ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

OPTIMIZING PARAMETERS OF FUZZY ART FOR IMPROVING THE ACCURACY OF NIDS

Krishna Champaneria*, Prof. Bhavin Shah, Asst. Prof. Krunal Panchal
[1]Student of Final Year M.E.(C.E.), L.J.Institte of Engineering and Technology, Ahmedabad.
[2]M.C.A. Programme, L.J. Institute of Management Studies, Ahmedabad.
[3]Department of Computer Engineering, L.J. Institute of Engineering & Technology, Ahmedabad, India.

ABSTRACT

Intrusion Detection System (IDS) has been developed in order to provide a defense mechanism against the intrusive activities carried over network. This paper discusses an approach of Intrusion detection system using Fuzzy ART technique for clustering with some pre-processing method. From the survey it was found that IDS built using Fuzzy ART has low detection rate and high false alarm rate. Parameters of Fuzzy ART technique such as choice parameter and vigilance parameter have major impact on final outcome. So to overcome the problem of low detection rate and higher false alarm rate we need to optimize these parameters of Fuzzy ART. For optimizing of these parameters external fuzzy controller is used. Experimental results shows the different values of parameters give different detection rates and false alarm rate. And by optimizing the parameters we got reduction in false alarm rate by 2.07%.

KEYWORDS: Intrusion Detection System (IDS), Neural Network, Clustering, Adaptive Resonance Theory, Fuzzy Adaptive Resonance Theory (F-ART), Fuzzycontroller.

INTRODUCTION

Computer networking has become one of the important aspect for our daily communication. Various activities such as e-commerce and e-government are rapidly growing through internet. Along with this progress there comes a threat from spammers, attackers and criminal enterprises. Different hacking tools are appearing on daily basis which exploits the vulnerability of the system. So computer network security has become very important in order to develop a mechanism that provides a defense against the intrusions from attackers.

Intrusion Detection System (IDS) thus acts as a second line important component of the defense-in depth security mechanism. The intrusion Detection problem has received great interest from past few years. It is a good choice as compared to antivirus, firewall and other security tools[18]. Many approaches have been proposed which include statistical [10], machine learning [11], data mining [12] and immunological inspired techniques [13]. Among all these approaches neural networks are found efficient as they have self learning capability and performs task that a linear program cannot [16].

Adaptive Resonance Theory is one of the neural network approaches that have been proved as an effective method for intrusion detection as they are adaptive in nature which does not requires any intervention by a domain expert [2]. Among all the ART models, Fuzzy ART model are mainly preferred as it can process binary as well as continuous values by the means of unsupervised learning. Further, it provides rapid stable clustering of both continuous as well as binary input patterns while other algorithms requires lengthy process, storage and manipulation of large matrices. Fuzzy Adaptive Resonance Theory (ART) is also capable of on-line learning [20].

The main thing in Fuzzy ART algorithm is parameters such as vigilance and choice function plays an important role in overall performance of the system [15]. Proper tuning must be done to achieve higher accuracy. So this proposed approach discusses optimizing the parameters of Fuzzy ART using fuzzy controller and to detect all four attacks with higher accuracy.

From the survey previously done in paper [14], the challenges were to improve detection rate and to

reduce false alarm rate at some proper parametric value. Features reduction and normalization also has impact on final outcome so, Fuzzy ART achieves results by proper tuning of parameter using fuzzy controller [9] and detecting all four attacks along with some pre-processing by using 22 features on the basis of paper [7]

RELATED WORK

Various IDS are built with the approach of ART [6], Fuzzy ART [1][2][3][21], ART 2A [5][15] and MART2 [4]. Majority of such systems have used KDD Cup1999 data set[22] for training and testing purpose. As it is standard data set and easily available. Main objective behind all such systems is to have high detection rate, and to reduce false alarm rate [3]. From the survey following challenges were found. They were low detection rate for all attacks, higher false alarm rate and how parameters have affect on final outcome. Hence, focus of our paper is to reduce false alarm rate and it will show how vigilance parameter has affect on each class.

Our system is similar to paper [2], there they are using Fuzzy ART approach combining with pre-processing technique to improve the detection rate of only for two attacks Dos and probe attacks. In our system we are also improving the detection rate of U2R and R2L attacks along with Dos and probe by using Fuzzy ART approach with 22 relevant features chosen from paper [7].

