IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 5, March 2019 E-ISSN: 2347-2693

A Study on Deep Learning approach for Network Intrusion Detection

S. Venkata lakshmi[1*], T.Edwin Prabakaran[2]

[1]Dept. of Computer Science, Loyola College, Chennai, India
[2] Dept. of Statistics, Loyola College, Chennai, India

[*]*Corresponding Author: jaibv2012@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7si5.221224 | Available online at: www.ijcseonline.org

Abstract— Deep learning is a part of the broader family of Machine Learning. It refers to learning multiple levels of representation and abstraction that helps to understand data such as images, sound and text. This paper aims at giving an overview of deep learning, its applications and an approach for Network Intrusion Detection. KDDCup dataset is used for Intrusion detection and a comparison of different deep learning techniques applied for Intrusion Detection is made. A special focus is given on Self taught learning using Sparse Coding and its usage in classification. Self taught learning (STL) is a machine learning framework for using unlabeled data in supervised classification tasks. It is a deep learning approach that comprises of two stages for the classification task. Initially, a good feature representation is learnt from a large collection of unlabeled data, called as Unsupervised Feature Learning (UFL). Finally, the learnt representation is applied to labeled data and then classification task is performed.

Keywords— Network Intrusion Detection, Classification, Deep Learning, Self-Taught Learning.

I. INTRODUCTION

Intrusion is defined as any set of action that can compromise the integrity, confidentiality and availability of system resources [1]. Network Intrusion Detection Systems (NIDSs) are the important tools for the network administrators to detect several security breaches in a network. There are two types of NIDSs namely signature based / misuse detection and anomaly detection[11]. In Signature based Network Intrusion Detection System (SNIDS), the rules or signatures are pre-installed whereas in Anomaly Detection Network Intrusion Detection System (ADNIDS) an intrusion is detected whenever a deviation from the normal traffic is observed. ADNIDS aims at identifying unknown patterns in network data.

SNIDS is very effective in the detection of known attacks but it fails to detect novel attacks. On the other hand, ADNIDS is capable of detecting unknown and novel attacks. There also lies a shortcoming in ADNIDS because it produces high false positive rates[10]. Researchers are with the opinion that proper feature selections from the network connection records for anomaly detection is difficult. This is because the attack scenarios are continuously evolving and the features that are selected for one class of attack may not suit for other classes of attacks. The next challenge with respect to Anomaly detection is that we do not have sufficient labelled traffic dataset from real networks.

The paper is organized as follows: Section 2 gives an introduction about KDD Cup Intrusion dataset. Section 3 explains the different types of attacks in the dataset. Section 4 gives an introduction of machine learning and deep learning. Section 5 gives a brief explanation about deep learning and the different techniques of deep learning. Section 6 lists the applications of deep learning. Section 7 discusses about the usage of deep learning in network intrusion detection and the performance metrics used. Section 8 gives the results of the study. Section 9 presents the conclusion.

II. INTRUSION DATASET

The **KDD Cup dataset** is considered to be the benchmark dataset in Intrusion detection [7]. The dataset is a collection of simulated raw TCP dump data over a period of time on a local area network. The known attack types are those present in the training dataset while the novel attacks are the new attacks which are not present in the training dataset. Various attacks are Buffer overflow, Perl, Portsweep, Neptune, Smurf, Teardrop, Guess password, IPSweep etc., The training dataset consists of 4,94,021 records. The testing dataset consists of 3,11,029 records. In each connection record there are 41 attributes describing various features of the connection. In the training dataset, a class attribute is given along with the 41 attributes. The attributes are protocol_type, service, flag, src_bytes, dest_bytes,

wrong_fragment, logged_in, count, etc., The features / attributes include the basic features derived directly from a TCP/IP connection, traffic features obtained from a window interval and the content features obtained from the application layer. One of the major drawback with this dataset is that it contains a large amount of redundant records in the training as well as testing dataset. And another drawback is the unequal distribution of the different types of attacks in the dataset.

III. TYPES OF ATTACKS IN THE KDD CUP DATASET

Denial of Service (DoS) : A DoS attack is a type of attack in which the perpetrator makes a computing or memory resource too busy or too full to serve legitimate networking requests and thereby denying the users to access the target system. This is generally done by flooding the target system.

Probe: Probing is an attack in which the intruder scans a system or a networking device in order to find out the weaknesses or vulnerabilities that may later be exploited to compromise the system.

Remote to Local (R2L): A remote to local attack is an attack in which an attacker tries to gain unauthorized access to a victim machine in the network.

