NETWORK INTRUSION DETECTION METHODS: A COMPARATIVE STUDY

Aswathy K P[1] Vimal Kumar D[2]

[1]Research scholar, [2]Associate professor Department of Computer Science, Nehru Arts and Science College,Coimbatore- 641105

----------***----------

Abstract

Internet is a wide platform which is used by the people all over the world. Nowadays the use of internet is gradually increasing. Internet changes our lively activities beyond an extent. There are somany things for they use internet like study, work or even live. People share their privacies through this platform without knowing the risk included. So, in recent years the intrusion detection system plays very important role in the security of network. Network intrusion means any attempt which affect the integrity, confidentiality or availability of the host or network. The paper discusses about different methods to detect thenetwork intrusion by using different technique. One method is a deep learning approach for intrusion detection using a multi-convolutional neural network (multi-CNN) fusion method. The other proposes a novel multi-stage optimized ML- based network intrusion detection systems (NIDS) framework that reduces computational complexity while maintaining its detection. The third one proposes the PSO-Xgboost model given its overall higher classification accuracy than other alternative models such like Xgboost, Random Forest, Bagging and Ad boost.

Key words: NIDS, Multi CNN Fusion, Multi stage optimized, PSO-Xg boost

1. INTRODUCTION

Nowadays internet is an essential part of daily lives. We cannot do anything without the help of internet. Our studies, works, communication and entertainment all are depending on internet. This dependence is coupled with these individuals and organizations' concern about the security and privacy of their online activities. With the rapid development of the Internet, artificial intelligence and big data technologies, network security confronts more complicated threats than ever before. There are so many resources which are being allocated to protect the modern network systems from attacks. There are so many such mechanisms like fire wall, user authentication and deployment of antivirus as a first level defence to protect the network. However, all these mechanisms are not sufficient to completely protect the network attack. A **network-based intrusion detection system** (**NIDS**) is used to monitor and analyse network traffic to protect a system from network**-**based threats. A **NIDS** reads all inbound packets and searches for any suspicious patterns.

Generally, a Network Intrusion Detection System is divided into two categories. One is signature-based detection systems (misused detection) and the other is anomaly-based detection systems. Signature-based detection systems perform their detectionon the basis of observation of pre-defined attack patterns. Thus, they have proven that it is effective only for well-known signature patterns. Therefore, the system is inefficient to detect a new attack because of their inability to find patterns for previous observations. On the other hand, anomaly-based detection system performs their

detection on the basis of their observations of pattern or behaviour which has any deviation from the normal. So that this system can detect any new attacks without any previous knowledge based on the built-in model.

There are so many techniques used to detect the network intrusion. This paper compares some methods in detail. In recent years deep learning is new widely used for detection of network intrusion. Deep learning has a potential to represent bulk of data to process and give better results. The recent development in deep learning was CNN. By using this CNN fusion method, we can detect the network intrusion. One method we are discussing in this paper is the multi-CNN fusion method in the detection. The other method discussing is the multi-staged optimized ML based NIDS framework which reduces the computational complexity while maintaining its detection. For that purpose, this method uses oversampling method. Moreover, different ML hyper-parameter optimization techniques are investigated to enhance the NIDS's performance and ensure its effectiveness and robustness. one of the most widely used swarm intelligence algorithms. The third method proposes a PSO-Xgboost model that combines swarm intelligence optimization with machine learning algorithm. In this hybrid model, the parameters of the Xgboost model are optimized by using the good search ability of PSO. All these methods detect the network intrusion in different way.

2. Related work:

Machine learning methods have been widely used to identify various types of attacks, and they can help network administrators take appropriate measures to prevent intrusions. The authors propose a three-layer RNN architecture with 41 features as inputs and 4 intrusion categories as outputs. . Torres et al. [19] transformed feature data into a sequence of characters and then learn their temporal features using RNN. Wang et al. [24] used a CNN to learn the spatial features of network traffic data, which were further applied to malware traffic classification. Similarly, several previous works focused on the use of ML classification techniques for network intrusion detection. Salo et al. conducted a literature survey and identified 19 different data mining techniques commonly used for intrusion detection. PSO and its variants are widely used in network intrusion detection. Tan et al. proposed to use PSO algorithm to optimize deep belief network (DBN) and apply it to network intrusion detection. Sakr et al. [26] applied the PSO-SVM algorithm to network intrusion detection in cloud computing, by using binary-based PSO (BPSO) for network feature selection, and standard-based PSO (SPSO) to adjust control parameters of SVM. In this paperwe discuss the three methods of networkintrusion in detail.

3. METHODS:

3.1 Multi CNN Fusion

Convolutional neural network plays an important role in so many areas recenltly.it takes advantage upon traditional neural network. CNN will learn different levels of feature from unlabelled data. In multi-CNN fusion method first take the network traffic data and it undergo pre-processing technique. After pre-processing we use CNN structure for different parts of the dataset. For developing the training dataset CNN is implemented in intrusion detection in the binary classification. In data segmentation part the featured data

is divided into four parts and each part is processed using the CNN structure. Multi CNN fusion methods takes advantage over single CNN method. Then the accuracy is better in multi-CNN fusion model

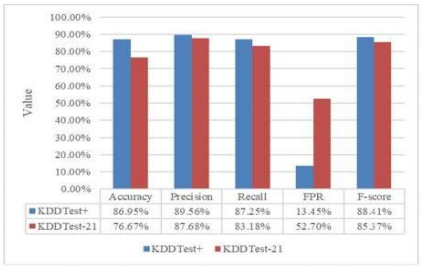

Fig. 4. The detailed performance of the multi-CNN fusion model in the binary classification.

