Designing the Abnormality Detection System Using Neural Networks

Homayun Motameni [1], Majid Aboutalebi[2], naznoosh etminan [3]

[1.] Member of Faculty Computer Engineering Department. Islamic Azad University Sari Branch, Sari, Iran
[2.] Computer enginnering department, Islamic Azad University Sari Branch, Sari, Iran
[3.] Computer enginnering department, Islamic Azad University Sari Branch, Sari, Iran
na.etminan@yahoo.com

Abstract: One of the solutions for securing the systems and computer networks is the set of intrusion detecting systems. These systems that are analogous to burglar alarms detect the suspicious events and intrusions in their supervising environment and alarm against such suspicious events. The objective of the security solutions such as encoding, shield, ID detection systems, etc. are to secure the systems and preventing any intrusion event. Since the complete security is an expensive process and it cannot be provided in practice, we will need a system for reporting the event and even find its roots and reasons instead of preventing such events. Intrusion detecting systems are designed and used for this reason. In this research we present a new method for designing the abnormality detection using neural networks. In this method, training the neural network of system is being done in a two-step and sequential form. We have tested this new model on five different neural systems and we have compared its efficiency with the models in which the training process is single-step. The five types of our used neural networks include PCA1-based Neural Network, SOFM2-based Neural Network, MLP3 neural network, GFF4 Neural Network, and Jordan- Elman Neural Network. Our tests and evaluations have been done using KDD CUP 99 database and we have used all network records for training and testing the network. The Results show that our offered model leads to a significant improvement in its detection scale and positive error scale in comparison with the simple system, so that our system has the same efficiency in comparison with its similar systems and even in some cases its efficiency is better than the similar systems.
[Homayun Motameni, Majid Aboutalebi, naznoosh etminan. Designing the Abnormality Detection System Using Neural Networks**.** *Academ Arena* 2018;10(2):113-118]. ISSN 1553-992X (print); ISSN 2158-771X (online). http://www.sciencepub.net/academia. 8. doi:10.7537/marsaaj100218.08.

Keywords: Abnormality Detection System, GFF Neural Network, Jordan- Elman Neural Network, MLP Neural Network, PCA Neural Network, SOFM Neural Network

[1] Principal Component Analysis
[2] Self-Organizing Feature Maps
[3] Multi-layer Perceptron
[4] Generalized Feed Forward

1. Introduction

Increasing growth of the computers has evolved the methods of information and data savings. Using such new methods for accessing the data has seriously threatened and jeopardized the security of the information by unauthorized users.

Being successful in securing the information depends on the protection of the information and information systems against the intrusions. Accordingly, several security services are being used. The selected services have to enjoy the needed potentials for creating a desirable protecting system, timely detection of the intrusions, and the potential for the prompt reaction. Thus we can consider the three components of protection, detection and reaction as the bases of the selected strategy. Secure protection, timely detection, and prompt reaction are the factors that have to be considered in establishing any security system. Beside the integrity of their protecting mechanisms, the organizations and institutes have to expect information intrusions and they must equip themselves with the detecting tools and prompt reaction routines in order to be ready to encounter the intruders and recycling their own information at a due time. One of the most important principles is to make the parallel between three elements of human, technology, and operation. Today, several technologies are being used in order to provide the needed services for securing the information and detecting the information intruders. The organizations and institutes must determine the desirable policies and process for using a specific technology so that the grounds for the selection and application of proper technology in the relevant organization can be

provided. In this regard, the organization has to pay special attention to the security policy, the principles of information security, the standards and architecture of information technology, using the products of well-known providers, the instruction of the configuration, and the needed processes for evaluating the risks of the integrated and interconnected systems. In this research we will study all types of the systems of intrusion detection and accordingly, we will design a system for strengthening the computer networks against all types of the network-based intrusions so that the systems can have a higher efficiency and lower errors. Moreover, since the available intrusion detection systems are single-step, one of our objectives is to design a hierarchical multi-step system for detecting the intrusion and the comparison of its efficiency with other similar systems. We have evaluated our suggested systems using stimulation and then compared its results with the available researcher of the literature. The environment of our stimulation of the neural network has been MATLAB and other applied softwares.

