International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 9, Issue 5, September - October 2020 ISSN 2278-6856

Analysis and Classification of Intrusion Detection for Synthetic Neural Networks using Machine Language Strategies

Manjunath H [1], Dr S Saravana kumar [2]

[1]Research Scholar,Department of Computer Science and Engineering, CMRU, Bangalore
[2]Professor, Department of Computer Science and Engineering, CMRU, Bangalore

Abstract

In the recent yearsdue to the increased throughput and the multi-uniformity of behaviors, the existing network is complex. An intrusion detection system is a critical component for reliable management of information. The advancement in system hardware field and raise in data growth related in new fields with respect to the deep learning technology along with intrusion detection systems. Learning data presentation studied through deep learning which a part of Machine learning. To be successful, network intrusion detection systems, which are part of the layered protection scheme, must be able to fulfill certain organizational objectives. This research paper describes the investigations performed on various neural network architectures using a variety of intrusion detection algorithms. New supervised algorithms in Intrusion Detection System (IDS) have been implemented that have faster convergence and better performance. The goal of this research work is to introduce a new balance of artificial neural networks.

Keywords: -Denial of Service, Artificial neural network, Malicious, Intrusion detection system.

1. Introduction

A computers system must include accountability, credibility and security against denial of service. Because of increased connectivity, and the broad spectrum of opening up financial possibilities, more and more systems are subject to intruders attack. Any internet-connected device cannot provide protection without additional software for the elimination of intrusion detection [1]. Each organization is linked to the internet, even of small scale. Employees operate from home due to practical requirements and cost considerations by integrating their systems with the head office. Employees share data in the form of revision, the work assigned to them is complete. Cellular networks, mobile phones, landline telephones, automatic teller machines, financial corporation offers internet services.

Due to software threats in the form of intrusion, equipment which relies on main database stored in severs should not be disrupted. Military bases, nuclear, research centers, institution with information of the highest level should not be harmed in the form of modification manipulation of information by any unknown operation entertained by any one via the internet.

Primary intrusion, remote intrusion and system intrusion are the major ways a system can be intruded by auser [2]. When detecting intrusions the IDS respond to set of actions. Many of the answers are listed in [3], which involves submitting results and findings to a pre-specified venue, whereas others are automated responses that are more functional. IDS can be regarded as the second measure of safety to networked information systems against unauthorized users because, with the best access control systems [4] and intruders, computer networks can still be hacked. Intrusion detection system extends the protection offered by access control systems by providing an intrusion warning to system administrators [5]. The importance of the current research work is to explore the potential benefits of Artificial Neural Network (ANN) algorithms as software for intrusion detection in a network of computers connected to the internet. Once an ANN is properly tested as intrusion detection software for its full implementation, it can detect most of the attacks.

Some of the attacks include: tentative break-ins, Masquerade attacks, security control system penetration, leakage, service denial, malicious use.

Artificial neural networks (ANNs) are computational structures that are focused on the biological neuron structure and function. Development of new algorithms, which are faster and offer better results, has shown considerable interest. ANN consists of processing units which are interconnected. The general processing unit framework includes, summing part followed by a portion of the output. The summing component receives 'n' input values and weight values, and a weighted sum is performed. The weighted sum is called a value for the activation. For each input the weight sign determines whether the input is either excitatory (positive weight) or inhibitory (negative weight). The values for input and output might be the digital or analog data. In order to accomplish a function of pattern recognition, multiple processing units are interconnected according to a specified topology of the network.A processing unit's input may come from outputs of other processing units, or from an external source. Each unit's output may be distributed to several units including it. A network may be static or dynamic; some of the static networks use multi-layerperceptron with the back propagation algorithm and radial base function. Many of the dynamic networks (recurring networks) have input from the output, state feedback and dynamics from feed forward. The network's learning may be monitored or not monitored. In supervised learning the network is provided with both inputs and outputs. The inputs are provided to the network by themselves in the unsupervised learning (self-recognizing networks). Some of the unsupervised learning algorithms are maps of adaptive resonance theory [6] self-organizingfeatures [7]. One of ANN's major uses is in the field of pattern recognition. A pattern is a sequence of entries and exits. Based on the topology of the network, either supervised or unsupervised training method may be employed to train an ANN. The difference between network measured performance and desired performance of pattern is minimized in the supervised training. Convergence weights are adjusted to get the minimum difference. This technique is adopted for all trends.

