ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.6, 3839–3848
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.6.63 Spec Issiue on ICAML-2020

EFFICIENT INTRUSION DETECTION TECHNIQUE USING STACKED AUTOENCODER

K. SINGH[1], L. KAUR, AND R. MAINI

ABSTRACT. Network intrusion detection (NID) plays a major role to provide the security to the network. Due to a large amount of data generated by networks, the machine learning models require a large amount of time to train on a specific behavior (normal/abnormal). The main objective of this paper is to reduce the volume and dimension of data used for training the intrusion detection techniques. To achieve this goal, efficient intrusion detection technique has been proposed, which uses; (i) extended KDD dataset which is created by adding testing data into training data of standard NSL-KDD to provide sufficient number of records in each class, (ii) 10% of extended NSL-KDD dataset for training instead of using whole dataset, (iii) column standardization to normalize data to speed up the classification process and (iv) two-layered stacked autoencoder (SAEs) for dimensionality reduction as well as for classification. To test the efficiency of the proposed work, different classifiers based on Autoencoders, SVM, Tree, and KNN has been applied and the results are compared. The results show that column standardization increases the accuracy of classification of all the considered classifiers on NSL-KDD Extended dataset. The comparison with the state-of-the-art techniques demonstrates that the proposed technique achieves higher or comparable accuracy even with 10% of training data.

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68P30, 68T99.

Key words and phrases. autoencoders, KDD, NIDS, deep learning, network security.

1. INTRODUCTION

The size of the internet is growing day by day and the emerging fields like the internet of things (IoT) increase the number of users and traffic on networks. Because of the expansion of networks, it is very difficult to handle security related issues like integrity, availability, and confidentiality of network resources. Due to the increase in the size of data on the internet and dynamic nature of most of the applications, the life of a proposed model to cope up with security issues are not so good. Although the machine learning and deep learning offers a wide variety of models to handle security-related issues all these have some shortcomings due to rapidly changing network environment. Hence the main challenge to network security is to provide an efficient, effective and robust network intrusion detection system (IDS) that will adapt according to dynamic changes in computer networks.

Recently, anomaly-based IDS have used Machine Learning (ML) and deep learning approaches for detection of attacks. ML-based IDS still have some flaws like it gives more accurate results for labeled data, but most of the data produced by different applications are unlabeled. Thus, it is difficult to assign the labels before train the IDS models. Although, ML-based classification model yields more accurate results with a large amount of data, but leads to a large amount of training time due to adjustment of weights in forward-backward passes [2], in training phase.

In this paper, NSL-KDD extended dataset has been used for experimentation. The data normalization process has been used, which increases the classification accuracy. The NSL-KDD train and test data are combined to increase the number of records in different classes especially in R2L and U2R attack classes. By using this model, the attacks in 2-class, 5-class, and 22-class classification are easily classified which were fails when we were using only NSL-KDD train dataset record. According to best of author's knowledge, 50-75% of data has been used by the researcher in the literature. In this paper, 10% of data has been used for training the deep learning stacked autoencoders which reduced lots of time for training the models.

1.1. **Motivation for proposed Intrusion Detection Technique (IDT).**

(1) Standard NSL-KDD dataset is not balanced i.e. some classes has lesser number of records which creates a problem of learning on specific behavior.
(2) All features of NSL-KDD dataset has a variable variance which also creates the problem for learning and most of the novel classifier unable to test for their better efficacy.
(3) All state-of-the-art intrusion detection classifiers use more than 20% [1, 9, 13], data for training which take a considerable amount of time for training that can be reduced.

1.2. **This paper offers the following novel contribution.**

(1) NSL-KDD extended dataset is created by combining NSL-KDD train and test data. Standard NSL-KDD dataset is not balanced because some classes have an insufficient number of records, which creates the problem for learning on specific behavior.
(2) Extended NSL-KDD dataset is normalized using two data normalization techniques; column standardization and column normalization to improve the accuracy.
(3) According to the best of author's knowledge, no research work of NID is performed using 10% training data so the first time this work uses 10% of NSL-KDD extended dataset for training which speeds up the process by reducing training time.

