DEEP LEARNING MODELS FOR INTRUSION DETECTION SYSTEM

M.Menaha,

Assistant Professor,

Department of Computer Science,

A.V.V.M Sri Pushpam College,Poondi.

Abstract:

Intrusion detection system (IDS) is one of the implemented solutions against harmful attacks. Nowadays increase in internet usage and network technologies have led to extent increase in number of attacks and intrusions. Detection of these attacks and intrusion has become an important part of the security. Multiple deep learning approaches have been proposed for intrusion detection systems. In this paper, we evaluate three models, a Artificial Neural Network(ANN),Recurrent Neural Network (RNN) and Convolutional Neural Network(CNN) on their accuracy. Our works use the KDD data set in our experiments and obtain the expected results.

1. INTRODUCTION

With the rapid increase in the internet technologies and smart devices, the number of intrusion also increases. Intrusion is the act of intruding or of entering into a place or virtual place without proper authorization [1] [2]. For System security and confidentiality intrusion detection plays an important role. Intrusion Detection Systems (IDS) are important security tools used to detect possible attacks, inappropriate, incorrect or abnormal activities and to alert the occurrence to network administrators. The main goal of an intrusion detection system is to detect the attacks efficiently and it is also equally important to detect attacks at a beginning stage in order to reduce their impacts.

IDS is an important asset to computer security because attacker tries to conceal his identity and launch attacks through intermediate hosts widely known as stepping stones intrusion. Secondly, changing nature of technology and technique makes it more difficult to detect attacks. IDS can therefore make use of learning techniques to detect unknown future attacks. In short, the main motivation of intrusion detection is to improve the accuracy of classifiers in effectively identifying the intrusive behavior.

The rest of the paper has been structured in following ways: A brief outline of related studies is covered in

Section 2,Section 3 introduces the proposed method, experimental results are given in Section 4 and Conclusions and future directions are provided in Section 5.

2. RELEATED WORK

Several techniques have been applied to IDS. Some of the most important techniques are explained in following sub sections.

2.1 BAYESIAN NETWORK

A Bayesian network is a model that encodes probabilistic relationships among important variables. It is usually used for intrusion identification in combination with numerical schemes, a process that yields numerous advantages [3], including the capability of encoding interdependencies between variables and of predict events, as well as the ability to incorporate both prior knowledge and data.

2.2 MARKOV MODELS

There are two subtypes of Markov models: Markov chains and hidden Markov models. A Markov chain is a set of states that are consistent through certain change probabilities,which verify the topology and the capabilities of the model. During a first training phase, the probabilities associated with the transitions are estimated from the normal behavior of the target system. The detection of anomalies is then carried out by comparing the anomaly score (associated probability) obtained for the observed sequences with a fixed threshold. In the case of a hidden Markov model, the system of interest is assumed to be a Markov process in which states and transitions are hidden. Only the so-called productions are observable. Markov-based techniques have been extensively used in the context of host IDS, normally applied to system calls. A hybrid fuzzy-based variance IDS using hidden Markov model (HMM) detection engine and a normal database detection engine to reduce FAR is proposed in [4]. Development of host-based anomaly IDS has been studied with highlighting places on system call-based HMM training explained in [5].

2.3 GENETIC ALGORITHMS

Genetic algorithms are classified as global search heuristics, and evolutionary computation that uses techniques inspired by evolutionary biology such as recombination, selection, inheritance and mutation. Thus, genetic algorithms represent another type of machine learning-based technique, capable of deriving categorization rules [6] and/or selecting appropriate features or optimal parameters for the detection process [7].

2.4 CLUSTERING AND OUTLIER DETECTION

Clustering techniques work by grouping the observed data into clusters, according to a given similarity or distance measure. The procedure the majority commonly used for this consists in select a representative point for each cluster. Clustering techniques to determine the occurrence of intrusion events only from the raw audit data, and so the effort required to tune the IDS is concentrated. One of the most popular and most widely used clustering algorithms is K-Means [8], which is a nonhierarchical Centroid-based approach.

2.5 DATA MINING

Data mining is an information activity to find out hidden facts contained in the database. These techniques are used to find patterns and intelligent relationships in data and infer rules that allow the prediction of future result. Association rule learning is one of many data mining techniques that describe events that tend to occur together. Association rule discovery is to define normal activity by which discovery of anomalies is easily enabled. Classification is to classify each audit record into one of the possible categories normal and anomaly. In [9] authors discussed the uses of data mining approach in Intrusion Detection. This data mining technique works by learning the training data know to be free of attacks (normal)and then uses an algorithm group an attack from the data. It uses associates rules to store knowledge data about the nature of pattern about individual records that can improve the classification efficiency.

2.5 SUPPORT VECTOR MACHINES:

Support vector machine (SVM) was introduced in mid-1990's [10]. The concept following SVM for intrusion recognition basically is to use the training data as a explanation of only the normal class of objects or which is known as non-attack in intrusion detection system, and thus assuming the rest as anomalies [11]. The classifier construct by support vector machines methodology discriminate the input space in a limited region where the normal objects are contained and all the rest of the space is unspecified to hold the anomalies [12].

