Bachelor of Science in Computer Science & Engineering

Malicious Node Detection and Blocking in OBS Network using Machine Learning Techniques

by

Avijeet Shil

ID: 1504052

Department of Computer Science & Engineering

Chittagong University of Engineering & Technology (CUET)

Chattogram-4349, Bangladesh.

April, 2021

Malicious Node Detection and Blocking in OBS Network using Machine Learning Techniques

Submitted in partial fulfilment of the requirements for
Degree of Bachelor of Science
in Computer Science & Engineering

by

Avijeet Shil
ID: 1504052

Supervised by

Dr. Md Mokammel Haque
Professor
Department of Computer Science & Engineering

Chittagong University of Engineering & Technology (CUET)
Chattogram-4349, Bangladesh.
April, 2021

The thesis titled '**Malicious Node Detection and Blocking in OBS Network using Machine Learning Techniques'** submitted by ID: 1504052, Session 2019-2020 has been accepted as satisfactory in fulfilment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering to be awarded by the Chittagong University of Engineering & Technology (CUET).

Board of Examiners

____________________________________ Chairman(Supervisor)

Dr. Md Mokammel Haque
Professor
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

____________________________________ Member (Ex-Officio)

Dr. Md Mokammel Haque
Professor & Head
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

____________________________________ Member (External)

Professor Dr. Asaduzzaman
Professor
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

Declaration of Originality

This is to certify that I am the sole author of this thesis and that neither any part of this thesis nor the whole of the thesis has been submitted for a degree to any other institution.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. I am also aware that if any infringement of anyone's copyright is found, whether intentional or otherwise, I may be subject to legal and disciplinary action determined by Dept. of CSE, CUET.

I hereby assign every rights in the copyright of this thesis work to Dept. of CSE, CUET, who shall be the owner of the copyright of this work and any reproduction or use in any form or by any means whatsoever is prohibited without the consent of Dept. of CSE, CUET.

Signature of the candidate

Date:

Acknowledgements

The satisfaction that accompanies the successful completion of this work would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. I am greatly indebted to my honorable project Supervisor Dr. Md. Mokammel Haque, Professor, Department of Computer Science and Engineering,Chittagong University of Engineering and Technology, for the guidance, inspiration and constructive suggestions which were helpful in the preparation of this project. Sir, I am really grateful to you for giving me chance to work with you in this project.I also thank Muhammad Kamrul Hossain Patwary, Research Lecturer, Institute of Information and Communication Technology, Chittagong University of Engineering and Technology for his continuous guidance, cooperation and support. I also convey gratitude to all my respected teachers of the department. I would also like to thank my friends and the staffs of the department for their valuable suggestion and assistance that has helped in successful completion of the project.

Abstract

Optical Burst Switching Network(OBS) is a next-generation internet infrastructure. Burst header packet flooding is a denial-of-service attack on an optical burst switching (OBS) network. This work proposes a malicious node detection and blocking approach to prevent burst header packet(BHP) flooding attack at an early step by reading the OBS node values. To implement this work, we used Decision Tree classifier model. We used cross-validation technique to mitigate overfitting and training the model effectively. We consider different feature selection techniques to build the final dataset to train the model. After testing the dataset, we compare the trained model with four models, Naïve Bayes, K-Nearest Neighbors(KNN), Logistic Regression, Support Vector Machine (SVM) classifier to compare the performance of our model. The experimental result shows maximum accuracy of 98.5% for our model using 752 training set and 323 testing set. Experimental results of the proposed framework have shown better accuracy compared to others. The best machine learning model is used to block the malicious nodes.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Burst Header Packet In OBS, data and control packet known as Burst Header Packet . 9

Optical burst switching Optical Burst switching (OBS) is an optical networking technique that allows dynamic sub-wavelength switching of data.. 7

Optical Circuit Switching In Optical Circuit Switching, the network is configured to establish a circuit, from an entry to an exit node, by adjusting the optical cross connect circuits in the core routers in a manner that the data signal.. 7

Optical Packet Switching Optical Packet Switching (OPS) is the simplest and most natural extension of packet switching over optics. It consists of sending IP packets directly over an all-optical backbone. 7

Chapter 1

Introduction

1.1 Introduction

The original purpose of our project was to develop a system for detecting malicious nodes in an optical burst switching network. With the increasing number of internet uses and exponential research and development in mobile and web applications, bandwidth is a concern to sustain the development and progress. Among the findings of Telcos and the scientific research communities, optical internet is on the top of the list [1].

From three classes of optical switching paradigms used in wavelength-division multiplexing(WDM) technology to solve the demand of high bandwidth requirement, Optical Burst Switching(OBS) technique is more preferable on Optical Circuit Switching(OCS) and Optical Packet Switching(OPS)[2]. OBS is considered an advanced technology for implementing network resources with the help of Optical Packet Switching(OPS). Though OBS is on the top of the list, still there is a problem to implement OBS as it mostly suffers from the Burst Header Packet Flooding attack, which occurred from the absence of buffers. Such attacks cause a decrease in bandwidth maintenance, network performance, and unwanted high data loss. Malicious nodes are these nodes that are prone to such attacks.

Our system uses machine learning to detect malicious nodes. The system can be used for blocking the nodes in the early stages.

1.2 Optical Burst Switching Network

For all-optical WDM networks, optical burst switching is a promising option. It incorporates the advantages of optical packet switching and wavelength routing thus keeping into consideration the latest all-optical technology's limitations[3]. Optical burst switching network is one of three models that is used wavelength-division multiplexing technology to meet the requirements of today's world. Among all three paradigms, OBS network is considered the next generation of the internet.

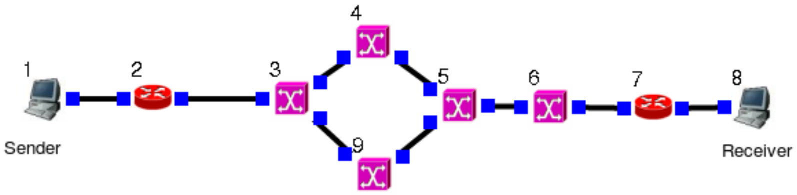


Figure 1.1: OBS network

It is an OBS network in Fig 1.1, where we consider a legitimate sender(1) and one receiver(8) only. And there are one ingress edge router(2) and one egress edge router(7). The topology contains five core switches(3,4,5,6,9) . In this modified NCTUns simulator[1], the User Datagram Protocol(UDP) is transmitted with greedy node with one second duration. For simplicity, we consider one legitimate sender and one receiver. Burst header packets (BHPs) are often sent prior to data bursts by utilizing OBS for data transfer to protect required resources and ensure network maintenance resources are maintained[4]. Ingress node which is an optical router, receives the optical packet, that travels from source to destination. After buffering for a very short time, the ingress node sends a burst header packet in order to allocate resources towards the destination for the packets. In order to transmit data from one node to another, burst header packets (BHPs)

[1] `https://www.isi.edu/nsnam/ns/`

ensure maintaining network management resources.

1.2.1 BHP Flooding Attack

For burst traffic ,OBS is at its best with sufficient details than other switching techniques in terms of optical internet. However, OBS is very concerned regarding security of the network and QoS(Quality of Service) , especially for burst header packet attacks by intruders. In the OBS network, an unallocated channel is used to reserve for incoming data bursts (DB) through BHP. Though OBS is on the top of the list to use in WDM technology, still there is a problem to implement OBS as it mostly suffered from Burst Header Packet Flooding attack, which occurred from absence of buffers. DoS attack is a consequence of malicious Burst Header Packet. BHP flooding is a sort of DoS attack in the OBS network in which a malicious node sends BHPs to the optical switch to distribute resources but does not submit any relevant data after it, it tries to keep the core node's resources to prevent legitimate nodes from accessing it.When a malicious node sends a large number of BHPs through the network without sending the individual DBs, the BHP flooding attack will subjugate the core switches. The state of allocated WDM channels switches from unoccupied to occupied when a core switch reserves them for incoming BHPs.The BHP flooding attack is demonstrated in Fig**??**

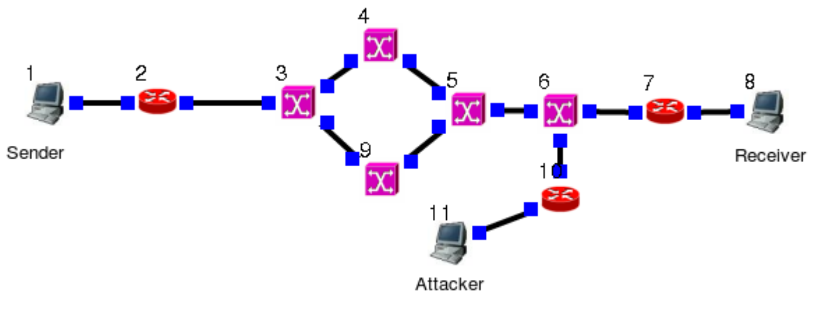
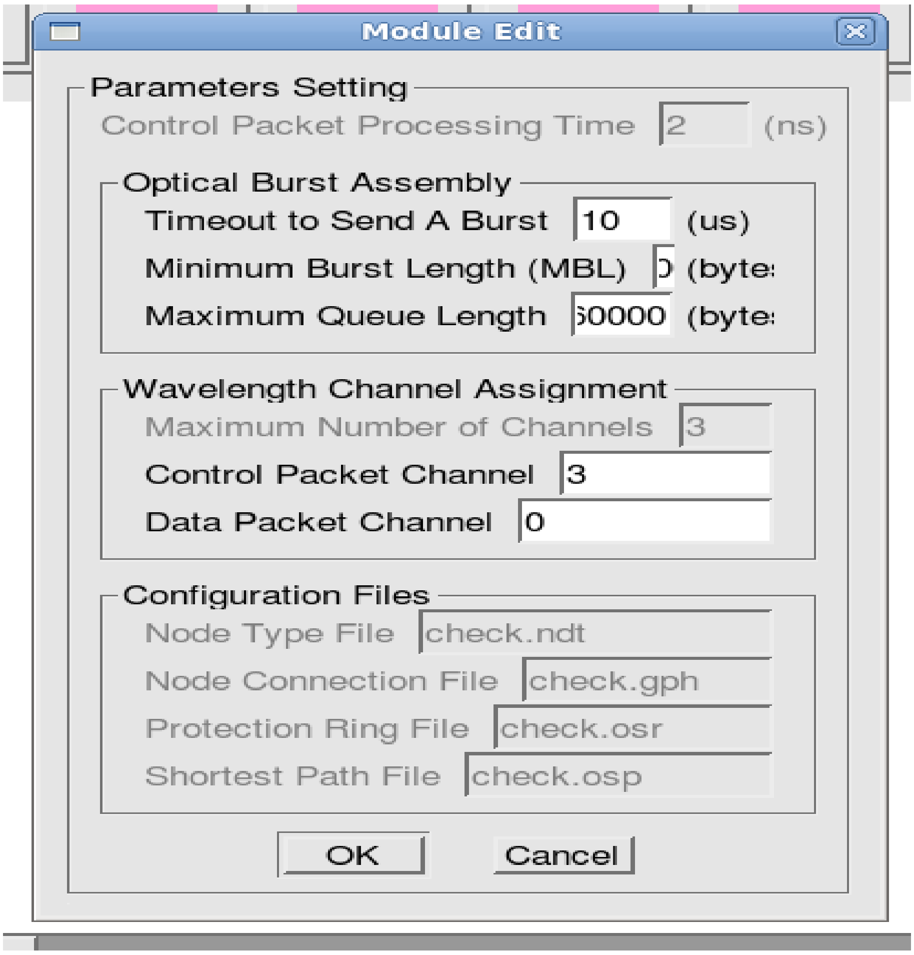


Figure 1.2: BHP Flooding Attack in an OBS Network

In the Fig 1.1 we only explained about the attack-free obs network. In Fig. 1.5, one more ingress edge router(11) is added in attacker role which try to occupy the network resources with no actual data. We have attached the router configuration for the edge router (10) in fig 1.3.