Lippmann [8] has given the state of the ANN in his pioneering work. The thesis has subsequently addressed the new advances in supervised learning in [9]. It was mentioned in [10] that the desire to grow ANN began in the late forties. Ebro’s' contribution to his doctoral thesis in the field of neural feed forward networks was the first and foremost. Conventionally a supervised learning employs the well-known BPA with a linear weight function and uses the steepest-descent method (SDM) as found in [11] for weight updating. Several others [12] have strengthened the BPA by implementing other improvements to quicker convergence. Hirose [13] used an algorithm to analyze the number of hidden nodes, based on the mean squared error.

Besides the above, optimal discriminating plane technique [14] was used to map n-dimensional pattern into a 2-dimensional pattern to train the ANN. Echo state Neural Network [15] possesses a highly interconnected and recurrent nonlinear Processing Elements (PEs) topology that constitutes a "reservoir of rich dynamics" and includes knowledge on the past of input and output sequence. This was attempted at detection of intrusion. Throughout the work the various algorithms developed were used for intrusion detection on data obtained during Knowledge Discovery and Data mining (KDD). Additionally, the well-known XOR issue was used as benchmark data.

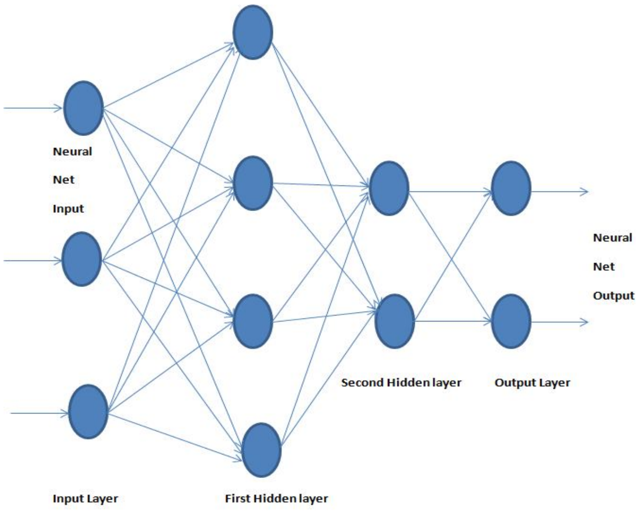

Fig. Construction of a multilayer perceptron neural network with one input layer, two hidden layers and one output layer

2. Up-Gradation of the Convergence Weights

Although a number of algorithms are investigated, a sample number of algorithms are presented here and their performances are discussed.

2.1 Convolution of an Image

1. Line up the image and the features.
2. Multiply each image pixel by pixel of the corresponding Feature.
3. Fill in the values to find the sum.
4. Split the sum by the total pixel count in the feature.
5. Find the preceding image.
6. The process is done with the first 2 moves itself.
7. Considered an image of a feature and one pixel of it.
8. With the current image we multiplied this, and the result is stored in another buffer feature image.
9. Complete the last 2 steps with the considered image. Apply certain values that contributed to the number.
10.Split this number in the feature image by the total number of pixels.
11. The final value obtained will be put in the center of the filtered image.
12.Now, pass around this filter and do the same for every pi xel in the image.

2.2 ReLu Layer

1. Rectified Linear Unit (ReLU) transform function only activates a node if the input is above a certain quantity, while the input is below zero, the output is zero.
2. When the input rises above a certain threshold, it has a linear relationship with the dependent variable.
3. Considered a simple function. So that function only performs an operation if that value is obtained by the dependent variable.
4. Remove all the negative values from the convolution. All the positive values remain the same but all the negative values get changed to zero.
5. After processing a particular feature we get an output, likewise do the same process to all the other feature images.

2.3 Pooling Layer

1. Consider an image and shrink the image stack into a smaller size.
2. After passing through the activation layer do the pooling.
3. Pick a window size (usually 2 or 3).
4. Pick a stride (usually 2).
5. Walk your window across your filtered images.
6. From each window, take the maximum value.
7. For instance with an image of 7*7 matrix, consider window size of 2 and stride being 2 we will be getting values to choose from and in that the maximum value is 1 and that gets picked.
8.Though started out with a 7×7 matrix, the same matrix after pooling will be down to 4×4 matrix.
9. Move the window across the entire image.
10. The procedure is exactly as same as above steeps, repeat that for the entire image.

