connectionless protocol that lacks flow control.

A DoS attack involves flooding a server with packets from a single machine. The purpose of this assault is to overwhelm the server's and other resources' bandwidth. A distributed denial of service attack is a type of DoS assault that employs numerous machines preventing legitimate users from using a service. It is a form of active assault and a powerful tool for attacking the internet's resources. This research will deal with three types of attack: Flooding, Blackhole, and Grayhole.

1.4.1 Flooding Attack

One of the most devastating attacks is the flooding attack. Malicious nodes transmit overflowing Route Request (RREQ) bundles to the elusive target in such an attack. Such a target is not available in the system due to the use of a bogus Internet Protocol address in the course request. All intermediary nodes between the source and destination sent such malicious packets around the network; eventually, such packages continue to spin among the nodes, resulting in flooding. Flooding ultimately results in a DoS attack [5].

Detecting and avoiding malicious nodes is one method of defending against various threats [6, 7]. These protocols are used to track the activity of all nodes. As a result, any node exhibiting malicious action will be ignored or avoided.

1.4.2 Blackhole Attack

Generally, attacks on the network layer have two objectives: preventing packets from being sent or altering the messages' sequence number and hop count. For example, during a black hole attack, the malicious node waits for the source or one of the nodes to broadcast an RREQ message into the network. When a node receives a broadcast message, it advertises itself as the most recent route to the destination, i.e., the route with the greatest sequence number, by sending the Route Reply (RREP) message. After receiving the reply message, presumably from the confident node, the source begins delivering packets to the destination. However, while it first passes packets to their destination, it eventually misbehaves by dropping packets frequently.

The way rogue nodes are integrated into data pathways varies. The black hole problem is illustrated in Figure 1.1 In this representative scenario, node “A” wants to interact with node “D” and transfer data packets, so the route discovery process begins. If node “C” is malicious, it immediately asserts that it has an active route to the specified target node upon receiving RREQ packets from node “A”. It then transmits RREP to node “A” before sending it to any other real node. This way, node “A” assumes that this is the active route, completing the process of active route discovery. Following then, node “A” disregards any further responses and begins delivering data packets to node “C”. Finally, node “C” discards all data packets, causing them to be eaten or lost.

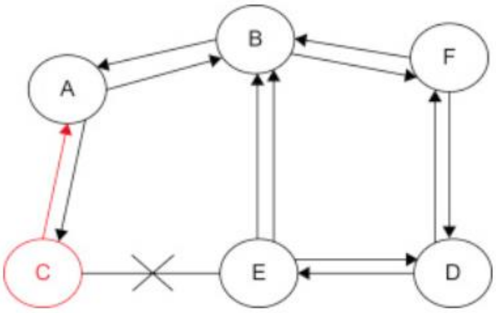


Figure 1.1: A sample blackhole attack scenario

1.4.3 Grayhole Attack

Grayhole [8, 9] attacks are like blackhole attacks in a way that the rogue node drops the targeted packets. In this case, the malicious node masquerades as a regular node and drops the targeted packets. As a result, finding these sorts of rogue nodes is challenging. Grayhole attacks consist of two phases: the first phase, similar to blackhole attacks, involves the malicious node exploiting the sender to advertise itself as having a valid route to a destination node, and the second phase, in which the malicious node drops packets with a certain probability or selectively.

A representative grayhole problem is illustrated in Figure 1.2 In this illustration, “A” is the source node, while “D” is the destination node. “B” and “C” are the neighboring nodes. “E” is the malicious node capable of manipulating the data. “B” and “C” are nodes that are next to “A”. “E” claims that by routing information through a non-existent neighboring node, the message reaches its destination quickly. On the other hand, “B” asserts that by routing data through its adjacent node “E”, which is an actual node, the message reaches its target quickly. This is where the concept of conflict occurs.

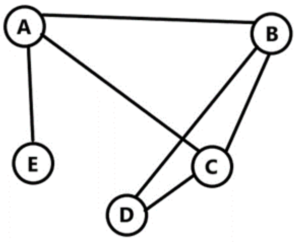


Figure 1.2: A sample grayhole attack scenario

1.5 Aim of the Research

Even though MANETs are inherently vulnerable to harmful behavior, achieving perfect security is highly challenging. An IDS that monitors system activity and detects intrusions is commonly employed in conjunction with other security measures due to the inadequacy of preventative strategies. Some solutions for coping with DoS assaults in MANETs have been presented in the literature. However, most approaches deal with only one kind of intrusion and ignore the others. Flooding, blackhole, and grayhole attacks are all examples of DoS attacks that try to make computer/network resources unavailable to legitimate users. Therefore, a new solution considering different intrusion and restrictions, as mentioned earlier, should be devised.

This study aims to develop a multistage IDS for identifying flooding, blackhole, and gray-hole intrusions employing SVMs. The SVM algorithm allows for binary classification and the division of data points into two categories. Hence, the SVM approach is employed in this research to classify and detect multiple attacks after breaking down the multiclassification problem into multiple binary classification problems.

This work presents a resilient solution for MANET that is resistant to UDP data flooding, grayhole, and blackhole assaults by employing an SVM-based intrusion detection system. Training is performed by the data collected from simulated situations using the AODV routing protocol, and it is shown that the new proposal effectively identifies various kinds of intrusions.

The following sections explain the methods and solutions necessary to train an SVM-based detection system, followed by a presentation and discussion of the system’s results and performance.

Chapter 2

INTRUSION DETECTION SYSTEM

Security threats and malicious conduct have always been a problem for any network. However, implementing all available security measures in advance allows the system to distinguish between harmful activity designed for evil purposes and misusage by a legitimate user. As such, in addition to preventive measures, we require an intrusion detection technique capable of detecting and responding to ongoing security breaches.

2.1 Multiclass classification

There are two types of classification tasks in machine learning: binary classification and multiclass classification. The classifiers model is created via training with only two classes in a dataset in the binary classification situation. The classifier is then tested on a specified test sample to +1 if specific attributes are pertaining to the model. Moreover, it classifies -1 if the example does not belong to the model. In contrast, multiclass classification trains many classes in a dataset. IDSs are used to defend against attack on data integrity and confidentiality. Numerous strategies such as data mining techniques are available to determine the sort of attack in an IDS. However, some are incredibly time-consuming and labor-intensive. As a result, we suggested using SVM to detect DoS attack variants such as flooding, blackhole, and grayhole attacks.

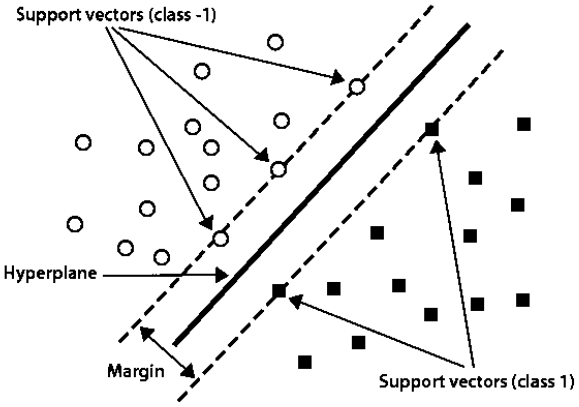


Figure 2.1: SVM Data Classification

2.2 Support Vector Machine

The SVM is a supervised learning technique known as a separating hyperplane. It is composed of a collection of training data. Classification and regression functions are the most common types of mapping functions. SVM classifiers are used to determine a group of vectors referred to as support vectors. It primarily provides the highest area for mapping data and is referred to as a hyperplane. With the assistance of provided training datasets, binary classification is used to define the normal and abnormal behavior of a pattern. Additionally, SVM will create data predictions. As a result, it produces effects in a shorter time [10].

