A Best Approach In Intrusion Detection For Computer Network PNN /GRNN/ RBF

Farzad Fekrazad[1]

[1] **Azad Islamic Universty ,computer Department**
Tehran,Iran

Abstract

As attacks became more complicated, the traditional and contemporary methods such as firewalls were not successful and suitable in exact diagnosis. This caused Intrusion detection system (IDS) to finally the strictly centralized role in network security. first is misuse and second is abnormal detection. Misuse detection compares data to well-known attack signature so it cannot diagnose unknown attacks. Abnormal detection has better performance to detect new attacks by modeling. In most cases, Attacks has been centralized into four groups: DoS, Probe, U2R, and R2L. There are many approaches have been used to identify attacks in Intrusion detection system. One of them is artificial neural network who called (ANN). This paper strictly centralized approach to implement a hybrid Artificial Neural Network in IDS based on RBF. This paper investigates the effectiveness we shall explor our results by compared to (SVM) .

Keywords: IDS, Neural Network, RBF/GRNN/PNN.

1. Introduction

Since the **contemporary** prevention methods have failed to protect network completely, IDS now has find an important role in providing security.

first, Misuse detection is done by comparing data to descriptions of intrusion behavior. In anomaly detection, normal behavior is modeled so abnormal behavior can be found out. Anomaly detection can be found out in two ways. In this method, it will been assumed that behavior of monitored target has been never changes. It extracts data from usual habit behavior of users [1].

Attacks fall into four main categories:

- R2L: Remote to local, unauthorized access from a remote machine, e.g. guessing password;
- U2R: User to root, unauthorized access to local super user (root) privileges, e.g., various ``buffer overflow" attacks;

probing: supervision and other probing, e.g., port scanning.

Up to now different approaches have been used in IDS. ANN and Fuzzy logic are two of the most popular and effective that which will be discussed later. is another effective approach. It can make flexible models for anomaly and misuse detection. Another good approach is evolutionary computation. It can greatly be used in searching for optimal solutions, automatic model design, and classifiers to solve detection problems. Artificial immune systems can widely increase misuse and abnormal detection. Their attributes can help to have a dynamic, distributed, and self organized intrusion detection system [1]. Ant colony optimization and particle swarm intelligence have also acceptable performance in intrusion detection system.

An (ANN)[1]consists of neurons which are processing units. They can be classified into two groups: supervised learning, and unsupervised learning. When IDS was first developed, Multi-layered feed forward neural network back-propagation (MLFF-BP) was effectively used for anomaly detection. In some studies, information such as command sets, and login host addresses were used to distinguish normal and abnormal behavior while others considered patterns of commands or software behavior [2-5]. Redial basis function neural networks (RBF) are popular type of feed forward (NN)[2]. They are faster than back propagation because they do classification by measuring distances between inputs and the centers of RBF hidden neurons. Until now different studies have been done on RBF. Previously a hierarchical RBF was proposed for misuse and anomaly detection [6]. In first layer, RBF anomaly detector decides an event is normal or not. Misuse RBF detector is done in second layer. Other studies showed that MLFF-BP is better than RBF for misuse detection but it is time consuming in training . For anomaly detection RBF has better performance [6,7].

Other studies have been done on other types of neural networksThese networks can be used to predict whether the event is an attack or not. They use memory for

[1] artificial neural network
[2] neural networks

prediction. SOMs are popular neural network for anomaly detection [13,14-16]. It has also been tested for misuse detection [17-19].

(PNN)[1] makes training faster. It uses a space of linear functions in high dimensional features. It can be effectively used in classification.. Simulation can be found in section III and section IV includes conclusion.