Multi CNN Fusion Model

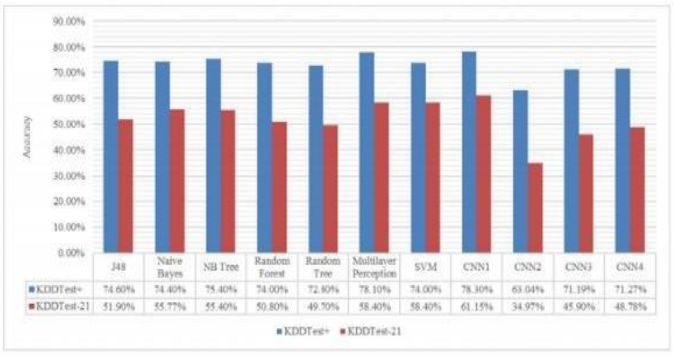

Fig. 5. Performance of the single CNN model and other traditional machine learning models in multiclass classification.

Single CNN Model

3.2 Multi Stage Optimized ML frame work:

The multi-stage optimized ML framework reduces the complexity and enhances detection accuracy. The detection takes place with a minimum sample size, but suitable one. Propose and investigate different ML hyper-parameter optimization techniques and their corresponding enhancement of the NIDS detection. There are different stages in the framework with different functionalities. The meta heuristic optimization include two types of algorithms. PSO and GA. The proposed multi-stage optimized ML-based NIDS framework is a signature-based NIDS system. Thus, the framework learns from the observed patterns of the known initiated attacks. The effectiveness and robustness of the proposed multi-stage optimized ML-based NIDS framework as it outperformed other NIDS frameworks.

3.3 PSO-Xgboost model:

The previous model discusses the PSO algorithm(particle swarm optimization). this paper proposes the PSO-Xgboost model given its overall higher classification accuracy than other alternative models such like Xgboost, Random Forest, Bagging and Adaboost. Firstly, a classification model based on Xgboost is constructed, and then PSO is used to adaptively search for the optimal structure of Xgboost. This paper proposes a PSO-Xgboost model that combines swarm intelligence optimization with machine learning algorithm. In this hybrid model, the parameters of the Xgboost model are optimized by using the good search ability of PSO. a novel model PSO-Xgboost based on Xgboost by using PSO to adaptively optimize its parameters. This can effectively improve the performance of network intrusion detection, including the improvement of the detection accuracy of various types of attacks, especially on minority groupsof attacks. To evaluate the PSO-Xgboost model's performance, we measure not only the overall metrics but also the metrics of each class, and compare them with Xgboost and other ensemble learning models (like Random Forest and Bagging). Xgboost model can be effectively applied to overcome multi-

classification problems. PSO can achieve approximate optimal solution at a fast rate. So Xgboost by PSO algorithm will give us better results.

Conclusion:

Improving the detection accuracy of NIDS is an important issue in the field of network security. Accordingly, different types of network intrusion detection systems (NIDSs) have been compared in the literature. Despite the continuous improvements in NIDS performance, there is still room for further improvement. In this paper, a network intrusion detection model was discussed, implemented and trained using different single CNN models and a multi-CNN fusion model. Compared with well-known machine learning classification methods and the latest deep learning algorithms, the multi-CNN fusion model obtained better results on any other machine learning algorithms. On the other hand, the multi-stage optimized ML framework extends the previous method to reduce the computational complexity. This uses high dimensional datasets and need for real time intrusion detection. So some deep learning classifiers can be explored this method as it uses high dimensional datasets. The third one discusses PSO algorithm with Xgboost model. Xgboost model can be effectively applied to overcome multi-classification problems. PSO can achieve approximate optimal solution at a fast rate. This paper discusses the method of optimizing the Xgboost model by PSO. The experimental results is higher when compared with other models such as Random Forest, Bagging and Adaboost.

References:

[1] Y. Y. Chung and N. Wahid, "A hybrid network intrusion detection system using simplified swarm optimization (sso)," Applied Soft Computing, vol. 12, no. 9, pp. 3014–3022, 2012

[2] ——, "Multi-split Optimized Bagging Ensemble Model Selection for Multi-class Educational Datasets," Applied Intelligence, 2020

[3] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," IEEE Access, vol. 6, pp. 56 046–56 058, 2018.

[4] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, ''Deep learning approach combining sparse autoencoder with SVM for network intrusion detection,'' IEEE Access, vol. 6, pp. 52843–52856, 2018.

[5] M. M. Sakr, M. A. Tawfeeq, and A. B. El-Sisi, ''Network intrusion detection system based PSO-SVM for cloud computing,'' Int. J. Comput. Netw. Inf. Secur., vol. 11, no. 3, pp. 22–29, Mar. 2019

[6] X. Li, Y. Guo, and Y. Li, ''Particle swarm optimization-based SVM for classification of cable surface defects of the cable-stayed bridges,'' IEEE Access, vol. 8, pp. 44485–44492, 2020.

[7] P. Torres, C. Catania, S. Garcia, C.G. Garino, An analysis of recurrent neural networks for botnet detection behaviour, in: 2016 IEEE biennial congress of Argentina (ARGENCON), IEEE, Buenos Aires, Argentina, 2016, pp. 1–6