User to Root (U2R): User to root attacks are exploitations in which the intruder logins into the system with a normal user account and attempts to get the access rights in order to gain super user privileges [7].

IV. MACHINE LEARNING VERSUS DEEP LEARNING

Machine Learning algorithms are generally used to parse data, learn from the data and make informed decisions based on the learning [4][5][6][8][9]. Deep learning is used in layers to create an Artificial Neural Network that can learn and make intelligent decisions on its own.
Deep learning is a subfield of Machine Learning. Deep learning performs very well when the amount of data is vast. It may not perform well when less data is used.
Deep learning algorithms takes more time to train than the machine learning algorithms.

V. DEEP LEARNING AND ITS METHODS

Deep Learning is a subarea of the Machine Learning that makes use of Deep Neural Networks comprising of many layers and specific novel algorithms for the preprocessing of data and training of the model [3][12].
The following are the definitions of deep learning:

Deep Learning is a class of machine learning techniques that exploit many layers of non-linear information processing for supervised or unsupervised feature extraction and transformation, and for pattern analysis and classification.
A sub-field within machine learning that is based on algorithms for learning multiple levels of representation in order to model complex relationships among data.

Deep Learning is a new area of Machine learning research, which has been introduced with the objective of moving Machine Learning closer to one of its original goals, Artificial Intelligence.

DEEP NEURAL NET

Deep Neural Network is a multilayer perceptron, which was developed by stacking the linear classifiers. The most basic type is the Deep Neural network. The model is fed with inputs first and then the inputs get multiplied by weights and then passed into an activation function. If a model contains 3 or more layers, it is considered as a deep network.

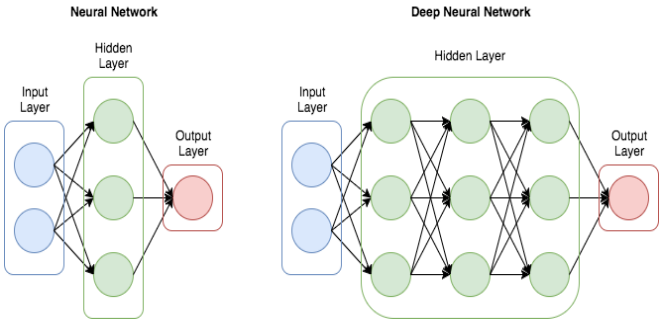

Fig. 1

SELF-TAUGHT LEARNING

Self-Taught Learning (STL) is a deep learning approach that comprises of two stages for the classification. At the first stage, a good feature representation is learnt from a large collection of unlabeled data, termed as Unsupervised Feature Learning (UFL). In the second stage, the learnt representation from the first stage is applied to the labelled data and thus used for the classification task.

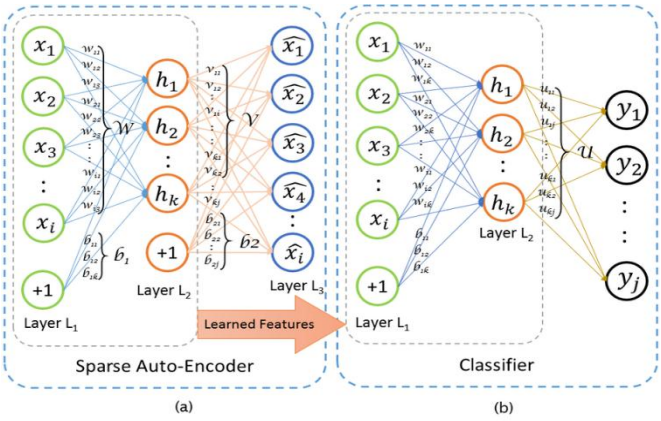

Fig. 2

RECURRENT NEURAL NEWORK (RNN)

These neural networks are a class of Artificial Neural Network. They take as their input not only the current input instance but also what they have perceived previously in time. An additional memory input is used here. In a RNN, the information cycles through a loop. The current input and also the learning from the previous inputs are taken into consideration for making a decision. A feed forward neural network assigns a weight matrix to its inputs and then produces the output. But, the RNN's apply weights to the current as well as the previous input. A RNN could be viewed as a sequence of Neural Networks that is trained one after another with backpropagation.

Long Short Term Memory (LSTM) networks are an extension of RNNs, which basically extends their memory. In other words, LSTM's enable RNNs to remember their inputs over a long period of time. In a LSTM, there are three gates namely input, forget and output gate.