2.3 Data Gathering

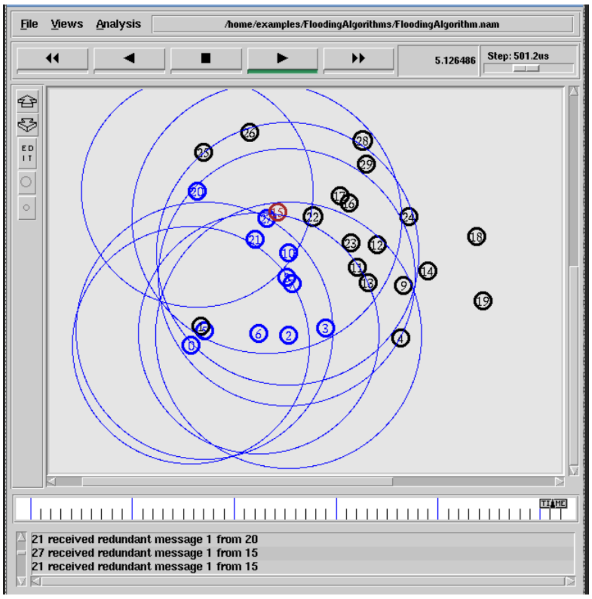
Although there are some well-known datasets, there is no specialized dataset for wireless networks such as MANET reported in the literature for detecting and classifying DoS type intrusions. Additionally, there is no specialized dataset containing the normal profiles together with the attack profiles in wireless sensor networks (WSN) that can be used to detect attackers in the system [3]. So, we constructed our specialized dataset for MANET to achieve better detection and classification of DoS attacks considered in this thesis. Furthermore, the collected futures are available at the node under consideration can be easily extracted from real-time scenarios [1]. NS2-simulator is employed to generate the training data. The type of attack being mitigated determines the parameters collected in this module. Each kind of network intrusion has a varied effect on the system’s performance metrics. Therefore, data is collected based on UDP flooding attack, blackhole attack, grayhole attack, and normal (no attack) scenarios.

2.3.1 Network Simulator 2

The Network Simulator (NS) is an object-oriented, discrete event simulator designed for networking research. NS supports extensive simulation of Transmission Control Protocol (TCP), routing, and multicast protocols over wired and wireless networks [10]. The simulator is the outcome of a continuous research and development effort. While there is tremendous trust in NS, it is not a polished and final product at this point, and faults are constantly being identified and rectified.

NS is developed in C++ and provides a command and configuration interface via an OTcl1 interpreter. The C++ portion is fast to execute but more prolonged to alter, is used to implement the detailed protocol. Conversely, the OTcl part, which runs significantly slower but can be altered extremely fast, is used to configure the simulation. Among the benefits of this split-language technique is that it enables the rapid development of massive scenarios. It is sufficient to be familiar with OTcl for utilizing the simulator.

On the other hand, changing and extending the simulator needs concurrent programming and debugging in both languages.



```
21 received redundant message 1 from 20
27 received redundant message 1 from 15
21 received redundant message 1 from 15
```

Figure 2.2: Network Simulation 2 Flooding Sample [11]

Table 2.1: Number of training and test samples

Attack class	Train	Test
Flooding attack	800	160
Blackhole attack	800	160
Grayhole attack	800	160
Normal (No attack)	800	160
Total	**3200**	**640**

2.3.2 Training Data

In this study, 3200 intrusion samples are generated for training the models. 80% of intrusion data is used for training and the remaining 20% for testing. All training samples are randomly selected from the generated dataset during the training. Table 2.1 summarizes the number of samples employed for training and testing. Training SVM models from a few data for blackhole and grayhole assaults is one of the most difficult challenges. One explanation for the ease with which SVM models might be overfitting is the unequal distribution of intrusion attack data. Ten features collected for the training and testing purpose of the SVM-based classifiers are listed in Table 2.2.

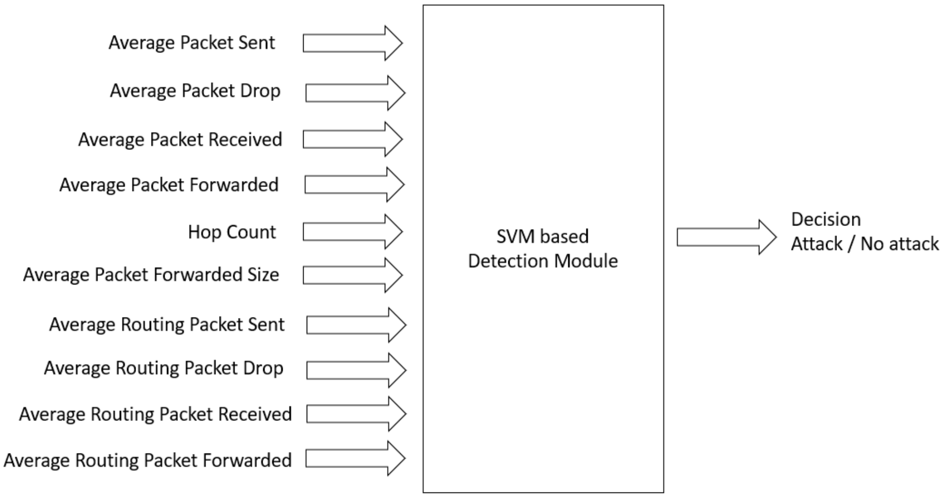

Average Packet Sent
Average Packet Drop
Average Packet Received
Average Packet Forwarded
Hop Count
Average Packet Forwarded Size
Average Routing Packet Sent
Average Routing Packet Drop
Average Routing Packet Received
Average Routing Packet Forwarded
SVM based
Detection Module
Decision
Attack / No attack

Figure 2.3: The Block Diagram of SVM-Based Classification Models

2.4 Detection Module

The detection module is the heart of the IDS and significantly influences the system's performance. SVMs are a sort of supervised machine learning model which excels at pattern recognition and classification tasks involving huge volumes of data [6].

An SVM-based learning model is used to create the detection module in this research. The detecting module's block diagram is shown in Figure 2.3 The detection module is trained using the characteristics given in this section. The SVM is constructed using a polynomial kernel of degree two, sometimes referred to as a quadratic kernel. We collected the training data during the simulations of the AODV routing protocol in both normal and attack conditions. We used ten wireless nodes in each training scenario: one serving as a receiving node, and nine serving as transmitting nodes. Three nodes were used as regular nodes transmitting at Constant Bit Rate (CBR) with

UDP traffic agents, and one as an external attacker in Flooding attack scenario. For the blackhole and grayhole we used eight attackers in the scenarios. The statistics for each feature are averaged across five-second intervals. After scaling, the data is divided into training and test sets and used as the system's input.