PROPOSED WORK

Our proposed model of Fuzzy ART and optimizing its parameters is shown in figure 1, we are using KDD Cup 1999 dataset as it is benchmark for the IDS system. This data set needs to be pre-processed before using it. Out of 41 features, 22 relevant features are selected according to paper [7][17]. It contains symbolic data and symbolic data is not accepted by neural network. So to process such data, normalization is needed to be done [19]. So in normalization symbolic data is converted to numeric data [8]. After this conversion, scaling is needed to be done in which the attribute having very higher range is scaled down to the [-1,1] or [0,1] range.

In Fuzzy ART algorithm weights are initialized to one and input vector is taken of M-dimension. i.e. 22 dimension vectors.

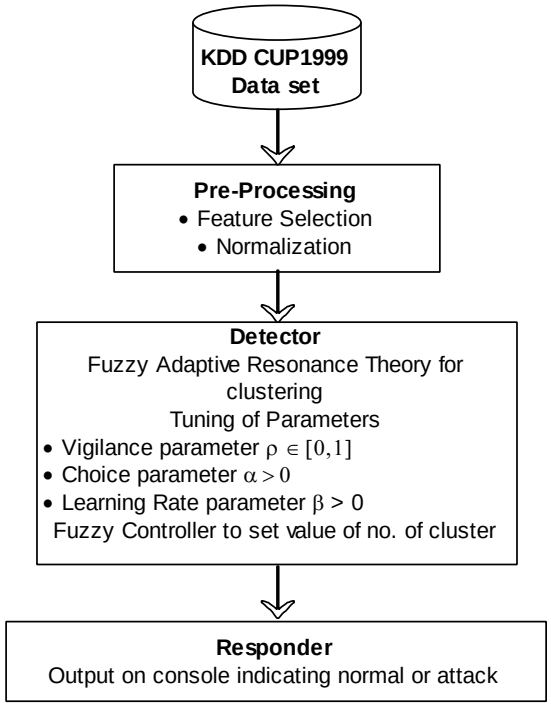

Figure 1: Proposed Model

According to our proposed model each neuron in the input layer will correspond to the single attribute of the dataset. Complement coding is done for this input vector. Following equations used for computation are similar to the standard fuzzy ART algorithm.

$$I = (a, a^c) \quad (1)$$

Three parameters are initialized according to their given range. Further these parameters are needed to be optimized for best results. Choice function is calculated for each node in the output layer and best matching category is selected.

$$T_j(I) = \frac{|I \wedge W_j|}{\alpha + |W_j|} \quad (2)$$

$$T_j = \max \{ T_j : j = 1,2,..N\} \quad (3)$$

After that resonance is checked for each of the selected category. If the condition expressed in the equation below is true then category is selected and the cluster is accepted.

$$\frac{|I \wedge W_j|}{|I|} \geq \rho \quad (4)$$

After selecting the category, its weight is updated according to equation (5).

$$W_j^{(new)} = \beta(I \wedge W_j^{(old)}) + (1-\beta) W_j^{(old)} \quad (5)$$

For my proposed work expected maximum numbers of clusters in output layer will be 5: These clusters are nothing but the similar input cases. For my proposed work there will be five clusters. Normal, Dos, Probe, U2R and R2L attack clusters.

After training is completed by using Fuzzy ART, the external controller [9] will check the actual number of clusters formed with the desired number of cluster. If mismatch occurs then tuning of vigilance parameter is required.

For instance if N_a (actual no. of clusters) < N_d (desired no. of clusters) then the increase in the value of vigilance parameter is required, and if $N_a > N_d$ then the decrease in the value of vigilance parameter is required.

After training is complete using Fuzzy ART algorithm cluster labelling is required. In cluster labelling, the Normal Membership Factor (NMF) is implemented in order to label the clusters. The NMF identifies number of instances in term of normal or four categories of attacks. Its relation to each of the clusters is taken into consideration by checking the degree of probability of clusters belongingness.
In testing, the Choice function is calculated for input vector and committed node, Choice function with maximum value is selected. After that the resonance is tested for the given category. This process is repeated for whole dataset and stored into some file for further analysis. The performance measure is done on the basis of True Positive, True Negative, False Positive, False Negative, Accuracy, Precision and Detection rate of individual attacks. Following are the equation used for performance analysis.

