DOI: http://dx.doi.org/10.26483/ijarcs.v11i6.6678

Volume 11, No. 6, November-December 2020

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A HYBRID APPROACH FOR INTRUSION DETECTION USING K-NEAREST NEIGHBOR AND ARTIFICIAL NEURAL NETWORK

Dissanayake D M C
Department of Computing and Information Systems
Sabaragamuwa University of Sri Lanka
Belihuloya, Sri Lanka

Anuradha U A D N
Department of Electronics
Wayamba University of Sri Lanka
Kuliyapitiya, Sri Lanka

Abstract: Network intrusion detection is an important process in this era due to the increase of cyber violations. In this article, a hybrid approach which utilizes K-Nearest Neighbor algorithm and Artificial Neural Network to detect intrusions, is proposed. NSL-KDD dataset was used for the study. Initially, data preprocessing was carried out. Encoding was done as the first step of the pre-process which was accomplished using one hot encoding. Then, features were inserted into feature scaling which was done using Min-max normalization. Feature reduction is the final step of the pre-process which was achieved using Principal Component Analysis. Subsequently, K-Nearest Neighbor algorithm was used as binary classifier that classify data into normal and abnormal classes. Then, the abnormal class was further classified into four major attack types using Artificial Neural Network. Finally, the model was evaluated and results show that the model has high accuracy and very low overfitting and underfitting.

Keywords: hybrid, k-nearest neighbor, artificial neural network, min-max normalization, one hot encoding, principal component analysis

I. INTRODUCTION

The technology has been developing rapidly. As a result of that, the cyber space is becoming an unsafe place day by day due to malicious activities. These malicious activities are also called as intrusions that effect integrity, confidentiality and availability of resources [1]. Intrusion detection system (IDS) is a system which protects resources against intrusions.

IDSs can be divided into two categories with respect to the system they protect which are called as Network-based Intrusion Detection System (NIDS) and Host-based Intrusion Detection System (HIDS) [2 - 4] . NIDS monitors devices in a network while HIDS monitors a particular device. On the other hand, IDSs can be further classified into two categories which are signature-based intrusion detection systems and anomaly-based intrusion detection systems with respect to the approach of detection [5, 6]. Signature-based intrusion detection systems use already surviving patterns and signatures to identify intrusions while anomaly-based intrusion detection systems check deviations of normal traffic [7, 8].

The development of NIDSs is mainly carried out by the Machine Learning (ML) [9]. ML techniques enable systems to learn signatures or patterns which is called as training and predict against real time network traffic. Researches proposed different kinds of approaches to develop NIDSs to detect intrusions using ML algorithms. Most of the researchers conduct their studies using single machine learning algorithm for intrusion detection [10]. Therefore, this study focuses on a hybrid machine learning approach for network intrusion detection. The aim of this study is to develop an approach to classify network traffic into “normal” and “abnormal” classes and further classify the abnormal traffic into four major classes while increasing the accuracy of the classification.

The rest of this article is structured as follows. The section II provides several related works which have done previously. The methodology used in this study is described comprehensively in the section III. Results which are obtained from this hybrid approach are shown in the section IV. Finally, conclusion of this study is provided in the section V.

II. LITERATURE REVIEW

A hybrid multilevel intrusion detection model which is called as KNN_NN is used by the study done by [11]. It uses K-Nearest Neighbor (KNN) algorithm for binary classification which classifies data into 'normal' and 'abnormal' classes. Neural Network is used to classify abnormal class into four major attack types. Instead of using Principal Component Analysis, which is used in this study, the study [11] uses Rough Set Theory and Information Gain for feature selection. Using these methods, they selected 25 features from the NSL-KDD dataset and experiment was done for 25 and 41 features while this study was done for three categories, which are 13, 25 and 35 features. Both classification and clustering methods are used for intrusion detection in the study [1]. They used all 41 features for their study. It clusters data using K-Means algorithm first. Then Adaptive-SVM algorithm is used for classification. Authors of [12] also used two supervised and unsupervised learning methods for their research. They applied Random Forest algorithm in misuse detection to build intrusion patterns and classify the data into main intrusion types using patterns. They used K-means algorithm with an improvement which is called weighted k-means algorithm in anomaly detection system with the patterns from the misuse detection.

