# Machine Learning Classifiers for Network Intrusion Detection

Samilat Kaiser and Ken Ferens

Department of Electrical and Computer Engineering, University of Manitoba, Canada.

{kaisers3@myumanitoba.ca, Ken.Ferens@umanitoba.ca}

***Abstract*— Network intrusion detection (IDS) is an important research area in the dynamic field of network security. Intrusion Detection System (IDS) is popular defense mechanism that often uses machine-learning algorithms to detect known and unknown attacks. In this study the ever-persistent network threats in the UNSW dataset were tested with artificial intelligence intrusion detection systems implementing different popular machine learning classifiers for classifying network datasets. After processing the raw data and fine-tuning through normalization, the post-processed data is analyzed and discussed upon. The data is then fed into different classifier models. The performance accuracy of the models were compared to select best suited classifier for a network data. This study is groundwork research for classifier model selection for network data that can be used as reference to future research work in this arena.**

## I. INTRODUCTION

As we are getting more and more connected by technology, the internet is getting more and more complex. We share numerous things every instance, some of them are more valuable than others. Hackers are always there trying to steal our data, personal information and industrial secrets for illegal financial gain.

Now that we are in an era where machines are used in every aspect of livelihood, the demand for machines that learn on themselves is at its peak. Application of machine learning is utilized to solve problems that were unimaginably complex until now. Intrusion detected and anomaly detection is a new field of data protection that no longer relies on rule based resolution to protect against network intrusion systems. Despite efforts made to secure critical assets, the infrastructure to be secured is becoming increasingly complicated, and the attack techniques for penetrating the system are ever evolving, which increases the challenges faced by the cyber security professionals. This is where an intrusion detection system (IDS) plays a vital role for monitoring malicious activity in a network system [1]. IDS works as a defense mechanism which can detect malicious activities or threats in a network environment.

An intrusion detection system work in such a way that any detected suspicious activity gets reported. This usually get reported to a system administrator or is collected and sent out to a centrally located or managed system which is called security information and event management (SIEM) system.

IDS can be generally divide into two types Network-based IDS (NIDS) and Host-based IDS (HIDS). In a network based IDS, data packets are collected from network traffic and later used to analyze the information to find suspicious or malicious traffic. So in a whole the role of a network IDS is to gather, identify, log and later alert about the captured malicious traffic. A host-based IDS identifies intrusions and malicious behavior of a specific device. It tracks, monitors and analyzes the change in important files and directories by checking application logs, modification in file system and other host activities.

IDS can also be classified according to the detection approach. These are: Misuse and Anomaly detection. In a Misuse detection also known as signature-based detection, the behavior or pattern is matched with known vulnerabilities. In other words the system seeks a known pattern or a signature match. This makes this a strong detection method with comparatively lower false positive alarms. The advantage of this misuse method is the ability to identify known attacks and relatively low false alarm rate provided the rules given are correctly defined. The disadvantage of misuse attack is, it could be helpless to unknown attacks since it depends on when the database of known enlisted attacks.

In an anomaly detection system, the system is designed to detect any deviation from normal activity. This requires making the system trained about the normal activity first. The powerful advantage of this system remains detecting novel attacks and attacks that are not known previously. However, lack of precision and accuracy to identify attack leads toward high rate of false positive alarm in anomaly based detection system. [2] [3]

With the challenge in hand, attack detection techniques need to cope with the advanced intrusion techniques, which are also persistently evolving. The existing systems for detecting anomalies analyses events case

ISBN: 1-60132-470-7, CSREA Press ©

by case and act based on preset logic. However, they are prone to limitations since there is a scarcity of information of actual attacks to learn from and false detection usually causes serious problems for usual traffic, leading to business impacting implications. In the future, however, what we need is autonomous anomaly detection systems equipped with high computation powers and cloud infrastructure, which can learn how the attacks are engaged in order to adaptively respond to advanced persistent threats (APTs). This paper presents a study of various AI-based abnormality detection systems using popular machine learning classification techniques.

## II. Literature Review

Much research have been done in the area of intrusion detection. In [4] array Support Vector Machine (SVM) was used for attack detection and later the authors tried to compare their results with other SVM methods in terms of training time and accuracy. In [5] authors have used both SVM and Random forest (RF) method for detection and showed RF method is more effective in terms of time. The authors in [6] showed a different approach one-class SVM for anomaly detection. Both misuse and anomaly-based detection model used in [7] which the authors are calling a hybrid model where they used Binary Tree as a classifier for misuse detection and SVM classifier for anomaly detection. Then there are some other approaches attempted by many researchers. Fuzzy rule-based model is used in [8] and has been compared with the traditional threshold-based model. Again [9] have also used default fuzzy logic for better sensitivity and speed in IDS. [10, 11, 12, 13] have used Artificial Neural Network (ANN) based models for IDS. [14, 15, 16] have used Genetic Algorithms for intrusion detection.

