IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Wireless Intrusion Detection system with Neural network

Pawan Prakash Gadve [#1], Dr.V.B.Kamble*[2]

[#] P.E.S. College of Engineering Aurangabad, India

[*] Associate Professor, Computer Science & Engg. P.E.S. College of Engineering Aurangabad, India

Abstract

A Network Intrusion Detection System using Neural Networks-

In view of the increasing number of attacks targeting information systems, a defense system is essential. The access system provides a first line of defense. The admission system monitors events within the information system or one of the components of the information system The purpose of this research project is to design a low-gain entry system using artificial intelligence techniques, especially in-depth learning strategies. The neural network will be trained and evaluated by the NSL KDD database.

Index Conditions — Neural Networks, Access, Computer Security

Introduction

Accessibility Login is an important concept in the security of modern computer networks. Rather than protecting the network from malicious computer programs that are known to block network connections, such as Intrusion Prevention Systems, Intrusion Detection is intended to analyze the current state of the network in real time and to identify potential confusing processes, reporting them as soon as they are detected[1]. This makes it possible to detect malicious computer programs before With the remarkable advancement of technology, criminals have been developing even more sophisticated malware attacks making login detection a very difficult task. In this context, traditional analytical tools face the daunting challenges of identifying and mitigating these threats. In this work, we present a novel analysis analysis and intelligent intelligence acquisition system driven by autoencoder (AE) (IDS)[2].

Specifically, the proposed IDS incorporates data analysis and statistical techniques and the latest developments in machine learning theory to exclude highly improved, highly correlated features. The proposed IDS is tested using the NSL-KDD benchmark website. Comparative test results show that the statistical analysis and IDE-based IDS achieve better classification performance compared to conventional deep and shallow machine learning and other recent proposed strategies.

Crime Detection Systems are generally divided into the following categories [2]:

- Uncertainty Detection Compared to Acquisition: In the detection of misuse, each event in the data set is labeled 'normal' or 'dangerous' and the learning algorithm is trained with labeled data. Conflict detection methods, on the other hand, create normal data models and detect deviations from the normal data model observed.
- Network-based compared to host-based: NIDS login systems are located in a strategic location or points within the network to monitor the return traffic to all network devices, while Hosting (HIDS) operating systems are operational. on individual hosts or on network devices.

The purpose of this work, in particular, is the production of labeled NIDS data labels that can detect suspicious behavior on the network and classify individual communications as normal or bizarre.

Neuroscent Networks

Artificial Neural Networks supervised machine learning algorithms are inspired by the human brain. The main idea is to have many simple units, called neurons, organized into categories. In particular, in the artificial neural network feed-forward all layer neurons are connected to all neurons of the next layer, and so on until the last layer, which contains the output of the neural network.

This type of network is a popular choice among Data Mining Strategies in modern times, and has proven to be an important Import and Export option[2].

In this work we use feed-forward neural networks trained in the NSL-KDD database to classify network connectivity as one of two possible possibilities: normal or abnormal. The goal of this work is to increase accuracy in identifying new data samples, while also avoiding overuse, which occurs when the algorithm is heavily attached to the read data and is unable to perform normally on previously unseen data.

NSL-KDD data set

Dataset had 43 attributes, attribute **'difficulty_level'** was dropped.

The database used to train and validate the neural network is the NSL-KDD database, which is an improved version of the KDD CUP '99 database. This data set is a well-known symbol in the field of Network Acquisition strategies, which provides 42 features per example and many amazing examples.

Summary	
train rows	125973
test rows	22544
total rows	148517
columns	42
duplicates	629
null values	None

Table1- Summary of KDD data Set.

As for the features of this dataset, they can be broken down into 4 types (excluding the target column):

4 Multi-Class

6 Binary

16 Discrete

15 Continuous

The NSL-KDD dataset contains a few binary and multi-class categorical features, which are used to label each connection

Multi-Class Features	
Feature	*Distinct Values*
protocol type	3
Service	70
Flag	11
su attempted	3

Table2- Summary of Multi-Class features.

Binary Features	
Feature	*Number of '0's*
Land	99.98%
logged in	59.72%
root shell	99.85%
num outbound cmds	100.00%
is host login	99.99%
is guest login	98.77%

Table3- Summary of Binary features.