Another study [13] proposed a new hybrid algorithm, which is called as PCANNA (Principal Component Analysis Neural Network Algorithm). It consists Principal Component Analysis as feature reduction tool. The proposed algorithm selected 8 features and compare it with 41 features while using Artificial Neural Network (ANN) as the classifier. The paper [14] present a model using C4.5 decision tree and one class support vector machine (SVM). Their approach consists a misuse detection model which uses C4.5 decision tree first

[13]. Then this model is used to decompose the training data into subset. Then multiple SVM was used to implement anomaly detection model for each decomposed set. As a result of that, anomaly detection model can use known attack information. Genetic algorithm (GA) and SVM are combined to build a hybrid algorithm in [15]. In their study, first, GA algorithm was used for generation of optimal feature subset. Then, the SVM algorithm was used for classification.

III. PROPOSED METHODOLOGY

The proposed approach is a combination of KNN and ANN machine learning techniques so as to obtain a better solution. This model consists three main phases which are data pre-processing, binary classification using KNN and further classification using ANN as shown in Figure 1.

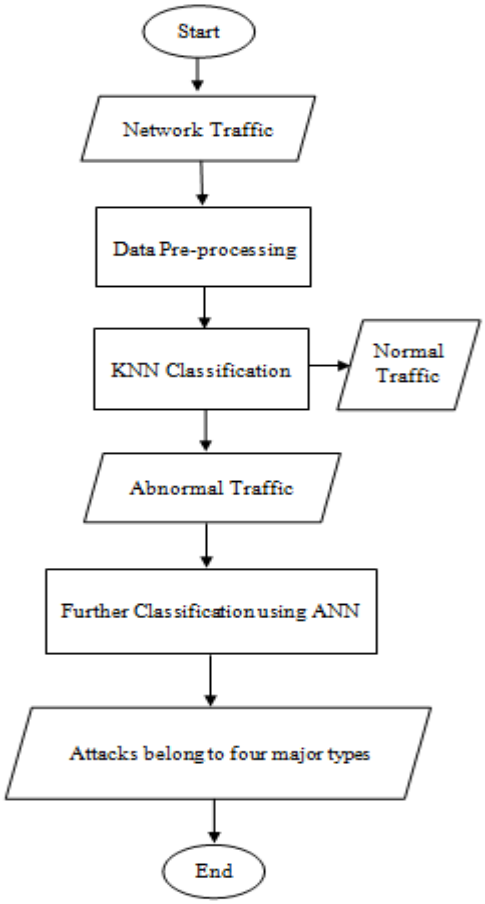

Figure 1. Flow chart of proposed model

Initially, data pre-processing was done on both training and testing data of NSL-KDD dataset which is shown in Table I.

Table I. Content of the dataset

	Training	Testing
Normal	67,343	11,245
Attack	58,630	11,299
Total	125,973	22,544

A. Data Pre-Processing

This phase mainly consists three sub phases which are feature conversion from categorical to numeric, feature scaling and feature reduction.

The dataset consists 41 features. Among those features, there are 38 numeric features and 3 categorical features which are Protocol_type, service and flag. These features should be converted into numeric. "One hot encoding is the most widely used coding scheme" [16] to convert categorical data to numeric. The proposed model uses one hot encoding method for the conversion.

Feature scaling is the next step of the pre-processing. There are different kinds of feature scaling techniques such as min-max normalization, mean normalization, unit vector normalization and standardization. Among these methods min-max normalization was utilized in this hybrid approach.