Several researchers have shown study on feature reduction methods many of which show different approaches. In [17] experimented with both SVM and ANNs, they have categorized and later have identified features. This was done considering some sort of criteria and by ranking which feature is important for each kind of attack. If we consider a large number of feature this method may not be practically feasible since it evaluates each feature separately. Based on the Markov blanket of the target variable, data is classified and features can be selected using Bayesian network [18]. The authors have proposed CART algorithm to classify data. A decision tree is prepared to identify the significant features with predictor ranking.

On the UNSW-NB15 dataset [19, 20] applied ARM algorithm for feature engineering in the dataset. An anomaly-based IDS is proposed in [21] using GA and SVM with a new feature selection method. Different machine learning feature reduction techniques were applied by Thanthrige [22] to evaluate dataset performance. Use of other methods like Information Gain, Chi-Squared statistics can be observed in this research. In 2015, Wang [23] has shown that how features can be found in the raw network flow data by using neural networks particularly the deep neural networks. Usha and Kavitha proposed a normalized gain based IDS for MAC Intrusions (NMI) to improve the performance of IDS significantly [24]. Some researchers have used clustering-based framework for intrusion detection in wireless computer networks [25]

## III. Dataset

In our research we have used the UNSW-NB 15 data set [20]. The data was created with the help of IXIA PerfectStorm tool in the Cyber Range Lab by the researchers at the Australian Centre for Cyber Security (ACCS). This data is said to be a hybrid which contains both real modern normal activities and attack which is with synthetic contemporary in nature.

The researchers have used the tcpdump tool which captured 100 GB of the raw traffic. The data set contains nine different types of attacks; namely, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms. Total 49 features were generated using the Argus, Bro-IDS tools and 12 algorithms. The data are class labeled. The totals of 2,540,044 data were available in the four CSV files [19], [26].

Our initial focus was to test the algorithm with the UNSW-NB15 dataset. UNSW-NB15 dataset has four files of the UNSW-NB15 dataset, which has 3.2M rows containing 85:14 attack-normal rows ratio. Each individual event, i.e. row, in the UNSW contains 49 columns. Like any other datasets, UNSW also has missing data which needs to be taken care of before any models can be applied. As part of our data pre-processing measures, we impute the missing values and change the categorical data into numeric representations for the several columns. Such approaches are conventional measures to make the data more interpretable to the machine learning model. Our belief is that such feature engineering will enhance meaningful representation of the events and hence will provide better results.

## IV. Methodology

For evaluating the popular machine learning classifiers, we are using a standard scikit library that has stood the test of time and has been fine-tuned over the time. The UNSW dataset is divided into 4 files, and we have used two of the files to create our own dataset for the purpose. This new dataset is now divided into three equal sections, two of the portions are used to create a train dataset and one portion is used as a test dataset. Since we intend to be consistent on the

approach for each classifier, we have used the same data for training and testing for all of them. Each classifier is built into a model and trained over the dataset, and are trained the same number of epochs. After the model is learned and fitted against each data row in the set, and has learned the representation of normal and attack events, we then test the model on the test dataset. Once the model is exposed to the test dataset, it predicts from the never-seen-before data and classifies them to be normal or attack. These predictions are stored into an array and matched with the actual output. The comparison between the prediction and actual output is used as a performance metric for the classifier. A perfectly learned classifier will be able to classify the test events with best accuracy. Then these performance metrics are captured and compared against each other. They are hence giving a projection as to which classifier is best for the security data. It is noteworthy here, that the nature of the network traffic data depends upon what is being communicated, and hence there are no one classifier that fits all. The nature of the traffic is heavily dependent upon the OSI layer of the data communication. UNSW is OSI packet transfer data and it is intended for layer 3 and higher communication.

*a. Techniques*

The classification techniques chosen for this study are as follows:

Random Forest algorithm is a supervised classification algorithm that creates multiple decision trees and merges them together to get better accuracy and prediction.

Ridge Regression, which is occasionally used in network intrusion detection, is a technique of analyzing multi-colinearity in multiple regression data.

Decision Tree Classifier, repetitively divides the working area (plot) into sub part by identifying lines.

Linear discriminant Analysis (LDA) is a method used in statistics, pattern recognition and machine learning to find a linear combination of features that characterizes or separates two or more classes.

K-Nearest Neighbors algorithm (k-NN) is a non-parametric method used for classification and regression focusing on neighbor contribution, so that the nearer neighbors contribute more to the average than the more distant ones.

Naive Bayes classifiers are a family of simple "probabilistic classifiers" based on applying Bayes' theorem with strong (naive) independence assumptions between the features.

