MULTI-CLASSIFIER DEEP NEURAL NETWORK FOR DETECTING INTRUDER BEHAVIOR IN CYBER SECURITY

DESIRE IRADUKUNDA[1], XIONG WAN AN[1], WAQAR ALI[2, 3]

[1]School of Electronic Science Engineering, University of Electronic Science and Technology of China, Chengdu, China
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China.
[3]Faculty of Information Technology, The University of Lahore, Lahore, Pakistan.
E-MAIL: iradudesire100@yahoo.fr, waxiong@uestc.edu.cn, waqar@std.uestc.edu.cn

***Abstract*—The security is becoming much more important due to the massive growth in computer network technologies. Finding anomalies from a system's network traffic has been a hot research topic over the last two decades. Most of the existing signature-based intrusion detection systems only rely upon the pre-configured and predetermined attack patterns that are practically not true for real life challenges. In this research work, we attempt to capture the dynamic behavior of intruders by utilizing a novel Multi-Classifier Deep Neural Network (MCDNN) framework. The proposed framework intuitively segregate the attackers and authorize user data packets for a given network traffic. The MCDNN is based on four layers architecture, each layer is based upon the logistic regression classifier and is fully connected. The MCDNN utilizes a two-stage novel feature learning framework. The model is capable to automatically learn useful features from large network traffic labeled data collection and classifies intruders efficiently. We evaluate the effectiveness of our proposed model on a well known publicly available challenging dataset KDD99. The experimental results demonstrate that our proposed framework significantly outperforms the existing models and achieves considerable high recognition rates on KDD99.**

***Index Terms*—Intrusion detection systems, deep neural network, network traffic, cybersecurity, machine learning**

I. INTRODUCTION

The growing application and use of computer networks across different fields, network security is becoming increasingly significant. Organizations have to use security tools such as firewalls, anti-virus anti-spam techniques, etc., to protect against network attacks. Unfortunately, these traditional tools are unable to recognize dynamic nature and sophisticated manual and machine generated attacks. For example, a data breach at Yahoo industries had caused an estimated loss of 350 Million US dollars, and a data breach at Bitcoin reported as a roughly estimated loss of $70 Million [1]. Networks intrusion detection has gained significant research attention in recent years. It is considered as the most powerful defense tool against critical cyberattacks and threats [2]. As illustrated in Fig. 1, intruders might be curious users who want to know deeply how the system works or might be attackers from the internet who are not authorized to use the system services by trying to access sensitive information [7]. Multiple systems can be used for shielding system vulnerabilities such as anomaly detection and intrusion detection systems [2].

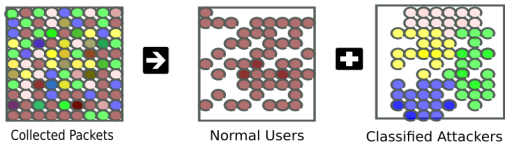


Fig. 1: Illustration of attackers and normal users in a network traffic

Detection of intruders from regular network traffic is not an easy task [1], [2]. In dynamic digital world, there are various complex challenges for effective and robust intrusion detection. For example, the diversity and variability of malicious attacks, classification of unseen or unlabeled data packets into authorized and malicious ones and computational limitations of existing machine learning models are few of them. One of the key limitations of existing intrusion detection methods is that they are unable to handle the stream of fast network traffic and the detection of new threats. Also, the classical machine learning approaches adopted for intrusion detection have to face lot of structural problems such as overfitting and high bias due to redundant and or irrelevant features, and the imbalanced class distribution of network traffic. Therefore, these methods are unable to effectively model the feature representation in order to build a more efficient predictive framework.