Data Normalization

A standard practice is to re-measure data from the actual range so that all values are within the new range of 0 and 1.

Familiarity requires that you know or be able to accurately measure minimum and maximum visible values. You can estimate these values in your available data.

Database measurement involves re-measuring the distribution of values so that the mean value of the target is 0 and the standard deviation is 1.This can be thought of as subtracting average or placing data in the centre. As a general rule, configuration can be useful, and is required for some machine learning algorithms where your data has input values with different scales. Direct and standard data conversions to stop predictive variables. To stop the forecast variance, the forecast value is deducted from all values. As a result of placement, the prediction has a zero meaning. Similarly, to measure data, each value of the prediction variance is divided by its standard deviation. Data measurement forces values to have a standard deviation of one.

- 38 Data Frame Number Columns are measured using Standard Scale.
- We will use the default configuration and scale values to remove the definition to set it to 0.0 and divide by the standard deviation to give a standard deviation of 1.0. First, the Standard Scalar model is defined by default hyper parameters[4].

  - Once defined, we can call the function fit_transform () and transfer it to our database to create a modified version of our database.

One-hot-encoding

One hot code coding is one way to convert data to optimize the algorithm and get a better prediction. With one heat, we convert each category value into a new category column and assign a binary value of 1 or 0 to those columns. The value of each number is represented as a binary vector. All values are zero, and the index is marked 1.

One hot code is useful for unrelated data to another. Machine learning algorithms treat numerical order as a value attribute. In other words, they will learn a higher number as better or more important than a low number.

While this is useful in some ordinal situations, some input data does not have a category value level, and this can lead to problems with guessing and poor performance. That's where one hot code copy saves the day.

One hot code coding makes our training data very useful and clear, and can be easily modified. By using numerical values, we easily determine the probability of our values. In particular, a single hot code text is used for our output values, as it provides predictions with a very different perspective than a single label.

- The columns 'protocol_type', 'service', 'flag' have one hot code using pd.get_dummies ().

- Dataframe 'category' had 84 attributes after one hot coding.

Binary separation

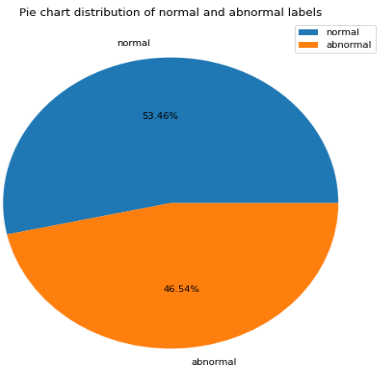

Fig.1-Pie Chart distribution of normal and abnormal labels

A copy of DataFrame was created for Binary Partition.

Attack label ('label') is divided into two 'normal' and 'unusual' categories.

'label' is encoded using LabelEncoder (), encoded labels are saved 'in'.

'label' is coded.

Divide into several categories

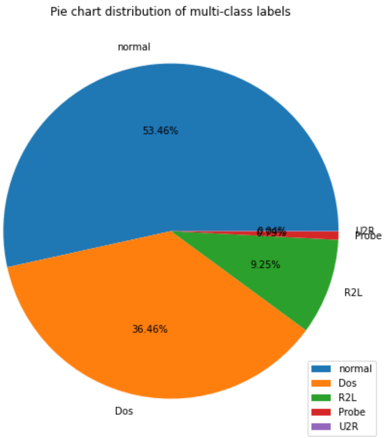

Fig.2- Pie Chart distribution of multi-class labels

A copy of DataFrame was created for Multi-Category.

Attack label (label 'label') is divided into five 'normal' categories, 'U2R', 'R2L', 'Probe', 'Dos'.

'label' is encoded using LabelEncoder (), encoded labels are saved 'in'. 'label encoded'.

Feature Domain

In machine learning, features are unique independent features that work as part of your system. In fact, while making predictions, models use such features to make predictions. And with the use of feature engineering, new features can be found in older machine learning features.

Number of features of 'bin_data' - 45

Number of 'big_data' features - 48

The 'bin_data' and 'many_data' attributes are selected using the 'Pearson Correlation Coefficient'.