*b. Physical Setup*

A four core Intel i5 equipped machine with 8GB memory with a 64-bit OS is used as the host for running this experiment. Various popular python libraries like pandas, scikit-learn, scipy, numpy, pickles etc. are used in the code for the project.

## V. RESULTS

Table I shows the comparison for the various classifiers. Most of the classifiers are performing high as the machine learning model is for supervised machine learning. As we can see the Random Forest classifier shows the best performance. Ridge regressor performs the lowest. Linear Discriminant Analysis, Decision Tree Classifier and K-Neighbors Classifier all perform with comparable accuracy. Also provided in fig. 2 is the ROC curve (receiver operating characteristic curve) which is a popular tool for model performance. The curve is created by plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings. True positive and true negative are cases where the attack and normal are accurately classified. False positive is when normal is detected as attack and false negative is when an attack is detected as normal. Higher false positives and higher false negatives both means misidentifications, it is arguable that which of these are more dangerous for the application. It depends on the application. For example, for spam detection cases, false positives are more damaging as a spam email ending up in the inbox is perhaps less damaging than an important email getting restricted as spam. On the contrary if the focus is to restrict network penetration, identifying and blocking each attempt is important, even if it generates some false alarms marking low threat events for immediate response. Nowadays, MSSPs (Managed Security Service Provider) are doing a better job in identifying repetitive alarms and filtering actual treats either manually or by other means.

We find out the accuracy which is the ratio of positive and negative cases correctly identified.
Accuracy= (TP + TN) / (TP + TN + FP + FN)

TABLE I: ACCURACY FOR DIFFERENT CLASSIFIER MODEL

| Classifier | Accuracy |
|---|---|
| Random Forest | 0.9871 |
| Ridge Regressor | 0.7809 |
| Decision Tree Classifier | 0.9823 |
| Linear Discriminant Analysis | 0.9856 |
| K-Neighbors Classifier | 0.9864 |
| Naïve Bayes Classifier | 0.9675 |

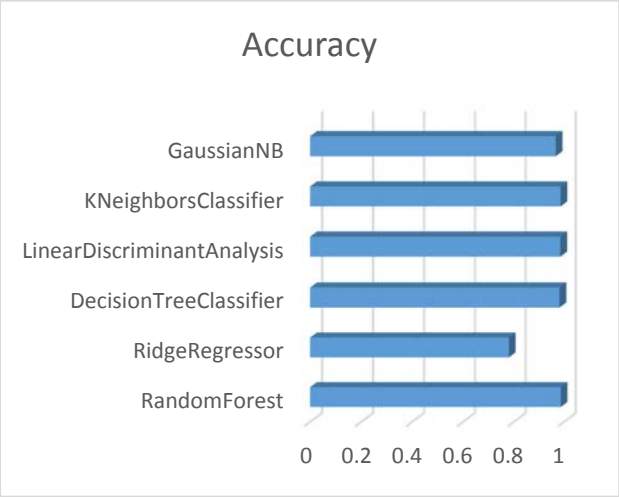


**Fig. 1: Accuracy of the ML Techniques**

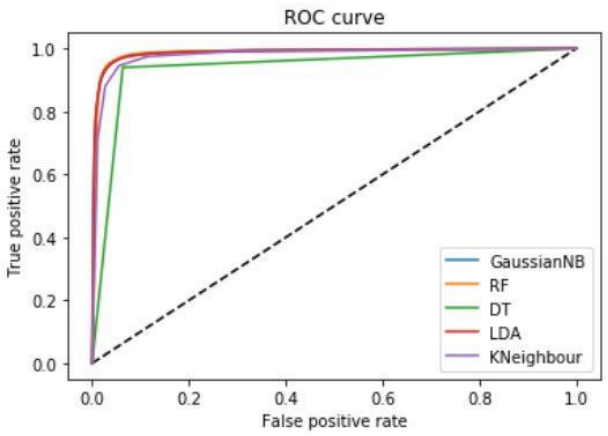


**Fig. 2: ROC Curve**

## VI. CONCLUSIONS

This study focuses on various machine learning tools that are foundational for exploring machine learning in general. It also discusses on various aspects of intrusion detection and network traffic data that is of vital importance for the model selection. It presents a baseline reference for comparison for other researches in this field. The provided accuracy and other metric comparisons depict which model is best suited for intrusion detection datasets. In future this work can be extended to design an algorithm that automatically selects which model to use based on simple intelligence collected from data. This way high computational expense from trial and error can be avoided.

## REFERENCES

[1] Michael E. Whitman; Herbert J. Mattord (2009). Principles of Information Security.

[2] Devikrishna K S, Ramakrishna B B. "An Artificial Neural Network based Intrusion Detection System and Classification of Attacks"; International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, pp. 1959-1964, Jul-Aug 2013.