1) True Positive

$$(TP) = \frac{\text{Correct Detected Attacks}}{\text{Total no.of Attacks}} \quad (6)$$

2) False Positive

$$(FP) = \frac{No.of\ Normal\ Detected\ as\ Attack}{Total\ no.of\ Normal} \quad (7)$$

3) True Negative

$$(TN) = \frac{\text{Correct Detected Normal}}{\text{Total no.of Normal}} \quad (8)$$

4) False Negative

$$(FN) = \frac{\text{No.of Intrusion Detected as Normal}}{\text{Total no.of Attacks}} \quad (9)$$

5) $$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

6) $$\text{Precision} = \frac{TP}{TP+FP} \quad (11)$$

7) $$\text{Detection Rate} = \frac{\text{correctly detected attacks}}{\text{Total number of attacks}} \quad (12)$$

Experimentation Results

In implementation we have carried out three experiments. First experiment shows performance evaluation based on accuracy and false alarm rate base on different vigilance parameter value. Second experiment shows detection rate of individual class and third experiment with live packets testing dataset.

Experiment-1 results:

Table 1: Accuracy at different vigilance parameter

Vigilance value	Accuracy	
	22 Features	41 Features
0.2	65.9682	60.3655
0.3	67.0369	62.1896
0.4	68.3667	64.5896
0.5	72.773042	65.30497
0.6	78.6975	72.6489
0.65	79.75977	80.08975
0.75	83.74551	81.78042
0.77	87.08211	85.077342
0.80	92.4739	87.6983
0.9	90.5697	87.1965
0.95	90.0216	86.8931

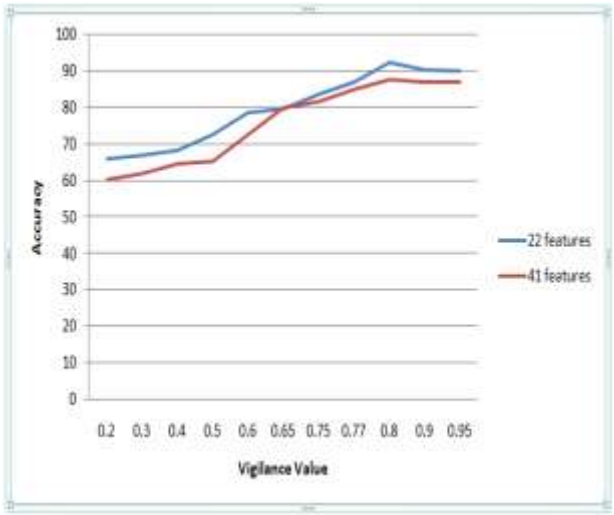

Figure 2: Accuracy at different vigilance

Table 1 and figure 2 shows that how accuracy for 22 features as well as 41 features are affected by vigilance parameter. When vigilance value increases its accuracy also increases. But there is one saturation point at which the detection rate further starts to decrease as soon as the vigilance value is being increased.

Table 2: False Alarm Rate at different vigilance parameter

Vigilance value	False Alarm Rate	
	22 Features	41 Features
0.2	0.86	1.50
0.3	0.91	1.54
0.4	0.93	1.59
0.5	0.94	1.61
0.6	0.98	1.75
0.65	1.52	1.77
0.75	1.28	1.27
0.77	1.67	1.57
0.80	1.79	1.87
0.9	2.16	2.79
0.95	2.56	2.98

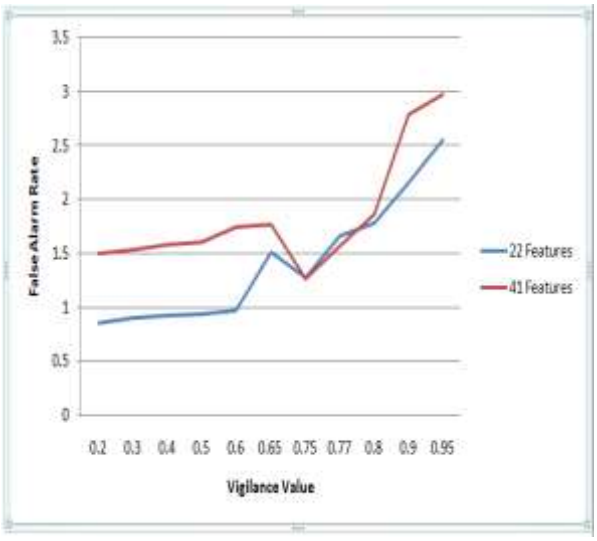

Figure 3: False Alarm Rate at different vigilance

From the above table 2 and figure 3 shows how false alarm rate for 22 features as well as 41 features changes at different vigilance value. When value of vigilance parameter is increased there is also increment in false alarm rate. But at vigilance value of 0.75 there is considerable reduction in false alarm rate.