2. PRELIMINARY BACKGROUND

This section provides the knowledge about to understand the proposed work.

2.1. **Dimensionality Reduction.**

Dimensionality reduction is the process of mapping the high dimensional feature space into low dimensional feature space, [8]. It reduces the processing time of data and also helps to visualize the data in 2-D or 3-D space, which can be easily analyzed.

Dimensionality reduction is mainly of two types, [8]; feature selection and feature extraction. In feature selection technique the important features of data are selected based on the ranking of features [3], by performing information

gain and only highly ranked features are selected. In feature extraction technique, high dimensional feature space is transformed into new low dimensional feature space without directly neglecting the low ranked features. Many supervised and unsupervised techniques have been used in the literature for dimensionality reduction like Principle Components Analysis (PCA), [4], Locality Preserving Projections (LPP), [5], Isomap, [6], deep learning autoencoders, [7] etc. In this paper, deep learning autoencoders have been used for dimensionality reduction. The 41 features of NSL-KDD dataset have been reduced to 30 features, which increases the speed of classification and also improves the performance in classification of attacks.

2.2. **Stacked Autoencoders.** Unlike the simple autoencoder which contains one hidden layer, the stacked autoencoders have multiple hidden layers clubbed together to learn the deep features from the given input data, [10]. The output of the one layer is given as an input to the next layer. Hence, the first hidden layer of stacked autoencoder learns the first order deep features from the input raw data. The second layer of stacked autoencoder learns the second order deep features corresponding to the features learn by the first layer and similarly, the next higher layer learns more deep features of the data. Hence stacked autoencoders saves the training time by freezing one layer and training the next subsequent layers and also improves the accuracy. Stacked autoencoders with three hidden layers shown in Figure 1.

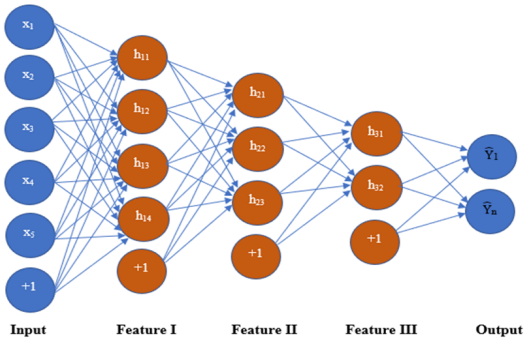

FIGURE 1. Stacked autoencoders with three hidden layers

2.3. **Normalization.** Normalization is the process of transforming the features on a common scale and changing the statistics like mean and standard deviation to speed up the calculations used in training and testing of the dataset. In this

paper, two types of data normalization have been used: column normalization and column standardization.

3. Proposed Intrusion Detection Technique

This work proposed an Intrusion Detection Technique (IDT), which uses the stacked autoencoders (SAEs) with two hidden layers to reduce the dimensions of the data for classification on NSL-KDD extended dataset. NSL-KDD extended dataset is formed by combining Train and Test set of original NSL-KDD dataset. Extended data is pre-processed by converting text values into numeric values and then normalization of data is performed. The various steps of the proposed technique are shown in Figure 2.

3.1. **Extended NSL-KDD dataset.** In this work, the standard benchmark NSL-KDD dataset has been used which was produced from KDD'99 dataset after removing the shortcomings and illuminating the duplicate records by Tavallaee et al. in [11]. Standard NSL-KDD dataset contains two sets, first set Train data having a total of 125917 records and the second set is Test data which have 22544 records. NSL-KDD has imbalance, [12], dataset because some classes have a large number of records while some classes have a smaller number of records. Hence, it creates a problem for different security models to learn the behavior of a class having a smaller number of records and subsequently degrades the overall performance of that model.

To resolve this problem extended NSL-KDD is formed by combining both Train and Test data. Extended NSL-KDD dataset having total 148517 records (as shown in Table 1), 41 features and 40 types of attack classes, which are grouped in 2-class, 5-class, and 22-class.