Table 2.2: SVM Detection Module Features

No	Feature Name	Description
1	Average Packet Sent	Average numbers of packets of data reaching their destination after being transmitted across a network
2	Average Packet Drop	Average numbers of packets of data not reaching their destination after being transmitted across a network
3	Average Packet Received	Average number of packets received
4	Average Packet Forwarded	Average number of packets forwarded
5	Hop Count	Average number of hops on the path between source and destination nodes.
6	Average Packet Forwarded Size	Average amount of data forwarded over TCP/IP networks
7	Average Routing Packet Sent	Average numbers of packets of data reaching their destination
8	Average Routing Packet Drop	Average numbers of packets of data not reaching their destination
9	Average Routing Packet Received	Average number of packets received
10	Average Routing Packet Forwarded	Average number of packets forwarded

2.5 Response Module

The detection module sends the output of the SVM-based classification models to the response module for making decision. After the inputs have been processed and the appropriate actions have been taken, the decision is generated. However, two essential factors must be considered before responding to the output of the detecting module:

the detection module’s accuracy and the likely patterns of upcoming DoS assaults. The SVM’s false negative and false positive output affects the detection module's accuracy. Consequently, decisions made solely based on a single output of SVM module are subject to mistakes, and the response module's performance must be enhanced prior to creating the final answer.

2.6 SVM Complexity and Feature Reduction

As is well known, SVM is not suitable for big data applications because of its very long training times. Although modern computers can handle a large amount of data without any problems, SVM is still not expected to work well with big data, involving millions of rows of data. SVM algorithm having large number of inputs could have considerable training complexity. However, in our proposal, the hierarchical SVM-based IDS contains only ten reasonably low numbers of inputs. Our proposed SVM IDS with linear kernel has very simple prediction complexity in the order of O(d), with d being the number of input dimensions since it is just a single inner product. To further simplify the prediction complexity of the proposed classifier), we also applied a feature ranking algorithm, namely Minimum Redundancy Maximum Relevance (MRMR), to reduce the dimensions of input feature by removing the ones with low impact on the decision performance [8].

MRMR algorithm selects a subset of features that correlate most with the class and the most negligible correlation between themselves [9]. Then, it ranks features according to the minimal-redundancy-maximal-relevance criterion based on mutual information. The collected features are ranked according to their relevance by applying the MRMR algorithm, and results are presented in Figure 2.4. This figure shows that “Average Packet Drop” and “Average Routing Packet Forwarded” are two features having the most significant importance score. Although tiny drops indicate that the differences in feature importance are not significant, we decided to use the top seven most important features by removing the last three features shown on the figures according to their scores. Figure 2.4 represents the block diagram of SVM-based classification models with feature reduction. We expect that removing redundant data that would not significantly impact the ML algorithm will reduce the computational power required for the classification algorithms as they would process fewer data.

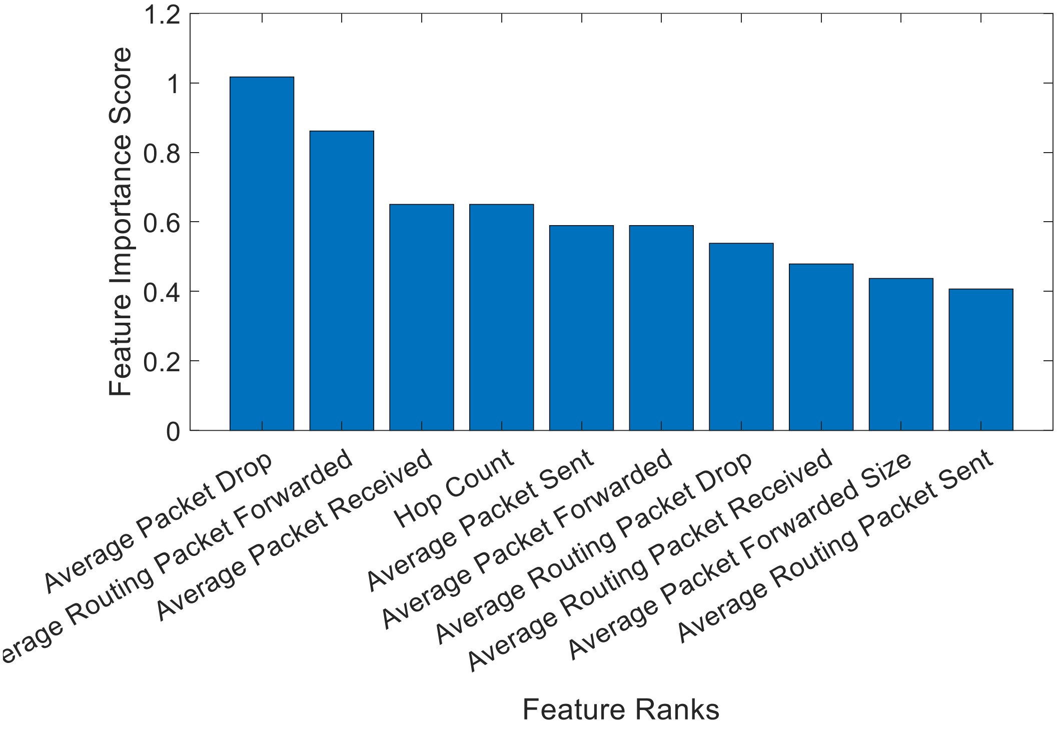


Figure 2.4: Feature Ranking Based on MRMR Algorithm

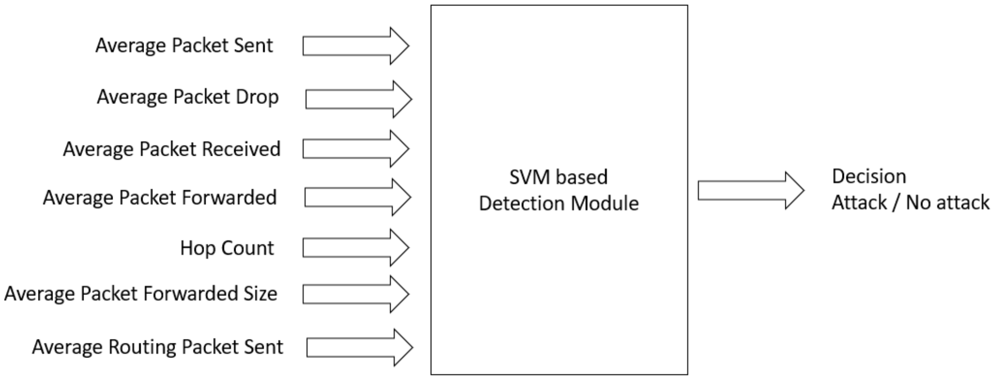
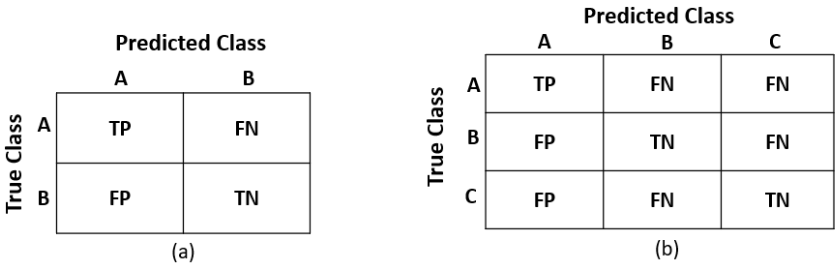


Figure 2.5: The Block Diagram of SVM-Based Classification Models with Feature Reduction

2.7 Confusion Matrix

A confusion matrix is a way of summarizing the performance of a classification algorithm. It is frequently used to define the classification effectiveness of the algorithm on a set of test data for which the actual values are known. The following factors, such as True Positive (PT), True Negative (TN), False Positive (FP), and False Negative (FN), are the most fundamental components of the confusion matrix, which are defined in Figure 2.6 for binary and multiclass classification problems.