Recently, deep-learning-based methods have been successfully applied in various domains such as image [3] and speech recognition [4], data analytics [5], recommender systems [6] and action recognition [7], etc. These methods aim to learn key features from a large sample of unlabeled data and then apply them to a limited amount of labeled data features. The data may be collected from different distributions but it must have relevant semantics as a whole. Similarly, deep learning methods have a great impact on cybersecurity industry and network intrusion detection. Most of the newly proposed techniques are based on deep neural networks [8]–[10], that have proved credibility and outstanding performance for intuitively learning

dynamic behavior of malicious data packets. The noticeable improvements have been seen especially when the information regarding the attack trafc may be insufcient, then the classical machine learning methods that utilize the history of previous attacks fail to build up the predictive model.

In this research, we utilize the power of deep neural networks effectively classify authorized data packets and malicious data packets. The proposed Multi-Classifier Deep Neural Network (MCDNN) is a feed-forward neural network that has four layers i.e. input layer, two hidden layers, and an output layer. Each layer is based upon the logistic regression classifier and is fully connected. The MCDNN utilizes a two-stage novel feature learning framework. The first stage is used for data preprocessing,and features vector encoding. The second stage is used for learning and results prediction. We used softmax activation function for the output layer, rectier linear unit for hidden layers and stochastic gradient descent (SGD) for an optimizer. In short, our key contributions regarding this research can be summarized as followings:

- We propose a novel two-stage feature learning framework for network intrusion detection by utilizing the power of multiple classifiers with a deep neural network that has proven outstanding results.
- The proposed deep learning framework is based on a unique architecture compared to existing models in this domain.
- The proposed model has comparatively lower computational cost as compared to the existing state-of-the-art methods, we have selected limited features to reduce computational cost.
- We conduct extensive experiments on the well-known publicly available challenging dataset KDD99 to evaluate the effectiveness of our proposed model and got outstanding results compared to the existing state-of-the-art methods.

The rest of this paper is organized as followings. Section 2 describe an overview of the existing work done by different researchers in this domain during last two decades. Section 3 illustrates the proposed MCDNN framework with preliminary concepts, formal notations and symbols, motivational factors, and network design. Section 4 presents the experimental details including datasets, comparison methods, accuracy measures and evaluation results. Finally, section 5 conclude the paper with possible future extensions of this research work.

II. RELATED WORK

In this section, we present stepwise development in intrusion detection methods. It should be considered here that we will only focus on the work that is considered a key milestone as there is a vast volume of literature published in past years. Also, we will discuss only a few early handcrafted and machine learning-based methods and mainly focus on recently proposed deep learning-based models. Over the last few years, there has been considerable research attention focused on this research domain. In most of the previous studies, attack patterns were identified with various machine learning methods, with efforts for precision learning to reduce the false detection rate. One of the earliest work we found that has utilized ANN with enhanced resilient back-propagation for intrusion detection was proposed by Naoum et al. [11].

The deep learning-based intrusion detection models have achieved outstanding results in the recognition, classication, and prediction of data types such visual, audio, text or image, etc. data formats. Also, it has outperformed existing machine learning-based methods. In the practical analysis of malicious code samples, we may convert malicious codes into image, text or audio datatypes. Therefore, the use of deep learning techniques excels malicious code detection performance [8], [9], [12], [13], etc. Any intruder code can be converted into mal-image datatype or mal-text datatype by its malicious algorithm. Deep learning-based models [8], [9], [14] have proven success for all the types of malicious code detection.

Recently, most of the researchers have compared the rule-based with machine learning systems and concluded that rule-based algorithms are more efficient and productive. However, the rule-based techniques cannot detect attacks for which it has no signature while machine learning-based techniques are able to do that and have a lower false-positive rate. Another key milestone was the use of classical machine learning algorithms to build intruder detection systems (IDSs). Although deep learning is computationally more expensive as compared to traditional machine learning techniques, their results are found to be more effective in some cases. Additionally, convolutional neural networks mostly used for image processing proposed a CNN model for IDS with KDDCup of 1999 and after comparing their results with other existing algorithms, they concluded that CNN is superior. Another deep learning-based intrusion detection approach proposed by Yin et al. [14] used recurrent neural networks.