3. Experimental Analysis

The algorithm relies on the supervised learning. Thenumber of iterations needed for different values fordifferent ranges of convergence weights for SVM, thenumber of iterations needed for constant weights forSVM and the number of iterations required for different hidden nodes for SVM with one hidden layer. A distinction is made between the iterations necessary by one hidden layer and two hidden layers in SVM, the iterations needed for the nodes in the hidden layer for various value of SVM and the iterations necessary by the collection was isolated from each other as teaching and testing (intrusion detection).Education involves the creation of weights suggesting a detailed understanding of intrusion and natural packets along with correct marking.

Figure 1 indicates the convergence rate of supervised algorithm success in classification is shown in Table 1. Table 2, shows false acceptance rates and false refusal rates .

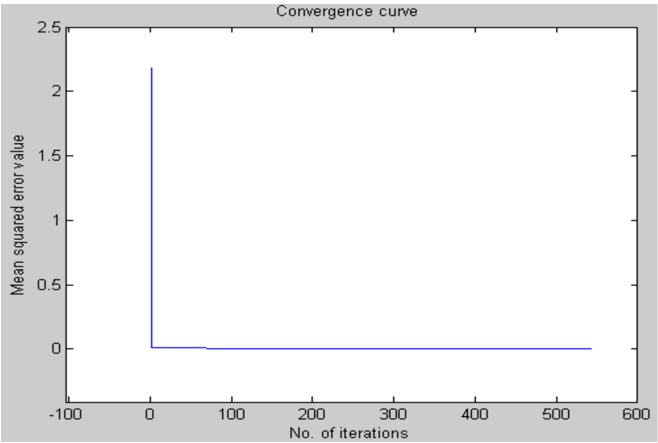

Fig1. Mean squared error curve

Table 1. Classification performance

Packet type	Total No. tested	No. classified	No. misclassified
Normal	1500	1492	8
Intrusion	2500	1415	140

Table 2. False acceptance / Rejection rate

Packet type	False Acceptance Rate (FAR)	False Rejection Rate (FRR)
Normal	5.6% (140/2500)	0.53% (8/1500)
Intrusion	9.4%(140/1500)	0.3%(8/2500)

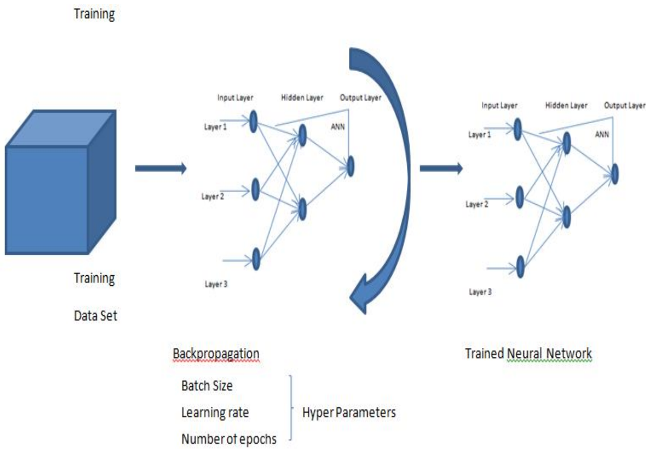

Fig2. Multiple layer perceptron

3.1 ANN's Structural variants-Hierarchical structures (HS)

Thedirectclassificationmethod forthe two classification problem is simple to implement andrequires no assumption about an effective partitioning of the whole problem into subtasks. With hierarchicalclassification one can independently design parts of theentire system.The aim of anyone is to break down thecomplexity of the problem and describe every differentsub problems those are easier to be solved by each. Thevarious approach has 2 advantages.Hierarchical classification is introduced with a view to classifying and preventingother attacks.Which results from thefactwhich discriminating regions are in conflict withthose of other groups for trends of these two classes.Second, we can create more complex decision making regions with this scheme than simple classification ones.

Statistical Methods

The characteristics ofthe patterns are standardized by taking the maximum value of each the attribute and splitting the same characteristic values for all patterns.

This is because the sigmoid function outputs will never reach 0.0 or 1.0.When using functional update method, the pattern is coded in binary.

It is necessary to selectpatterns for the training the neural network, since they should be representative of all patterns collected duringmachining. So,the statistical methods were used for identify the patterns of training and research. Selected for each class pattern with maximum, VEi2 variance. .