Table 1. Composition of NSL-KDD train and test data in totality

NSL-KDD	Records	**Normal**	**DoS**	**Probe**	**R2L**	**U2R**
Train + Test	148517	77054	53387	14077	3880	119
	%	51.88	35.94	9.47	2.6	0.08

All 41 features are mainly grouped under three data types; nominal, binary, and numeric. Features 2, 3, 4 are nominal, 7, 12, 14, 15, 21, 22 are binary and

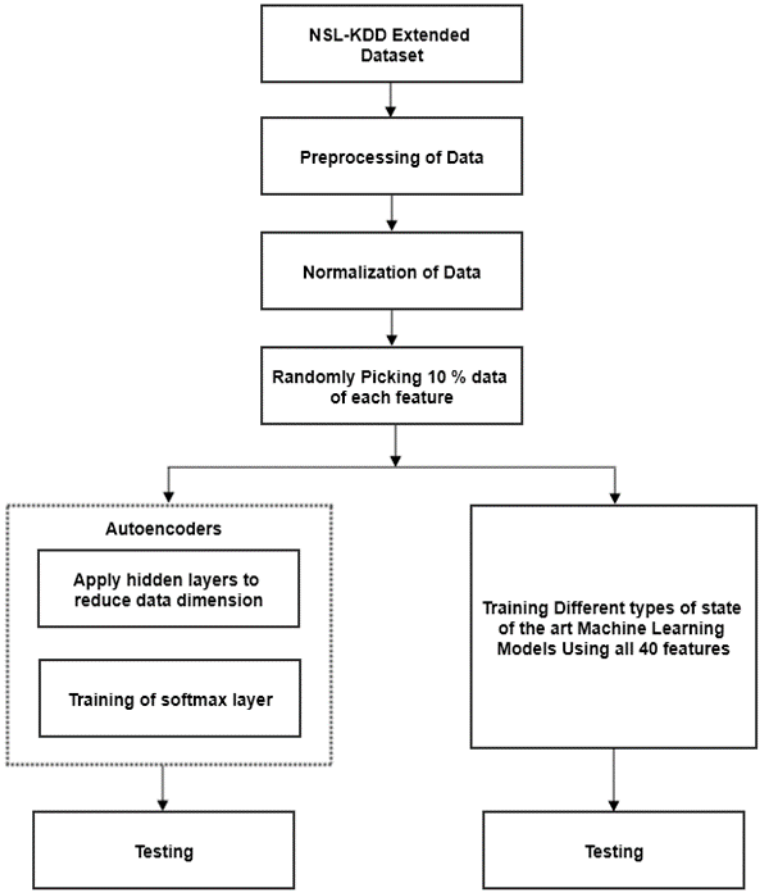

FIGURE 2. Flowchart of proposed intrusion detection technique.

all remaining features are a numeric type. In this research work, to perform the experiment the nominal features are converted into numeric features by assigning numbers (like tcp=1, udp=2, ...). One feature is eliminated from dataset due to its zero value.

4. EVALUATIONS AND RESULTS

For demonstrating the effectiveness of proposed contributions on the performance of stacked autoencoder and state of the art machine learning classifiers, results are taken on (i) Data without normalization, (ii) Data with column normalization and (iii) Data with column standardization have been performed. For each class, the 10% of data has been used for training each classifier and then each trained classifier is tested on 90% data.

TABLE 2. Performance of different classifiers for 2-class classification with and without normalized data

Classifiers	Accuracy on		
	Unnormalized Data	Column Normalized Data	Column Standardized Data
Proposed Technique	95.81	51.88	97.07
Linear SVM	92.44	92.45	92.44
Fine Gaussian SVM	95.21	95.21	95.21
Coarse KNN	94.03	94.03	94.03
Weighted KNN	96.16	96.15	96.15
Boosted Tree	96.07	96.07	96.07
Subspace KNN	96.15	96.05	96.01

To test the learning rate with 10% of NSL-KDD Extended dataset three set of experiments have been performed using; a) Binary-class classification b) 5-class classification c) 22-class classification of a dataset. In binary classification, all labels are grouped into two classes one is normal and other is abnormal. In 5-class classification all labels are grouped into 5 class namely DoS, Probe, R2L, U2R and normal. In 22-class classification all 40 types of attacks present in NSL-KDD dataset are grouped into 22 class labels in which 21 labels are used as attacks and one is normal class label. Some attacks have a smaller number of records which creates a problem in learning while training that's why these attacks are grouped under one class label.