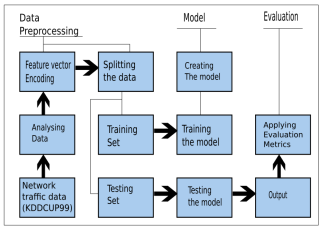
III. PROPOSED FRAMEWORK

The overall framework of the network intrusion detection system alert administrators when it detects the various security breaches inside an organization. Deep learning has reaped tremendous success in different application domains. We proposed a multi-classifier framework powered by a deep neural network for categorizing the intruders. For building a powerful Intrusion detection system, it is essential to provide features that describe information regarding the network traffic. After feeding the first layer with these features, MCDNN applies nonlinear transformation onto its input layer and create a statistical model of what it learned. Fig. 2 (a) illustrates the stepwise workflow of the proposed MCDNN approach. The MCDNN is a feed-forward neural network that has four layers, as presented in Fig. 2 (b) the layers of MCDNN are fully connected where each layer takes all neurons in the previous layer and connects it to a single neuron it has.

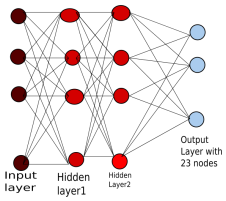
IV. EXPERIMENTAL RESULTS

A. Dataset Description

KDDCUP99 was part of the DARPA project in 1998 where the MIT Lincoln Lab set up an environment where they



(a) Workflow in MCDNN framework



(b) Network Architecture

Fig. 2: An overview of the Proposed MCDNN architecture (a) Workflow (b) Network architecture

used nine weeks to record data in any way from the US air force traffic [15]. It has been a point of interest for research community related to intrusion detection for about last two decades. Many researchers have exploited its tricky design and heterogeneous nature of data elements for different research objectives. They just wanted to have a real network traffic data and they got like five millions of collections. The KDDCUP99 dataset has 494020 number of instances with 42 attributes. There are four main types of attackers in this dataset:

- Denial of service (Dos): An attacker seeks to make a computer or network unavailable to its intended users by disrupting services of a host connected to the Internet.
- Probing-Attack: The type in which the attacker tries to gather information about the machine and attempt to bypass the firewall and gaining root access.
- Remote-to-Local-Attack (R2L): Attacker sends data packets to the target but has no user account of the system and he tries to exploit the vulnerability to get access.
- User-To-Root (U2R): Attacker tries to gain local account privilege for unauthorized access.

B. Data Preprocessing

For each network traffic record in 41 different features of the KDDCUP99 dataset, there are 3 non-numeric features in all features. In our experiments, we transformed the type of three features into the numeric type. The conversion process is listed as follows [6]: (i) TCP, UDP, and ICMP in the protocol type feature are marked as 1, 2, and 3, respectively. We split the dataset into two parts; training set (75%) and testing set(25%). Before feeding the training set to our neural network, we normalized all instances from 0 to 1.

C. Evaluation Metrics

The effective of the proposed MCDNN model is evaluated using standard metrics; Precision(PR), Recall(RC), F-score, Accuracy(ACC), True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) in Fig.5. Where true positive takes place when the MCDNN model predicts an attacker when there was no attack and false positive happens when it predicts not attacker when in fact there was an attacker. The true positive rate is also referred to as sensitivity or recall where sensitivity = True Positives / (True Positives + False Negatives). The false-positive rate is also referred to as the inverted specificity where specificity is the total number of true negatives divided by the sum of the number of true negatives and false positives.

$$Precesion = \frac{TP}{TP + FP} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$F_1 - Score = \frac{2 * PR * RC}{PR + RC} \tag{3}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