Characters with an interaction coefficient greater than 0.5 and the target 'entry' attribute are selected.9 adjectives'count','srv_serror_rate','serror_rate','dst_host_serror_rate','dst_host_srv_serror_rate','logged_in','dst_host_same_srv_rate','dst_host_srv_count'.Number of 'bin_data' attributes after selecting a feature and joining 'Categorical' DataFrame – 97 Number of 'data_more' adjectives after selecting a feature and joining 'Categorical' DataFrame - 100

Database division

Divide the database into a 1: 4 Test and Training Rate.

93 out of 97 attributes were selected, to exclude targeted (coded, single-coded, real) Dividend attribute.

The 'login' attribute is selected as the target attribute.

93 attributes were selected out of 100 attributes, so as not to include the targeted (coded, hot-coded, real) attribute of Multi-Category.

Linear Support Vector Machine

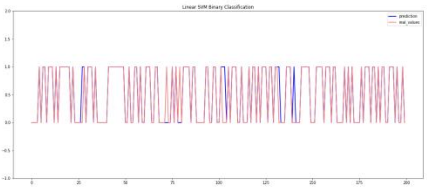

Fig.3-LinearSVMBinaryClassification

When we **can easily separate data** with hyperplane by drawing a straight line is Linear SVM. When we cannot separate data with a straight line we use Non – Linear SVM. In this, we have Kernel functions. They transform non-linear spaces into linear spaces

Binary Split Specification - 96.69%

Multi-Category Accuracy - 95.24%

Used Kernel Type – Linear

SVC (C = 1.0, break_ties = False, repository_size = 200, class_weight = None, coef0 = 0.0, decision_function_shape = 'ovr', degree = 3, gamma = 'auto', kernel = 'linear', max_iter = -1, possibly = False, random_ status = None, diminished = True, tol = 0.001, verbose = False)

Quadratic Support Vector Machine

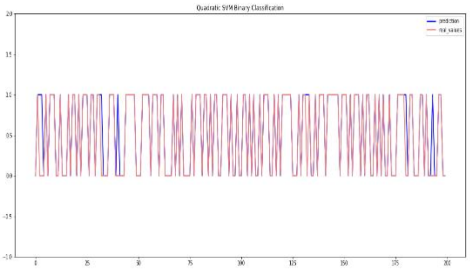

Fig.4- Quadratic SVM Binary Classification

Binary Split Specification - 95.71%

Multi-Category Accuracy - 92.86%

Used Kernel Type - Poly

SVC (C = 1.0, break_ties = False, repository_size = 200, class_weight = None, coef0 = 0.0, decision_function_shape = 'ovr', degree = 3, gamma = 'auto', kernel = 'poly', max_iter = -1, possibly = False, random_ status = None, diminished = True, tol = 0.001, verbose = False)

K-Nearest-Neighbor

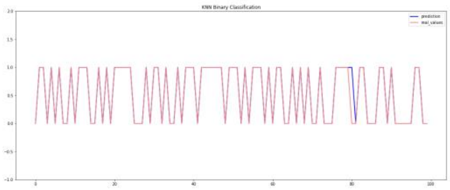

Fig.5- KNN Binary Classification

Binary Separation Accuracy - 98.55%

Multi-Category Accuracy - 98.29%

Neighborhood Number - 5

Weight - Uniform

KNeighborsClassifier (algorithm = 'auto', leaf_size = 30, metric = 'minkowski', metric_params = None, n_jobs = None, n_neighbors = 5, p = 2, weights = 'uniform')

Linear Discrimination Analysis

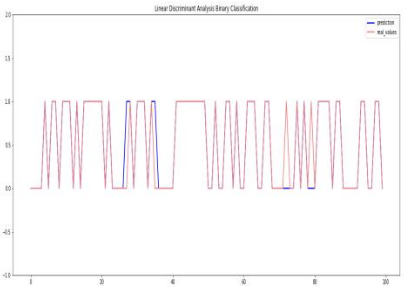

Fig.6- Linear Discriminant Analysis Binary Classifiaction

Binary Split Specification - 96.70%

Multi-Category Accuracy - 93.19%

Used solution - svd (single value)