2. PROPOSED Methods

PNN is used for kernel analysis. Its a normalized RBF network in which there is a hidden unit centered at every training case. These RBF units are called "kernels" and are usually (PDF)[2] such as the Gaussian. The (HTO)[3] weights are usually 1 or 0; for each hidden unit, a weight of 1 is used for the connection going to the output that the case belongs to, while all other connections are given weights of 0. These weights can be adjusted for the prior probabilities of each class. So the only weights that need to be learned are the widths of the RBF units. These widths (often a single width is used) are called "smoothing parameters" or “bandwidths" and are usually chosen by cross-validation or by more esoteric methods that are not well-known in the neural net literature.

Speech’s claimed that a PNN trains 100,000 times faster than back propagation is atbest misleading [23-25]. While they are not iterative in the same sense as back propagation, kernel methods require estimating the kernel bandwidth and this requires accessing the data many times. Furthermore, computing a single output value with kernel methods requires either accessing the entire training data or clever programming and either way is much slower than computing an output with a feed forward net. There are a variety of methods for training feed forward nets that are much faster than standard back propagation. PNN is a universal approximate or for smooth class-conditional densities, so it should be able to solve any smooth classification problem given enough data. The main drawback of PNN is that, like kernel methods in general, it suffers badly from the curse of dimensionality. PNN cannot ignore irrelevant inputs without major modifications to the basic algorithm.

We know that the number of patterns in the training set affects the number of centers (more patterns imply more Gaussians), but this is mediated by the dispersion of the clusters. For standard RBF's, the supervised segment of the network only needs to produce a linear combination of the output at the unsupervised layer.

[1] Probabilistic Neural Network
[2] probability density functions
[3] hidden-to-output

3. SIMULATION

The 1998 DARPA Intrusion Detection Evaluation Program was prepared and managed by MIT Lincoln Labs. Their purpose was to evaluate research in intrusion detection. A standard set of data which includes a large variety of intrusion simulated in a military network environment was prepared.

A connection is a sequence of TCP packets starting and ending at some well defined times, between which data flows to and or from a source IP address to a target IP address under some well defined protocol. Each connection is labeled as either normal, or as an attack, with exactly one specific attack type. TABLE I illustrates the spectrum of EachTCP connection has 41 features.

Table I: FEATURES OF EACH TCP CONNECTION

Feature	Attribute
Duration	Continuous
service	Symbolic
protocol_type	Symbolic
Land	Symbolic
src_bytes	Continuous
dst_bytes	Continuous
Flag	Symbolic
wrong_fragment	Continuous
Urgent	Continuous
Hot	Continuous
num_failed_logins	Continuous
logged_in	Symbolic
num_compromised	Continuous
root_shell	Continuous
su_attempted	Continuous
num_root	Continuous
num_file_creations	Continuous
num_shells	Continuous
num_access_files	Continuous
num_outbound_cmds	Continuous
is_host_login	Symbolic
is_guest_login	Symbolic
Count	Continuous

In order to evaluate our methods, the following parameters are calculated and the results are shown in TABLE. II.

- (TPR)[1]: $\frac{TP}{TP+FN}$, also known as detection rate (DR)or sensitivity.
- (FNR)[2]: $\frac{FP}{TN+FP}$: 1 _ specificity

Table II : SIMULATION RESULTS FOR RBF/GRNN/PNN

Attack	True positive rate	False negative rate	False positive rate
Normal	99.6	17.4	0.4
Probe	96.27	2.94	3.27
R2L	85.7	15.9	14.3
U2R	96	0	4

Our simulation was done in 2 min. The mean square error in all our simulations were around 0.0000001 to 0.0000005 which shows its high accuracy. In order to evaluate our suggested approch method, we compare our results to SVM and SOM. Self-organizing feature maps (SOFMs) transform the input of arbitrary dimension into a one or more dimensional discrete map subject to a topological (neighborhood preserving) constraint. The feature maps are computed using Kohonen unsupervised learning. The output or result of the SOFM can be used as input to a supervised classification neural network such as the MLP. This network's key advantage is the clustering produced by the SOFM which reduces the input space into representative features using a self-organizing process. Hence the underlying structure of the input space is kept,

We simulated our data with SVM and SOM. The results can be seen in TABLE III and IV.