2. Literature review

2.1. Intrusion

Tens of operating systems and thousands of applicable programs have been provided up to now. The history shows that all operating systems have been full of vulnerabilities regardless of their capacities and magnitudes. All versions of Windows, XP and Vista to its most recent ones are full of weaknesses and security breaches. An intruder targets these weaknesses and breaches. The first target for the intrusion is the OS stack. The spill-over of the stack can interrupt any applicable program or the operating system. Today, the mechanisms of the (intentionally) stack spill-over is one of the most fatal and current ways of attacking the vulnerable machines. Any program or process that has used the stack or buffer in any part of its code can be interrupted due to the mentioned spillover. The intruder discovers and targets the processes that have used the stack or buffer without any prediction for their spillover. A very complicated and dangerous type of attacking the stack is that the intruder manages to spill-over the stack in a way that he can capture the control of the running that program or process after the mentioned spillover. The mechanism of attacking the stack can be describes as follow: the intruder sends some data to the running processes whose size is bigger than the size of the buffer space. These data can be the codes of the running machine. Due to the shortage of the buffer space, these data violate the borders of the stack and ever rewrite the return pointer from the function. After completing the function, the running control returns to the place where the return pointer commands. If the value of this return pointer is bigger than the pointer function, then the program will be interrupted and hanged; but if it is adjusted on a precise value, then the running control will be transferred to a place where the intruder points to.

2.2. Detecting the intrusion

Intrusion detection is a process in which an intrusion to the system is detected by observing the accessible information about the system mode and supervision over the activities of the user. The intruder can be an external entity or an internal user within the system who tries to access the unauthorized information. The intruders can be classified in two general groups:

External intruders: those who have not allowed access to a system they are working with;

Internal intruders: those who have the allowed and limited access to the system but violate their legal rights of access.

Internal users are classified in two groups as well: anonymous users, and illegitimate users. Anonymous users are those who use the certificates and authority of other legal users, while illegitimate users are those who manage to escape from the supervising and revising parameters in any possible way (Siddiqui, 2000). (Figure 1).

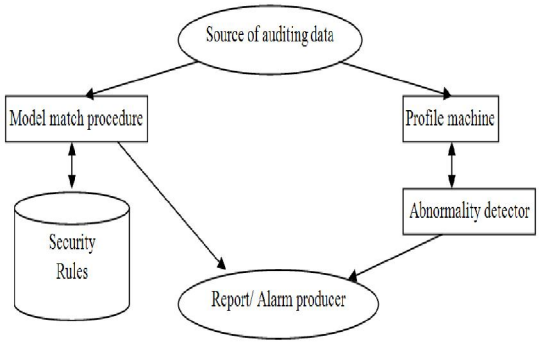

Figure 2. General Intrusion Detection System

2.3. Different types of intrusions

The intrusions can be classified in 4 groups depending on the goals of the intruder and the dimension of the security targeted (Sharafat and Rasti, 2006):

R2L attacks (remote attacks)

U2R attacks (user's attack to the root)

Probe attacks (scanning attacks)

DoS attacks (service shutting down attacks) (Figure 2)

This attacks can be fulfilled locally (on the target system) or remotely (using the network). There are several studies on the systems of abnormality detection in the literature. The most important researches of this subject are as follow.

The first intrusion detection system for detecting the abnormalities was designed by Javitz and Valdes (Wang, et al, 2006). Ghosh and Wanken offered a method for detecting the abnormalities and anonymous intrusion in 1998 (Amini, et al, 2006). Besides, in

2002, Heywood and Likodwiski designed a system for detecting the active abnormalities using the neural networks (Jazzar, et al, 2008).

In 2005, Nguyen conducted his research using two SOM neural networks where the training of these two networks was attacking more than the intrusion connections. The neural network of this research has an intermediate layer with 20 input neurons and 1 output neuron (Cordella, 2007).

Following their research using DARPA database in 2003, in 2006 Money and Kaplantizir extracted 41 characteristics of the intrusion and non-intrusion connections and then, based on the 41 extracted characteristics, they trained the designed neural network (Lui, et al, 2006).

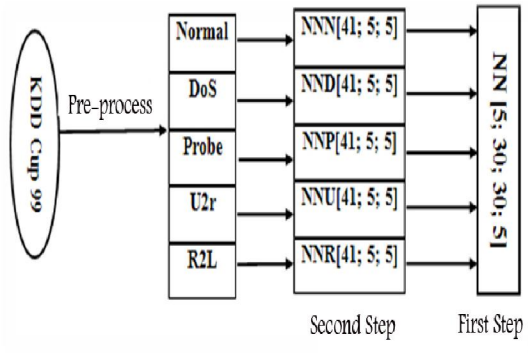

Figure 1. The structure of suggested model for abnormality detection system

In 2006, ALAN BIVENS Group from the American Enslaver Polytechnic Institute used the SOM Neural Network and DARPA database to design a network- based modular system of intrusion detection. In this research, after training the designed neural network, the network was able to detect the intrusion on the basis of the intensity of the traffic of input connections (Zhang, et al, 2005; Kayasick, et al, 2000).