LinearDiscriminantAnalysis (n_components = None, priors = None, shrinkage = None, solver = 'svd', store_covariance = False, tol = 0.0001)

Quadratic Discriminant Analysis

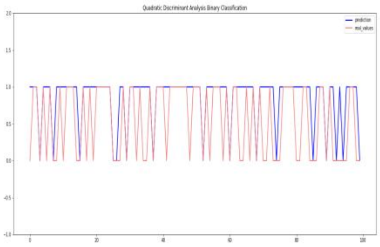

Fig.7-QuadraticDiscriminant Analysis Binary Classification

Binary Split Specification - 68.79%

Multi-Category Accuracy - 44.96%

QuadraticDiscriminantAnalysis (priors = None, reg_param = 0.0, store_covariance = False, tol = 0.0001)

Multi Layer Perceptron

Binary Split Specification - 97.79%

Input layer with 93 input size

1 Hidden layer with 50 Neurons and a function of relaxation

Outgoing layer with the function of activating 1 neuron and sigmoid

Loss - binary_crossentropy

Optimizer - adam

Batch size – 5000

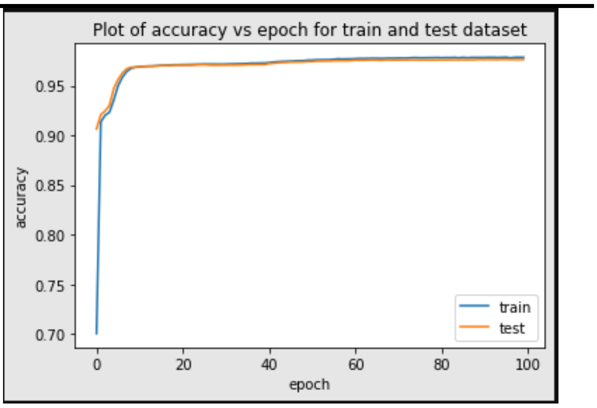

Figure.8- Plot of accuracy vs epoch for train and test dataset

Epochs - 100

Multi-Classification Accuracy - 96.92%

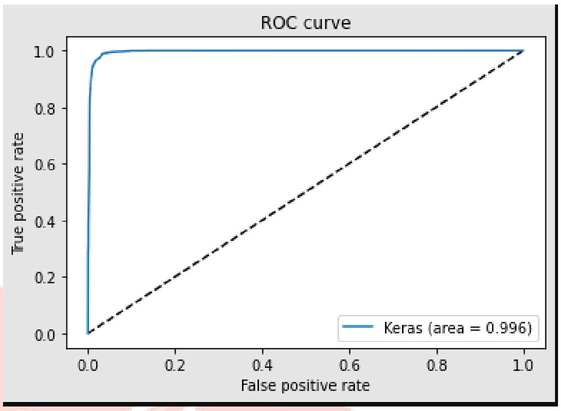

Figure.9- Plot of loss vs epoch for train and test dataset

Input layer with 93 input size

1 Hidden layer with 50 Neurons and a function of relaxation

Output layer with 5 neurons and softmax activation function

Loss - in stages_crossentropy

Optimizer - adam

Batch size - 5000

Epochs - 100

LSTM

Binary Separation Accuracy - 83.05%

Input layer with 93 input size

LSM layer with 50 codec cells

Outgoing layer with the function of activating 1 neuron and sigmoid

Loss - binary_crossentropy

Optimizer - adam

Batch size - 5000

Epochs - 100

Autoencoder

Binary Split Specification - 92.26%

Multi-Category Accuracy - 91.22%

Input layer

Text layer with 50 coding cells

Output and Separate Layer with softmax activation function

Loss - mean_squared_error

Optimizer - adam

Batch size - 500

Epochs – 100

Conclusion

Aiming at problem of network intrusion detection technology based on Neural network method that has low detection efficiency and is prone to face over fitting and generalization issues in the model training process. This paper proposes network intrusion detection based on improved convolution neural network. The classification training and test experiments are carried out by using the pre-processed training set and test set data. The experimental results show that the accuracy and true positive rate of intrusion detection in network are higher and the false positive rate is lower. Overall, leverages the advantage of the Neural network model for feature extraction of sample data. IDS structures are gear that system a big amount of statistics on a day by day basis. This entails collecting, normalizing, and detecting assaults and sending notifications in actual time. this studies takes under consideration the processing energy that is devoted to the operation of IDS structures and proposes a brand new system mastering version with excessive detection functionality and occasional computation resources.