Feature reduction is a vital process in data science which is used to reduce the original dimensionality space into meaningful dimensionality space. Principle Component Analysis (PCA) is, one of feature reduction techniques which is utilized in this study too. Different studies proposed to reduce features of the NSL-KDD dataset which is caused to increase the performance. Reducing the number of features to 13 increases the performance than using all 41 features [17]. For intrusion detection system, 10 is an ideal number of principal components which has accuracy that nearly equal to the original feature space [18]. According to above studies, the propose approach also reduces the feature space of NSLKDD dataset into three different feature spaces which are tested for the performance. Therefore, the experiment was done on 13, 25 and 35 feature spaces.

B. KNN Classification

The second phase of the proposed approach is, binary classification which was done using KNN algorithm. KNN is a one of simplest machine learning algorithm which is also very popular in classification. The dataset which is preprocessed, is deployed to KNN algorithm in order to obtain two classes traffic which are "normal" and "abnormal". KNN classifies input data according to fixed number of training instances which are closest to the input data. The k value is an important parameter in KNN algorithm. Small k value selection results low accuracy if noisy dataset is used for training while high k value effects to model will be overfit that results low accuracy [19]. Therefor the KNN classification of this approach was done by fixing k as 8 training instances. The distance between input data and training instances which are defined by the k value is measured by different methods. Euclidean distance is the most popular method. There are other methods such as Manhattan distance, Minkowski distance and Hamming Distance [20]. Euclidean distance was used as the distance measuring method in this study as well.

C. Further Classification using ANN

Final phase of this approach is further classification which was done using ANN in order to classify abnormal traffic into four major abnormal classes. Multilayer feed-forward neural network with Backpropagation algorithm was applied in this study which contains one hidden layer. "Backpropergation algorithm propagates the error from the output layer to hidden layers and change weights recursively through network from output layer to input layer" [21].

An activation function of a neural network is used to transform the activation level of neurons to output signal [22]. There are different kinds of activation functions which are used relative to the scenario. ReLU is a powerful

activation function which is used in the current deep learning era. This study also utilized ReLU activation function for hidden layers. Among different kinds of kernel initializers, he_uniform was selected due to high applicability with ReLU activation function. Since the neural network handle multiple classes, softmax activation function was used for the output layer along with glorot_uniform initializer.

IV. RESULTS

The proposed hybrid model provides validation and test accuracies as shown in Table II and the model is evaluated during the training process of ANN which is represented by figure 2, 3 and 4.