3. Methodology

First we extract the intrusion and non-intrusion connections from DARPA database each of which has 41 features. Then we select N number out of the 41 features. Then we train these connections along with the N feature to the neural network. Then we apply another number of the connections that have been extracted before but have not been participated in the training of neural network in order to test the system and finally the intrusion event and the type of intrusion are specified. The main goals of this research are as follow:

- Obtaining a new method in designing the intrusion detection system.
- Strengthening the computer networks against all types of attacks.
- Using the system in securing databases, security centers, and commercial centers.

4. Data analysis

In order to have a better comparison between the designed system of the suggested method and the simple method, we have summarized the results in table 1. In this table, the method that has been used in the process of training the neural network in the system, along with the percentage of the system outputs (classification scale) and the parameters for the comparison of the system are presented.

Table 1. Comparing the results of the intrusion detection system in the suggested method and simple method

	Classification Scale of Neural Network					Evaluation Parameters		
Neural Network Training Method	Normal (%)	DoS (%)	Probe (%)	U2R (%)	R2L (%)	DR (%)	EP (%)	CPE
Suggested method with PCA	100	99.554	100	0	99.981	99.596	0.404	0.008105
Simple method with PCA	99.67	25.6	9.65	0	0	38.46	61.54	0.841
Suggested method with SOFM	100	100	100	100	100	100	0	0
Simple method with SOFM	99.73	96.30	51.61	0	0.0124	91.29	8.71	0.272
Suggested method with MLP	99.998	100	100	96.49	100	99.997	0.003	0.000804
Simple method with MLP	96.46	96.75	84.64	67.54	3.49	91.66	8.4	0.258
Suggested method with GFF	99.997	99.993	100	96.930	99.981	99.992	0.009	0.000122
Simple method with GFF	97.08	96.59	82.99	25	6.8	91.77	8.33	0.252
Suggested method with J/E	99.997	99.452	100	100	100	99.594	0.406	0.007649
Simple method with J/E	98.6	96.6	91.89	22.81	2.81	91.99	8.01	0.259

As it is shown in the table, the new method for training the abnormality detection system on all 5 types of neural network in the system has led to significantly better results in comparison to the single-step training method, especially in the case of SOFM neural network the results are excellent. At the following, we compare the designed system of the suggested method with other designed systems in their best and worst modes. The results can be seen in table 2.

Table 2. Comparing the results of the suggested method with other methods

Neural Network Training Method		Classification Scale of Neural Network					Evaluation Parameters		
		Normal (%)	DoS (%)	Probe (%)	U2R (%)	R2L (%)	DR (%)	EP (%)	CPE
Suggested method	Best result	100	100	100	100	100	100	0	0
	Worst result	99.957	99.452	100	100	100	99.594	0.406	0.007649
Jazzar, et al, 2008		99.51	98.37	88.4	84.33	71.13	90	10.9	-
Beghdad, 2007		94.9	99.46	95.17	0	90.76	98.49	-	-
Shanmugam & Idris, 2007		99.70	99.95	99.45	79.96	100	99.90	-	-
Beghdad, 2007		99.85	99.36	92.45	0	0	92.16	-	-
Toosi & Kahani, 2007		98.2	99.5	84.1	14.1	31.5	95.3	1.9	0.1579
Degang, et al, 2007		-	85	69.3	64.9	70	76.3	0.78	-

If we compare the results on the basis of their classification scale, the main problem is the low classification scale in U2R and R2L classes in most abnormality detection systems. The main reason of this low numbers is the low number of the records of these categories in the database (52 records for U2R and 1126 records for R2L). But in the suggested method, these values have reached to their highest number, i.e. 100%. The reason of this improvement is the two-step training method in the system designation. In our new method, the values are higher than all other systems. Considering the scale of proper detection of the type of the intrusions, according to tables 1 and 2, the best results in other methods is 99.90% while our worst result in our suggested method is competitive with this method. In other words, the scale of DR in our method is something between 99.594 to 100%. Any desirable abnormality detection system must have a very low rate of positive errors. This rate of positive error in our system equals to 0.406% that is considerably lower than other methods.

