Retraction

Retraction: Distributed Ensemble based Deep Learning architecture for Intrusion Detection against Cyber attacks (J. Phys.: Conf. Ser. 1916 012080)

Published 23 February 2022

This article (and all articles in the proceedings volume relating to the same conference) has been retracted by IOP Publishing following an extensive investigation in line with the COPE guidelines. This investigation has uncovered evidence of systematic manipulation of the publication process and considerable citation manipulation.

IOP Publishing respectfully requests that readers consider all work within this volume potentially unreliable, as the volume has not been through a credible peer review process.

IOP Publishing regrets that our usual quality checks did not identify these issues before publication, and have since put additional measures in place to try to prevent these issues from reoccurring. IOP Publishing wishes to credit anonymous whistleblowers and the Problematic Paper Screener [1] for bringing some of the above issues to our attention, prompting us to investigate further.

[1] Cabanac G, Labbé C and Magazinov A 2021 arXiv:2107.06751v1

Retraction published: 23 February 2022
Distributed Ensemble based Deep Learning architecture for Intrusion Detection against Cyber attacks

Kavitha M¹, Elamukhil K², Ajeeth R², Ashwin R² and Balasubramaniam V²

¹Assistant Professor, Department of Computer Science and Engineering
²Final Year, Computer Science and Engineering, Sri Krishna College of Engineering and Technology
kavitham@skcet.ac.in

Abstract. The increasing scale and importance of web contact around the Internet has increased the need for improved cyber security defence against cyber attacks. On modelling the machine learning based intrusion detection system, features of the attacks helps to discover, determine and identify unauthorized behaviour. Behaviour modelling has been used as training model to detect the evolving attacks to the servers or learning model has been constructed to build a training model to identify the intrusion in the network on basis of signature of the attacks. However machine learning model fails in handling attacks propagating on the applications with large scale or large dimensional data which further leads to high false alarm rate. In order to tackle those issues, a new distributed ensemble based deep learning architecture has been employed using Convolution Neural Network, Recurrent Neural Network and Multilayer Perceptron towards intrusion detection on cyber attacks on the web servers. Convolution Neural Network, Recurrent Neural Network and Multilayer Perceptron has been modelled as training model to detect the intrusion, trained model will generate best model which acts as classifier or prediction model for cyber attacks. The particular model will be employed further to detect the intrusion propagating in the web server. The proposed ensemble based deep learning architecture is compared to state-of-the-art approaches on performance measures such as precision, recall, and f-measure on true positive, false positive, true negative, and false negative computations using the KDD CUP 99 dataset.

Keywords: Intrusion Detection, Deep learning, Ensemble Model, Convolution Neural Network, Recurrent Neural Network, Multi-Layer perceptron.

1. Introduction

As intruders use system vulnerabilities to functionalize data theft or complete the destruction of entire system infrastructure or network infrastructures, cyber attacks have become more frequent. Since cyber attacks are growing at an unprecedented pace [1], intrusion detection is a significant research field. Essentially, effective strategies for detecting and defending attacks, as well as maintaining server protection, are needed. Furthermore, various types of attacks must normally be dealt with in different ways. A machine learning-based model has been developed to detect various types of server-based attacks. It categorises the attacks without knowing their specific characteristics [2]. Traditional machine learning methods, on the other hand, are unable to provide distinct feature descriptors to explain the problem of attack detection due to model complexity limitations.
Deep learning architecture, which is made up of several layers to solve complex problems, is becoming increasingly common. In addition to deep learning architecture, an ensemble model based on deep learning was used to increase prediction accuracy in this study. The proposed implementation of the ensemble dependent learning algorithm called best classifier enhanced predictions using the KDD cup dataset. One such ensemble based learning paradigm is combining multiple machine learning algorithms as a meta-model to combine different predictions from single algorithms in order to boost the overall performance of the model [3]. Combining the advantages of many prediction algorithms will increase the mechanism's detection capability.

The remaining parts of the paper are listed below. In Section 2, we present related works on intrusion detection systems based on Deep learning and Machine learning classifiers. The proposed Ensemble Paradigm for intrusion detection on emerging attack types based on a combination of deep learning architectures is defined and designed in Section 3. In comparison to state-of-the-art methods, Section 4 describes a research setting, results, and efficiency of the proposed model. The paper comes to a close with Section 5.

2. Related works

In this section, various existing model enumerating Intrusion detection system with desirable properties using machine learning and deep learning architectures has analysed on basis of feature extraction and signature matching aspects towards cyber security establishment on the servers in against cyber attacks in detail as follows

2.1. Support Vector Machine-based Intrusion Detection System for Cyber Protection

The intrusion detection method that uses support vector machines [4] is modelled using a machine learning model as a supervised learning model. SVM stands for Support Vector Machine and is a flexible and effective machine learning algorithm. Data space decision boundaries are the cornerstone of the Support Vector Machine model. A decision boundary divides a series of data instances into different groups during processing of the KDD Cup 99 dataset, with values ranging between two benevolent and malicious categories.