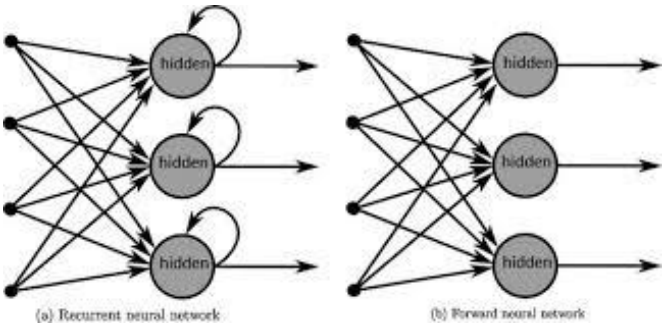

Fig. 3

VI. APPLICATIONS OF DEEP LEARNING

There are several applications of deep learning namely, Colorization of Black and White Images, Adding Sounds, Object Classification in Photographs, Automatic Handwriting Generation, Character Text Generation, Image caption generation, Automatic Game Playing etc.,
Self driving cars, Healthcare, Voice Search and voice activated assistants, Automatic Machine Translation, Automatic Text Generation, Predicting Earthquakes and so on.

VII. DEEP LEARNING IN NETWORK INTRUSION DETECTION

Deep learning was inspired by the structure and depth of human brain. Deep Network Intrusion Detection systems can be classified based on how the techniques are being used. There are some models which are proposed for analysis namely, vanilla deep neural net classifier, self-taught learning model using autoencoder and the third is the Recurrent Neural Network.

The performance of deep learning techniques is measured on the following metrics:

Accuracy: It is defined as the percentage of correctly classified records over the total number of records.

Precision (P): It is defined as the % ratio of the number of true positives (TP) records divided by the number of true positives (TP) and false positives (FP) classified records.

$$P = TP / (TP + FP) * 100\%$$

Recall (R) : It is defined as the % ratio of number of true positives divided by the number of true positives and false negatives (FN) classified records.

$$R = TP / (TP + FN) * 100\%$$

f-Measure (F) : It is defined as the harmonic mean of precision and recall and represents a balance between them.

$$F = 2.P.R / (P + R)$$

VIII. RESULTS OF THE STUDY

As per the study made on the related papers, the deep neural network attained an accuracy of 66%. The model was able to classify DoS and probe attacks well. But this model failed to identify U2R attacks.

The STL approach has attained an accuracy of 98.9%. In this approach too, since the distribution of R2L and U2R type of attacks are low, it is observed that the precision and recall of these attack types are low when compared to the other attack types.

The LSTM model has an accuracy of 79.2%. This model fails to predict attacks other than DoS. Again the reason could be the higher distribution of DoS instances in the dataset [3].

The NIDS for three different types of classification (i) Normal and Anomaly (2-class), (ii) Normal and four different attack categories (5-class) , (iii) Normal and 22 different attacks (23-class) is implemented. The model evaluation metrics for this were Accuracy, Precision, Recall and f-Measure. A deep learning based approach to build an effective NIDS is proposed. A sparse auto-encoder and soft-max regression based NIDS is also implemented. NSL-KDD dataset is used to evaluate anomaly detection accuracy. It has been observed that this NIDS performed very well compared to the previously implemented NIDS [12].

IX. CONCLUSION

Many research works including ours [13][14][15][16][17][18][19] have used machine learning algorithms to classify the network connection records as

normal or attack record in intrusion detection. Classification algorithms like kNN, J48, Simple CART, Bagging and Random Forest are used and lot of research work is done in this area [2]. This paper is an attempt to study the possibilities of implementing Network Intrusion Detection System using Deep learning techniques. It is found that STL with Sparse encoding proves to be effective in implementing Network Intrusion Detection Systems with KDD Cup dataset when compared to other deep learning techniques. Further research could be done with deep learning techniques applied on real time network traffic. One of the biggest advantages of using deep learning is that it works best when the volume of data to be analyzed is more.

REFERENCES

[1]. Adebayo O. Adetunmbi, Samuel O. Falaki (2008). "*Network Intrusion Detection based on Rough Set and k-Nearest Neighbour*", International Journal of Computing and ICT Research, Vol.2, No.1, pp.60-66., http://www.ijcir.org/volume1number2/article7.pdf.

[2]. Bhatnagar and Vishal. (2014). "*Data Mining and Analysis in the Engineering Field*", IGI Global.

[3]. Brian Lee, Sandhya Amaresh, Clifford Green, Daniel. (2018). "*Comparative Study of Deep Learning Models for Network Intrusion Detection",* SMU Data Science Review", Vol.1, No.1.

[4]. Breiman, L. (2001). "*Random Forests*", Machine Learning, Vol.45, Issue 1, pp.5-32.