.

References

[01]. HONGYU YANG AND FENGYAN WANG: 'Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network ', School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China

[02] Guojie Liu1 and Jianbiao Zhang CNID: Research of 'Network Intrusion Detection Based on Convolution Neural Network', 1Beijing University of Technology, Beijing 100124, China.

[03].Vinaykumar,Mamoun Alazab, Soman kp,Prabharan Pooranchandran, Ameer al-Nemrat, and Sitalaxmai Venkatraman , 'Deep Learning Approach for Intelligent Intrusion Detection System' ,1Center for Computational Engineering and Networking (CEN), Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India 2Charles Darwin University, Australia 3Centre for Cyber Security Systems and Networks, Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham, India 4School of Architecture Computing, and Engineering (ACE), University of East London. 5Melbourne Polytechnic, Australia.

[04] Hansman, S. and Hunt, R., 'A taxonomy of network and computer attacks, Computers & Security', vol. 24,pp. 31–43, Feb 2005.

[05] Lough, D,' A taxonomy of computer attacks with applications to wireless networks', PhD Dissertation.

[06] B.Wang, Y. Zheng,W. Lou, and Y. T. Hou, `DDoS attack protection in the era of cloud computing and software-defined networking', Comput. Netw., vol. 81, pp. 308_319, Mar. 2015.

[07]Straub, Jr., D.W. and Widom, C., Deviancy by bits and bytes: 'Computer abusers and control measures', in Proc. of the 2nd IFIP Interna2tional Conference on Computer Security, pp. 431–441, Toronto, Canada, 1984.

[08] Nabil Moukafih , Ghizlane Orhanou, and Said El Hajji ,'Neural Network-Based Voting System with High Capacity and Low Computation for Intrusion Detection in SIEM/IDS Systems' ,Laboratory of Mathematics, Computing and Applications-Information Security, Faculty of Sciences, Mohammed V University in Rabat, BP1014 RP, Rabat, Morocco.

[09] Xiaolong Huang ,'Network Intrusion Detection Based on an Improved Long-Short-Term Memory Model in Combination with Multiple Spatiotemporal Structures' ,School of Information Engineering, Baise University, Baise 533000, China.

[10] Therese R. Metcalf Leonard J, LaPadula 'Intrusion Detection System Requirements,Center for Integrated Intelligence Systems'. Bedford, Massachusetts.

[11] Bin Li, Member, IEEE, Weisi Guo, Senior Member, IEEE, Ying-Chang Liang, Fellow, IEEE, Chunyan An, Chenglin Zhao Asynchronous Device Detection for Cognitive Device-to-Device Communications.

[12] NA LI 1,2, JIAN LI1, XIUBO CHEN3, AND YUGUANG YANG4,Quantum Wireless Network Private Query With Multiple Third Parties, 1School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China 2Jilin Medical University, Jilin City 132013, China 3State Key Laboratory of Networking and Switching Technology, Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China 4College of Computer Science and Technology, Beijing University of Technology,Beijing100124,China.

[13]. Waleed Bul'ajoul 1,2, Anne James1, and Siraj Shaikh3 A New Architecture for Network Intrusion Detection and Prevention,1Computing and Technology Department, New Hall, Nottingham Trent University, Clifton Campus, Nottingham NG11 8PT, U.K. 2Computing Department, School of Science, University of Omar Al-Mukhtar, Al Bayda' 543, Libya 3Systems Security Group, Institute for Future Transport and Cities, CoventryUniversity,CoventryCV1 5FB, U.K.

[14] Ruizhe Yao, Ning Wang *, Zhihui Liu, Peng Chen and Xianjun Sheng Intrusion Detection System in the Advanced Metering Infrastructure: A Cross-Layer Feature-Fusion CNN-LSTM-Based Approach Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian116024,China;yrzhe@mail.dlut.edu.cn(R.Y.)