The help vector machine can classify various types of cyber security intrusions into two categories: binary and multi-class. The support vector computes the best hyperplane separation for function instance on the server [5], and it is the data point that is nearest to the dividing hyperplane based on the signature or features. The classification method is the transformation of the input vectors of the feature space on either side of the hyper plane as classes, and the positions of the features falling into either side are referred to as normal side and abnormal side, respectively.

2.2. Recurrent neural network-based intrusion detection framework for web-based cyber protection

An RNN is a reduced-size neural network that is used in a web-based cyber defence intrusion detection system. This model employs a three-layer Recurrent Neural Network architecture, with 41 features as inputs and four intrusion classes as outputs. In a deep learning approach for web-based cyber intrusion detection using recurrent neural networks, input units, output units, and hidden units are used (RNN-IDS). The network's storage portion is thought to be RNN's hidden units, which store all of the network's end-to-end data. The current output of a set of intrusion-related features [6] is also connected to the previous output layer.

3. Proposed model
In this segment, a distributed ensemble-based deep learning architecture for cyber security has been modelled using the following intrusion detection steps:

3.1. Dataset Pre-processing

The Dataset KDD cup 99 has been pre-processed using data transferring, data normalization and feature reduction. Each process is detailed as follows

- **Data Transferring**

  At first, any function in a dataset is translated to a numerical value. These numerical values expressed as symbolic features include information such as protocol type (TCP, UDP, ICMP), service type (HTTP, FTP, Telnet), and TCP status flag (SF, REJ). The data transferring method replaces the categorical attributes of the dataset information with numeric values[7].

- **Data Normalization**

  Symbolic attributes have been assigned to the normalization segment, which have been converted into numerical values for processing. Data normalization is the method of increasing the value of all attributes into a well-proportioned range, removing bias from the dataset of features with higher values. The larger margin value is used to normalise the features of each record, resulting in a range of [0-1]. The transferring and normalisation process will be used to evaluate results. In the production of five classes for the KDD Cup 99, the proposed models were compared to existing systems that had been tested on different types of attacks. One of these classes will hold regular records, while the other four will hold various forms of attacks (DDoS, Probe, U2R, and R2L, respectively)[8].

- **Selection of Features**

  To compute the more informative features, a method of choosing features is needed. For ranking, selection of features algorithms use the feature's relevance score. The aim of the computation is to find the optimum number of features. Then, using selective techniques one by one, it incrementally applies features to any of the classifiers. The training dataset with the highest classification accuracy has been chosen as the final determination of the optimal number of features on employing each technique.

3.2. Intrusion Detection System using Convolution Neural Network

The IDS network architecture consists of four convolutional layers for the volume, each with three three-element kernels. The number of convolutional layers was calculated empirically based on the detection model's results against the validation collection. The number of training sessions has been carried out iteratively in order to automatically decide on the outcome based on the validation and training set results [9]. The design of intrusion detection using CNN is depicted in Figure 1.

![Figure 1. Architecture of CNN towards intrusion detection](image-url)
Max pooling Layer

A max-pooling layer is used to compute the maximum value in the Intrusion feature set which considered after parameter reduction and spatial difference on the invariance computation of the Intrusion propagating in the server.

Network Layer

The network layers capture the features of intrusion through their inherent mechanism of coherence and covariance on the low level to more abstract features in the hierarchical to learn the discriminative features between the normal and cyber attacks.

Activation Function

The deep learning architecture utilizes the rectified linear units (ReLU) activation function, to estimate the non-linearity on the max pool of feature set. Each activation function on the specified set of feature is followed by batch normalization on feature category, as it eliminates the overfitting and improves the system performance on intrusion generalization by normalizing the output of the activation function on category of intrusion types.

3.3. Recurrent Neural Network-based Intrusion Detection System

The use of recurrent neural networks in an intrusion detection model is a powerful tool that enables neural networks to manage arbitrary length sequence data to the server. Of course, they demand that the sequence be a contextual sequence based on normalisation, with the signature generated entirely by forward propagation in the preceding section Figure 2.

Figure 2. Intrusion Detection based RNN architecture

The previous information containing the signature's weight has been stored to the current output using a directional loop in the RNN. It's the fundamental difference computation looping process that Feed-forward Neural Networks have passed down to us (FNNs). The intrusion's previous performance has been linked to the current outcomes of a function series. Back Propagation is used to transform the function by passing the residuals accumulated during the update of the extracted feature weights, which is close to how the classifier is trained using a standard neural network [10].

3.4. Intrusion Detection system using multilayer perceptron
MLP is most specialized and powerful deep learning technique for intrusion classification as Intrusion Detection System. MLP network has been designed on composition of two layers, each composed of 8 neuron. These numbers of neurons has been selected to protect various the size of input data based on the intrusion perception. In this levenberg-Maquardt technique has been observed as Intrusion detection objective function.