3. PROPOSED WORK

The proposed model is the Intrusion Detection System (IDS) using three deep learning model that is Artificial Neural Network(ANN),Recurrent Neural Network(RNN) and Convolutional Neural Network(CNN).To measure the performance of these models we use the standard metrics

such as Accuracy, Detection Rate and False Positive Rate.

3.1 Artificial Neural Network(ANN)

Artificial Neural Network (ANN) used for supervised categorization learning. ANN is a computational model consists of a number of simple, highly interconnected neurons[13].An Ann with 3 layers: input layer, hidden layer and output layer. In theKDDTrain+.TXT and KDDTest+.TXT is used for training and testing dataset respectively. The train dataset have 125973records**.**Before using the training dataset, we first convert the non-numeric attributes into numeric attributes because the training input and testing input is given to ANN should be numeric matrix. It can perform a min-max normalization on this feature vector. The class characteristic labeled as numeric type. Therefore, the input measurement is 41 and output dimension is 5 (4 attacks and 1 normal). ANN IDS system uses Leven berg-Marquardt (LM) and BFGS quasi-Newton Back propagation algorithm for learning. This algorithm is used for training 18718 selected patterns and testing 22544 pattern of dataset. In this model using 41 features, 23 hidden nodes and 771 epoch. Finally to classify the attack types and get the classification results also. The accuracy is a lower than expected from an ANN.

3.2 Recurrent Neural Network (RNN)

In our second model is Recurrent Neural Network for intrusion detection. It is used for supervised classification learning. It perform modeling and prediction tasks for sequences with highly difficult structure. RNN is collected of input layer, hidden layer and output layer. It accepts an input vector, updates its hidden state and uses it to make a prediction of its output. The hidden unit completes the most important work, and hidden units are the storage of the whole network, which remember the end-to-end information.KDD is the dataset used to train recurrent neural network for Intrusion detection. Before to training the model we first convert the categorical features to numeric values then logarithmic scaling is applied to perform a min-max normalization on this feature vector. The final dimension of the dataset were 41 different input features with 5 different predicted output classes. Training of that model using Forward Propagation and Back propagation algorithms [14]. Forward propagation is to predict the output values and Back propagation is to update the weights. Finally we evaluate performance of the model. This

model will provide low accuracy and will spend more time for training [15].

3.3 Convolutional Neural Network(CNN)

In our final model is Convolutional Neural Network (CNN).It is apply to image processing natural language processing and other kinds of cognitive tasks. It consists of an input layer, a convolutional layer, a pooling layer, a fully connected layer, and an output layer. Convolution layer is to extract different features information from the input and the pooling layer is mainly reduces the dimension of the feature but retains the important information. The fully connected layers perform classification based on the features extracted by the previous layers. One typical CNN model, Lenet-5, is presented as follows:

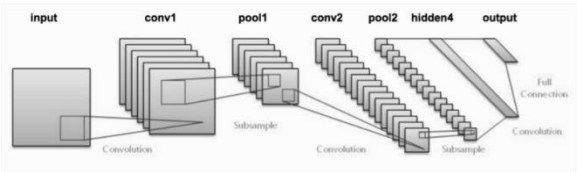

Figure 1: Lenet-5 Network architecture

In this model applies data preprocessing methods to remove the data and irrelevant features in the network traffic data. Next, traffic is transformed into a two-dimensional matrix form, the transformed two-dimensional network connection feature matrix can be used as input samples of the CNN input layer. Second, the label is processed as one-hot encoding, which is convenient for training and testing. The input layer maps a one-dimensional network dataset into two-dimensional plane information, facilitating CNN feature learning. The implied layer includes a convolution layer and a pooling layer. The convolution layer maps the sample data to the high-dimensional space continuously and learns the feature information of the network connection data. The pooling layer reduces the computation and improves the detection efficiency of the model. The output layer maps the result of feature extraction to a one-dimensional array to predict classification. Softmax classifier and CNN are combined to output the classification results. In this model using Batch Normalization(BN) algorithm [16] for to increase the network learning rate and the Back Propagation (BP) algorithm is used to fine-tunes the parameters of the network model.

Finally CNN model is suitable for the massive network environment. Besides, compared with other DL algorithms, the greatest advantage of CNN is that, it can more quickly identify attack type of traffic data. It will produces highest accuracy then the other two deep learning models.

4.EXPERIMENTAL RESULTS

We have used three parameters to evaluate the intrusion detectionModel:accuracy (ACC), detection rate (DR)and false alarm rate (FAR). The givenparameter calculated usingTruePositive(TP), False Negative(FN), False Positive (FP) and True Negative (TN). Confusion matrix is used to evaluate these parameters as shown in Table 1.

Table1: Confusion matrix

Actual	Predicted	Predicted
	Attack	Normal
Attack	TP	FN
Normal	FP	TN

ACC is ratio of correctly classified instances and the total number of instances.

