International Journal for Modern Trends in Science and Technology, 8(06): 188-191, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0806029
Available online at: http://www.ijmtst.com/vol8issue06.html

A Deep Learning Approach for Effective Intrusion Detection in Wireless

Dr.B.Raja Srinivasa.Reddy[1], K.Bhavana[2], P.Tejeswari[2], V.Komala Sri[2], B.V.N.Kishore[2]

[1]Professor, Department of Computer Science & Engineering, Sri Vasavi Institute of Engineering & Technology, Pedana, A.P, India
[2]Department of Computer Science & Engineering, Sri Vasavi Institute of Engineering & Technology, Pedana, A.P, India

To Cite this Article
Dr.B.Raja Srinivasa.Reddy, K.Bhavana, P.Tejeswari, V.Komala Sri and B.V.N.Kishore. A Deep Learning Approach for Effective Intrusion Detection in Wireless. International Journal for Modern Trends in Science and Technology 2022, 8(06), pp. 185-187. https://doi.org/10.46501/IJMTST0806029

Article Info
Received: 09 May 2022; Accepted: 02 June 2022; Published: 07 June 2022.

ABSTRACT

Security is playing a major role in this Internet world due to the rapid growth of Internet users. The various intrusion detection systems were developed by many researchers in the past to identify and detect the intruders using data mining techniques. However, the existing systems are not able to achieve sufficient detection accuracy when using the data mining. For this purpose, we propose a new intrusion detection system to provide security in data communication by identifying and detecting the intruders effectively in wireless networks. Here, we propose a new feature selection algorithm called conditional random field and linear correlation coefficient-based feature selection algorithm to select the most contributed features and classify them using the existing convolutional neural network. The experiments have been conducted for evaluating the proposed intrusion detection system that achieves 98.88% as overall detection accuracy. The tenfold cross validation has been done for evaluating the performance of the proposed model.

KEY WORDS: Deep learning, CNN, LCFS,CRF

1. INTRODUCTION

The rapid growth of computer networking technology is facilitating the comfort in the businesses, organizations and social communities. Simultaneously, different types of Internet security threats kept developing due to the regular rise of various vulnerabilities and attacking techniques. Hence, some security systems should be used for preventing the attacks and to provide the confidentiality as well as the availability of resources and integrity for the Internet communications. To determine and restrict the mischievous network traffic, intrusion detection system (IDS) has become the most important network security solution (Liao et al. 2013).

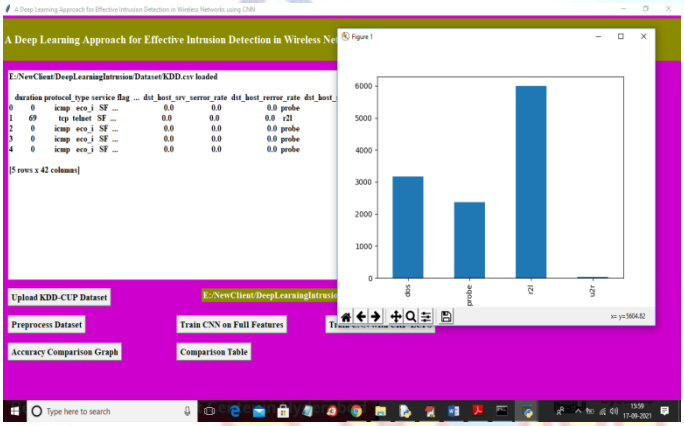
The major advantage of this CNN is used to reduce the number of selected features that are used to detect the attack types quickly (Wang and Li 2017). This CNN (Nguyen et al. 2018) has three layers, namely convolutional layer, pooling layer and fully connected layer. Moreover, these layers are shaped to form a complete convolutional architecture. These convolutional layers use more number of kernels (filters) for the given input features and generate various feature maps in the process. In addition, the pooling layer of CNN is used to shorten the dimensions of the feature map to reduce the processing time. Finally, the fully connected layer performs the classification process on the extracted features from the convolutional and pooling layers. Here, each node in

this fully connected layer is connected to every node of the previous layer.