![Figure 3. Architecture of MLP towards Intrusion Detection](image)

Figure 3 represents the architecture of MLP on intrusion detection; it is processed in two phases. In initial phases, dataset with 41 features is trained and output is obtained on basis of 8 neuron with utilization of its two hidden layers and two outputs layers in order to represents the attack and normal characteristics.

3.5. Distributed Ensemble Deep Learning Architecture

In this architecture, Ensemble based model has been employed using Convolution Neural Network, Recurrent Neural Network and Multilayer Perceptron for intrusion detection on cyber attacks on the web servers. Convolution Neural Network, Recurrent Neural Network and Multilayer Perceptron has been modelled as training model to detect the intrusion, trained model will generate best model which acts as classifier or prediction model for cyber attacks.

![Figure 4. Ensemble Deep learning architecture of Intrusion Detection](image)

Figure 4 represents ensemble architecture of the proposed technique. Ensemble Classifiers is collection of classifier trained with the instance and constructs a decision boundary around the training data. The particular model will be employed further to detect the intrusion propagating in the web server.

4. Experimental Results

Experimental results have been carried out on KDD cup 99 dataset using python platform. In this experiment, performance of the proposed model has been computed using precision, recall and f measure. On evaluation, it has been proved that ensemble based on deep learning techniques in order to perform intrusion detection outperforms against ensemble technique on machine learning technique on detection rate with respect to level of false positives.
True Positive (TP) refers to features that are correctly classified as intrusion and represents the number of abnormal features that are deemed anomalous. The word False Positive (FP) refers to features that have been incorrectly classified as interference, as well as the amount of normal features that have been classified as anomaly.

\[\text{Performance Comparison}\]

The True Negative (TN) is defined as the number of normal features that are considered normal, and it is related to those features that are correctly classified as intrusion. The False Negative (FN) is the number of anomaly records that are incorrectly classified as natural, and it is linked to those features that are incorrectly classified as intrusion. The efficiency of the intrusion detection techniques was evaluated in Figure 5. On a specific dataset, Table 1 compares the output of the proposed methodology to that of a current model.

\[\text{Table 1. Performance Comparison of Intrusion Detection models}\]

| Methodology                  | Precision | Recall | F measure |
|------------------------------|-----------|--------|-----------|
| Ensemble Model using machine learning - Existing | 61.51     | 82.99  | 70.65     |
| Ensemble model using Deep learning - Proposed     | 89.96     | 77.67  | 83.37     |

Ensemble model-based deep learning achieves higher precision than other state-of-the-art machine learning methods by using the training set and has a high accuracy rate, even when there are many classifications. These results demonstrate the efficacy of the proposed model, which is thought to be more accurate and reliable than current methods.

5. Conclusion

We designed and implemented a distributed ensemble deep learning architecture towards the intrusion detection of the cyber attacks on the cyber security models. In contrast to conventional classification methods, the proposed model achieves a higher accuracy rate for the function obtained as well as a higher detection rate on classification with a lower false positive rate. Both the accuracy of the intrusion detection model and the ability to identify the intrusion type can be enhanced with this model. It detects the intrusion with less preparation time.

References

[1] J. A. Khan and N. Jain, A survey on intrusion detection systems and classification techniques, Int. J. Sci. Res. Sci., Eng. Technol., vol. 2, no. 5, pp. 202–208, 2016
[2] B. Kavitha, D. S. Karthikeyan, and P. Sheeba Maybell, An ensemble design of intrusion detection system for handling uncertainty using neutrosophic logic classifier, Knowledge-Based Systems, vol. 28, pp. 88–96, 2012.

[3] A. L. Buczak and E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.

[4] M. Suganya and H. Anandakumar, Handover based spectrum allocation in cognitive radio networks, 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Dec. 2013.doi:10.1109/icgce.2013.6823431. doi:10.4018/978-1-5225-5246-8.ch012

[5] Haldorai and A. Ramu, An Intelligent-Based Wavelet Classifier for Accurate Prediction of Breast Cancer, Intelligent Multidimensional Data and Image Processing, pp. 306–319.

[6] E. Bahri, N. Harbi, and H. Nguyen Huu, Approach based ensemble methods for better and faster intrusion detection, in Computational Intelligence in Security for Information Systems, pp. 17–24, Springer, Berlin, Germany, 2011.

[7] P. Yang, Y. Hwa Yang, B. B. Zhou, and A. Y. Zomaya, A review of ensemble methods in bioinformatics, Current Bioinformatics, vol. 5, no. 4, pp. 296–308, 2010.

[8] A. Aburomman and M. B. I. Reaz, A survey of intrusion detection systems based on ensemble and hybrid classifiers, Computers & Security, vol. 65, pp. 135–152, 2017.

[9] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, An adaptive ensemble machine learning model for intrusion detection, IEEE Access, vol. 7, pp. 82512–82521, 2019.

[10] M. Tavallaee, E. Bagheri, W. Lu, and A.-A. Ghorbani, A detailed analysis of the kdd cup 99 data set, in Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications, Ottawa, ON, Canada, July 2009.