Experiment-2 Results:

Table 3,4 and 5 shows the detection rate for each class at three different vigilance parameter. First value of vigilance parameter in table 3 shows that when value is small it produces larger cluster and detection rate for individual class is less. Gradually we increase vigilance parameter value. Second value for vigilance value in table 4 shows that when value is increased finer clusters are formed and detection rate for individual class also increases. Table 5 shows the optimized value of vigilance parameter. At that value we get maximum detection rate for each class. Further increment in vigilance parameter can degrade the detection rate for individual class. From the analysis we can also say that more the vigilance value finer the clusters are formed.

Table 3: Results at vigilance 0.2

Vigilance Parameter	Class	Detection Rate
0.2	Normal	75.4896
	U2R	32.7893
	R2L	50.3569
	Probe	61.3569
	Dos	70.9865

Table 4: Results at vigilance 0.77

Vigilance Parameter	Class	Detection Rate
0.77	Normal	84.8432
	U2R	49.9830
	R2L	57.1983
	Probe	64.5893
	Dos	72.3649

Table 5: Results at vigilance 0.8

Vigilance Parameter	Class	Detection Rate
0.8	Normal	89.8656
	U2R	54.6635
	R2L	60.6685
	Probe	65.3849
	Dos	74.6845

Experiment 3 results:

Implementation was done with KDD cup 1999 training dataset. It consists of normal data as well as four types of attack. Experiment was carried out by using 22 relevant features. During testing live data was captured by using BRO IDS and converted in to KDD cup 1999 features using various programs like bro script, C program and Java program. Note that testing dataset do not contain any attack so the detection rate of Normal was calculated. The detection rate of Normal was 86.89 %

COMPARISON ANALYSIS

Table 6 shows the comparison with the previous work using Fuzzy ART. In that paper [2] they have detected only two attacks with some reduced features and they got detection rate of 99.44 % and below in table 6 shows our proposed work in which all four attacks are detected by using 22 features of KDD Cup data set. The comparison was carried out at same value of Vigilance.

Table 6: Comparison with previous work [2]

Vigilance Value	Over all Detection Rate	Class	
0.80	99.44 %	DOS	NA
		Probe	NA
0.80	92.47%	Normal	89.86
		U2R	54.66
		R2L	60.66
		DOS	65.38
		Probe	74.68

Table 7: Comparison with previous work [3]

Model	False Alarm Rate
PCA FART[3]	3.86 %
Proposed work	1.79 %

Table 7 shows the comparison of proposed work with previous work carried out using PCA-FART [3]. In that model they are getting good detection rate as compared to our proposed work but the higher false alarm rate. Proposed work shows lower false alarm rate as compared to this previous work.

CONCLUSION

This paper provides detailed information regarding IDS using Fuzzy ART technique. Fuzzy ART is proved to be beneficial because it supports adaptive learning. Proposed work shows that how parameters of Fuzzy ART technique such as choice parameter and vigilance parameter affects the final outcome. Value of this vigilance parameter is optimized in order to get good results. When value of vigilance parameter is small it produces large classes and when value of vigilance parameter increases its produces smaller size of classes. In this way vigilance parameter is used to decide class size. Proper tuning of vigilance parameter is required and for that Fuzzy controller is used. Experimental results shows detection rates at different vigilance value for all attacks. Comparison with previous paper is also shown in which they have detected only two attacks which we have extended to all classes of attack. Proposed work shows the reduction of 2.07% in false alarm rate compared to previous work.

DECLARATION

The content of this paper is written by Author 1(Krishna Champaneria) while Author 2(Prof. Bhavin Shah) had guided the work and Author 3(Asst. Prof Krunal Panchal) has reviewed this paper. Hence Author 1 is responsible for the content and issues related with plagiarism.