Predicted Class
True Class
(a)
(b)

	A	B
A	TP	FN
B	FP	TN

	A	B	C
A	TP	FN	FN
B	FP	TN	FN
C	FP	FN	TN

Figure 2.6: Confusion matrices: (a) Binary Classification confusion matrix, (b) Multiclass classification confusion matrix

True Positive (TP): The term “True Positive” refers to the number of predictions in which the classifier correctly predicts the positive class to be positive.

True Negative (TN): This metric indicates the number of predictions in which the classifier correctly classifies the negative class as negative.

False Positive (FP): This term refers to the number of predictions made by the classifier in which the negative class is wrongly predicted as positive.

False Negative (FN): This term refers to the number of predictions made by the classifier in which the positive class is wrongly predicted as negative.

2.8 Performance Metrics

In this research, five performance metrics are employed to measure the performance of the proposed classifiers known as accuracy, precision, recall, and f-score.

2.8.1 Accuracy

Accuracy is a measure of the overall percentage of correctly classified objects. However, it is unreliable for unbalanced data sets, especially for the IDS problem. It may be calculated as follows:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \quad (1)$$

2.8.2 Precision

Precision refers to a classification system’s ability to reliably identify attacks among all positive predictions. It may be calculated as follows:

$$Precision = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \quad (2)$$

2.8.3 Recall

Recall, also called detection role, is a categorization capability that indicates an attacker’s ability to forecast assaults from real attacks properly. It may be calculated as follows:

$$Recall = \frac{\mathrm{T\,P}}{\mathrm{T\,P} + \mathrm{F\,N}} \tag{3}$$

2.8.4 F-Score

The f-score, sometimes referred to as the f-measure, is a statistical tool for determining the accuracy of information retrieval or binary classification, regardless of whether the element categorized or retrieved is relevant or irrelevant. f1 score is the harmonic mean of recall and precision. It can be computed as:

$$F1 = 2\,.\frac{Precision.\,Recall}{Precision + Recall} \tag{4}$$

Chapter 3

SIMULATION RESULTS

In this part, experimental results are presented first to illustrate the construction of hierarchical multiclass SVM-based IDS. Then the performance of the proposed classifier is evaluated. Five performance metrics are chosen to evaluate the system's performance, as mentioned before: accuracy, precision, recall, and f-score.

In the first stage, NS2 [11] is used to generate scenarios to collect data necessary for the proposed SVM-based IDS training phase. Each scenario is generated under UDP traffic, lasts 4000 seconds and uses the AODV routing protocol. To obtain an average performance, each simulation scenario is repeated 500 times for each configuration. The simulation area is 1000x1000 meters for all scenarios. The number of nodes is set to 10. There are four scenarios; in each one, two nodes communicate with each other. In UDP flooding scenario, one of the remaining nodes is selected as the attacker. In blackhole and Grayhole scenarios, all the remaining nodes (eight) are defined as attackers. The speeds are configured to range from 1 to 10 meters per second. Finally, all the remaining parameters of the scenarios are chosen, as shown in Table 3.1.

The constructed dataset contains five prominent cases and 3200 instances, namely normal, flooding, blackhole, and grayhole, each having 800 samples, as shown in Table 2.1.

Feature scaling or standardization is vital for SVM-based classification algorithms. SVM optimization is based on minimizing the decision vector, and the scale of the input features influences the optimal hyperplane. Therefore, it is recommended that data be standardized before training the SVM model. Standardizing the dataset transforms them to have mean 0 and standard deviation 1. This process also removes the dependence on arbitrary scales in the dataset and generally improves performance. In this research, all feature vectors (x) in the dataset are standardized by using the following feature standardization formula shown below:

$$x_s = \frac{x - \mu}{\sigma}$$

where μ and σ represent the features' mean and standard deviation.

Table 3.1: Simulation Parameters

Parameters	Values
Simulation Area	1000 m by 1000 m
Simulation Time	4000 s
Routing Protocol	AODV
Mac Protocol	IEEE 802.11
Bandwidth	2 Mbps
Packet Size	512
Node Speed	1 to 10 meters per second
Node placement / Movement	Random Waypoint
Traffic Rate (Normal, Blackhole, Grayhole)	200 Kbps
Traffic Rate (Flooding)	2048 kbps
Traffic Model	CBR
Random Noise in CBR	Enabled

To accomplish intrusion detection in MANETs, we apply statistical classification techniques. These algorithms have the benefits of mainly being automated, reasonably precise, and based on statistics. SVMs have a wide range of applications, including intrusion detection in wired networks [18]. It has been widely investigated theoretically and empirically and has been successfully deployed in various applications. One of our key goals is to figure out the best feature for attack description. Distinct properties are critical for developing accurate classifier models. We conducted various studies to ensure that the selected attributes can generate more accurate descriptions of intrusion detection attacks.

3.1 Hierarchical Multiclass SVM-Based IDS

In this stage, binary classifiers are designed to select the best one performing for each step of the multiclass classifier. The SVM-based multiclass classification models used in this study are one-vs-all types. In this approach, the multistage IDS is constructed from binary SVM models generated to detect only one kind of intrusion by picking the most robust model for each stage, shown in Table 3.2. The analysis for the stages of the hierarchal classifier is given in the following sections. All the classification models are constructed using SVM with linear kernel. Each simulation was repeated 500 times and averaged using 80% of the samples for training and the remaining 20% for testing in each trial.

3.1.1 First Stage of Hierarchical Classifier

The principal objective of the first stage is to find out the best binary classification models from a set of four classification models. Four SVM classification models are constructed as normal vs. {flooding, blackhole, grayhole}, flooding vs. {normal, blackhole, grayhole}, blackhole vs. {normal, flooding, grayhole} and grayhole vs. {normal, flooding, blockhole}. Each SVM model is trained with all samples in the class as label “zero” and the other samples as label “one”. For example, to train flooding vs. {normal, blackhole, grayhole} model, all samples from flooding classes are labeled as “zero” and other samples from normal, blackhole, and grayhole as “one”. The testing performances of the classifiers are presented in Table 3.2 as clearly seen, the performance of flooding vs. {normal, blackhole, grayhole} classifier outperforms the others in terms of all the metrics. Therefore, binary flooding vs. {normal, blackhole, grayhole} SVM-based classifier is selected as the classifier of the first stage. Performances of the classifiers in terms of f-scores are also shown in Figure 6 as a chart.