Parameters Setting

Control Packet Processing Time 2 (ns)

Optical Burst Assembly

Timeout to Send A Burst 10 (us)

Minimum Burst Length (MBL) 0 (byte

Maximum Queue Length 0000 (byte

Wavelength Channel Assignment

Maximum Number of Channels 3

Control Packet Channel 3

Data Packet Channel 0

Configuration Files

Node Type File check.ndt

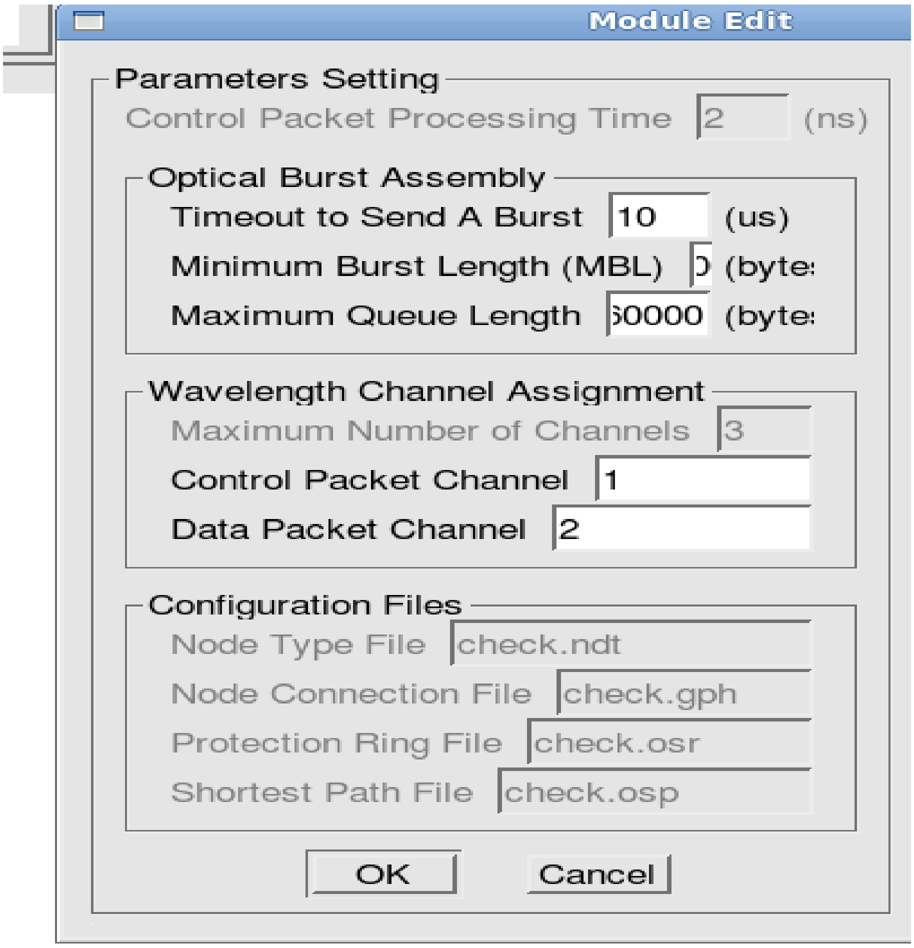
Node Connection File check.gph

Protection Ring File check.osr

Shortest Path File check.osp

Figure 1.3: Attacker Router Configuration

whereas, the ingress edge router configuration is given in Fig. 1.4



Module Edit

Parameters Setting

Control Packet Processing Time 2 (ns)

Optical Burst Assembly

Timeout to Send A Burst 10 (us)

Minimum Burst Length (MBL) 0 (byte:

Maximum Queue Length 50000 (byte:

Wavelength Channel Assignment

Maximum Number of Channels 3

Control Packet Channel 1

Data Packet Channel 2

Configuration Files

Node Type File check.ndt

Node Connection File check.gph

Protection Ring File check.osr

Shortest Path File check.osp

OK Cancel

Figure 1.4: Legitimate Router Configuration

.The BHP flooding attack is demonstrated in Fig??

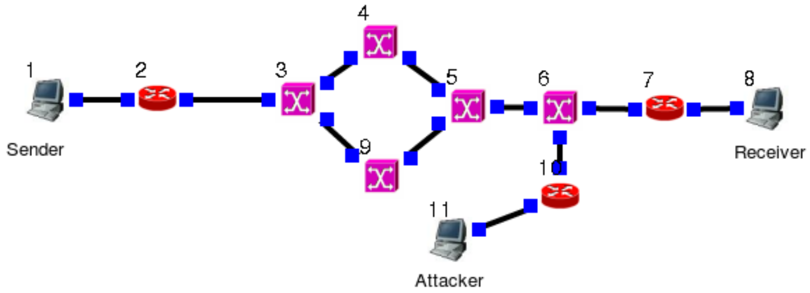


Figure 1.5: BHP Flooding Attack in an OBS Network

In the Fig 1.1 we only explained about the attack-free obs network. In Fig. 1.5, one more ingress edge router(11) is added in attacker role which try to occupy the network resources with no actual data. In Fig 1.5, attacker is considered near the egress edge router to emphasize its effect, as a result the probability of being undetected is high. But the position of attacker is independent and can be any places on the topology. For simplicity, we have considered one attacker node and one legitimate node.

Due to BHPs flooding attack, the network resources are occupied. So it causes decrease in bandwidth maintenance , network performance , and unwanted high data loss. Hence it is a threat to quality of services. Machine learning is one of the promising concepts in this sense to analyze unwanted DoS attack or burst header packet flooding in OBS network.

1.3 Malicious Node Detection and Blocking

Now, machine learning has gained significant attention to analyze the attack and detect the issues of DoS attack and prevent the attack in real time and effectively. For detecting the issues of attack, we first try to comparatively study the role of being a cause of malicious attack of the features we got from the dataset, and then after studying the role, then we try to fit the most important attributes to measure the performance of different machine learning solutions on a certain moment, we will study different machine learning techniques KNN(K-nearest neighbors), SVM(Support Vector Machine), Naïve Bayes(NB), Decision Tree, Logistic Regression. After studying the performance and detecting the malicious node, we will use a method to block the node and remove the nodes to enhance the performance. We will use the confusion matrix to calculate Precision, Recall, TN, TP ,FP, FN,F_1 score, accuracy.

After testing is complete, we'll analyze the best classifiers from f_1 score and accuracy. We'll then use the model classifier on a set of OBS node to predict the class of the nodes. If any node behaves maliciously and prone to BHP flooding attack, we will block the node and iterate through all the OBS nodes.

1.4 System Overview

In our system, we have overall 5 modules. Our system starts with data processing. After data preprocessing is completed, we will use different feature selection techniques to finalize the dataset which can give a good result to predict the testing or private dataset. The framework overview is demonstrated in Fig 1.6.

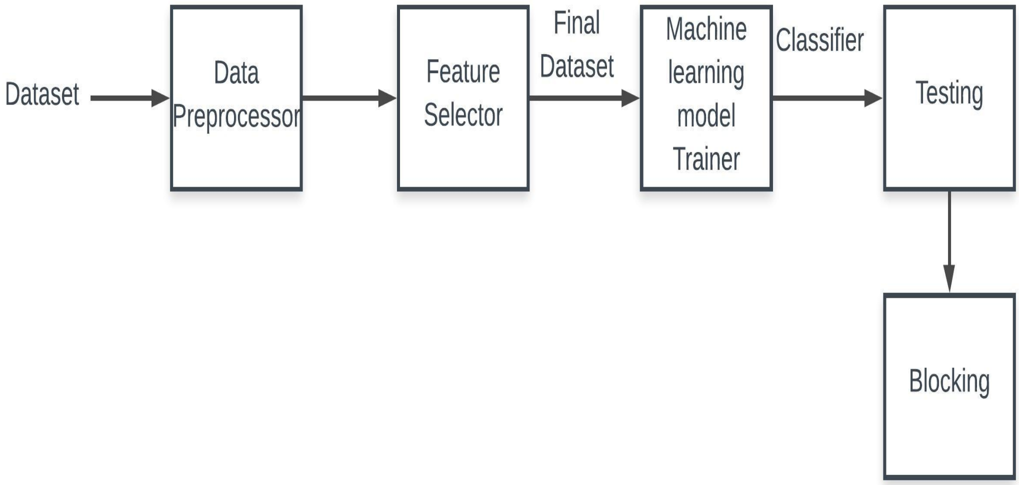


Figure 1.6: System Overview

After testing the dataset, we will use the model classifiers to block these node which are malicious and threatening for the system.

1.5 Difficulties

Optical burst switching(Optical burst switching) network is a next-generation optical networking paradigm that incorporates the benefits of Optical Circuit Switching and Optical Packet Switching.

To make free from vulnerability in early stages, we will need to establish a system which will automatically detect the misbehaving OBS node and take necessary step.