ACC=TP+TN / FN+TP+FP+FN ------(1)

DR is the ratio between the number of correctly detected attacks and the total number of attacks.

DR=TP / TP+FN ---------- (2)

FAR is the ratio between the number of normal instances detected as attack and the total number of normal instances.

FAR=FP / FP+TN ---------- (3)

After all model training is completed, the model is evaluated according to the classification of network traffic in the test dataset. The final experimental results shows in Table 2.

We can see the comparison of the performance metrics in figure 2. The comparison is made between the results of our three models: ANN, RNN, and CNN deep learning algorithms. Overall, CNN is produces the highest Accuracy, Detection Rate and low FAR in network traffic.

Table 2 :Experimental Results of three deep learning models

Classifiers	Accuracy	Detection Rate	False Alarm Rate
ANN	80%	67%	3.2%
RNN	81%	70%	3.4%
CNN	94%	93%	0.5%

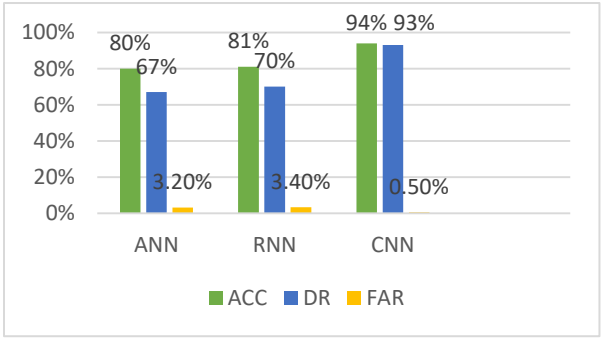

Figure2: Performance comparison

5.CONCLUSION AND FUTURE WORK

In this paper deep learning models based intrusion detection system was implemented using KDD dataset. Dataset was trained and tested for five class attack categories. Our proposed models using different algorithm for training and testing applied on dataset and then result was evaluated. The CNN is able to classify the attack types with an accuracy of 94%.In contrast, the RNN model yielded an 81% and ANN model yielded lower 80%.We can conclude that the CNN deep learning algorithm is a good model for IDS.

Reference:

[1] Webster's Dictionary, Intrusion [online], available:http://www.websterdictionary. org/definition/Intrusion. Accessed on 10/16/2013.

[2] S. Kumar, A. Yadav. Increasing Performance of Intrusion Detection System Using Neural Network. 2014 IEEE International Conference on Advanced Communication Control and Technologies (ICACCCT), pp. 1935-1939.

[3] Heckerman D."A tutorial on learning with Bayesian networks," Microsoft Research; 1995. Technical Report MSRTR-95-06

[4] X.D. Hoang, J. Hu, P. Bertok, "A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference," Journal of Network and Computer Applications 32 (2009) 1219–1228.

[5] Jiankun Hu, Xinghuo Yu, Qiu D, Hsiao-Hwa Chen; "A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection," IEEE Transaction on Network, Volume: 23, Issue:1 DOI: 10.1109/MNET.2009.4804323, Year: 2009, Page(s): 42 – 47.

[6] Li W. "Using genetic algorithm for network intrusion detection," C.S.G. Department of Energy; 2004. pp. 1–8.

[7] Bridges, Vaughn, "Fuzzy Data mining and genetic algorithms applied to intrusion detection," In: Proceedings of the National Information Systems Security Conference; 2000. pp. 13–31.

[8] T.Lunt and I.Traore, Unsupervised Anomaly Detection Using an Evolutionary Extension of K-means Algorithm,International Journal on Information and computer Science, Inderscience Pulisher 2 (May, 2008), 107-139.

[9] B. Daniel, C. Julia, J. Sushil, P. Leonard, N. N. Wu, "ADAM: Detecting intrusions by data mining", Proceedings of the 2001 IEEE, workshop on Information Assurance and Security, West Point, NY, 2001.

[10] Bernhard E Boser, I. M. (1992). A Training Algorithm for Optimal Margin Classiers. Proceedings of the 5th Annual ACM Workshop

on Computational , 144-152.
[11] Tax, D. &. (1999). Data domain description using support vectors.
Proceedings of the european symposium on artificial neural
networks , 251-256.
[12] Carlos A. Catania, F. B. (2012). An autonomous labeling approach
to support vector machines algorithms for network traffic anomaly
detection. Expert Systems with Applications,ELSEVIER .
[13] Robert Hecht-Nielsen “Theory of the Backpropagation Neural Network”
Book Neural networks for perception (Vol. 2) Pages 65-93.

14.J. Martens and I. Sutskever, ``Learning recurrent neural networks with
hessian-free optimization," presented at the 28th Int. Conf. Int. Conf.
Mach. Learn., Bellevue, WA, USA, Jul. 2011, pp. 1033_1040.
15. Y. Chuanlong, 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.
16. S. Ioffe and C. Szegedy ``Batch normalization: Accelerating deep network
training by reducing internal covariate shift," in Proc. Mach. Learn. Res.,
2015, pp. 448_456.