Table 3.2: Performances of SVM Models for the First Stage

Intrusion Type	Precision	Accuracy	Recall	F-score
Flooding attack vs. others	100.00 %	100.00 %	100.00 %	100.00 %
Blackhole attack vs. others	98.57 %	98.22 %	92.83 %	95.46 %
Gray-hole attack vs. others	95.43 %	92.30 %	70.26 %	81.95 %
Normal vs. others	74.05 %	90.95 %	98.38 %	84.46 %

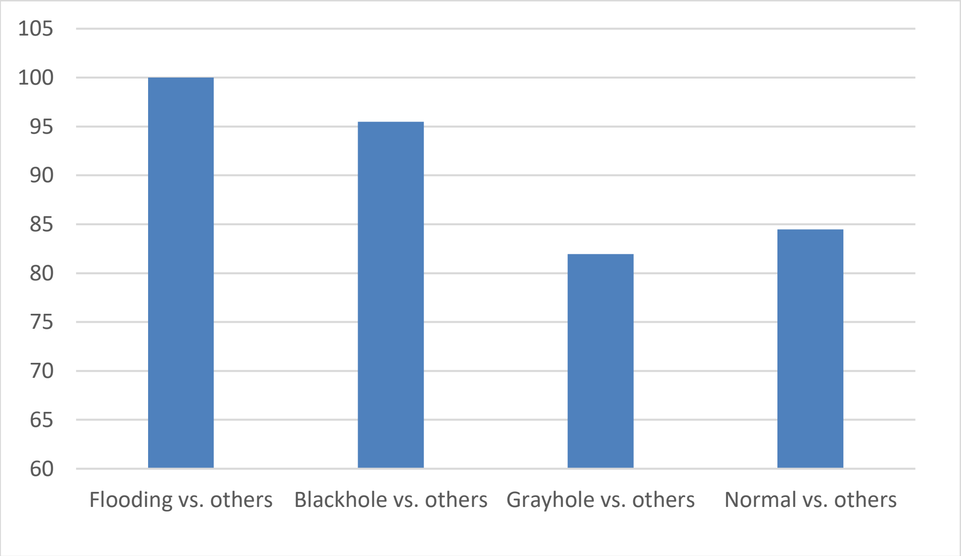


Figure 3.1: F-Scores of the SVM models for the First Stage

3.1.2 Second Stage of Hierarchical Classifier

The same analysis as the first stage is repeated by removing the flooding data from the dataset. The second stage's purpose is to choose the best binary classification model from three new models, namely normal vs. {blackhole, grayhole}, blackhole vs. {normal, grayhole} and grayhole vs. {normal, blockhole}. The testing performances of the classifiers are presented in Table 3.3 as a result of the findings, it can be deduced that the accuracy, precision, and f-score performance of blackhole vs. {normal, grayhole} classifier are 98.22%, 97.03%, and 95.43%, respectively. Therefore, since all the scores are above 90%, this SVM-based classifier is selected as the classifier of the second stage. Performances of the classifiers in terms of f-scores are also shown in Figure 3.2

Table 3.3: Performances of SVM Models for the Second Stage

Intrusion Type	Precision	Accuracy	Recall	F-score
Blackhole attack vs. others	98.22 %	97.03 %	92.81 %	95.43 %
Gray-hole attack vs. others	95.31 %	89.89 %	70.83 %	82.30 %
Normal vs. others	73.95 %	87.85 %	98.36 %	84.40 %

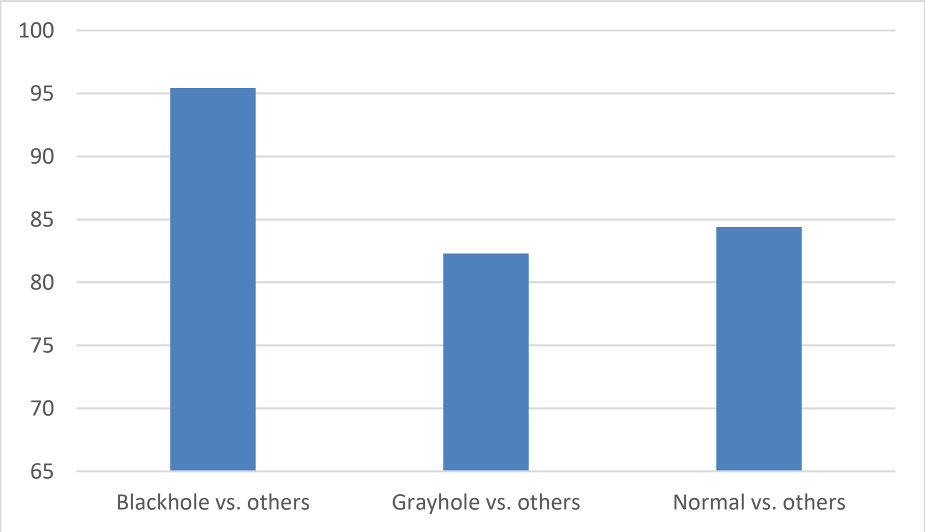


Figure 3.2: F-Scores of the SVM models for the Second Stage

Table 3.4: Performances of SVM Models for the Third Stage

Intrusion Type	Precision	Accuracy	Recall	F-score
Grayhole attack vs. normal	97.63 %	85.16 %	72.18 %	82.96 %
Normal vs. Grayhole	77.76 %	85.06 %	98.33 %	86.81 %

3.1.3 Third Stage of Hierarchical Classifier

For the third stage, flooding and blackhole data are removed from the dataset. We left only with two binary SVM models, namely normal vs. {grayhole} and grayhole vs. {normal}. Therefore, the performances of these two classifiers are presented in Table 3.4. The accuracy of grayhole attack and blackhole attack slightly differ for intrusion detection because grayhole attack is an advanced transformation of blackhole attack [11].

It is important to note that, in the case of grayhole, the intruder node behaves maliciously for some particular time duration by dropping packets but may switch to normal behavior later. Hence, it is not easy to distinguish this behavior when it switches to normal mode from the normal node behavior. This is why the performances of these last two SVM models are not as good as the previous models. The testing performances of the classifiers are presented in Table 3.4 The performances of both classifiers are comparable, but since the precision of normal vs. {grayhole} classifier is significantly lower than the precision of grayhole vs. {normal} classifier, grayhole vs. {normal} classifier is employed in the last stage. F-score performances of these last two classifiers are given in Figure 3.3.