5. General conclusion and suggestions

Today, the information security is tied to the national security of the countries. Considering the application of experimental methods in providing applied programs, and considering the security in designing the protocols like TCP/IP and the universality of the computer networks and the process of securing and security evaluation of the computer networks, it is necessary to discuss the security process. In the security process of the computer networks, we have to pay attention to the security troubleshooting of applied programs and operating systems while using defense mechanisms such as the firewalls and intrusion detection systems. In evaluating the security of the computer networks we have to evaluate the obtained security in the securing process. As a part of the securing process, we designed an abnormality detection system in this research. In contrast to many intrusion detection systems, the suggested system of this research operates hierarchically. This abnormality detection system uses neural networks due to their feature of being generalized. The employed training of neural systems in this research is being conducted in two sequential steps. The key of the successfulness of this system is that the system detects the intrusions and abnormalities in two steps where in the first step it offers a partial awareness about the data and different intrusions; then in the next step, the system detects the intrusions and abnormalities in full. Any desirable intrusion detection system has a low rate of errors and high rate of detection. Moreover, the method of the training in the system has to be so that all records that have a lower aggregation in the set of training data have to be clearly introduced to the system to increase the system's ability of the detection. A main problem of the most intrusion detection systems is their low ability of the detection of this type of the intrusions. The structure of our system has been designed in a way to work with all its five applied neural networks while having very good results and efficiency, so the system meets all our expectations.

Suggestions

a. Since there are different intrusions and attacks in each group, it is suggested to identify the effective features in detecting each type of computer intrusions.

b. In our offered system, the neural networks are similar in both layers, but it is possible to design the system with different neural networks.

c. In order to train the neural networks of this system we have used all records of the database. This issue has led to the increase of the size of computations and the increase in the time of network training. But it is also possible to select the most effective records by doing pre-processes and statistical operations such as sampling.

d. In our designed system we have used neural networks while it is possible to use other intelligent methods such as genetic algorithm, fuzzy systems, or a combination of intelligent methods.

e. Since the results of this intrusion detection method have been offline, we just can use it as a sign in making the suggested structure capable. But to have a more precise evaluation, these results have to be applied in a real environment.

f. Considering the designed neural network of this research and considering its detection abilities, it is suggested to use this neural network in other detection systems such as the voice detection system, image processing, illness detection, medicine detection, etc. to test and evaluate its detection and diagnostic powers.

References

1. Charron F, Ghosh A and Wanken J. 1998. Detecting Anamalous and Unknown Intrusion against Programs. Proceedings of 14th Annual Computer Security Applications Conference. Arizona, U.S.A., Dec. 7-11, pp: 259-267.
2. Amini M, Jalili R and Shahriari HR. 2006. RT-UNNID: A practical solution to real-time network based intrusion detection using unsupervised neural networks. Computers & Security, 22: 459-468.
3. Wang W, Guan X, Zhang X and Yang L. 2006. Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data, Computers & Security, 22:539-550.
4. Jazzar M and Jantan A. 2008. A novel soft computing inference engine model for intrusion detection. IJCSNS International Journal of Computer Science and Network Security, 8:1-8.
5. Beghdad R. 2007. Applying Fisher's filter to select KDD connections features and using neural network to classify and detect attacks. Neural Network World, ProQuest Science Journals, 36:1-16.
6. Shanmugam B. and Idris NB. 2007. Improved hybrid intelligent intrusion detection system using AI technique. Neural Network World, ProQuest Science Journals, 36:351-362.
7. Beghdad R. 2007. Training all the KDD data set to classify and detect attacks, Neural Network World, ProQuest Science Journals, 36:81-96.
8. Cordella LP and Sansone C. 2007. A multi stage classification system for detecting intrusions in computer networks. Springer, Pattern anal. Applic., DOI 10.1007/s10044-006-0053-7: 83-100.
9. Liu G, Yi Z and Yang S. 2006. A hierarchical intrusion detection model based on the PCA neural networks. Science Direct Neurocomputing, 30: 1561-1568.
10. Zhang C, Jiang J. and Kamel M. 2005. Intrusion detection using hierarchical neural networks. Science Direct Neurocomputing, 26: 779-791.
11. Kayacik HC, Zincir AN and Heywood MI. 2000. A hierarchical SOM based intrusion detection system. Dalhousie University.
12. Moradi M and Zulkernine M. 2004. A neural network based system for intrusion detection and classification of attacks. Proceeding of 2004 IEEE International Conference on Advances in Inteligent System- Theory and Application. Kirchberg, Luxembourg, Nov. 15-18.
13. Siddiqui M. 2000. High performance data mining techniques for intrusion detection for the degree of Master of Science. B.E. NED University of Engineering & Technology School of Computer Science in the College of Engineering & Computer Science at the University of Central Florida Orlando.
14. Sharafat AR and Rasti M. 2006. Real time anomaly detection in computer networks using self organizing and back propagation neural networks. Published in the proceedings of the IST, Frascati, Italy, Apr 29-31, pp:287-290.
15. Kendall K. 1999. A Database of Computer Attacks for the Evaluation of Intrusion Detection System, for the degrees of Bachelor of Science in Computer Science and Engineering and Master of Engineering in Electrical Engineering and Computer Science. Massachusetts Institute of Technology, USA.
16. Sharafat AR and Fallah MS. 2002. A measure of resilience against denial of service attacks in computers networks. International Journal of Computer Systems Science and Engineering, 17: 259-267.
17. Porass PA and Neumann PG. 1997. EMERALD, Event monitoring enabling responses to anomalous live disturbances. Proceedings of the 20th National Information Systems Security Conference, Canada, Baltimore, Oct 4-8, pp. 353-365.
18. Lunt TF, Jagannathan R, Lee R, Listgarten S, Edwards DL, Neumann PG, Javitz HS, Valdes

