IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Network Intrusion Detection Using Genitic Algorithm: A Comparision

Sayi Sruthi K.[1*], Liston Deva Glinds[2], Saran Raj[3]

[1,2,3]Dept. of Computer science Engineering, Dhanalakshmi srinivasan college of Engineering, Coimbatore, India

DOI: https://doi.org/10.26438/ijcse/v7i4.134136 | Available online at: www.ijcseonline.org

Accepted: 12/Apr/2019, Published: 30/Apr/2019

***Abstract*:** The network intrusion detection system is used to detect and analyze the network traffic and all possible network threats that may affect the system. When the threats are identified the network intrusion detection system immediately takes action such as alerting the administrator or blocking the source of ip address from accessing the network. Various research activities are already conducted to find a efficient and effective solution to prevent intrusions in the network in order to ensure the network security and privacy .machine learning is the one of the efficient and effective techniques to detect network intrusion. Due to high traffic flow, the traditional signature based intrusion detection system is inefficient one to detect anomalies the machine learning techniques is the solution for this. In this paper a combination of two machine learning algorithm is proposed to classify any anomalous behavior in the network traffic. The overall efficiency of the proposed method is dignified recall. However using area under the Receiver operating curve (ROC) metric, we find that genetic algorithm is the best among the two algorithm proposed in this work.

Keywords-Intrusion detection,Genetic Algorithm, Rbf algorithm, Roc metrics calculation

I. INTRODUCTION

Now a days we are facing lots of security threats day by day each of them were very dangerous and harmful to our system. So we need an efficient and safe security system against these attacks. There are different approaches and techniques already implemented in intrusion detection system, but most of them are inefficient one. Here in this work I have designed a network intrusion detection system using genetic algorithm. This system which continuously monitor and track each and every activities of computer network using set of rules. The experiments and evaluation of the proposed intrusion detection system are performed with KDD cup99 intrusion detection data set. In this work we use two machine learning algorithm that is RBF and Genetic Algorithm. First the performance evaluation of these two machine learning algorithm are done in term of accuracy, precision, and recall. These two algorithms are well evaluated with these terms and next we use ROC metric calculation. It shows that the ROC metrics is more suitable for ranking the result of these algorithms more accurately.

II. EXISTING SYSTEM

The existing system for network intrusion detection is based on signature basic. These techniques are not much feasible for better intrusion detection. Several machine algorithms like k-means clustering algorithm, svm algorithm, fuzzy logic are the k-means clustering algorithm based on information entropy and frequency sensitive discrepancy metrics. A svm algorithm for intrusion detection is used based on space block and sample density. The svm based model can be used to detect data accurately; readily miss probability can be effectively used for real time intrusion detection. The fuzzy logic techniques which use fuzzy classifier for detecting intrusion. This system is based on two rules set one for normal class and other for abnormal class. This system which can continuously monitor each and every parameter and classification attributes for better result.

III. METHODOLOGY

Here we implement two machine learning algorithm RBF and genetic algorithm. Radical basis function network (RBF) algorithm is a artificial neural network algorithm. That used in machine learning techniques. The RBF algorithm mainly used to solve supervised learning problem.

FUNCTIONALITY OF RBF ALGORITHM:
This algorithm divided into three layers an input layer, a hidden layer with a non-linear output layer. The input can be modeled as a vector of real number X £ R^n the output of the network is a scalar function of the input vector.μ: R^n→R and as given by μ (x)= $\sum_{i=1}^{N} \infty$ IP (11X-$C_1$11) feed forward connections exist between input and hidden layer ,input and output layer, and with hidden and output layer additionally there are connection between a bias node and each output node. A solar weight is associated with the connection between nodes. The RBF networks are trained in a similar way of MLP. The output layer, weight are trained using the rules. The activation of each input node is equal to its

external input where the element of external input vector of the network.

GENETIC ALGORITHM

In the field of artificial intelligence a genetic algorithm is a search heuristic that mimics the process of natural selection. This heuristic is roughly used to generate useful solution to optimization and search problems. The genetic algorithm which used in network intrusion detection system is a machine learning techniques, where in the testing phase the network security laboratory-knowledge discovery and data mining (NSL-KDD99) benchmark data set has been used to detect the misuse activities. By combining the IDS with genetic algorithm increase the performance of the detection rate of the network intrusion detection model and reduce the false positive rate. In intrusion detection anomaly detection and misuse detection is very important this can efficiently done by using genetic algorithm. The anomaly detection means identifying any unaccepted deviation cause due to attack. Misuse detection is signature based which is represented by signature. To detect this attack the genetic algorithm use two approaches are important in two different stages. In training stage, a set of rules are generated from the audit data. These rules are used to classify incoming network connection is real time. By combining with RBF algorithm it shows the genetic algorithm is best in intrusion detection.