Autoencoders and all other machine learning classifiers are trained by using 10% data of each class in NSL-KDD extended. The performance of different classifier for 10% training data is calculated by using different performance metrics like precision, recall, false negative rate, specificity, false positive rate, and accuracy. Some results are presented in table 2 and some are shown in figure 3 to 5.

From table 2 and figure 3, it is evident that the proposed technique yields better performance than all state-of-the-art classifiers in terms of all metrics. Also,

FIGURE 3. Comparison of overall accuracy of different classifiers for binary classification of normalized/unnormalized data with proposed stacked autoencoders

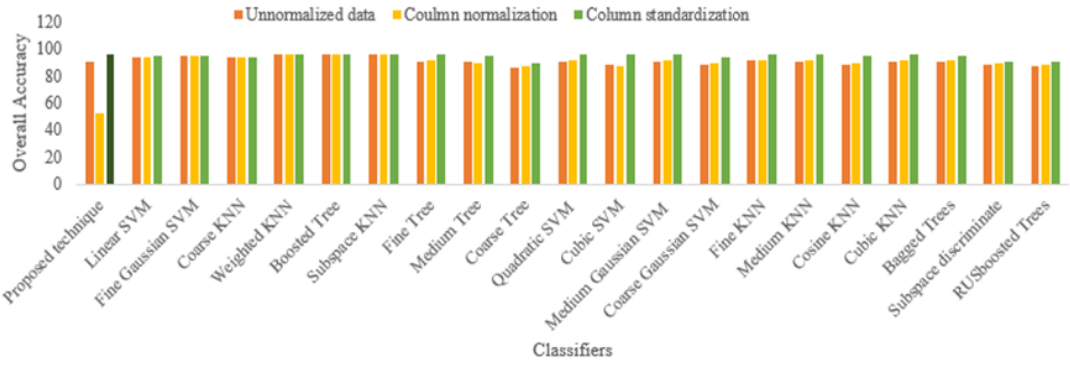

FIGURE 4. Comparison of overall accuracy of different classifiers on different normalized data with proposed stacked autoencoders on 5- class classification

it has been observed that that column standardization technique increases the performance of classification as compared to unnormalized/column normalization technique. Proposed SAEs has higher class-wise as well as overall accuracy than all other ML-based classifiers. It has the same or significantly lower FP and FN rate than other classifiers. Some metric has the unknown value which is represented by 'x' in the resultant tables. Similarly, for 5-class and 22-class, the results are presented in figures 4 to 5. The results demonstrate the significance of the use of column standardization as it improves the classification performance of all the techniques even when they fail.

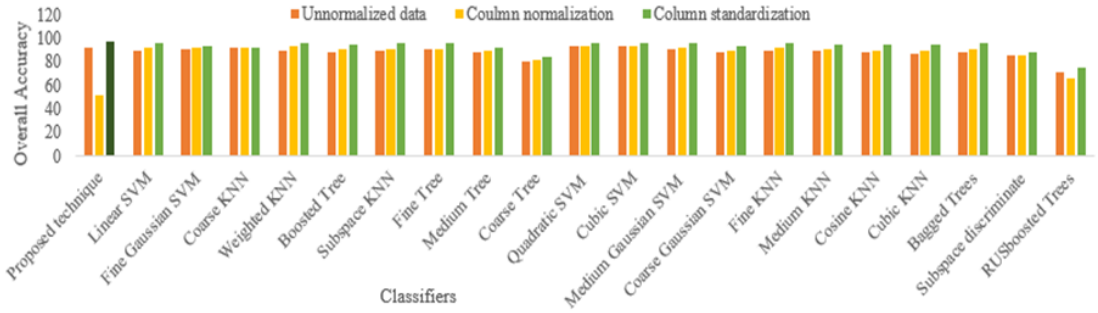

FIGURE 5. Comparison of overall accuracy of different classifiers for 22- class classification of normalized/unnormalized data with proposed stacked autoencoders.