REFERENCES

[1] Bin Haji Ismail, Abdul Samad, et al. "A novel method for unsupervised anomaly detection using unlabelled data." Computational Sciences and Its Applications, 2008. ICCSA'08. International Conference on. IEEE, 2008. ISBN: 978-0-7695-3243-1

[2] Ngamwitthayanon, Nawa, and Naruemon Wattanapongsakorn. "Fuzzy-ART in network anomaly detection with feature-reduction dataset." Networked Computing (INC), 2011 The 7th International Conference on. IEEE, 2011. ISBN: 978-1-4577-1129-9

[3] Somwang, Preecha, and Woraphon Lilakiatsakun "Intrusion detection technique by using fuzzy ART on computer network security" Industrial Electronics and Applications (ICIEA), 2012 7th IEEE Conference on. IEEE, 2012. ISBN: 978-1-4577-2118-2

[4] Xiao, Junbi, and Hao Song. "A novel intrusion detection method based on adaptive resonance theory and principal component analysis." Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on. Vol. 3. IEEE, 2009.

[5] Han, Xiao. "An improved intrusion detection system based on neural network."Intelligent Computing and Intelligent Systems, 2009. ICIS 2009. IEEE International Conference on. Vol. 1. IEEE, 2009. ISBN: 978-1-4244-4754-1

[6] Prothives, Kanok, and Surat Srinoy. "Integrating ART and Rough Set Approach for Computer Security." Proceedings of the International MultiConference of Engineers and Computer Scientists. Vol. 1. 2009

[7] Tesfahun, Abebe, and D. Lalitha Bhaskari. "Intrusion Detection Using Random Forests Classifier with SMOTE and Feature Reduction." Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 2013 International Conference on. IEEE, 2013.

[8] Prof.Bhavin Shah, Prof.Bhushan H Trivedi. "Data Set normalization: For Anomaly Detection Using Back Propagation Neural Network"

[9] Choi, Jai J., et al. "Fuzzy parameter adaptation in neural systems." Neural Networks, 1992. IJCNN., International Joint Conference on. Vol. 1. IEEE, 1992.

[10] Bace, Rebecca, and Peter Mell. NIST special publication on intrusion detection systems. BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2001.

[11] Sundaram, A. "An introduction to intrusion detection, Crossroads": The ACM student magazine, 2 (4)." (1996).
[12] Denning, Dorothy E. "An intrusion-detection model." Software Engineering, IEEE Transactions on 2 (1987): 222-232. ISSN: 0098-5589
[13] T.Lane, "Machine Learning techniques for the computer Security," PhD thesis, Purdue University,2000
[14] Champaneria, Krishna, Bhavin Shah, and Asst Prof Krunal Panchal. "Survey of Adaptive Resonance Theory Techniques in IDS."
[15] Frank, Thomas, K-F. Kraiss, and Torsten Kuhlen. "Comparative analysis of fuzzy ART and ART-2A network clustering performance." Neural Networks, IEEE Transactions on 9.3 (1998): 544-559.
[16] Shah, Bhavin, and Bhushan H. Trivedi. "Artificial neural network based intrusion detection system: A survey." International Journal of Computer Applications 39.6 (2012).
[17] Shah, Bhavin, and Bhushan H. Trivedi. "Reducing Features of KDD CUP 1999 Dataset For Anomaly Detection Using Back Propagation Neural Network."Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on. IEEE, 2015.
[18] Shah, Bhavin, and Bhushan H. Trivedi. "Improving Performance of Mobile Agent Based Intrusion Detection System." Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on. IEEE, 2015.
[19] Shah, Bhavin, and Bhushan H. Trivedi. "Optimizing Back Propagation Parameters For Anomaly Detection." IEEE-International Conference on Research and Development Prospectus on Engineering and Technology (ICRDPET). 2013.
[20] Harald Ruda and Magnús Snorrason "Adaptive Preprocessing for On-Line Learning with Adaptive Resonance Theory (ART) Networks"
[21] Rung-Ching Chen, Kai-Fang Cheng, Cheng-Chia Hsieh "USING FUZZY NEURAL NETWORKS AND RULE HEURISTICS FORANOMALY INTRUSION DETECTION ON DATABASE CONNECTION" Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008.
[22] KDD Cup 1999 Data: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html