While doing the project, we have faced some challenges. The challenges are given below

- Dataset: The first and crucial challenge we face, the dataset. We don't have real OBS network to collect and investigate the system to find vulnerabilities. So, we have to consider simulated OBS network for our system. We choose NS2 simulator with nOBS extension. But nOBS extension does not work, we tried to follow the user manual. We tried different LTS of fedora. We failed to generate the environment. As the fedora distro is improving and no longer support nOBS extension, we have to rely on the available dataset on OBS network from UCI machine learning repository[2].
- Implementation: To detect malicious node automatically, is our goal. We have to look through different techniques and choose one to implement. After going through the techniques, we choose machine learning techniques. Choosing machine learning is the starting point of our work. We have to learn and read about different classifiers and data visualization tools to make the data interactive so that we can get ideas about correlation between the features and how they contribute to predict the target features.
- We have to learn our different machine learning models and label encoding techniques, hyper-parameter tuning,different techniques for example, feature selection techniques- chi-squared test of independence, random forest feature selection libraries, SelectKBest method etc.
- There are many classifiers used in classification problems. We choose five model classifiers based on their accuracy and overall performance.
- After detecting the malicious node, our work is to propose a way to block the node. We propose an algorithm by following the nature of the malicious BHPs.

1.6 Applications

Making a network less vulnerable and more secured, it is a challenging work. Researchers, security engineers and network engineers are trying hard to tackle

[2] `https://archive.ics.uci.edu/ml/datasets/Burst+Header+Packet+(BHP)+flooding+attack+on+Optical+Burst+Switching+(OBS)+Network`

every possible types of attack to secure the internet. Our system has a lot of applications. Some of them are listed below

- Burst Header Packet flooding attack is a big concern for Quality of Service(QoS) and maintainability. If the network is not secured but still the users have to face different attacks and there are chances of being hijacked, then the network is not suitable for the usage. But with the help of malicious node detection technique, such attacks can be solved in early stages and make the network less vulnerable.
- Malicious node detection can be used to network analysis whether any switch is misbehaving or not. If the switching is misbehaving, then it will be easier to make necessary changes.
- Network engineers can use the application to detect the nodes which leads/lead to the DoS attack and take necessary decision to make it secured.

1.7 Motivation

Optical burst switching network is one of three models that is used wavelength-division multiplexing technology to meet the requirements of today's world. To make the system less vulnerable, is our main goal. As OBS network is the future internet, so it is a big issue to make the network more user friendly. While using the OBS network if any problem arise, then it is no good to being advanced technology. Today's world is considered as global village, people are communicating with the world through a thin wire. If a network is affected by DoS attack, then the technology won't be used. It may create some unnecessary and unexpected harm to the users. Nowadays, people is using internet to do their works. Due to pandemic, every country is having a work from home. To make the OBS network open to everyone, it is really important to have it less vulnerable and more updated in its functionalities. In our system, malicious node detection is an automatic process where human administration is not required. For this reason, we are intended to work on this network to remove its vulnerability.

1.8 Contribution of The Thesis

Optical burst switching network[3] is the next generation of optical internet. To have a secure internet for everyone, it is important to be secured in every possible ways. The main aspects of our proposed system is listed below.

- To design an automated malicious node detection system for OBS network.
- To develop a blocking algorithm for detected malicious node,
- To evaluate the system accuracy by comparing with other related works.

1.9 Thesis Organization

This report is organized into five chapters. This chapter provides an introductory concept of the work done. In the second chapter, we give an overview of related work done in the field and also include their limitations. Chapter 3 describes elaborately the working procedure of our proposed system with appropriate figure and tables. We also explain malicious node detection mechanism and blocking mechanism0 with appropriate iteration and figure. At the end of, we have illustrated our implementation of the project and explain the implementation step by step. The graphical representation, abstract view of the system is explained here with necessary figures. In this chapter we also specify the system requirements of the proposed model. Chapter 5 focuses on the experimental result of the proposed system. In order to evaluate the system, we have used subjective as well as quantitative measures. In this chapter a shown effective performance analysis system of language processing. The thesis concludes with a summary of research contributions and future plan of our work in chapter 5.

[3] `https://en.wikipedia.org/wiki/Optical_burst_switching`

1.10 Conclusion

In this chapter, we have discussed about the introduction of our work. We also discussed about the motivation, contribution of the work along with the application of our work. At the end of the chapter, we include the organization of the thesis.

Chapter 2

Literature Review

2.1 Introduction

In this chapter, we present studies on the terminologies related to malicious node detection and blocking on optical burst switching network and later on we will also discuss on some related previous work in this field.

2.2 Optical Switching Network

Optical network is more convenient than any other way as it is supportive to provide services to run a wide range of wide range of new, high-bandwidth and bandwidth hungry applications. It is used to improve scalability, manageability, and efficiency.

Optical switching networks denotes all the major switching models. These models are developed for modern optical network systems, based on their operations, merits, demerits and implementation.

Optical switching can be classified into three categories[1]

- Optical Circuit Switching
- Optical Packet Switching
- Optical Burst Switching

2.2.1 Optical Circuit Switching(OCS)

In Optical Circuit Switching, the network is configured in form of circuit. It is done by adjusting the optical cross connect circuit so that the data signal can

[1] https://www.slideshare.net/NITHEESHKUMARCHITUMA/optical-switching-129355028

travel in an All-optical manner.[2]

When OCS is on light path, then it is known as Optical Wavelength Switching.

2.2.2 Optical Packet Switching(OPS)

It is more efficient than OCS if statistical multiplexing is considered.

In Optical Packet Switching(OPS), every optical packet consists of few things

- Header
- Payload
- Additional guard bands adding before and after payload.

2.2.3 Optical Burst Switching(OBS)

Optical Burst Switching is a combination of OCS and OPS. OBS is typically packet based so it uses bandwidth more efficiently than OCS.

In OBS network, larger data bursts(DB) assemble packet. For every burst, three components, a burst header packet(BHP), DB assembly, and generation of BHP are done in OBS edge nodes. Bursts are transmitted over a data channel, while BHP is sent to the same node over a dedicated control channel.

OBS network has become the promising switching technique for modern optical network. It is now considered as next generation internet infrastructure because of its efficiency on bandwidth usages. For burst traffic ,OBS is at its best with sufficient details than other switching techniques in terms of optical internet.

2.3 Machine Learning

Machine learning is a sub-branch of Artificial intelligence. Machine learning has been used widely for more than two decades. It has variety of fields and application. Industries are using machine learning for automating the tasks and many complex data analysis. With the help of machine learning computers can perform tasks without being programmed explicitly. Machine learning are being used for boundless cases, from agriculture to medical treatments, from detecting particles

[2] https://www.slideshare.net/NITHEESHKUMARCHITUMA/optical-switching-129355028

to self-driven cars.Machine learning's aim is to construct computer programs that learn and improve by gaining experience automatically. Machine learning enables computers to predict something for training from available data given in purpose to train. Based on the study of pattern and working different computational learning theory in artificial intelligence, machine learning can construct algorithms that can help the computer or device to learn and make predictions on unseen input data. By constructions algorithms from pattern and computational theory, help to overcome strictly program instructions. Rather computer learns by making predictions by through a machine learning model from training dataset and then compares with other machine learning models. Machine learning is closely connected to computational statistics. Besides, machine learning has strong relation with mathematical optimization. Different machine learning frameworks, libraries, for example- Seaborn, NumPy, Pandas, Sklearn, Matplotlib, are used different statistical approach to analyze the dataset to generate insights, the process is known as Exploratory Data Analysis. One of the types of machine learning is unsupervised learning where data are used to learn and establish relationship on the features. Kmeans [5] is an unsupervised techniques. Kmeans helps to find the outliers and meaningful anomalies. Because of the flexibility and capabilities, machine learning is used in expanding deep learning fields. In data analytics, machine learning is actively used where machine can behave autonomously. In predictive analytic, machine learning models are helping to predict different diseases for instance breast cancers. Not only that due to its versality,machine learning is being used in different commercial fields such as stock price predicting, crime rate predictions. These analytical models allows data scientists, data engineer, researchers to implement their thought with freedom of choice, without any constraints to solve any complex problems, untracked problem till now.

2.3.1 Machine Learning(ML) Techniques

Machine learning techniques are used for making generalizations and driving patterns. Machine learning is used for predicting labels or determining some values based on same data. Predicting labels is called classification and calculating values is known as regression.

2.3.1.1 Supervised Learning in Classifications Problems

Supervised learning is an machine learning algorithm that is used to maps an input to an output. It is totally based on sample input and output pairs. Supervised learning is a sub-categorical version of artificial intelligence and machine learning. From labeled training data, supervised machine learning implies a function. Supervised learning is very common in classification problems because the goal is often to get the machine to learn the method to deduce a label. Detection of a malicious node from OBS network is a classification problem. Classification learning is used for any problem when determining a classification is useful and easy to determine. Supervised learning is the most common method if classification is considered. Many machine learning models, for example, decision tree, support vector machine, KNN classifiers etc. are used for solving classification problems.

2.4 Different Methods of Classification

2.4.1 Decision Tree Classification

Decision tree is a supervised machine learning model where the data is split continuously on a set of certain parameters. Decision trees are a non-parametric supervised learning method. Decision trees are used for regression and classification. Decision tree classifications are used for solving categorical problem. The main target is to create a machine learning model which it is used to predict the value of a target variable by learning and building decision rules inferred from the features. A tree is built with a set of if-then-else decision rules. The complexity of decision rules increases by the depth of the tree. DecisionTreeClassifier[3] is a class which is used to perform multi-class classification.

[3] https://scikit-learn.org/stable/modules/tree.html

2.4.2 KNN Classification

K-nearest Neighbors(KNN) algorithm is a simple, supervised machine learning which can be used for regression and classification problems. KNN algorithm uses dataset and based on the different measure functions,for instance, Euclidean distance[4], the algorithm classifies new data point. Majority vote to the neighbors in the algorithm does classifications. To implement the classification in K-nearest neighbor algorithm, KNeighborsClassifier method is used.

2.5 Related Work

A significant number of works has been done to find the solution of high burst loss in OBS networks. Most of the them focus on using different machine learning models to detect the flood detection. We have tired to mention some of them below. Alshboul[6] proposed a rule based model for BHP Flood attacks using data mining . The model was generated on 21 features and over 1000 data instances , the model was run on NCTUns simulator[5]. The dataset that was used is collected from the University of California Irvine data repository[6]. For a probabilistic approach, Bayes Net, and Naïve Bayes algorithm were used and for induction ,decision tree is used. The model was trained on a flood attack dataset gathered by using NCTUns network simulator and consists of over twenty variables associated with network performance as well as the edge nodes. In the work, the accuracy of Repeated Incremental Pruning to Produce Error Reduction (RIPPER) rule induction algorithm, Bayes Net and Naïve Bayes were 98%, 85% and 69%respectively.