Table III: SIMULATION RESULTS FOR (SVM)

Table IV: SIMULATION RESULTS SELF ORGANIZING MAP

[1] True positive rate

[2] False negative rate

Attack	True positive rate	False negative rate	False positive rate
Normal	99	11	3
Probe	100	0	77
R2L	58	50	50
U2R	80	30	35

Table IV: Several attack in Net work

Attack	Solution	FPR
Probe	90	83.2
U2R	70	63.4
Normal	89	90
R2L	50	98.2

4. Conclusions

The simulation results show that RBF/GRNN/PNN has better performance comparing to (SVM) and self organizing map. This is proved by higher DR and lower FPR. This illustrates that RBF/GRNN/PNN acts more successfully in classification.

References

[1] A. A. Name, and B. B. Name, Book Title, Place: Press, Year.

[1] S. X. Wu, W. Banzhaf, “The use of computational intelligence in intrusion detection systems: A review,” Applied Soft computing, vol. 10, pp. 1-35, 2010.

[2] J. Ryan, M.J. Lin, and R. Miikkulainen, “Intrusion detection with neural networks,” Advances in Neural Information Processing Systems, vol. 10, pp. 943–949, 1998.

[3] K. Tan, “The application of neural networks to unix computer security,”Proceedings of IEEE International Conference on Neural Networks, vol. 1, Perth,WA, Australia, November/December 1995, IEEE Press, pp. 476–481, 1995.

Attack	True positive rate	False negative rate	False positive rate
Normal	99	10	81.5
Probe	95.0	16.8	5.87
R2L	96.3	1. 8	33.6
U2R	77.8	36.6	8.4

[4] A.K. Ghosh, A. Schwartzbard, “A study in using neural networks for anomaly andmisuse detection,” Proceedings of the 8th USENIX Security Symposium,

vol. 8,Washington, DC, USA, 23–36 August, pp. 141–152, 1999.

[5] A.K. Ghosh, J. Wanken, and F. Charron, "Detecting anomalous and unknown intrusionsagainst programs,"Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC'98), Phoenix, AZ, USA, 7–11 December 1998, IEEEComputer Society, pp. 259–267,1998.

[6] J. Jiang, C. Zhang, and M. Kame, "RBF-based real-time hierarchical intrusion detectionsystems,"Proceedings of the International Joint Conference on Neural Networks (IJCNN'03), vol. 2, Portland, OR, USA, 20–24 July, IEEE Press, pp.1512–1516, 2003.

[7] E. Leon, O. Nasraoui, and J. Gomez, "Anomaly detection based on unsupervised nicheclustering with application to network intrusion detection,"Proceedings of the IEEE Congress on EvolutionaryComputation (CEC'04), vol. 1, Portland, OR,USA, 19–23 June 2004, IEEE Press, pp. 502–508, 2004.

[8] A. Hofmann, C. Schmitz,and B. Sick, "Rule extraction from neural networks forintrusion detection in computer networks,"IEEE International Conference on Systems, Man and Cybernetics, vol. 2, 5–8 October 2003, IEEE Press, pp.1259–1265, 2003.

[9] J. Jiang, C. Zhang, and M. Kame, "RBF-based real-time ierarchical intrusion detectionsystems,"Proceedings of the International Joint Conference on Neural Networks (IJCNN'03), vol. 2, Portland, OR, USA, 20–24 July, IEEE Press, pp.1512–1516, 2003.

[10] Z. Liu, G. Florez, and S.M. Bridges, "A comparison of input representations in neuralnetworks: a case study in intrusion detection,"Proceedings of the International Joint Conference on Neural Networks (IJCNN'02), vol. 2, Honolulu, HI, USA,12–17 May 2002, IEEE Press, pp. 1708–1713, 2002.