IV. EXPERIMENTAL RESULT AND DISCUSSION

To evaluate the intrusion detection system performance and accuracy there are four possible condition, they are TRUE POSSITIVE, FALSE POSSITIVE, TRUE NEGATIVE, and FALSE NEGATIVE. TP (true positive) are the occurrence that is correctly marked anomalous. FP (false positive) is legal occurrence of data on the network that are incorrectly detected as anomalous. FN (false negative) is the anomalous occurrence that is not detected by the detector and it is not marked as anomalous. TN (true negative) is the occurrence that is correctly marked as legal activities. It is very important to evaluate that the intrusion which detect is false positive and false negative. Both this situations are very dangers but most risky factor is false negative. False negative is a abnormal activities which passes through the intrusion detection system as a normal activities. So such intrusions are very harmful to the system. Our aim is to maximize TP and TN by minimizing FP and FN. Based on these we also derive the following metrics:

Precision=TP/ (TP+FP)

Recall=TP/ (TP+FN),

Accuracy= (TP+TN) + (TP+TN+FP+FN)

Al these analysis factors were performed using the R programming language. The precision, accuracy, and recall metrics for RBF and GENITIC ALGRITHM are represented in Table 1. The recall result is quite low for RBF algorithm when compare with GENITIC ALGORITHM it indicate that it has high value of false negative. For RBF algorithm the precision value is 0.92% and accuracy is 0.9754. The genetic algorithm which shows better result while comparing with RBF algorithm. Genetic algorithm which has high flexibility as compared to many other machine learning techniques. Genetic algorithm which uses rules based classification for detecting intrusion. While comparing with RBF algorithm genetic algorithm has accuracy 0.9812%, precision 0.921% and recall has 0.9643%. Genetic algorithm which shows good result with high accuracy and precision value.

Table 1: Accuracy, Recall, and Precision

ALGORITHM	ACCURACY	RECALL	PRECISION
RBF	0.9754	0.9583	0.92
GENITIC ALGORITHM	0.9883	0.9643	0.9213

It is somewhat very difficult to compare this algorithm based on this performance metrics. So we use another metrics called ROC metrics (the receiver operating curve) this help to rank algorithms in better and in accurate way. The comparison of this two algorithm with ROC metrics is shown in Table 2. Among this Genetic algorithm perform well with ROC calculation. It has ROC value 0.9812 and RBF algorithm has ROC value 0.9741. Some work has been already conducted using Ensemble methodologies for anomaly detection that perform better result than individual algorithms. There is scope of future research in this area.

Table 2: ROC metrics evaluation of algorithms.

ALGORITHM	ROC
RBF	0.9741
GENITIC ALGORITHM	0.9812

V. CONCLUSION AND RESULT

In this work we compare two machine learning algorithm for network intrusion detection using performance metrics like accuracy, precision and recall by using sample dataset. This evaluation is not enough for better ranking of these algorithms so we use ROC metrics calculation for better result. By comparing with this two performance evaluation metrics it shows that the Genetic algorithm is best in network intrusion detection than RBF algorithm. Even though this is an efficient method it also has some limitation. Day by day several new types of powerful attacks are generating to crack our system so the intrusion detection system should also be upgrade and updated with new powerful technologies. As future scope we can use other efficient machine learning algorithms.

REFERENCE

[1] Syarif I, Prugel Bennett A, Wills G., “Unsupervised clustering approach for network anomaly detection”, Networked Digital

Technologies Communications in Computer and Information Science, vol. 293. Berlin Heidelberg: Springer, 2012, pp.135–45.

[2] S. Novakov, C.-H. Lung, I. Lambadaris, Ioannis N. Seddigh, "Studies in applying PCA and wavelet algorithms for network traffic anomaly detection", Proc. of IEEE 14th International Conference on High Performance Switching and Routing, 2013, pp. 185-190.

[3]Intrusion Detection using an Ensemble of Classification Methods, M.Govindarajan and RM.Chandrasekaran, Proceedings of the World Congress on Engineering and Computer Science 2012 Vol I WCECS 2012, October 24-26, 2012, San Francisco, USA

[4] S. Novakov, C.-H. Lung, I. Lambadaris, Ioannis N. Seddigh, "Combining statistical and spectral analysis techniques in network traffic anomaly detection", Proc. of IEEE Conf. on Next Generation Networks and Services, 2012, pp. 94-101.

[5] S.A. Mulay, P. R. Devale, G.V. Garje, "Intrusion Detection System using Support Vector Machine and Decision Tree", International Journal of Computer Applications, vol. 3, no. 3, 2010.

[6] J. Cannady, "Artificial neural networks for misuse detection," in Proceedings of the 1998 National Information Systems Secu- rity Conference, pp. 443–456, Arlington, VA, USA, 1998.

[7] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power sys- tems," IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 3104–3113, 2015.