To order to detection of intrusion, different machine learning techniques and some deep learning techniques have been used to detect different kinds of attacks in several works[4, 7–9] . A set of related works focusing o detection of BHP flooding attacks have also been using different machine learning models such as decision tree(DT) in [10]. In the model, the accuracy is reported 93% in classifying binary

[4] `https://en.wikipedia.org/wiki/Euclidean_distance`

[5] `https://www.isi.edu/nsnam/ns/`

[6] `https://archive.ics.uci.edu/ml/datasets/Burst+Header+Packet+(BHP)+flooding+attack+on+Optical+Burst+Switching+(OBS)+Network`

classes and 87% in classifying multi classes.

Another machine learning approach is in [11] for detecting DDoS attack. In the work, a decision tree method with a grey relational analysis is used. For tracking the attacker's estimated location , pattern matching technique is also used. The authors in [12] applied data mining techniques for classifying BHP flooding attack. Correlation-based Feature Selection(CFS) is used for feature selection. Different machine learning models are used.Among them, J48 outperforms and achieves 100% accuracy both with feature selection and CFS selection. Due to small number of samples and without hyperparameter turning, at a moment, the model overfits, so that feature selection does not make any impact.
Md. Zahid Hasan et al.[13] proposed a Deep Convolution Neural Network(DCNN) model to automatically detect every node at early stages to prevent the attack. According to the authors, DCNN model works better than any other machine learning techniques, such as Naïve Bayes, KNN and Support vector machine(SVM). Though, due to smaller dataset and limited resource constraints of OBS switched network, such model can not be considered as an effective one to detect BHP flooding attacks and thus the model is not computationally efficient to run on these network.

2.6 Conclusion

In this chapter, a detailed literature review is discussed. For convenience, the discussion are divided on different types of attacks and machine learning techniques. We discussed different approaches along with feature selection and classifiers used by the researchers. The next chapter contains the detailed explanation of the proposed methodology of the detection and blocking.

Chapter 3

Methodology

3.1 Introduction

In this chapter, we will discuss about our proposed methodology and will try to explain each module of the system. We will also try to discuss our used algorithms. In the end of the chapter, we will discuss require implementation of malicious node detection and blocking system. After that we will review the final dataset with the input and output of our proposed system.

3.2 Proposed Framework for Malicious Node Detection

Development a framework for the problem is very important to solve the problem efficiently. It involves the development of a procedure that can detect a malicious node when the related data of a node is given as an input. In the system there are three parts. One part is for training the system and next part is to label the input and the last part is to take required step according to the label of the node. Our proposed system takes the input in .arff format. We will use the standardized data taken from NS2 Simulator [1] with nOBS extesnsion in fedora4 machine. The dataset is collected from UCI Machine Learning Repository[2]. In the training phase. we take the dataset, do preprocessing or normalizing the data and extract a set a features by applying different feature selection techniques like chi-square test [3] , SelectKBest method, random forest feature_importances_ instance for

[1] `https://www.isi.edu/nsnam/ns/`

[2] `https://archive.ics.uci.edu/ml/datasets/Burst+Header+Packet+%28BHP%29+flooding+attack+on+Optical+Burst+Switching+%28OBS%29+Network`

[3] `ttps://towardsdatascience.com/using-the-chi-squared-test-for-feature-selection-with-impl`

comparison, finally selects a subset of features. Using the subsets, system calculates each feature value and uses it for generating a machine learning model, calculate the ranking of the features and predicts the class using the trained model. We have explained the three phases of our system in upcoming sections. Here we have given an abstract framework for detecting malicious node in Fig. 3.1.

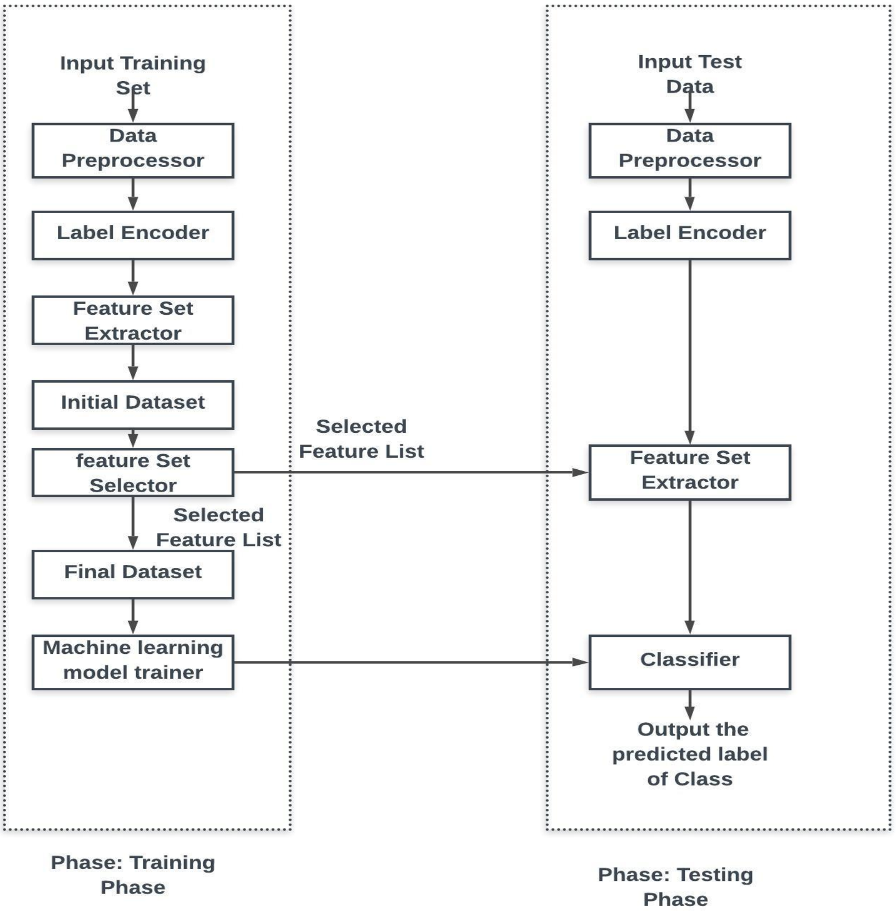


Figure 3.1: Abstract Framework for Malicious Node Detection

After detecting the status of node from machine learning classifiers, we'll go through the set of OBS node, and we will check whether the node is malicious and needed to block or not. Blocking malicious node is important otherwise it will become a cause for BHP flooding attack. The algorithm to block a node is depicted in the following flowchart shown in Fig. 3.2.

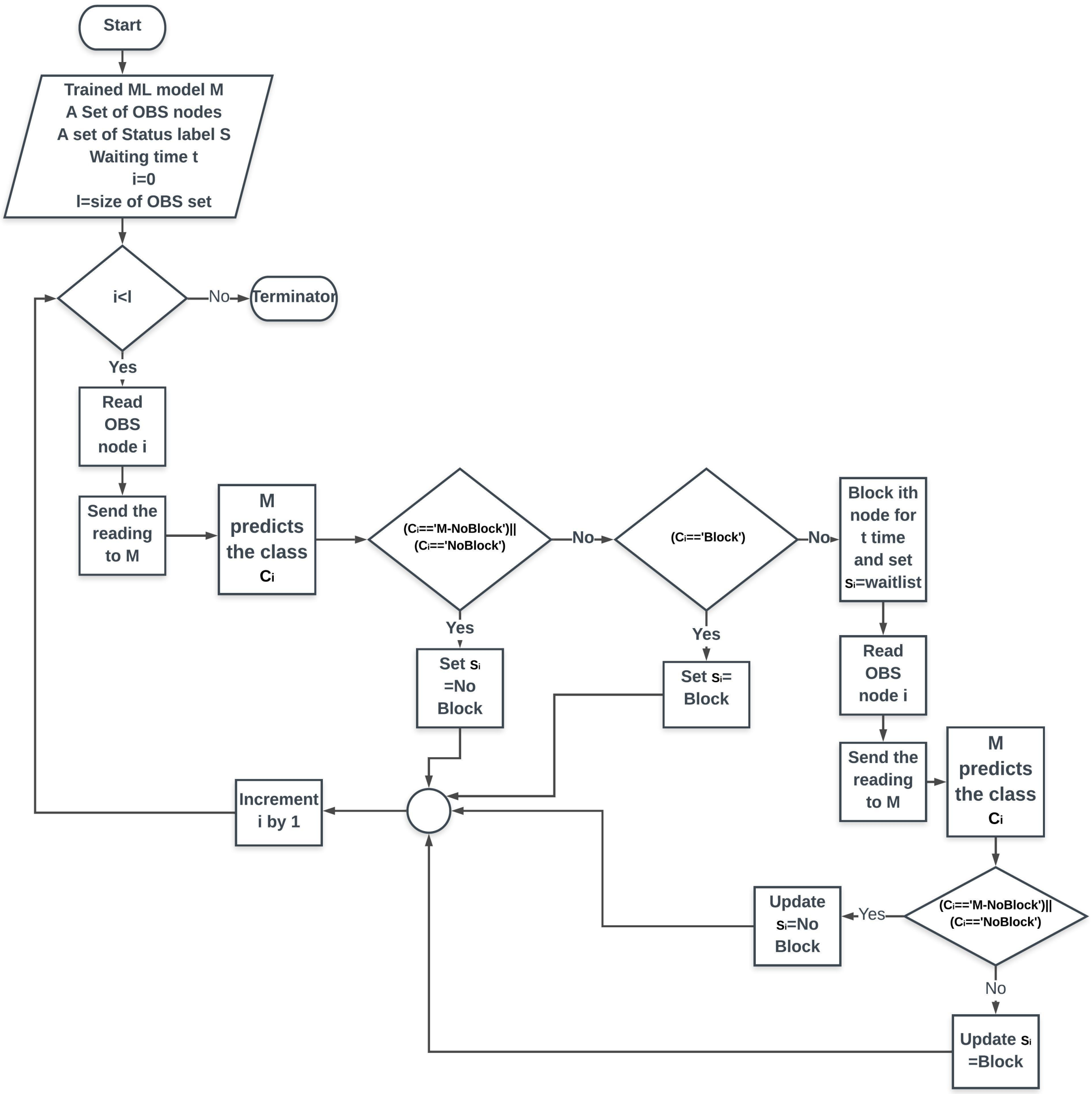


Figure 3.2: Flowchart for Blocking Malicious Node

3.3 Detailed Explanation

3.3.1 Training Phase

3.3.1.1 Data Preprossessing

Data preprocessing is an immediate step after accessing the data from a data source. It involves the initial preparation, aggregation and data cleaning. It has to be done before exploratory data analysis[4].