[5]. Dietterich, T.G. (2000). "*An Experimental Comparison of Three Methods for Constructing Ensembles of Decision Trees: Bagging, Boosting, and Randomization*", Machine Learning, Vol.40, Issue 2, pp.139–157.

[6]. Ho, T.K. (1998). "*The Random Subspace method for constructing decision forests*", IEEE transaction on Pattern Analysis and Machine Intelligence, Vol.20, Issue 8, pp.832-844.

[7]. KDD CUP DATASET (1999). http://kdd.ics.uci.edu/databases/kddcup99/

[8]. Kok-Chin Khor, et al (2009). "*From Feature Selection to Building of Bayesian Classifiers: A Network Intrusion Detection Perspective*", American Journal of Applied Sciences, Vol.6, No.11, pp.1948-1959.

[9]. Lee,W., Stolfo,S.J., and Mok, K.W. (1999). "*Algorithms for Mining System Audit Data*", Proceedings of KDD.

[10]. Neveen I.Ghali. (2009). "*Feature Selection for Effective Anomaly Based Intrusion Detection*", International Journal of Computer Science and Network Security, Vol.9, No.3, pp.285-289.

[11]. "*Understanding Intrusion Detection Systems*", SANS Institute InfoSec Reading Room.

[12]. Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, Mansoor Alam (2015). "*A Deep Learning Approach for Network Intrusion Detection System*", ACM Digital Library, BICT'15, pp.21-26.

[13]. Venkata Lakshmi, S. and Edwin Prabakaran, T. (2014). "*Application of k-Nearest Neighbour Classification Method for Intrusion Detection in Network Data*", International Journal of Computer Applications, (0975-8887) Vol.97, No.7, pp.34-37.

[14]. Venkata Lakshmi, S. and Edwin Prabakaran, T. (2014). "*A comparative study of classification of application of classification algorithms on KDDCup dataset to detect intrusions using WEKA tool*", International Journal of Engineering Research and Technology, Conference Proceedings of RACMS, pp.69-71.

[15]. Venkata Lakshmi, S. and Edwin Prabakaran, T. (2015). "*Performance Analysis of Multiple Classifiers on KDD Cup dataset using WEKA tool*", Indian Journal of Science and Technology, Vol.8, No.17, pp.1-10.

[16]. Venkata Lakshmi, S. and Edwin Prabakaran, T. (2015). "*Deployment of Models developed in Knowledge Flow Process using WEKA tool on KDDCup dataset*" presented in the International Conference on Information Technology organized by Thiruthangal Nadar College, Chennai.

[17]. Venkata Lakshmi, S. and Edwin Prabakaran, T. (2015). "*Feature selection and classification of network connection data into normal or attack records using WEKA tool*", Proceedings of the International Conference on Recent Trends in Computer Science and Digital Technology, ICCSDT-2015, pp.72-77, at Guru Shree Shanthi Vijay Jain college, Chennai and received the BEST PAPER AWARD.

[18]. Venkata Lakshmi, S. and Edwin Prabakaran, T. (2016). "*Feature selection and Identification of Attacks in Network connection records using classifiers in WEKA tool*", Proceedings of the WCC Centenary International Conference on Viable synergies in Mathematical and Natural Science, pp.215-227 at WCC, Chennai.

[19]. Venkata Lakshmi, S. and Edwin Prabakaran, T. (2018). "*Application of Ensemble, Voting and Stacking methods for Better Classification of Network Intrusion Detection and Improving the Performance of Random Forest Method by a new method of Feature Selection*", Mathematical Sciences International Research Journal, Vol.7, Spl.Issue 4, pp.6-16.

[20]. Xindong Wu (2008). "*Survey Paper, Top 10 algorithms in data mining*", Knowledge Information Systems, Vol.14, pp.1–37.

Authors Profile

Mrs. S.Venkata lakshmi pursued Bachelor of Science and Master of Computer Applications under University of Madras. She is currently pursuing Ph.D., and working as Assistant Professor in the Department of Computer Science, Loyola College, Chennai, India. She is a life member of Computer society of India since 2008. She has published 7 research papers in reputed international journals including Scopus indexed journals. Her research work focuses on Data Mining and Network Intrusion Detection. She has 12 years of teaching experience and 3 years of Research Experience.

Dr. T.Edwin Prabakaran pursued Bachelor of Science, Master of Science and Doctorate under University of Madras. He is currently working as the Associate Professor in the Department of Statistics, Loyola College, Chennai, India. He has published many papers in reputed International and National Journals. He has 31+ years of teaching experience and guided many M.Phil and Ph.D scholars.