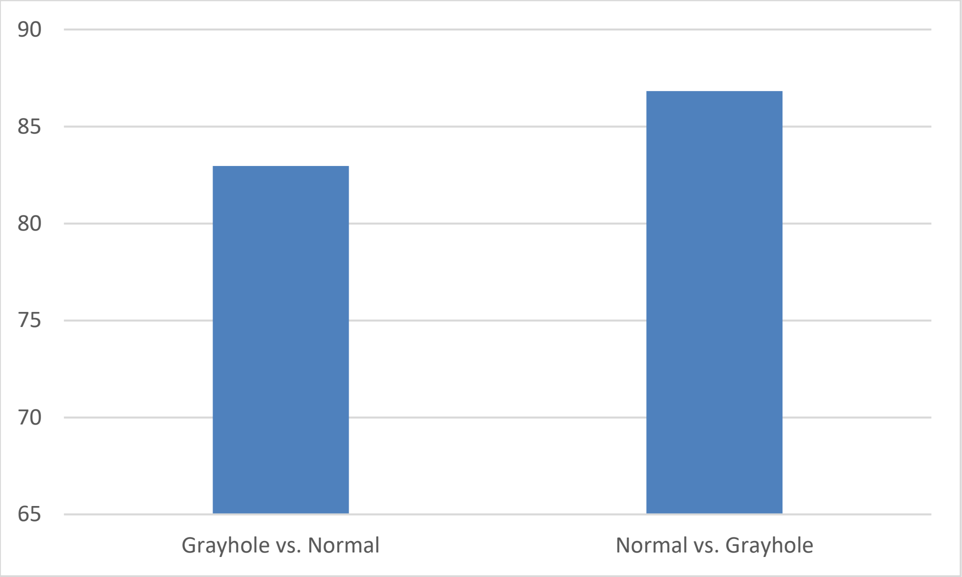


Figure 3.3: F-Scores of the SVM models for the Third Stage

3.2 Performance of Hierarchical Multiclass SVM-Based IDS

We have introduced a method based on hierarchical SVM classifiers to detect multistage attacks. As explained in the previous sections, the most robust models are chosen for each stage. The proposed system is constructed after selecting the best SVM models for the stages of hierarchical multiclass SVM-based IDS, as shown in Figure 3.4 In this proposed architecture, the first stage decides if a flooding attack occurs. Otherwise, the second stage decides if a blackhole attack occurs, and if both classifiers cannot detect any attack, then the last stage decides whether there is a grayhole type attack or normal attack. Finally, the experimental analyses to evaluate the performance of this proposed hierarchical multiclass IDS for solving the four-class intrusion classification problem is conducted.

The system’s performance is evaluated by selecting 320 samples randomly from the data for each simulation. Then, the simulation is repeated 500 times to generate the confusion matrix shown in Figure 3.5.

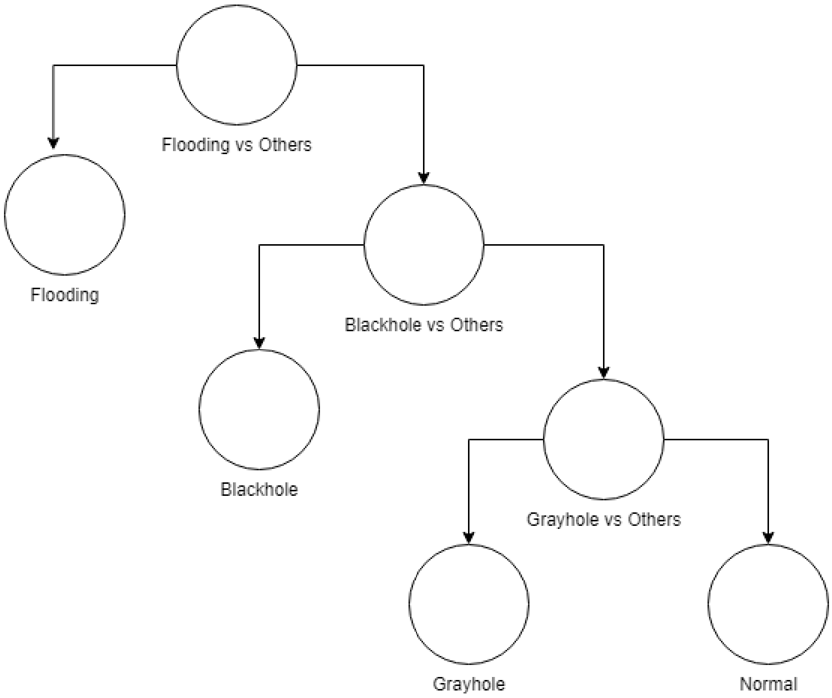


Figure 3.4: The proposed hierarchical Multiclass SVM-based classifiers for Intrusion Detection.

Predicted Labels

True Labels

	Normal	**Flooding**	**Grayhole**	**Blackhole**
Normal	39321	0	375	308
Flooding	0	39898	0	0
Grayhole	11158	0	28450	354
Blackhole	2780	0	72	37284

Figure 3.5: Confusion Matrix for hierarchical Multiclass SVM-based classifiers

As observed from the confusion matrix, almost one-third of the grayhole attack is predicted as there is no attack in the system. However, this result is expected since, in the case of grayhole, the intruder repeatedly switches to attack and normal mode. The performance of the proposed IDS is presented in Table 3.5 in terms of accuracy, precision, recall, and f-score. The calculation of these metrices for Normal case is explained. *TP*, *TN*, *FP* and *FN* values can be obtained from the confusion matrix as shown below:

TP=39321

TN=39898+28450+72+354+37284=106058

FP=11158+2780=13938

FN=375+308=683

Then, the performance metrices for the Normal attack free situation can be calculated as follows:

$$accuracy = \frac{TP+TN}{TP+FP+FN+TN} = \frac{39321 + 106058}{39321 + 13938 + 683 + 106058} = 0.9086, 90.86\%$$

$$precision = \frac{TP}{TP+FP} = \frac{39321}{39321 + 13938} = 0.7382, 73.82\%$$

$$recall = \frac{TP}{TP+FN} = \frac{39321}{39321 + 683} = 0.9829, 98.29\%$$

$$f - score = \frac{2\times TP}{2\times TP+FP+FN} = \frac{2\times 39321}{2\times 39321 + 13938 + 683} = 0.8432, 84.32\%$$

Table 3.5: Performance of Proposed Hierarchical Multiclass SVM-Based IDS

Intrusion Type	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F-score (%)**
Normal	90.86	73.83	98.29	84.32
Flooding	100.00	100.00	100.00	100.00
Grayhole	92.53	98.45	71.19	82.63
Blackhole	97.80	98.26	92.89	95.50
Average	**95.297**	**92.633**	**90.596**	**90.614**

As observed from Table 3.5, the average performance of the system in terms of performance metrics is all above 90%. Hence, it can be concluded that the proposed hierarchical multiclass SVM-based IDS successfully detects the intrusions and can classify the type of intrusions in the system. The f-score performances of the system for each attack type and the average performance are illustrated in Figure 3.6.

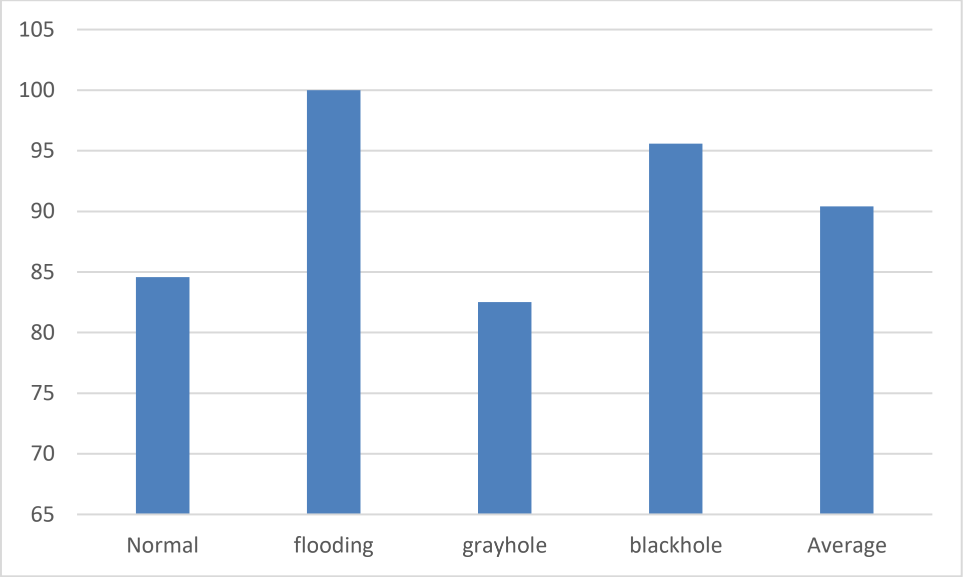


Figure 3.6: F-Score Performance of The Prosed Hierarchical Multiclass SVM-based Classifiers