[4] https://towardsdatascience.com/using-the-chi-squared-test-for-feature-selection

- Step 1: The available file format is given in .arff format, we convert the file format into comma-separated values(csv) format. We shuffle the dataset to get variation in dataset row.
- Step 2: There is a column Packet_lost where some values are missing. So we fill the missing value with the median of the column.
- Step 3: We introduce a new feature by analyzing the importance for calculation
- We drop a column Packet Size_Byte as it contains a constant value
- We convert the value of Node Status and Class into numeric value by using labelencoder[5] to facilitate training the algorithms

3.3.1.2 Correlation Matrix Generation

Here it is a correlation matrix, where dependencies between two random variables of feature are drawn. In our case, the matrix denotes the strong statistical relationship between the feature variables whether there are positively correlated or negatively. The positively correlated relationship defines by 1 and negatively correlated relationship is denoted by -1. We have plotted the correlation matrix in heatmap format for better understanding and representation of correlation. Pearson correlation coefficient calculates the correlation matrix. Correlation matrix is shown in Fig 3.3

[5] `https://www.kite.com/python/docs/sklearn.preprocessing.LabelEncoder`

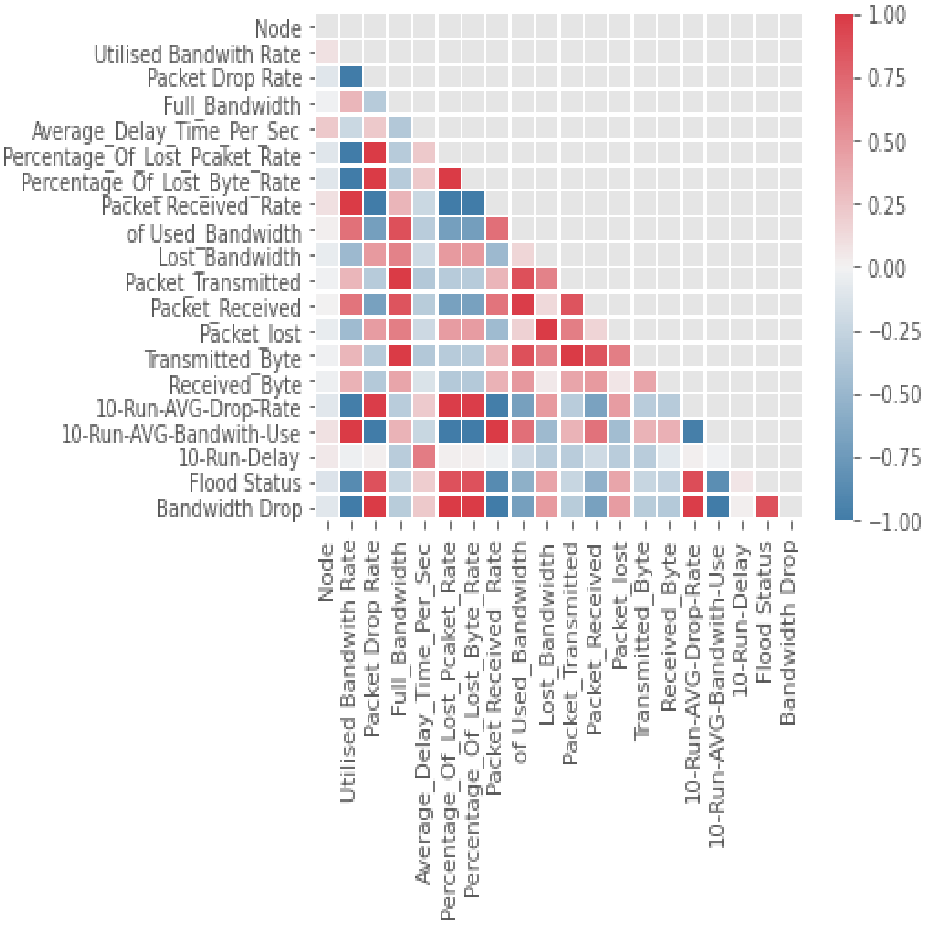


Figure 3.3: Correlation Matrix

The formula of correlation matrix to find the relationship between two features x and y is given by

$$corr(X,Y) = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2(y_i - \overline{y})^2}}$$

where $\overline{x}$ and $\overline{y}$ are denoted by the sample mean of X and Y accordingly. 3.3 shows the representation of correlation matrix in heat map. In this, darker color denotes strong relationship whereas the lighter color denotes weak relationship or correlation.

3.3.2 Building Predictive Models

3.3.2.1 Feature Selection

We used different type of feature selection technique to find the dependency between the feature value and target value 'Class'. At first, to calculate the relationship between every feature variable and target value, we use Pearson's chi-squared test[14]. A contingency table of two variables is calculated from chi-squared test. Chi-squared χ^2 is calculated

$$\chi^2 = \sum_{k=1}^{n} \frac{(O_k - E_k)^2}{E_k}$$

Where,
O_k= observed value
E_k= expected value
From the value of χ^2, we got that all variables are independent of one another, so it has a null hypothesis.
We take probability value=0.95 from then we calculate *alpha*=1-*probablity*. If $\chi^2 >$ critical χ^2 , we get that it reject the null hypothesis. From χ^2, we get the key feature variables.

After than we select the eight best features by using SelectKBest method[6]. We also use Random forest feature selection tools. After final analysis, we choose a set of 4 feature variables. After that we use the machine learning classifiers to train our models for multi-class classifications. For every classifiers, we'll use hyper-parameter tuning[7] to get the efficient model classifiers. After training the models with hyper-parameter, we'll use the classifiers to train the model.

3.3.3 Testing Phase

A sample input of a node is taken for testing the classifier. After following all the preprocessing step, we used trained model to test the test date to predict the probable label of class.

[6] https://www.datacamp.com/community/news/feature-selection-using-selectkbest-0dv0fo0qqe48

[7] https://en.wikipedia.org/wiki/Hyperparameter_optimization

3.3.4 Blocking Malicious Node

After being trained, best machine learning classifier will be used for checking the node label and update the label to be blocked or not. In Fig. 3.2, we choose the waiting time, t=5 sec. The waiting time, t will be used for testing $M - Wait$ nodes where these nodes are misbehaving. For a time t, we will block the node and after t time, we'll read the condition of the node, send the value to machine learning model M, to predict the labels, if the label is $M - NoBlock$ or $NoBlock$, we'll update the status as $NoBlock$, otherwise we will decide to block the node and iterate to the next OBS node, until we check all the nodes.

3.3.5 Implementation

In this chapter, we will go through system requirements, and details of the dataset. We'll also explain how the system processes the input at each step to produce the required output

3.3.5.1 System Requirements

The system requirements for the implementation is mentioned below:

- Hardware requirements
  - Personal computer
- System Configuration
  - Operating system: Linux
  - A 64-bit Intel core i3 processor or higher
  - 4GB RAM or higher
- Software requirements
  - Operating system: Linux
  - Anaconda 2019.03
  - Spyder 3.3.3
  - Jupyter Notebook 5.7.8

- Python 3.7
- numpy 1.16.2
- pandas 0.24.2
- scikit-learn 0.20.3
- matplotlib 3.0.3
- VS Code 1.35.1

All of the software tools are not compulsory to run the project. Some packages are required only for different steps of the project. For running the system, an IDE with some important packages is required.

3.3.5.2 Implementation Details

3.3.5.2.1 Dataset

Table 3.1 represents the features along with the description and the type of the feature.

3.3.5.2.2 Feature Selection Technique

After applying feature selection chi^2[8] test and selectKbest[9] method respectively we get two subsets of features. And we further use Random forest feature selection techniques and by analyzing further, we reduce to 4 feature variables. The result is shown in table 3.2.

[8] https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.chi2.html

[9] https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.SelectKBest.html

Feature No	Feature Name	Description	Type
1	Node	The number of node that sends the data	Numeric
2	Utilized Bandwidth Rate	Normalized value of used bandwidth	Numeric
3	Packet Drop Rate	Normalized value of dropped package rate	Numeric
4	Full__Bandwidth	Initial bandwidth(Reserved) assigned to each node	Numeric
5	Average__Delay__Time__Per__Sec	The average end to end delay time	Numeric
6	Percentage__Of__Lost__Pcaket__Rate	The percentile of lost packet of a node	Numeric
7	Percentage__Of__Lost__Byte__Rate	The percentile of lost packet of a node	Numeric
8	Packet Received Rate	The percentile of received package of a node	Numeric
9	of Used__Bandwidth	The bandwidth used or reserved for a node	Numeric
10	Lost__Bandwidth	The bandwidth lost by a node	Numeric
11	Packet__Transmitted	Total transmitted packet per second for a node	Numeric
12	Packet__Received	Total received packet per second for a node	Numeric
13	Packet__lost	Total lost packet per second for a node	Numeric
14	Transmitted__Byte	Total transmitted byte per second for a node	Numeric
15	Received__Byte	Total received byte per second for a node	Numeric
16	Packet Size__Byte	Total packet size given in byte explicitly allotted to transmit for a node. Here, total packet size= 1440bytes	Numeric
17	10-Run-AVG-Drop-Rate	For 10 iterations, the rate of average packet drop	Numeric
18	10-Run-AVG-Bandwith-Use	For 10 iterations, the rate of average packet drop	Numeric
19	10-Run-Delay	The rate of average delay for 10 iterations and runs	Numeric
20	Flood Status	The percentile flood by a node	Numeric
21	Bandwidth Drop	Resultant of division of Lost Bandwidth and Full Bandwidth	Numeric
22	Node Status	Initial classification of node;Behaving, Not Behaving,Potentially Not behaving	Categorical
23	Class	Final classification of node	Categorical

Table 3.1: The Description of Features with Type

	Feature Set	Target feature
Chi-squared test	Packet Drop Rate,Flood Status, 10-Run-AVG-Bandwith-Use, 10-Run-AVG-Drop-Rate,10-Run-Delay, Utilised Bandwith Rate, Packet Received Rate, Average_Delay_Time_Per_Sec,Bandwidth Drop	Class
SelectKbest	Percentage_Of_Lost_Byte_Rate, Percentage_Of_Lost_Pcaket_Rate, Packet Drop Rate,10-Run-AVG-Bandwith-Use, 10-Run-AVG-Drop-Rate, Utilised Bandwith Rate,Packet Received Rate, Average_Delay_Time_Per_Sec	Class
Random Forest Feature Selection	Received_Byte,Transmitted_Byte,Packet_Received, Packet_Transmitted, Packet_lost,of Used_Bandwidth,Full_Bandwidth, Lost_Bandwidth, Bandwidth Drop	Class
Feature reduction	Packet Drop Rate,Utilised Bandwidth Rate, Packet Received Rate,Bandwidth Drop	Class

Table 3.2: Feature Selection Technique

3.3.5.2.3 Final Dataset

First few rows of the dataset

	Packet Drop Rate	Utilised Bandwidth Rate	Packet Received Rate	Bandwidth Drop	Class
1	0.441645	0.658350	0.558355	34.16500	1
2	0.460800	0.547650	0.539200	45.23500	2
3	0.722378	0.281950	0.277622	71.80500	0
4	0.323749	0.686888	0.676251	31.31125	1
5	0.716558	0.287850	0.283442	71.21500	0

Table 3.3: Selected Features with Target Feature

Class label=0 denotes 'Block'

Class label=1 denotes 'M-NoBlock'

Class label=2 denotes 'M-Wait'

Class label=3 denotes ‘No Block’

3.4 Sample Input and Output

We try five machine learning classifiers, Decision Tree, Support vector machine, logistic regression, Naïve Bayes, KNN. Mainly we use decision tree classifier to make the prediction, and other four classifiers to compare the results.