A. 1988. IDES: The enhanced prototype, A real time intrusion detection system", Technical Report, SRI Project 4185-010, SRI-CSL-88, Oct 12.
19. Anderson D, Frivold T and Valdes A. 1995. Next-generation intrusion-detection expert system (NIDES), Technical Report, SRI-CSL-95-07.
20. Sebring MM, Shellhouse E, Hanna ME and Whitehurst RA. 1988. Expert systems in intrusion detection: A case study. Proceedings of the 11th National Computer Security Conference, Baltimore, Maryland, Oct 17-20, pp: 74-81.
21. Chen SS, Cheung S, Crawford R, Dilger M, Frank J, Haogland J, Levitt K, Wee C, Yip R and Zerkle D. 1996. GrIDS – A graph based intrusion detection system for large networks. Proceedings of the 19th National Information Systems Security Conference, U.S.A., California, pp: 83-94.
22. Heberlein T, Dias G, Levitt K, Mukherjee B, Wood J and Wolber D. 1990. A network security monitor. Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, U.S.A., Los-Alamitos, California, May 7-9, pp: 296-304.
23. Lee W, Stolfo SJ. 1999. Combining Knowledge Discovery and Knowledge Engineering to Build IDSs. Proceedings of the Second International Workshop on the Recent Advances in Intrusion Detection, Germany, Berlin, Sept. 8-11, pp:77-91.
24. Barbara D, Couto J, Jajodia S, Popyack L and Wu N. 2001. ADAM: Detecting intrusions by data mining. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, U.S.A, New York, June 5-6, pp:33-39.
25. Ryan J, Lin MJ and Miikkulainen R. 1998. Intrusion detection with neural networks. Advances in Neural Information Processing Systems, England, Cambridge, pp:114-132.
26. Freguson P and Senie D. 1998. Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing, RFC 2276.
27. Computer Crime Research, "Losses from computer crime down over 50%", Available [Online]: http://www.crime-research.org/eng/news/2003/06/Mess0302.html, June 2003.
28. Labib K, Venmuri R. date. NSOM: a real-time networked based intrusion detection system using self-organizing maps. Available [online]: http://www.cs.ucdavis.edu/~vemuri/papers/som-ids.pdf.
29. Hines JW. 1996. A logarithmic neural network architecture for unbounded non-linear function approximation. IEEE International Conference on Neural Networks, U.S.A., Washington DC, June3-6, pp:1245-1250.
30. Agarwal M. 1997. A systematic classification of neural-network-based control. IEEE CONTROL SYSTEM, U.S.A., pp:75-93.
31. Ghosh AK, Wanken J and Charron F. 1998. Detecting anomalous and unknown intrusion against programs. Proceedings of the IEEE Conf. on Security Applications, U.S.A., Arizona, Tucson, Dec. 7-11, pp: 259-267.
32. Fausset L. 1994. Fundamentals of Neural Networks: Architectures, Algorithms, and Applications. Prentice Hall, Ed., pp:1-96 and 289-324.
33. Werbos JP. 1994. The roots of Back propagation. John Wiley & Sons, New York, 3rd Ed., pp: 133-141.
34. Toosi AN and Kahani MM. 2007. A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. Computer Connections, Science Direct, 43: 2201-2212.
35. Degang Y, Guo C, Hui WW and Xiaofeng L. 2007. Learning Vector Quantization Neural Network Method for Network Intrusion Detection. Wuhan university journal of natural sciences (WUJNS), 25: 147-150.

2/25/2018