3.3 Performance of Hierarchical Multiclass SVM-Based IDS with Feature Reduction

A similar analysis done before with all ten features is repeated by removing the three features having the lowest impact scores, namely "Average Routing Packed Received", "Average Packet Forwarded Size", and "Average Packet Routing Sent". The testing performances of the classifiers for each stage are presented in Tables 3.6, 3.7, and 3.8. The outcomes obtained with the reduced features are very close to those obtained with all the features. So same classifiers were chosen to construct hierarchical multiclass SVM-based IDS with fewer features. The selected classifiers for each stage can be listed as flooding vs. {normal, blackhole, grayhole}, blackhole vs. {normal, grayhole} and grayhole vs. {normal} for stage 1, 2 and 3 respectively. The performance of the hierarchical SVM-Based classifier is presented in Table 3.9. The f-score performances of the system for each attack type and the average performances are illustrated in Figure 3.6 with feature reduction and with all features to compare their performances. It is also seen from this figure that; feature reduction does not create any performance loos but lowers the computational complexity of the system.

Table 3.6: Performances of SVM Models with Feature Reduction for the First Stage

Intrusion Type	Precision	Accuracy	Recall	F-score
Flooding attack vs. others	100.00 %	100.00 %	100.00 %	100.00 %
Blackhole attack vs. others	98.31 %	97.81 %	92.81 %	95.47 %
Gray-hole attack vs. others	95.40 %	92.29 %	70.26 %	81.94 %
Normal vs. others	73.72 %	90.90 %	98.78 %	84.40 %

Table 3.7: Performances of SVM Models with Feature Reduction for the Second Stage

Intrusion Type	Precision	Accuracy	Recall	F-score
Blackhole attack vs. others	98.30 %	97.09 %	92.86 %	95.49 %
Gray-hole attack vs. others	99.09 %	89.98 %	70.49 %	82.33 %
Normal vs. others	73.54 %	87.79 %	98.74 %	84.27 %

Table 3.8: Performances of SVM Models with Feature Reduction for the Third Stage

Intrusion Type	Precision	Accuracy	Recall	F-score
Grayhole attack vs. normal	98.73 %	84.97 %	70.89 %	82.47 %
Normal vs. Grayhole	76.97 %	84.76 %	99.11 %	86.63 %

Table 3.9: Performance of Proposed Hierarchical Multiclass SVM-Based IDS with Feature Reduction

Intrusion Type	Accuracy (%)	Precision (%)	Recall (%)	F-score (%)
Normal	90.84	73.74	98.79	84.41
Flooding	100.00	100.00	100.00	100.00
Grayhole	92.49	98.95	70.75	82.51
Blackhole	97.76	98.19	92.77	95.40
Average	**95.263**	**92.688**	**90.553**	**90.561**

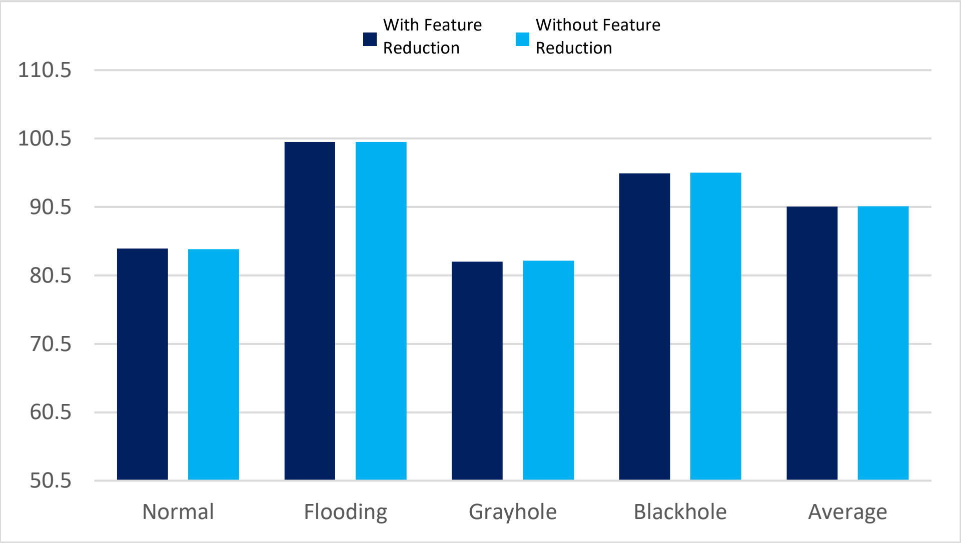


Figure 3.7: F-Score Performances of The Prosed Hierarchical Multiclass SVM-based Classifiers with and without Feature Reduction

3.4 Performance Comparison of Hierarchical Multiclass SVM-Based IDS with the Other ML Approaches

In this section, we also evaluated the performances of three classifiers, namely K-Nearest Neighbors (KNN), Naïve Bayes (NB), and Decision Tree (DT). The performances of the abovementioned classifiers were calculated after feature reduction by taking the average of 500 experiments and compared with the results of the proposed Hierarchical SVM-based classifier. The results are presented in Tables 3.10, 3.11, and 3.12 for KNN, NB, and DT. The average performances of the classifiers are summarized in Table 3.13. It can be concluded from the results of this table that the proposed hierarchical SVM-based approach performs better than DT, KNN, and NB-based classifiers for detecting attacks. It is also worth mentioning that the performance of the DT approach is very close to the performance of our proposal. NB-based classifiers perform the worst. Figure 3.8 also presents the average F-Score performances of the classifier as a bar chart.