Packet Drop Rate	Utilised Bandwidth Rate	Packet Received Rate	Bandwidth Drop	Predicted class	Actual Class
0.168401	0.844525	0.831599	15.5475	2	2

Table 3.4: Sample Input and Output

Here Actual class label=2 denotes ‘M-Wait’ whereas
Actual class label=0 denotes ‘Block’
Actual class label=1 denotes ‘M-NoBlock’
Actual class label=3 denotes ‘No Block’

3.5 Conclusion

In the chapter, we have discussed about the proposed system and the implementation details of the system. We explained the training stage, and showed a sample input output for a specific case where our system can detect and block the class.

Chapter 4

Results and Discussions

4.1 Introduction

The chapter contains the dataset description, impact analysis and evaluation of framework, some evaluation of performance that have been calculated during the experiment. The experimental setup takes a set of feature variables as input and predict the label of the node as an output. In the chapter, we will focus on the correctness of the system and evaluate it's accuracy. At the end of the chapter, we will discuss about the blocking technique.

4.2 OBS Network Configuration

Table 4.1 represents the configuration of OBS parameter in NCTUns simulator. To simulate OBS network for academic research purposes, NCTUns is developed.

Parameter	Value
Transport Layer Protocol	UDP
Wavelength Conversion	No
Maximum burst length	1500 bytes
Number of Control Packet Channels	1
Number of Data Packet Channels	2
Timeout to send burst	10 μs
Propagation Delay	1 μs
Bandwidth	1000 Mbps
Bit Error Rate	0.0

Table 4.1: OBS Network Configuration

4.3 Dataset Description

We have used a "Burst Header Packet (BHP) flooding attack on Optical Burst Switching (OBS) Network Data dataset" which is publicly available at UCI machine learning repository[1]. This dataset contains 22 attributes. There are two categorical fields, Node Status and Class. Node Status defines the initial status of a node, and class defines the final status of a node, described at table 3.1.
In the dataset, the number of instances is 1075. We have included one more attribute, Bandwidth Drop which is the result of division of Lost_Bandwidth and Full_Bandwidth.

$$\texttt{Bandwidth Drop} = \frac{Lost\_Bandwidth}{Full\_Bandwidth} \tag{4.1}$$

In the dataset, we have done some preprocessing steps, discussed in Section 3.3.1.1 of preparing for using to build the machine learning model and testing.

4.4 Impact Analysis

OBS network plays a great role to provide wide bandwidth traffic for web and bandwidth hungry applications where to run the application, high traffic of bandwidth is required to run smoothly. As it is prone to BHP flooding attack, which is denial of service attack, it is possible to create problems to the user-end.

4.4.1 Social and Environmental Impact

The privacy and data security of the end user is very important in today's world, where OBS network has the capability to provide faster internet for heavy usages. As more people are using optical fibre internet, and Bangladesh holds 21th position[2] for fixed-broadband subscriptions, the social impact is huge. If we can prevent BHP flood attacks, it will make the optical network much more secured.

[1] https://archive.ics.uci.edu/ml/datasets/Burst+Header+Packet+%28BHP%29+flooding+attack+on+Optical+Burst+Switching+%28OBS%29+Network

[2] https://en.wikipedia.org/wiki/List_of_countries_by_number_of_broadband_Internet_subscriptions

The impact of the system is foreseen as it is considered that OBS network is considered as the backbone infrastructure for next-generation internet[4].

4.4.2 Ethical Impact

It has an ethical impact as it is for securing the internet from some unwanted attack. Such attacks give the attackers flexibility to

- Compromise the network to hijack to false destination node
- Manipulate bursts size to increase reservation time
- Increase the bursts latency[1].

Our proposed system can detect the compromised node or malicious node and then block the node as a prevention for unwanted navigation.

4.5 Evaluation Methods

In our dataset, total number of Instances is 1075 where the number of initial attributes is 22 and final attributes is 23. In the dataset, there are two suitable categorical feature variables for prediction, Node Status and Class. As discussed in subsection 4.3 , we chose Class. Class denotes the final condition of a node.
At first, we split our dataset into two parts, training and testing data.

	No. of samples	Percentage
Training data	752	70%
Testing data	323	30%

Table 4.2: Size of the Training and Testing Dataset

The training set is divided into two parts training and validation set. We use K Fold cross validation strategy. Here k=5, that means 20% of the training set is validation set. Validation set is important to find the best models by evaluating the performance of various models using train set which are trained.
The training data is used for training the model. We use validation set to validate and evaluate the models. The testing dataset is to test and finally evaluate the private data. The accuracy of the system will depend on how many classes it

recognized correctly and how many classes it did not recognized correctly.

To find out the relationship of the each feature variables with the target feature, we use correlation matrix, discussed on subsection 4.1. Using different feature selection techniques for instance, chi-squared test, selectKbest, random-forest feature importance, as discussed on subsubsection 3.3.5.2.2, we select different set of feature variables. At the last step of training phase, we calculate cross validation score[3] to compare best models for training set. For each models, we calculate cross validation score mean, accuracy, generate classification report for each class.

4.6 Evaluation of Performance

There are different types of performance measurement technique to evaluate the performance of a model to measure the level of accuracy of the system. We consider five different measurement techniques

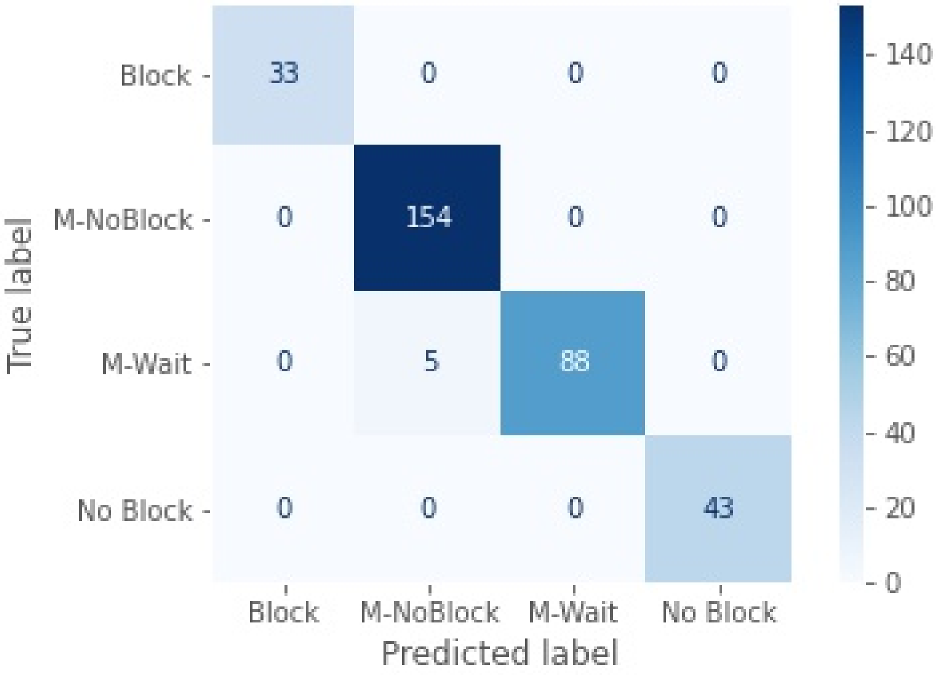
- Confusion Matrix
- Precision
- Recall
- F_1 score
- Accuracy

4.6.1 Confusion Matrix

A confusion matrix, also known as an error matrix, is a specific table form that enables visualization of the performance of an algorithm, usually a supervised learning one (unsupervised learning it is typically known a matching matrix) in the field of machine learning and explicitly the issue of statistical classification. In confusion matrix, each row indicates the predicated label of the class whereas, each column indicates the true label of the class.

[3] `https://en.wikipedia.org/wiki/Cross-validation_(statistics)`

Confusion matrix of decision tree classifier is shown in Fig 4.1.



True label \ Predicted label	Block	M-NoBlock	M-Wait	No Block
Block	33	0	0	0
M-NoBlock	0	154	0	0
M-Wait	0	5	88	0
No Block	0	0	0	43