The maximum VEi2 of a pattern can be found at the equation,

$$\text{VEi2}=\frac{\sum_{j=1}^{nf}(A_{ij}-\overline{A}_j)^2}{\sigma_i^2}$$

$$\sigma_i^2=\frac{1}{L}\sum_{i=1}^{L}(A_{ij}-\overline{A}_j)^2$$

Where,

nf is the number of features
L is the number of patterns
pi is the pattern number
Aij features of pattern ‘A’
$\overline{A}_j$ is the mean for each feature
VE_i^2 is the variance of patterns
j is the feature
i is the pattern

5. CONCLUSION

We provided an overview of deep learning in this paper, and what the most meanings emphasize. We reviewed the latest Deep Learning papers in the domain of intrusion detection. Some widely used architectures of deep learning are being investigated, and one of the classes was discussed and implemented, namely discriminative (supervised) architecture. This architecture class provides plenty of flexibility and has proven itself to be useful and reliable in a wide range of issues over decades. For example, it is possible to classify the supervised architecture into the support vector machine (SVM), CNN and RNN.We looked at the related works for this class and above mentioned method which are applied in the domain of intrusion detection. After that we pointed out the most common intrusion detection Datasets used by deep learning and the most common implementation frameworks by deep learning. We know the input and output so we used the supervised learning algorithms that deal with labeled data. Intrusion detection data sets are very important for the training and testing systems. Dataset always contains an enormous number of features in which most are redundant or irrelevant.

Deep learning methods preferably serve as extraction of features or reduction of complex features. If we have no idea about the association between the raw input data and the targeted classification output, we may use deep learning methods.

Based on previous works, it was found that in the classification, RNN are used more than CNN, and also the performance of RNN is better than CNN, while CNN is faster than RNN. If researchers need to use CNN method then they may first transform the raw input into image file before using this approach, it is worth mentioning here. This is because the CNN algorithm is very efficient in managing image files, e.g. Google uses CNN to search through imagesof users. To sum up, it can be said that the technique has shown a more automatic ability to obtain high precision levels.

REFRENCES

[1] R. Bace and P. Mell, “NIST special publication on intrusion detection systems,” BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2001

[2] B. Durakovic, “Design of experiments application, concepts, examples: State of the art,” Period. Eng. Nat. Sci., vol. 5, no. 3, 2017

[3] Carpenter, G.A., and Grossberg, 1987, “Self-organization of stable category recognition codes for analog input patterns”, Applied optics, Vol.26, No.23, pp.4919-4930

[4] F. Farahnakian and J. Heikkonen, “A deep auto-encoder based approach for intrusion detection system,” in Advanced Communication Technology (ICACT), 2018 20th International Conference on, 2018, pp. 178–183

[5] Daniel C. Nash, Thomas L. Martin, Dong S. Ha, and Michael S. Hsiao, 2005, Towards an Intrusion Detection System for Battery Exhaustion Attacks on Mobile Computing Devices, Proceedings of the 3rd International Conference on Pervasive Computing and Communications Workshops (PerCom 2005 Workshops)

[6] Foley.D.H, 1972, “Consideration of Sample and Feature Size,” IEEE Transaction on Information Theory, Vol.18, No. 5, pp. 626 – 681

[7] Friedman. F, J.W Turkey, 1974, “A Projection Pursuit Algorithm for Exploratory Data Analysis,” IEEE Trans. on Comp., vol. 23, no. 9, pp. 881–890

[8] Gallinari.P, S. Thira., F.Badran, F Fogelman-Soulie F., 1991, “On The Relations Between Discriminant Analysis and Multilayer Perceptrons,” Neural Networks, Vol. 4, No.3, pp.349 – 360

[9] Hong.Z.Q, Y.J.Yang, 1991, “Optimal Discriminate Plane for a Small Number of Samples and Design Method of Classifier on the Plane,” pattern recognition, Vol. 24, pp. 317 – 324

[10] Hu Zhengbing, Li Zhitang1, Wu Junqi, 2008, “A Novel Network Intrusion Detection System(NIDS) Based on Signatures Search of Data Mining”, 2008 Workshop on Knowledge Discovery and Data Mining

[11] Kok-Chin Khor, Choo-Yee Ting, Somnuk-Phon Amnuaisuk, 2008.“A Probabilistic Approach for Network Intrusion Detection”, 2nd Asia International Conference on Modeling& Simulation

[12] Meng Joo Er.Shiqian Wu, Juwei Lu and Hock Lye Toh, “Face Recognition with Radial Basis Function(RBF) Neural Networks,” IEEE Trans. on Neural Networks, Vol. 13, No.3, pp. 697 – 910, May 2002

[13] Moses Garuba, Chunmei Liu, and Duane Fraites, 2008, Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems, Fifth International Conference on Information Technology: New Generations,978-0-7695-3099-4/08 $25.00 © 2008 IEEE