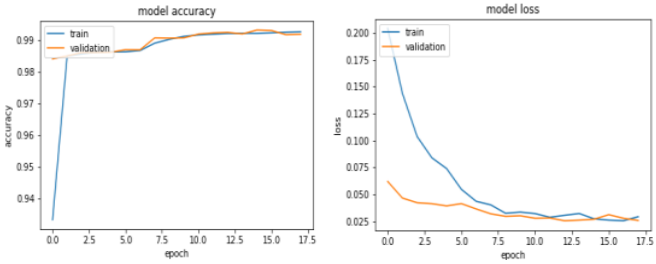


Fig. 3: Validation Accuracy and Loss of MCDNN model

TABLE I: Performance of Proposed MCDNN on each class of KDDCUP99 (Test Set), the acronym F1 is used $F_1 - Score$

Classes	Attack Type	Precision	Recall	F1	Support
back	Dos	1.00	0.99	0.99	541
buffer_overflow	U2R	0.00	0.00	0.00	11
ftp_write	R2L	0.00	0.00	0.00	1
guess_passwd.	R2L	0.00	0.00	0.00	10
imap	R2L	0.00	0.00	0.00	3
ipsweep	Probe	0.73	0.99	0.84	324
land	Dos	0.00	0.00	0.00	5
loadmodule	U2R	0.00	0.00	0.00	2
multihop	R2L	0.00	0.00	0.00	2
neptune	Dos	0.99	1.00	0.99	26708
nmap	Probe	0.00	0.00	0.00	52
normal	97278	1.00	1.00	1.00	24267
perl	U2R	0.00	0.00	0.00	2
pod	Dos	0.00	0.00	0.00	46
portsweep	Probe	0.00	0.00	0.00	287
rootkit	U2R	0.00	0.00	0.00	1
satan	Probe	0.41	0.98	0.58	388
smurf	Dos	1.00	1.00	1.00	70336
teardrop	Dos	0.00	0.00	0.00	240
warezclient	R2L	0.00	0.00	0.00	274
warezmaster	R2L	0.00	0.00	0.00	6

D. Experimental Settings

We used softmax activation function for the output layer, rectifier linear unit for hidden layers and stochastic gradient descent (SGD) for an optimizer. The softmax layer is used to compute the log-loss of model prediction, and stochastic gradient descent is an iterative learning algorithm that uses a

training dataset to update a model. The MCDNN has a total of 2327 trained parameters and zero non-trained parameters, a learning rate of 1e-3, and to avoid overfitting we applied the early stopping method with the patience = 5, that is the number of epochs with no improvement after which training will be stopped, and ran optimization for a total of 1000 epochs.

The MCDNN was trained for each category class to determine the performance of the algorithm on individual classes. Table III shows the experimental results. The MCDNN is implemented on a 64-bit Ubuntu 18.04 Operating System with 8 GB of RAM, 2.20GHz CPU, and GTX 1050 Graphic Card. Tools used are Keras library which uses TensorFlow backend, and Python programming language for numerical computations.

E. Comparison of MCDNN and other Classical Algorithms

The object of deep learning framework is to independently learning feature space. The proposed framework learn features automatically at multiple levels of abstraction, therefore, it can discover the complicated functions mapping between input and output directly from raw data. We select 6 state-of-the-art methodologies of intrusion detection for comparing the performance of our proposed MCDNN method. Our experimental results demonstrate that MCDNN has outperformed compared to other classical deep learning algorithms. Table II presents the resulting values against selective measures and a comparative analysis of MCDNN and other selected state-of-the-art methods.