Table 3.10: Performance of Decision Tree Classifier

Intrusion Type	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F-score (%)**
Normal	90.75	73.96	97.36	84.06
Flooding	100.00	100.00	100.00	100.00
Grayhole	92.40	97.25	71.67	82.52
Blackhole	97.76	98.09	92.81	95.37
Average	**95.23**	**92.32**	**90.46**	**90.48**

Table 3.11: Performance of KNN Classifier

Intrusion Type	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F-score (%)**
Normal	90.75	73.58	98.35	84.18
Flooding	100.00	100.00	100.00	100.00
Grayhole	90.69	89.72	70.81	79.15
Blackhole	96.03	98.17	85.80	91.57
Average	**94.368**	**90.368**	**88.742**	**88.726**

Table 3.12: Performance of Navii Base Classifier

Intrusion Type	Accuracy (%)	Precision (%)	Recall (%)	F-score (%)
Normal	80.41	89.13	24.60	38.56
Flooding	100.00	100.00	100.00	100.00
Grayhole	92.35	97.48	71.25	82.33
Blackhole	7472.80	4962.26	99.06	66.12
Average	**86.898**	**84.110**	**73.743**	**71.796**

Table 3.13: Average Performances of the Classifiers

Classifier	Accuracy (%)	Precision (%)	Recall (%)	F-score (%)
KNN	94.368	90.368	88.742	88.726
DT	95.23	92.32	90.46	90.48
NB	86.898	84.110	73.743	71.796
Proposed SVM	95.297	92.633	90.596	90.614

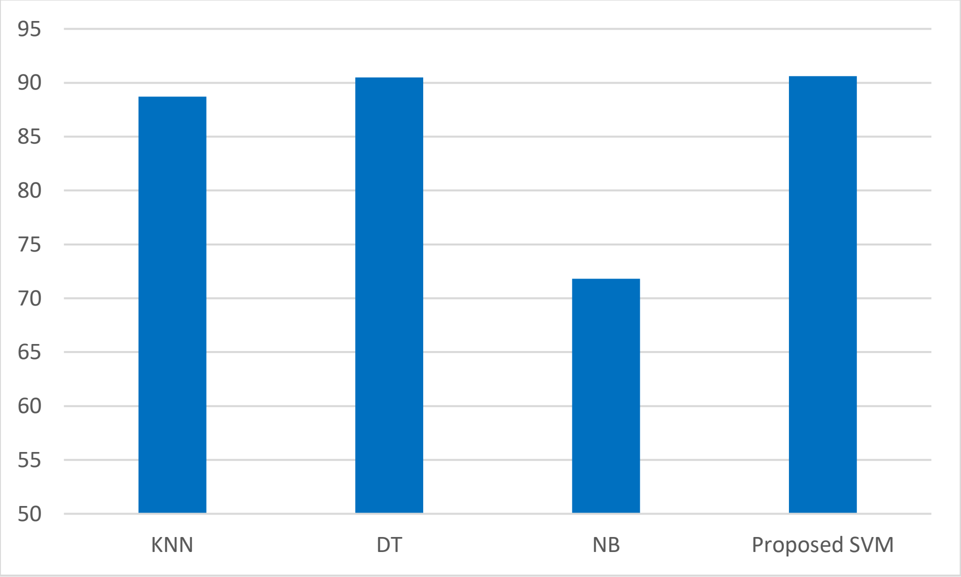


Figure 3.8: Average F-Scores of the classifiers

Chapter 4

CONCLUSIONS AND FUTURE WORK

This thesis presents a multistage ID technique based on SVM to identify attacks such as flooding, blackhole, grayhole in MANET systems. The multistage IDS was constructed from binary SVM models generated to detect only one type of intrusion by selecting the most robust model for each stage. The results of extensive simulations and studies revealed that the proposed hierarchical multiclass IDS, based on SVM, detects the intrusions successfully and can classify the type of intrusions in the system. Hence, the presented multistage classifier is highly effective in detecting network DoS attacks.

As a future work, designed multistage IDS will be simulated in MANET systems using NS2, and performance improvement of the system with the assistance of proposed IDS will be investigated. It is expected that the inclusion of the suggested SVM-based IDS will increase the system's performance and bring it closer to the ideal system by eliminating the disruptive effects of the intrusions on packet delivery ratio, latency, and throughput.

REFERENCES

[1] Abdelshafy, M.A. and King, P.J., 2013. AODV routing protocol performance analysis under MANET attacks. *International Journal for Information Security Research (IJISR)*, *3*(1/2), pp.418-426.

[2] Ali, S. and Nand, P., 2016, April. Comparative performance analysis of AODV and DSR routing protocols under wormhole attack in mobile ad hoc network on different node’s speeds. In *2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 641-644). IEEE.

[3] Almomani, I., Al-Kasasbeh, B. and Al-Akhras, M., 2016. WSN-DS: a dataset for intrusion detection systems in wireless sensor networks. Journal of Sensors, 2016, Article ID 4731953.

[4] Bhardwaj, N. and Singh, R., 2014. Detection and avoidance of blackhole attack in AOMDV protocol in MANETs. *International Journal of Application or Innovation in Engineering & Management*, *3*(5), pp.376-383.

[5] Bhati, B.S. and Rai, C.S., 2020. Analysis of support vector machine-based intrusion detection techniques. *Arabian Journal for Science and Engineering*, *45*(4), pp.2371-2383.

[6] Chatterjee, N. and Mandal, J.K., 2013. Detection of blackhole behavior using triangular encryption in NS2. *Procedia Technology*, *10*, pp.524-529.

[7] Chettibi, S., Labeni, Y. and Boulkour, A., 2015, November. Trace file analyzer for ad hoc routing protocols simulation with NS2. In *2015 First International Conference on New Technologies of Information and Communication (NTIC)* (pp. 1-6). IEEE.

[8] Ding, C. and Peng, H., 2005. Minimum redundancy feature selection from microarray gene expression data. Journal of bioinformatics and computational biology, 3(02), pp.185-205.

[9] Ghayvat, H., Pandya, S., Shah, S., Mukhopadhyay, S.C., Yap, M.H. and Wandra, K.H., 2016, November. Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET. In *2016 10th international conference on sensing technology (ICST)*. IEEE.

[10] Ghumro, A., Ahmed, A. and Memon, A.K., 2019, April. Node Misbehavior Attacks in WBAN: Effects and Countermeasures. In *1st International Conference on Computational Sciences and Technologies (INCCST'19).*

[11] Gorine, D. and Saleh, R., 2019. Performance Analysis of Routing Protocols in MANET under Malicious Attacks. *International Journal of Network Security & Its Applications (IJNSA) 11(2),* pp.*1-12.*

[12] Gurung, S. and Chauhan, S., 2019. Performance analysis of blackhole attack mitigation protocols under gray-hole attacks in MANET. *Wireless Networks*, *25*(3), pp.975-988.

[13] Kakkar, P. and Saluja, K., 2016, March. Performance investigations of reactive routing protocols under flooding attack in MANET. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 623-627). IEEE.

[14] Kaur, P. and Gurm, J.S., 2016. Detect and prevent HELLO FLOOD attack using centralized technique in WSN. *International Journal of Computer Science & Engineering Technology*, *7*(8), pp.379-81.

[15] Muthusenthil, B. and Murugavalli, S., 2015. Performance evaluation of GPSR with ALERT in Mobile Ad-hoc Networks. *International Journal of Applied Engineering Research, 10*(17), pp. 13482-13491.

[16] Prabha, K., 2014. *Support Vector Machine Based Techniques for Network Intrusion Detection System*. Bharathiar University.

[17] Tan, N.D. and Van Tan, L., 2020. Implementation of Black Hole Attack on AODV Routing Protocols in MANET Using NS2. *UTEHY Journal of Science and Technology*, *25*, pp.45-51.

[18] Vhora, S., Patel, R. and Patel, N., 2015, March. Rank Base Data Routing (RBDR) scheme using AOMDV: A proposed scheme for packet drop attack detection and prevention in MANET. In *2015 IEEE international conference on electrical, computer and communication technologies (ICECCT)* (pp. 1-5). IEEE