[11] Z. Zhang, J. Li, C. Manikopoulos, J. Jorgenson, and J. Ucles, "IDE: a hierarchicalnetwork intrusion detection system using statistical preprocessing and neuralnetwork classification,"Proceedings of the 2001 IEEE Workshop Information Assurance and Security, West Point, NY, USA, IEEE Press, pp. 85–90, 2001.

[12] Y. Yu, F. Gao, and Y. Ge, "Hybrid BP/CNN neural network for intrusion detection,"Proceedings of the 3rd International Conference on Information security, vol. 85 of ACM International Conference Proceeding Series, pp. 226–228, 2004.

[13] T. Kohonen, "Self-organizing Maps," vol. 30 of Springer Series in InformationSciences, Springer, No. 3, Berlin, 2001.

[14] K. Fox, R. Henning, and J. Reed, "A neural network approach toward intrusion detection,"Proceedings of the 13th National Computer Security Conference, vol. 1,Washington, DC, USA, 1–4 October 1990, pp. 124–134,1990.

[15] A.J. Hoglund, K. Hatonen, and A.S. Sorvari, "A computer host-based user anomalydetction system using the self-organizing map," Proceedings of the IEEEINNS-ENNS International Joint Conference on Neural Networks (IJCNN'00), vol.5, Como, Italy, 24–27 July 2000, IEEE Press, pp. 411–416, 2000.

[16] W. Wang, X. Guan, X. Zhang, and L. Yang, "Profiling program behavior for anomalyintrusion detection based on the transition and frequency property of computeraudit data,"Computers & Security,vol. 25, No. 7, pp. 539–550, 2006.

[17] J. Cannady, J. Mahaffey, "The application of artificial neural networks to misusedetection: initial results," Proceedings of the 1st International Workshop on Recent Advances in Intrusion Detection (RAID 98), Louvain-la-Neuve, Belgium,14-16 September 1998, 1998.

[18] A. Bivens, C. Palagiri, R. Smith, B. Szymanski, and M. Embrechts, "Networkbasedintrusion detection using neural networks,"Intelligent Engineering Systems through Artificial Neural Networks,vol. 12, No. 1, pp. 579–584, 2002.

[19] C. Jirapummin, N. Wattanapongsakorn, and P. Kanthamanon, "Hybrid neural networksfor intrusion detection system,"The 2002 International Technical Conference on Circuits/Systems, Computers and Communications (ITCCSCC'02), vol. 7, Phuket, Thailand, 2002, pp. 928–931, 2002.

[20] Nello Cristianini and John Shawe-Taylor, "AnIntroducton to (SVM) s and other kernelbased learning methods", Tenth Reprint, Cambridge, University PressHand, 2006.

[21] Pai-Hasuen Chen, Chih-jen lin , and Bernhard, "Atutorial on (SVM) ", Department ofComputer Science & Information Engineering, NationalTaiwan University.

[22] S Mukkamala, G Janoski, A Sang "Intrusion Detectingusing Neural Network and (SVM) ",Proceeding of IEEE International Joint Conference inNeural Network, pp 1702-1707, 2002.

[23] D.J., "Kernel Discriminant Analysis,"Research Studies Press,1982.

[24] Lowe, D.G., "Similarity metric learning for a variable-kernel classifier," Neural Computation, vol. 7, pp. 72-85, 1995.

[25] McLachlan, G.J.,"Discriminant Analysis and Statistical Pattern Recognition,"Wiley, 1992.

[26] The KDD99 Dataset. Retrieved January 26, 2008, from http://kdd.ics.uci.edu/databases/kddcup99/task.html.

First Author Biographies should be limited to one paragraph consisting of the following: sequentially ordered list of degrees, including years achieved; sequentially ordered places of employ concluding with current employment; association with any official journals or conferences; major professional and/or academic achievements, i.e., best paper awards, research grants, etc.; any publication information (number of papers and titles of books published); current research interests; association with any professional associations. Do not specify email address here.