TABLE II: Performance Evaluation of MCDNN and other Classical Algorithms on KDD99

Algorithm(s)	Accuracy	Precision	Recall	$F_1 - Score$	Year
(CNN) [16]	0.946	–	–	–	2017
(DNN-3) [17]	0.93	0.99	0.915	0.955	2018
(DNN-2) [17]	0.92	0.998	0.914	0.954	2018
(Decision Tree)	0.92	0.999	0.912	0.953	2018
(K-NN)	0.92	0.998	0.915	0.955	2018
(SVM)	0.81	0.99	0.977	0.868	2018
(MCDNN)	0.993	0.989	0.991	0.992	–

V. Conclusion

In this paper, we considered the problem of detecting intruder behavior in network traffic. We developed a Multi-Classifier Deep Neural Network (MCDNN) framework and experimentally evaluated it on the KDDCUP99 dataset, which commonly employed for testing real-world application of malicious behavior classification in network traffic. Our proposed model has outperformed compared to other classical machine learning algorithms. We believe that the current work can be a key milestone for the research community in this hot research domain. We are working to further extend the MCDNN model by utilizing Transfer learning capabilities with the same network architecture.

References

[1] D. Larson, "Distributed denial of service attacks - holding back the flood," *Network Security*, vol. 2016, no. 3, pp. 5–7, 2016.

[2] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, 2019.

[3] M. Tan, J. Yu, H. Zhang, Y. Rui, and D. Tao, "Image recognition by predicted user click feature with multidomain multitask transfer deep network," *IEEE Trans. Image Processing*, vol. 28, no. 12, pp. 6047–6062, 2019.

[4] T. Tan, Y. Qian, H. Hu, Y. Zhou, W. Ding, and K. Yu, "Adaptive very deep convolutional residual network for noise robust speech recognition," *IEEE/ACM Trans. Audio, Speech & Language Processing*, vol. 26, no. 8, pp. 1393–1405, 2018.

[5] W. Zhao, Z. Guan, L. Chen, X. He, D. Cai, B. Wang, and Q. Wang, "Weakly-supervised deep embedding for product review sentiment analysis," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 1, pp. 185–197, 2018.

[6] K. A. A. T. S. ALI Waqar, SHAO Jie, "Context-aware recommender systems: Challenges and opportunities," *Journal of University of Electronic Science and Technology of China*, vol. 48, no. 5, p. 655, 2019.

[7] A. B. Sargano, X. Wang, P. Angelov, and Z. Habib, "Human action recognition using transfer learning with deep representations," in *2017 International Joint Conference on Neural Networks, IJCNN 2017, Anchorage, AK, USA, May 14-19, 2017*, pp. 463–469, 2017.

[8] S. Venkatraman, M. Alazab, and R. Vinayakumar, "A hybrid deep learning image-based analysis for effective malware detection," *J. Inf. Sec. Appl.*, vol. 47, pp. 377–389, 2019.

[9] K. He and D. Kim, "Malware detection with malware images using deep learning techniques," in *18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 13th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE 2019, Rotorua, New Zealand, August 5-8, 2019*, pp. 95–102, 2019.

[10] N. A. Golilarz, H. Gao, W. Ali, and M. Shahid, "Hyper-spectral remote sensing image de-noising with three dimensional wavelet transform utilizing smooth nonlinear soft thresholding function," in *2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 142–146, Dec 2018.

[11] R. S. Naoum, N. A. Abid, and Z. N. Al-Sultani, "An enhanced resilient backpropagation artificial neural network for intrusion detection system," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 12, no. 3, p. 11, 2012.

[12] Y. Zhang, C. Rong, Q. Huang, Y. Wu, Z. Yang, and J. Jiang, "Based on multi-features and clustering ensemble method for automatic malware categorization," in *2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, August 1-4, 2017*, pp. 73–82, 2017.

[13] J. Drew, M. Hahsler, and T. Moore, "Polymorphic malware detection using sequence classification methods and ensembles," *EURASIP J. Information Security*, vol. 2017, p. 2, 2017.

[14] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[15] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009, Ottawa, Canada, July 8-10, 2009*, pp. 1–6, 2009.

[16] M. M. U. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, and J. Li, "A few-shot deep learning approach for improved intrusion detection," in *8th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017, New York City, NY, USA, October 19-21, 2017*, pp. 456–462, 2017.

[17] K. Rahul Vigneswaran, R. Vinayakumar, K. Soman, and P. Poornachandran, "Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, July 2018.