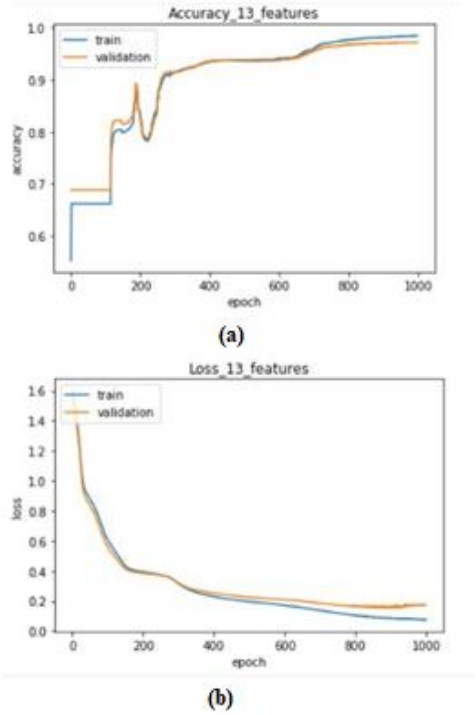

Figure 2. Accuracy (a) and loss (b) curves of 13 features

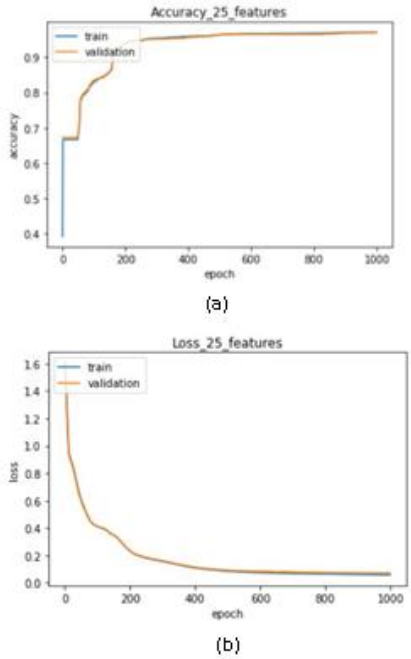

Figure 3. Accuracy (a) and loss (b) curves of 25 features

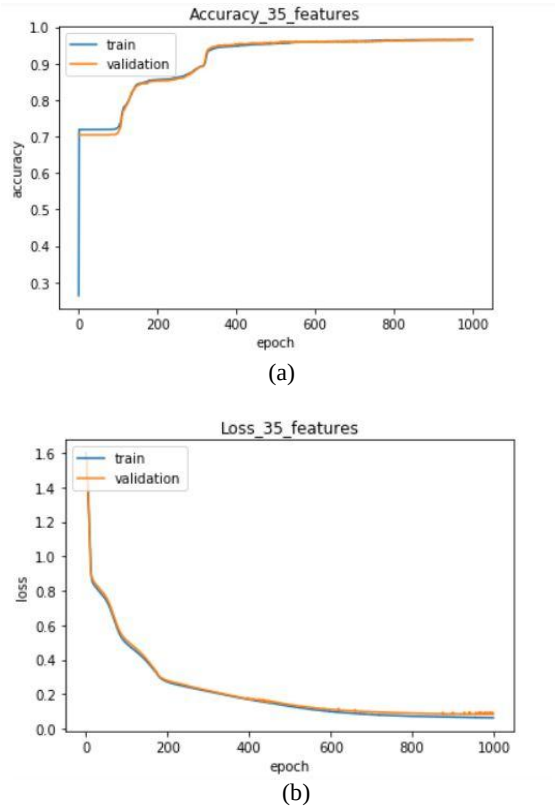

Figure 4. Accuracy (a) and loss (b) curves of 35 features

Table II. Validation & test accuracies of the model

No. of features	Validation accuracy (%)	Test accuracy (%)
13	97.87	97.46
25	96.97	96.39
35	97.03	96.59

V. CONCLUSION

This paper proposes a hybrid model which is a combination of KNN and ANN algorithms for network intrusion detection. It classifies network traffic into normal and abnormal classes using KNN and further classifies abnormal traffic into four major types of attacks using ANN. The proposed multilevel classifier was tested on NSL-KDD dataset. The dataset was utilized in three different ways with respect to number of features. Therefore, the model was tested with three feature spaces which are 13, 25 and 35. For all three feature spaces, the model showed over 96% accuracy. It was also observed that, 13 features space provides more accuracy. According to the loss curves, the proposed model shows very low underfitting since training loss does not remain flat and continue to decrease until the end of training. The model also shows very low overfitting which is proven by the accuracy curves since there is a small gap between training and validation accuracy curves. Ultimately, the experimental results suggest that, the proposed hybrid classification model is an effective methodology for network intrusion detection.

VI. REFERENCES

[1] J. K. Chahal and A. Kaur, "A hybrid approach based on classification and clustering for intrusion detection system," Int. J. Math. Sci. Comput., vol. 4, no. November 2016, pp. 34–40, 2016.

[2] J. J. Davis and A. J. Clark, "Data preprocessing for anomaly based network intrusion detection: A review," Comput. Secur., vol. 30, no. 6–7, pp. 353–375, 2011.

[3] S. Choudhury and A. Bhowal, "Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection," in 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, ICSTM 2015 - Proceedings, 2015, no. May, pp. 89–95.