5. CONCLUSION

This work proposed an efficient IDT as well as improves the classification performance of the state-of-the-art classifiers for intrusion detection. The novelties of the proposed work are four folds; creation of NSL-KDD extended dataset to provide the sufficient number of records in each class, column standardization for normalization of data, 10% use of data for training purposes and two-layered stacked autoencoders to reduce the dimension of data from 40 features to 30. To demonstrate the performance of the proposed technique, the experiments have been performed on 2-class, 5-class and 22-class classification of attacks. As the proposed technique achieves accuracy higher than 1% than the state-of-the-art classifiers considered here. More Specifically, column standardization also improves the performance of state-of-the-art classifiers. The comparison with the state-of-the-art techniques demonstrates that the proposed technique achieves higher or comparable accuracy even with 10% of training data.

REFERENCES

[1] S. ALJAWARNEH, M. ALDWAIRI, M. B. YASSEIN: *Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model*, Journal of Computational Science, **25** (2018), 152–160.

[2] A. L. BUCZAK, E. GUVEN: *A survey of data mining and machine learning methods for cyber security intrusion detection*, IEEE Communications Surveys & Tutorials, **18** (2016), 1153–1176.

[3] I. MANZOOR, N. KUMAR: *A feature reduced intrusion detection system using ANN classifier*, Expert Systems with Applications, **88** (2017), 249–257.

[4] F. E. HEBA, A. DARWISH, A. E. HASSANIEN, A. ABRAHAM: *Principle components analysis and support vector machine-based intrusion detection system*, 10th international conference on intelligent systems design and applications, (2010), 363–367.

[5] S. T. ROWEIS, L. K. SAUL: *Nonlinear dimensionality reduction by locally linear embedding*, American Association for the Advancement of Science, **290** (2000), 2323–2326.

[6] V. D. SILVA, J. B. TENENBAUM: *Global versus local methods in nonlinear dimensionality reduction*: Advances in neural information processing systems, **15** (2003), 721–728.

[7] Y. WANG, H. YAO, S. ZHAO: *Auto-encoder based dimensionality reduction*, Neurocomputing, **184** (2016), 232–242.

[8] L. VAN DER MAATEN, E. POSTMA, J. VAN DEN HERIK: *Dimensionality reduction: a comparative*, J. Mach. Learn. Res., **10** (2009), 66–71.

[9] F. FARAHNAKIAN, J. HEIKKONEN: *A deep auto-encoder based approach for intrusion detection system*, 20th International Conference on Advanced Communication Technology (ICACT), (2018), 178–183.

[10] S. SINGH, S. S. KASANA: *Efficient classification of the hyperspectral images using deep learning*, Multimedia Tools and Applications, (2018), 1–14.

[11] M. TAVALLAEE, E. BAGHERI, W. LU, A. A. GHORBANI: *A detailed analysis of the KDD CUP 99 data set*, IEEE symposium on computational intelligence for security and defense applications, (2009), 1–6.

[12] J. MCHUGH: *Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory*, ACM Transactions on Information and System Security (TISSEC), **3** (2000), 262–294.

[13] M. Z. ALOM, V. BONTUPALLI, T. M. TAHA: *Intrusion detection using deep belief networks*, National Aerospace and Electronics Conference (NAECON), (2015), 339–344.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
PUNJABI UNIVERSITY PATIALA,PUNJAB INDIA
Email address: sidhu.kuldeep89@gmail.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
PUNJABI UNIVERSITY PATIALA,PUNJAB INDIA
Email address: mahal2k8@gmail.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
PUNJABI UNIVERSITY PATIALA,PUNJAB INDIA
Email address: research.raman@gmail.com