[3] I. Guyon, S. Gunn, M. Nikravesh, and L. A. Zadeh, *Feature extraction: foundations and applications*. Springer, 2008, vol. 207.

[4] J. Mill and A. Tnoue. "Support Vector Classifiers and Network Intrusion Detection"; *IEEE International Conference on Fuzzy Systems*, Page(s): 407- 410, 25-29 July 2004.

[5] Md. Al Mehedi Hasan, Mohammed Nasser, Biprodip Pal, Shamim Ahmad, "Support Vector Machine and Random Forest Modeling for Intrusion Detection System (IDS)"; *Journal of Intelligent Learning Systems and Applications*, 2014-02-01, 6卷1期 (Vol.6, Issue 1), pp.45-52

[6] K. Li, H. Huang, Sh. Tian I , and W. Xu. "Improving One-Class Svm For Anomaly Detection." *The Second International Conference on Machine Learning and Cybernetics*, Page(s): 3077- 3081, 2-5 Nov. 2003.

[7] Amar Agarwal, Saba Mohammed, Jinan Fiaidhi. "Developing Data Mining Techniques for Intruder detection in Network Traffic"; International Journal of Security and Its Applications, Vol. 10, No. 8, pp. 335-342, 2016.

[8] P. Tillapart, Th. Thumthawatworn and P. Santiprabhob. "Fuzzy Intrusion Detection System"; AU J.T. 6(2): 109-114, Oct. 2002.

[9] Z. Jian, D. Yong, and G. Jian. "Intrusion Detection System based on Fuzzy Default Logic"; The 12th IEEE International Conference on Fuzzy Systems, Page(s): 1350- 1356 Vol.2, May 2003.

[10] J. Li, G. Zhang, and G. Gu. "The Research and Implementation of Intelligent Intrusion Detection System Based on Artificial Neural Network"; IEEE Proceedings of the Third International Conference on Machine Laming and Cybernetics, Shanghai, Page(s):3178 - 3182 Vol.5, Aug. 2004.

[11] C. Zhang, J. Jiang, and M. Kamel. "Intrusion detection using hierarchical neural networks"; Pattern Recognition Letters 26, Page(s): 779–791, Feb 2004.

[12] L. Silva, A. Santos, J. Silva, and A. Montes. "A Neural Network Application for Attack Detection in Computer Networks"; IEEE International Joint Conference on Neural Network, 25-29, Page(s):1569 -1574 Vol.2, July 2004.

[13] Devikrishna K S, Ramakrishna B B," An Artificial Neural Network based Intrusion Detection System and Classification of Attacks"; International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 4, pp. 1959-1964, Jul-Aug 2013.

[14] W. Li. "Using Genetic Algorithm for Network Intrusion Detection"; unpublished technical report. Department of Computer Science and Engineering, Mississippi State University. http://www.security.cse.msstate.edu/docs/Publications/wli/DOECSG2004.pdf.

[15] Mostaque Md. Morshedur Hassan, "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic"; International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 7, September 2013.

[16] Vivek K. Kshirsagar, Sonali M. Tidke & Swati Vishnu, "Intrusion Detection System using Genetic Algorithm and Data Mining: An Overview"; International Journal of Computer Science and Informatics, Vol-1, Issue-4, 2012.

[17] Andrew H. Sung, Srinivas Mukkamala. "Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks"; *Symposium on Application and Internet (SAINT'03)*, Page(s): 209- 216, 27-31 Jan. 2003.

[18] Chebrolu, S., A. Abraham and J.P. Thomas. "Feature deduction and ensemble design of intrusion detection system"; Computers & Security. Vol.24, No.4: pp.295-307, 2005

[19] N. Moustafa and J. Slay, ""UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)"," in 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, 2015.

[20] N. Moustafa and J. Slay, "The Significant Features of the UNSW-NB15 and the KDD99 Data Sets for Network Intrusion Detection Systems"," in 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), Kyoto, 2015.

[21] H. Gharaee and H. Hosseinvand, ""A new feature selection IDS based on genetic algorithm and SVM"," in 8th International Symposium on Telecommunications (IST), Tehran, 2016.

[22] J. S. a. X. W. U. S. K. P. M. Thanthrige, ""Machine learning techniques for intrusion detection on public dataset"," in IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Vancouver, 2016.

[23] Wang, Z.: The application of deep learning on traffic identification. BlackHat USA (2015).

[24] Usha, M., Kavitha, P.: Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier.

[25] Khoshgoftaar, T. M., Nath, S. V., Zhong, S., & Seliya, N. (2005). Intrusion detection in wireless networks using clustering techniques with expert analysis. In Process fourth international conference machine learning and applications. doi: 10.1109/ICMLA.2005.43

[26] Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set." Information Security Journal: A Global Perspective (2016): 1-14.