[4] W. Wang, X. Guan, and X. Zhang, "Processing of massive audit data streams for real-time anomaly intrusion detection," Comput. Commun., vol. 31, no. 1, pp. 58–72, 2008.

[5] A. Özgür and H. Erdem, "The impact of using large training data set KDD99 on classification accuracy," PeerJ, vol. 5, no. March, 2017.

[6] T. Mehmood and H. B. Rais, "Machine learning algorithms in context of intrusion detection," in 3rd International Conference on Computer and Information Sciences (ICCOINS), 2016, pp. 369–373.

[7] V. Kshirsagar and M. S. Joshi, "Rule based classifier models for intrusion detection system," Int. J. Comput. Sci. Inf. Technol., vol. 7, no. 1, pp. 367–370, 2016.

[8] T. R. Devi and S. Badugu, "A Review on Network intrusion detection systems using machine learning," in International Conference on Emerging Trends in Engineering, 2020, pp. 598–607.

[9] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proceedings - IEEE Symposium on Security and Privacy, 2010, pp. 305–316.

[10] G. M. Gandhi, K. Appavoo, and S. K. Srivatsa, "Effective network intrusion detection using classifiers decision trees and decision rules," Int. J. Adv. Netw. Appl., vol. 2, no. 3, pp. 686–692, 2010.

[11] P. Ghosh, C. Debnath, D. Metia, and D. R. Dutta, "An efficient hybrid multilevel intrusion detection system in cloud environment," IOSR J. Comput. Eng., vol. 16, no. 4, pp. 16–26, 2014.

[12] S. Lakhina, S. Joseph, and B. Verma, "Feature reduction using principal component analysis for effective anomaly–based intrusion detection on NSL-KDD," Int. J. Eng. Sci. Technol., vol. 2, no. 6, pp. 1790–1799, 2010.

[13] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," Expert Syst. Appl., vol. 41, no. 4 PART 2, pp. 1690–1700, 2014.

[14] B. M. Aslahi-Shahri et al., "A hybrid method consisting of GA and SVM for intrusion detection system," Neural Comput. Appl., vol. 27, no. 6, pp. 1669–1676, 2016.

[15] R. M. Elbasiony, E. A. Sallam, T. E. Eltobely, and M. M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means," Ain Shams Eng. J., vol. 4, no. 4, pp. 753–762, 2013.

[16] K. Potdar, T. S., and C. D., "A comparative study of categorical variable encoding techniques for neural network classifiers," Int. J. Comput. Appl., vol. 175, no. 4, pp. 7–9, 2017.

[17] O. I. Aladesote, A. Olutola, and O. Olayemi, "Feature or attribute extraction for intrusion detection system using gain ratio and Principal Component Analysis (PCA)," Commun. Appl. Electron., vol. 4, no. 3, pp. 1–4, 2016.

[18] K. K. Vasan and B. Surendiran, "Dimensionality reduction using Principal Component Analysis for network intrusion detection," Perspect. Sci., vol. 8, no. September, pp. 510–512, 2016.

[19] I. S. Atawodi, "A machine learning approach to network intrusion detection system using K Nearest Neighbor and Random Forest," Masters Thesis, 2019.

[20] K. Chumachenko, "machine learning methods for malware detection and classification," Proc. 21st Pan-Hellenic Conf. Informatics - PCI 2017, p. 93, 2017.

[21] F. Haddadi, S. Khanchi, M. Shetabi, and V. Derhami, "Intrusion detection and attack classification using feed-forward neural network," in 2nd International Conference on Computer and Network Technology, ICCNT 2010, 2010, pp. 262–266. doi: 10.1109/ICCNT.2010.28

[22] P. Sibi, S. Allwyn Jones, and P. Siddarth, "Analysis of different activation functions using back propagation neural networks," J. Theor. Appl. Inf. Technol., vol. 47, no. 3, pp. 1344–1348, 2013.