Figure 4.1: Confusion Matrix of Decision Tree Classifier

4.6.1.1 Comparing with Other Classifiers

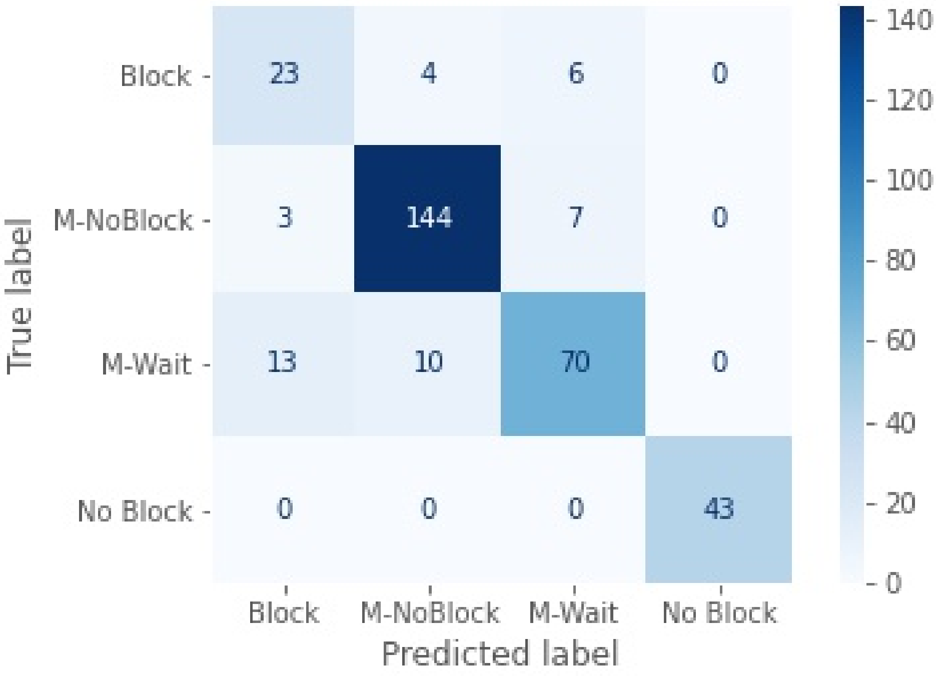


Figure 4.2: Confusion Matrix of KNN Classifier

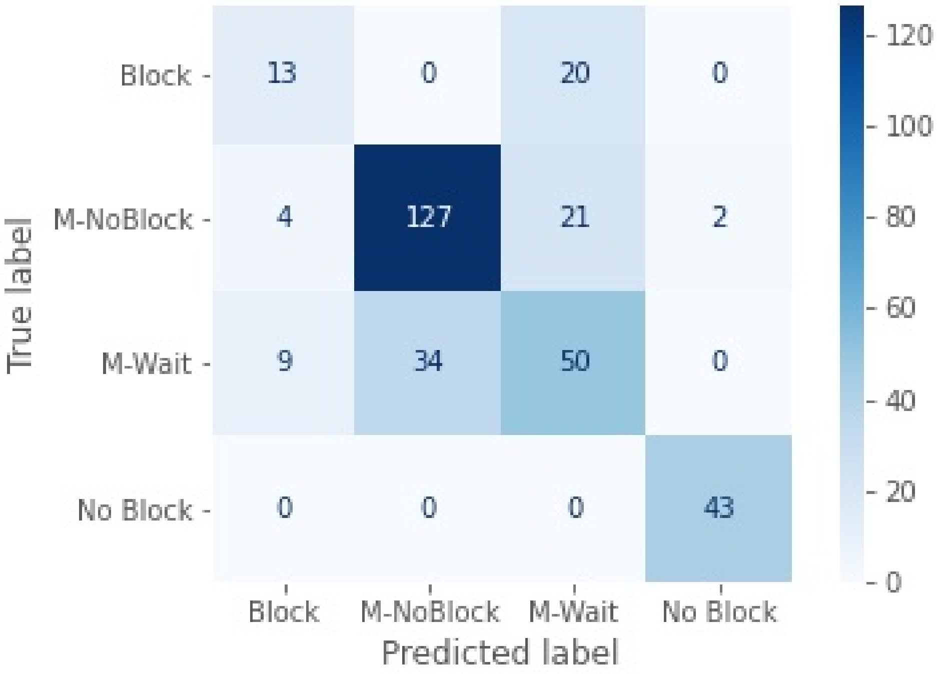


Figure 4.3: Confusion Matrix of SVM Classifier

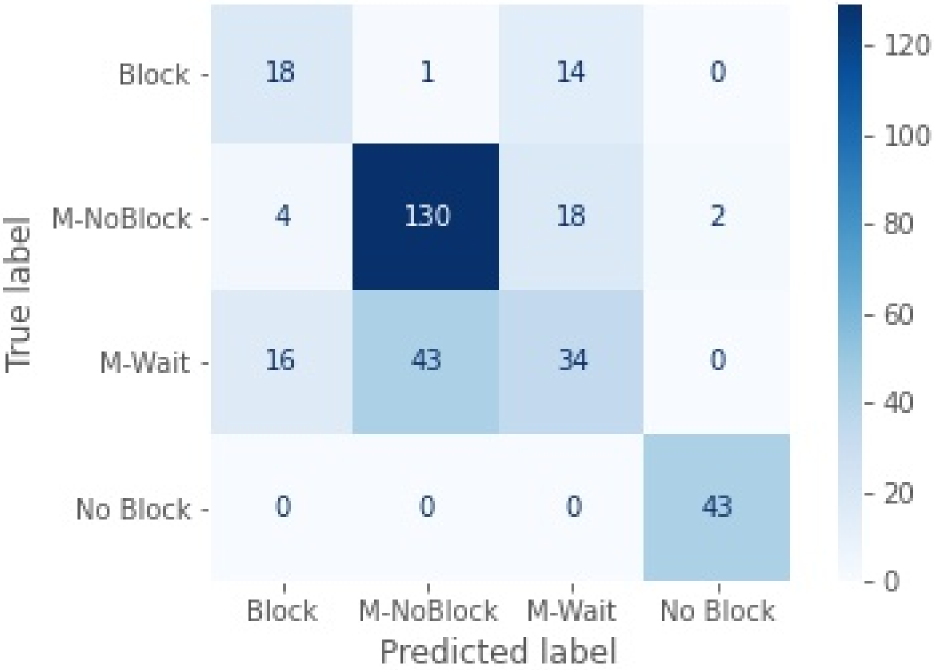


Figure 4.4: Confusion Matrix of Logistric Regression Classifier

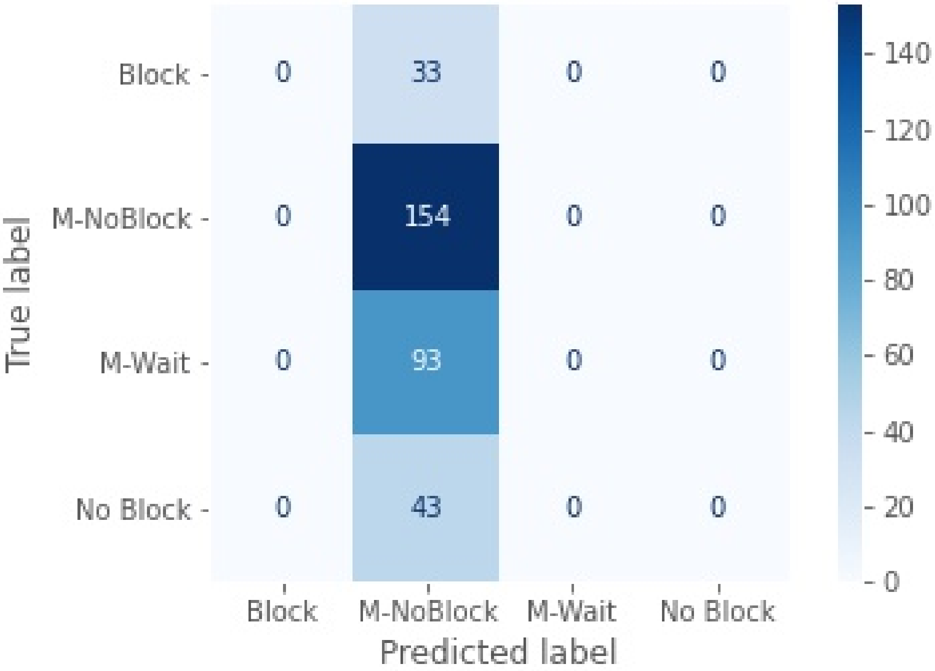


Figure 4.5: Confusion Matrix of Naïve Bayes Classifier

4.6.2 Precision

In a classification problem, the precision is very informative measurement scale to evaluate the performance of the system. Precision is also known as Positive predicted Value(PPV). The precision is calculated by the number of correctly labeled as positive class) divided by total number of observations labels as to the positive class(i.e. the sum of true positives and false positives). False positives denotes the number of incorrectly labeled class.

$$\texttt{Precision} \ = \frac{TP}{TP + FP} \tag{4.2}$$

A perfect precision score of 1.0 means each result retrieved was relevant by a test. In a classification prediction model, a perfect precision score of 1.0 for a class A represents each item labeled by the predicted system is correctly classified as class A.

4.6.3 Recall

In a classification problem, the recall is very informative measurement scale to evaluate the performance of the system. This is also known as True Positive Rate or Sensitivity. The recall is calculated by the number of correctly labeled as positive class) divided by total number of observations that actually belong to the positive class(i.e. the sum of true positives and false negative).

$$\texttt{Recall} = \frac{TP}{TP + FN} \tag{4.3}$$

Both precision and recall are important to understand and measure of relevance. A perfect recall score of 1.0 means each result retrieved was relevant by a search. In a classification prediction model , a perfect precision score of 1.0 for a class A represents each item labeled by the predicted system is classified as class A.

4.6.4 F_1 Score

F_1 score is used for measuring the accuracy of the test data. F_1 score also known as F-measure. The balance between the recall and the recall can be represented as F-measure. Precision and recall are used to compute F-measure. The maximum value of F-measure is 1 and the minimum value of F-measure is 0. F-measure is a harmonic mean of recall and precision.

$$\texttt{F-measure} = \frac{2 * Precision * Recall}{Precision + Recall} \tag{4.4}$$

To choose a learning algorithm from various kinds of algorithm, we have to look at the measured value of F-measure. The algorithm with highest F-measure value is chosen as our learning algorithm.

4.6.5 Accuracy

The most intuitive measurement for performance of a model can be measured by the accuracy. Accuracy is calculated by dividing total correct observation by total observation. For our system, accuracy is obtained by the following equation,

$$\texttt{Accuracy} \ = \frac{TP + TN}{TP + TN + FP + FN}$$

Iteration No.	Feature list	Model	Cross validation	Target	Accuracy
1	col1	Naïve Bayes Classifier	5	Class	0.61
		Decision Tree			0.97
		KNN			0.86
		Logistic Regression			0.70
		Support Vector Machine			0.73
2	col2	Naïve Bayes Classifier	5	Class	0.46
		Decision Tree			0.983
		KNN			0.89
		Logistic Regression			0.72
		Support Vector Machine			0.71
3	col3	Naïve Bayes Classifier	5	Class	0.46
		Decision Tree			0.96
		KNN			0.85
		Logistic Regression			0.70
		Support Vector Machine			0.98
4	col4	Naïve Bayes Classifier	5	Class	0.47
		Decision Tree			0.985
		KNN			0.87
		Logistic Regression			0.70
		Support Vector Machine			0.72

Table 4.3: Evaluation Summary

From the evaluation summary we can observe that in all cases, decision tree classifier perform more accurate than other models. The overall accuracy comparison for each models on col4 is shown in Fig 4.6.