2. PRORPSED SYSTEM

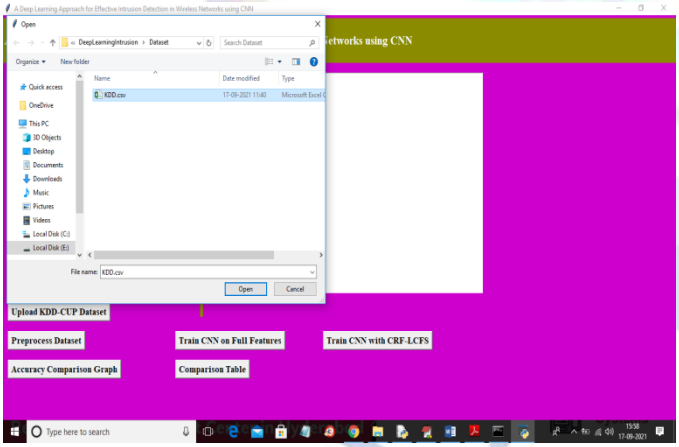
Author extracted relevant features from dataset by applying CRF-LCFS algorithm and then extracted features will be trained with CNN algorithm.

CNN algorithm can be define with multiple layers and each layer will build a features map and then CNN will trained model by extracting important features. CNN trained model can be used to predict attack from network packets.

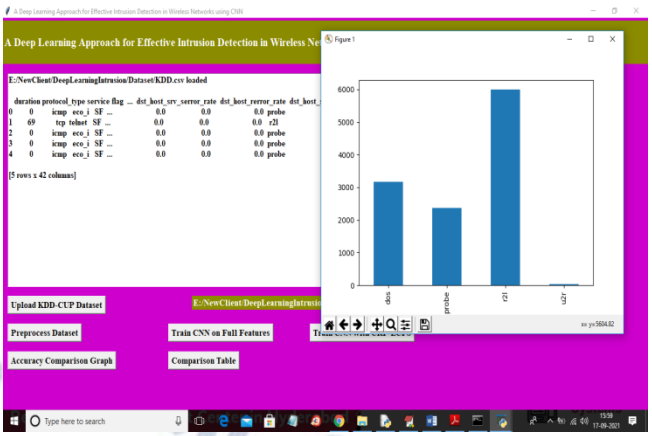


3. PROPOSED ALGORITHM

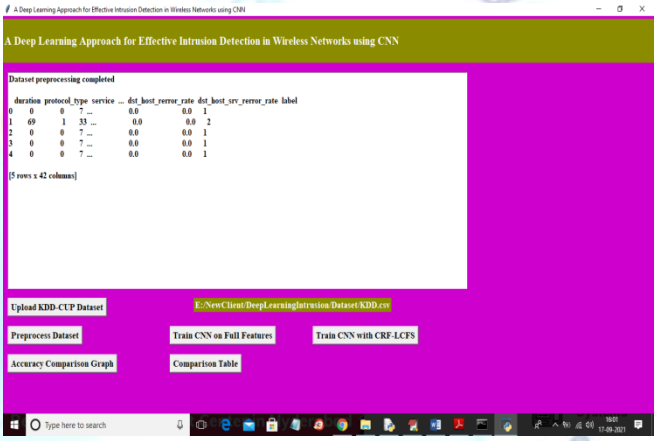
In above screen click on 'Upload KDD-CUP dataset' button to upload dataset and to get below screen



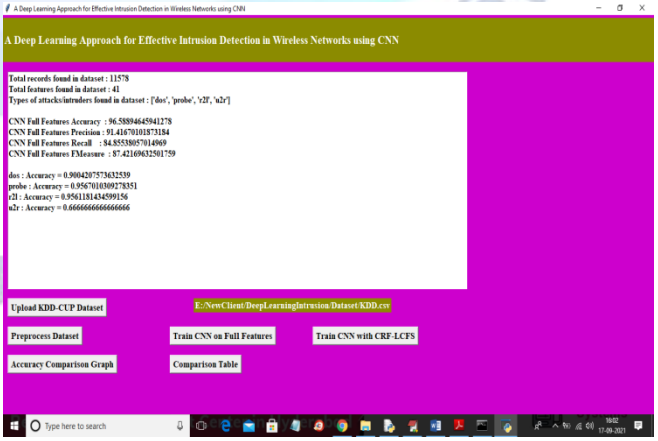
In above screen selecting and upload 'KDD.csv' dataset and then click on 'Open' button to get below output