[14] I. Bozcan, Y. Oymak, I. Z. Alemdar, and S. Kalkan, “What is (missing or wrong) in the scene? A Hybrid Deep Boltzmann Machine for Contextualized Scene Modeling,” in 2018 IEEE International Conference on Robotics and Automation (ICRA), 2018, pp. 1–6

[15] L Deng, "Deep learning: Methods and applications," Found. Trends Signal Process. vol. 7, no. 3/4, pp. 197-387, Aug. 2014

[16] P Vincent, H. Larochelle, I. Lajoie, Y. Bengio, and P.-A. Manzagol,"Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion," J. Mach. Learn. Res.,vol. 11, pp. 3371-3408, 2010

[17] G E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," Science, vol. 313, no. 5786, pp. 504-507,2006

[18] Y. Wang, H. Yao, and S. Zhao, "Auto-encoder based dimensionality reduction," Neurocomputing, vol. 184, pp. 232-242, 2016

[19] Z. Liang, G. Zhang, J. X. Huang, and Q. V. Hu, "Deep learning for healthcare decision making with EMRs," in Proc. IEEE Int. Conf. Bioinformat.Biomed., Nov. 2014, pp. 556-559

[20] F. Falcini, G. Lami, and A. M. Costanza, "Deep learning in automotive software," IEEE Softw., vol. 34, no. 3, pp. 56-63, May 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7927925/

[21] A. Luckow, M. Cook, N. Ashcraft, E. Weill, E. Djerekarov, and B. Vorster,"Deep learning in the automotive industry: Applications and tools," in Proc. IEEE Int. Conf. Big Data, Dec. 2016, pp. 3759-3768. [Online].Available: http://ieeexplore.ieee.org/document/7841045/

[22] H. Lee, Y. Kim, and C. O. Kim, "A deep learning model for robust wafer fault monitoring with sensor measurement noise," IEEE Trans. Semicond.Manuf., vol. 30, no. 1, pp. 23-31, Feb. 2017

[23] L. You, Y. Li, Y. Wang, J. Zhang, and Y. Yang, "A deep learning based RNNs model for automatic security audit of short messages," in Proc. 16th Int. Symp. Commun. Inf. Technol., Qingdao, China, Sep. 2016. 225-229

[24] R. Polishetty, M. Roopaei, and P. Rad, "A next-generation secure cloudbased deep learning license plate recognition for smart cities," in Proc.15th IEEE Int. Conf. Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016. 286-293

[25] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in Proc. 15th IEEE Int. Conf. Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016. 195-200.

[26] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," in Proc. IEEE Int. Conf. Big Data Smart Comput., Hong Kong, China, Feb. 2017, pp. 313-316

[27] E. Hodo, X. J. A. Bellekens, A. Hamilton, C. Tachtatzis, and R. C. Atkinson, Shallow and deep networks intrusion detection system: A taxonomy and survey, Submitted to ACM Survey, 2017, [Online]. Available:http://arxiv.org/abs/1701.02145

[28] Q. Niyaz, W. Sun, and A. Y. Javaid, A deep learning based DDOS detection system in software-defined networking (SDN), Submitted to EAI Endorsed Transactions on Security and Safety, In Press, 2017, [Online].Available: http://arxiv.org/abs/1611.07400

[29] Y. Wang, W.-D. Cai, and P.-C. Wei, "A deep learning approach for detecting malicious JavaScript code," Security Commun. Netw, vol. 9, no. 11,pp. 1520-1534, Jul. 2016

[30] H.-W. Lee, N.-R. Kim, and J.-H. Lee, "Deep neural network self-training based on unsupervised learning and dropout," Int. J. Fuzzy Logic Intell.Syst., vol. 17, no. 1, pp. 1-9, Mar. 2017

AUTHOR

Mr. Manjunath H, received the B.Tech in Computer Science and Engineering, MTech degree in Computer Science Engineering from VTU. He is working as Assistant Professor in Department of CSE at CMRU and is a research scholar. He doing is research in Arificial Intelligence at CMRU, Bangalore.He has worked in Evry India as Oracle developer for 3 years.

Dr S Saravana Kumar received the B.Tech in Information Technology, M.E. degrees in Computer Science Engineering from Anna Universityand PhD in Artificial Intelligence. He working as Professor in Department of CSE at CMRU. He has Published 105 international Journal and Presented 80 papers in International Conference. His research area in Artificial Intelligence, Deep Learning and Computer Vision.