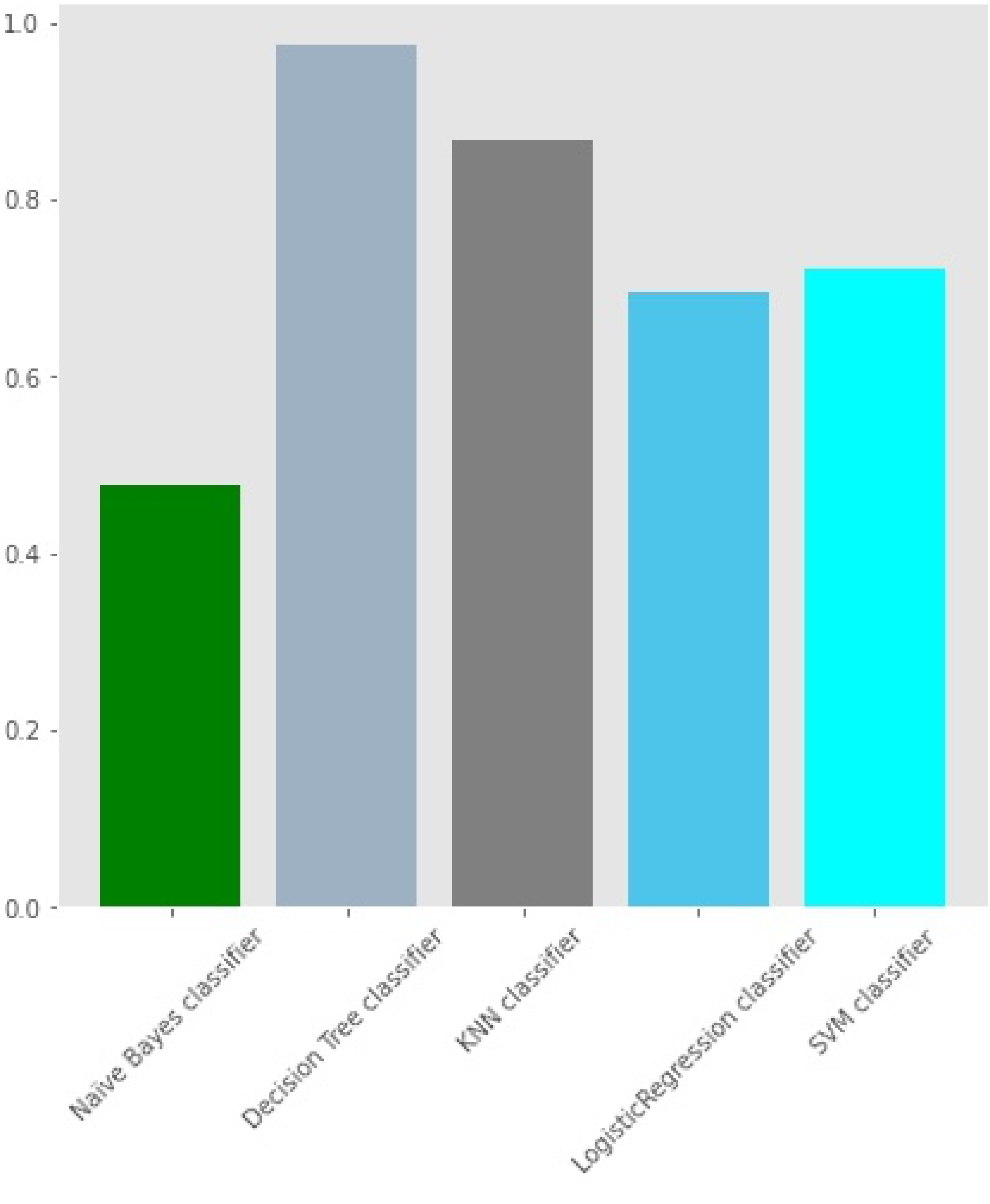


Figure 4.6: Overall Percentage Accuracy of Each Classifier

From the table 4.4 we can see that decision tree classifier performs better than any other classifiers.

	Precision	Recall	F_1
Decision Tree Classifier	0.985	0.985	0.985
Naïve Bayes Classifier	0.23	0.48	0.31
KNN Classifier	0.87	0.87	0.87
LogisticRegression Classifier	0.68	0.70	0.68
SVM Classifier	0.71	0.72	0.72

Table 4.4: Comparison of Results

4.7 Malicious Node Blocking

After building a predictive models by different machine learning models, we will use the model to block the node. We have explained an algorithm in section 3.2. In the algorithm we have set the waiting time, t=5sec. We have seen, the algorithm works for almost all of the cases.

4.8 Comparison with Related Works

A comparison of proposed work with other other similar works is represented in table 4.5. In first column, reference of the work is mentioned, second column is represented for the type of work. Third column is for the indication of the algorithm used for. And the last column of the table contains the accuracy of the model with number of label instances. From the table, we can perform very well compared to other similar works.

Works	Types of work	Classification Method	No of Features	Accuracy
Rajab et al.[10]	Supervised Learning	Decision Tree	7	87%
Hasan et al.[13]	Supervised Learning	Deep convolutional neural networks	21	99%
Patwary rt al.[15]	Semi-supervised learning	K-means	8	95.6%
Alshboul[6]	Supervised learning	RIPPER rule induction algorithm	21	98%
Proposed work	Supervised learning	Decision tree with feature selection	4	98.5%

Table 4.5: Comparison of the Proposed Work with Related Works

4.9 Conclusion

In this chapter, we discuss about the description of the dataset, and the social, environmental and ethical impact of our work. We talk about different evaluation methods of our system and analysis of our system with performance measure with different machine learning models and parameter to choose the best accurate model for blocking of misbehaving nodes. At the end of the chapter, we compare our work with related works. The overall accuracy of the proposed system can be increased by a larger dataset.

Chapter 5

Conclusion

5.1 Conclusion

In the project, our task was to develop an automated system that can recognize a node behavior and decide to step further steps through training and testing with various feature variables. Finding a good dataset is a challenging task. With exploratory data analysis, we added one more feature variables. The dataset found from different feature selection techniques, is used for training the model and testing on private data. We implemented the system using python and manipulate the dataset by following different techniques for preparing the dataset with the help of different packages and libraries. Some of the useful libraries are matplotlib, pandas, numpy, seaborn, cross validation score. We trained the system with different feature sets and tested our system with different classifiers and further we analyzed the performance with confusion matrix, accuracy, precision, recall etc. The experiment result yielded 98.5% accuracy with 1.5% label error rate. We used the best trained model decision tree classifier for blocking algorithm.

5.2 Future Work

Detection of a misbehaving node in OBS network, is a challenging and difficult task. We tried to achieve the best possible result, but there are still possible rooms for improvements. The following steps may be taken to make the project more reliable and more accurate in the future

- Further investigation on proposed method
- Increase the accuracy by tuning the model classifiers.

- This work can be extended to add more data by simulating the network so that the model does not overfit.

- The accuracy of the project can be improved through more exploratory data analysis.

- The work can be expanded by implementing other machine learning models to compare the performance and accuracy with our system.

References

[1] Y. Coulibaly, A. A. I. Al-Kilany, M. S. Abd Latiff, G. Rouskas, S. Mandala and M. A. Razzaque, 'Secure burst control packet scheme for optical burst switching networks,' in *2015 IEEE International Broadband and Photonics Conference (IBP)*, IEEE, 2015, pp. 86–91 (cit. on pp. 1, 31).

[2] Y. Chen, C. Qiao and X. Yu, 'Optical burst switching: A new area in optical networking research,' *IEEE network*, vol. 18, no. 3, pp. 16–23, 2004 (cit. on p. 1).

[3] T. Battestilli and H. Perros, 'An introduction to optical burst switching,' *IEEE Communications Magazine*, vol. 41, no. 8, S10–S15, 2003. DOI: `10.1109/MCOM.2003.1222715` (cit. on p. 2).

[4] A. Rajab, C.-T. Huang, M. Al-Shargabi and J. Cobb, 'Countering burst header packet flooding attack in optical burst switching network,' in *International Conference on Information Security Practice and Experience*, Springer, 2016, pp. 315–329 (cit. on pp. 2, 16, 31).

[5] M. Zubair, M. Iqbal, A. Shil, E. Haque, M. M. Hoque and I. H. Sarker, 'An efficient k-means clustering algorithm for analysing covid-19,' *arXiv preprint arXiv:2101.03140*, 2020 (cit. on p. 14).

[6] R. Alshboul, 'Flood attacks control in optical burst networks by inducing rules using data mining,' *IJCSNS International Journal of Computer Science and Network Security*, vol. 18, no. 2, pp. 160–167, 2018 (cit. on pp. 16, 40).

[7] I. N. Rizkiana, A. Rahmatulloh and R. Gunawan, 'Penerapan metode clustering k-means untuk menentukan nilai burst header packet flooding attack pada optical burst switching,' *Indonesian Journal of Applied Informatics*, vol. 4, no. 2, pp. 107–114, (cit. on p. 16).

[8] F. A. Khan and A. Gumaei, 'A comparative study of machine learning classifiers for network intrusion detection,' in *International Conference on Artificial Intelligence and Security*, Springer, 2019, pp. 75–86 (cit. on p. 16).

[9] S. S. Chawathe, 'Analysis of burst header packets in optical burst switching networks,' *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pp. 1–5, 2018 (cit. on p. 16).

[10] A. Rajab, C.-T. Huang and M. Al-Shargabi, 'Decision tree rule learning approach to counter burst header packet flooding attack in optical

burst switching network,' *Optical Switching and Networking*, vol. 29, pp. 15–26, 2018 (cit. on pp. 16, 40).

[11] Y.-C. Wu, H.-R. Tseng, W. Yang and R.-H. Jan, 'Ddos detection and traceback with decision tree and grey relational analysis,' *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 7, no. 2, pp. 121–136, 2011 (cit. on p. 17).

[12] V. Uzel and E. S. EŞSİZ, 'Classification bhp flooding attack in obs network with data mining techniques,' in *International Conference on Cyber Security and Computer Science (ICONCS 2018), Safranbolu, Turkey*, 2018, pp. 18–20 (cit. on p. 17).

[13] M. Z. Hasan, K. Z. Hasan and A. Sattar, 'Burst header packet flood detection in optical burst switching network using deep learning model,' *Procedia Computer Science*, vol. 143, pp. 970–977, 2018, 8th International Conference on Advances in Computing Communications (ICACC-2018), ISSN: 1877-0509. DOI: `https://doi.org/10.1016/j.procs.2018.10.337`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S1877050918320325` (cit. on pp. 17, 40).

[14] M. L. McHugh, 'The chi-square test of independence,' *Biochemia medica*, vol. 23, no. 2, pp. 143–149, 2013 (cit. on p. 23).

[15] Patwary, 'A semi-supervised machine learning approach using k-means algorithm to prevent burst header packet flooding attack in optical burst switching network,' *Baghdad Science Journal*, vol. 16, pp. 0804–0804, 2019 (cit. on p. 40).