In above screen we can see dataset loaded and some values are non-numeric and CNN will accept such values so we need to process them to assign numeric id to each non-numeric values. In above graph x-axis represents attack name and y-axis represents total count of that attack. Now close above graph and then click on 'Preprocess Dataset' button to process dataset

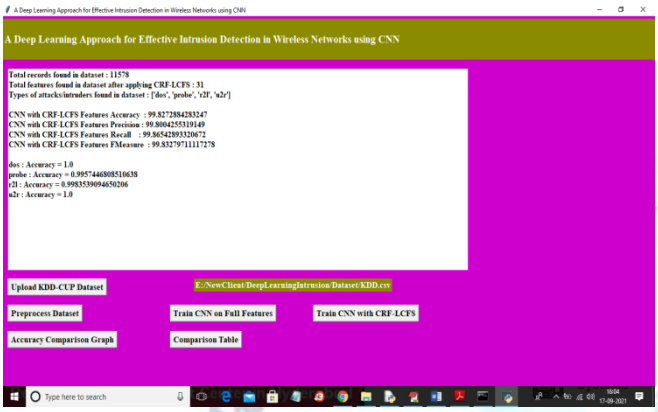


In above screen we can see all values are converted to numeric format and now click on 'Train CNN on Full Features' button to train CNN on all features and to get below screen

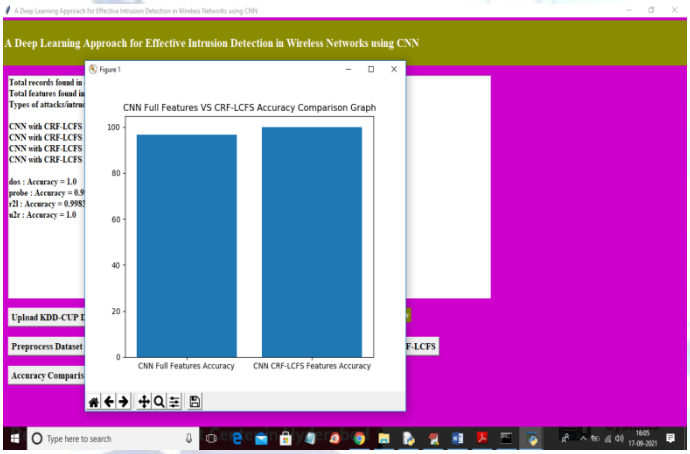


In above screen we can see CNN full features accuracy is 96% and then individually we calculate predicted accuracy of different attacks such as DOS, R2L, U2R and Probe. In above screen we calculate precision, recall and

FSCORE also. In above screen we can see dataset contains total 41 features. Now click on 'Train CNN with CRF-LCFS' button to train CNN with CRF selected features and to get below output

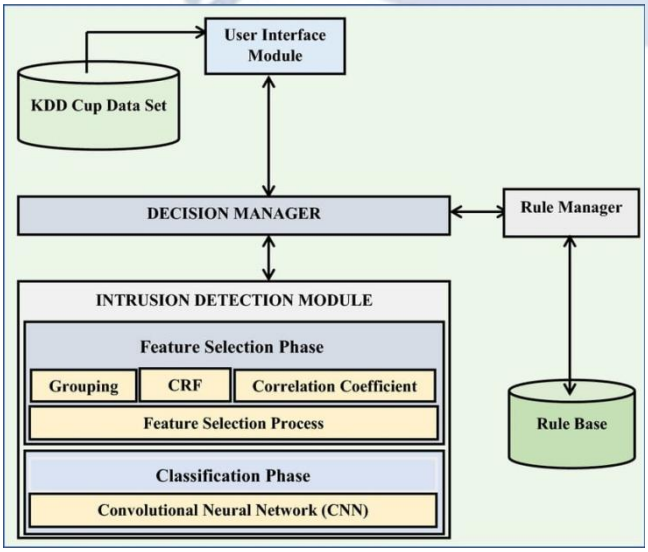


In above screen we can see selected features are 31 and we got CNN CRF accuracy as 99% which his higher than CNN with full features and now click on 'Accuracy Comparison Graph' button to get below graph

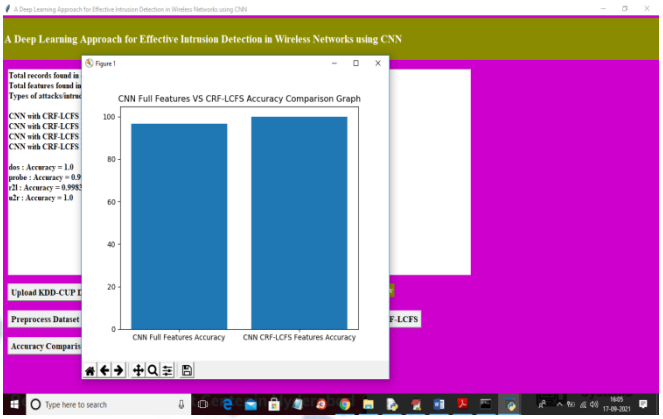


In above graph x-axis represents technique name and y-axis represents accuracy of that technique and in above graph we can see CNN with CRF has got high accuracy.

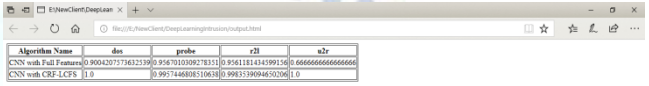
4. FLOW CHART



5. RESULTS



OUTPUT



Algorithm Name	dos	probe	r2l	u2r
CNN with Full Features	0.9004207573632399	0.9567010309278351	0.9561181434599156	0.6666666666666666
CNN with CRF-LCFS	1.0	0.9957446808510638	0.9983539094650206	1.0

6. CONCLUSION

In this paper, a new intrusion detection system has been proposed and implemented for identifying and detecting the intruders effectively in wireless networks. The proposed intrusion detection system uses a newly proposed feature selection algorithm called conditional random field and linear correlation coefficient-based feature selection (CRF-LCFS) algorithm and an existing convolutional neural network (CNN) for performing intrusion detection. The major contribution of this paper is to the introduction of conditional random field for selecting two variables that are used in the existing correlation coefficient variancebased feature selection algorithm. Moreover, it is useful for selecting the most important features that are used to enhance the classification accuracy of deep learning approach. In addition, the CNN is also helpful for improving the performance in terms of attack detection accuracy. Finally, the proposed model achieved better performance in terms of detection accuracy (98.8%), less training(0.57 s) and testing time(0.26 s) and the false alarm rate of proposed model is less than 1% when it is compared with the existing CNN. Future works in this direction could be the use of intelligent agents for

making effective decisions and also for enhancing the data communication speed.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Abualigah LMQ (2019) Feature selection and enhanced krill Herd algorithm for text document clustering. Studies in computational intelligence, vol 816. Springer, Switzerland

[2] Abualigah LM, Khader AT (2017) Unsupervised text feature selection technique based on hybrid particle swarm optimization algorithm with genetic operators for the text clustering. J Supercomputers 73(11):4773–4795 s

[3] Abualigah LM, Khader AT, Hanandeh ES (2017a) A new feature selection method to improve the document clustering using particle swarm optimization algorithm. J Comput Sci 25:456–466

[4] Abualigah LM, Khader AT, Hanandeh ES, Gandomi AH (2017b) A novel hybridization strategy for krill herd algorithm applied to clustering techniques. Appl Soft Comput 60:423–435

[5] Abualigah LM, Khader AT, Hanandeh ES (2018a) A combination of objective functions and hybrid krill herd algorithm for text document clustering analysis. Eng Appl Artif Intell 73:115–123