HYBRID NEURAL NETWORK AND C4.5 FOR MISUSE DETECTION

ZHI-SONG PAN[1, 2], SONG-CAN CHEN[1] , GEN-BAO HU[2], DAO-QIANG ZHANG[1]

[1] Department of Computer Science,Nanjing University of Aeronautics and Astronautics Nanjing, 210016, China
[2] 73672 Army Unit Nanjing, 210016, China
E-MAIL: hotpzs@hotmail.com

Abstract:

Intrusion detection technology is an effective approach to dealing with the problems of network security. In this paper, we present an intrusion detection model based on hybrid neural network and C4.5.The key idea is to take advantage of different classification abilities of neural network and the C4.5 algorithm for different attacks. What is more, the model could also be updated by the C4.5 rules mined from the dataset after the event (intrusion). We employ data from the third international knowledge discovery and data mining tools competition (KDDcup'99) to train and test feasibility of our proposed model. From our experimental results with different network data, our model achieves more than 85 percent detection rate on average, and less than 19.7 percent false alarm rate for five typical types of attacks. Through the analysis after-the-event module, the average detection rate of 93.28 percent and false positive rate of 0.2 percent can respectively be obtained.

Keywords:

Intrusion Detection; Neural Network; Back-propagation; Decision Tree; C4.5

1 Introduction

Growing Internet connectivity comes growing opportunities for attackers to illicitly access computers over the network. Security of network system is becoming increasingly important as more sensitive information is being stored and manipulated online. It is difficult to prevent attacks only by passive security policies, firewall, or other mechanisms. Intrusion Detection Systems (IDS) have thus become a critical technology to help protect these systems as an active way. An IDS can collect system and network activity data, and analyze those gathered information to determine whether there is an attack.

In this paper, we present a hybrid neural network and C4.5[1] model for misuse detection. Since most of the intrusions can be located by examining patterns of user activities, many IDSs have been built by utilizing the known attack behaviors. We build the model to improve the detection rate for known attack. First, we train and test our hybrid model on the normal and the known intrusion data. BP network and C4.5 have different classification capabilities for different intrusions. Therefore, Hybrid model improves the performance to detect intrusions. In addition, the model also could be updated by accepting the C4.5 rules mined from the dataset after the event. In our experiment result, we demonstrate that efficient and accurate classifiers can be built. We compare the performance of Hybrid model, single BP network, and single C4.5 algorithm.

2 Related works

There are a few different groups advocating various approaches to using neural networks for intrusion detection. Artificial neural networks offer the potential to resolve a number of the problems encountered by the other current approaches to intrusion detection. A couple of groups created keyword count based misuse detection systems with neural network[2,3]. The data that they presented to the neural network consisted of attack-specific keyword counts in network traffic. Such a system is close in spirit to a host-based detection system because it looks at the user actions. In a different approach, researchers created a neural network to analyze program behavior profiles instead of user behavior profile[4]. This method identifies the normal system behavior of certain programs, and compares it to the current system behavior. Self-Organizing Maps (SOMs) have also been used as anomaly intrusion detectors[5]. Lee and Heinbuch[6] used hierarchical back-propagation neural network to detect TCP SYN flooding and port scanning intrusions. Lee also use the Ripper rules and other data mining technologies to build An intrusion detection models[7]. Cannady developed a network-based neural network detection system with a neural network[8]. This method is similar from ours because we also proposed detection on a packet level. Our model deals with 41 features of network packet, which enable us to recognize more information of attacks. In addition, the model have high detection rate because we utilize C4.5

0-7803-7865-2/03/$17.00 ©2003 IEEE

rules for R2L and U2R intrusions, which are difficult to be classified correctly by neural network.

3 Intrusion Detection System

Intrusion detection systems were introduced Denning's Generic Intrusion Detection Model[9] that was independent of any particular system, application environment, system vulnerability, or type of intrusion. IDS can be classified into two categories: anomaly detection and misuse detection. Anomaly detection models compare audit data and other features of system to normal patterns learned from the training data. If the audit data deviates from normal behavior, the anomaly detection model classifies the data as an attack. Anomaly detection models are popular because they are seen as a possible approach to detecting unknown or new attacks. However, it's difficult to select threshold levels and features of system to monitor.

Misuse detection algorithms refer to known attack behavior. They compare monitored data to attack patterns learned from the training data. If the monitored data matches the pattern of some known attack data, the observed data is considered intrusive. Misuse models are typically obtained by training on a large set of data in which the attacks have been manually labeled. The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. They can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods.

The main issues in misuse detection are how to write a signature that encompasses all possible variations of the pertinent attacks, and how to write signatures that do not also match non-intrusive activity. It is difficult to build such a model. An artificial neural network and Decision Tree can automatically learn the given input pattern instead of having to describe them by hand-coding possible intrusion behaviors. This paper is based on the idea.

4 Hybrid BP Network and C4.5 for Misuse Detection

In this work, we aim to automate the process of detecting intrusive actions as much as possible. Our system is a modular network-based intrusion detection system that analyzes Tcpdump data. The hybrid model is composed of three modules, training module, real-time detection module and after-the-event analysis module. as shown in Figure 1. In our learning approach, the BP network and C4.5 algorithm need time to be trained on data which is processed from the raw TCP/IP dump form to the machine-readable form by using automated parsers before detection is possible. The model reads in Tcpdump data and sends it first to the preprocessing module which process the raw data into machine-readable form. the preprocessing module also convert 41 features into a standardized numeric representation. the process involved the creation of relational tables for each of the data type and assigning number to each unique type of element.(e.g. protocol_type feature is encoded according to IP protocol field: TCP=6, ICMP=1, ICMP=17). Therefore, the data of uniform representation can be processed by the neural network.

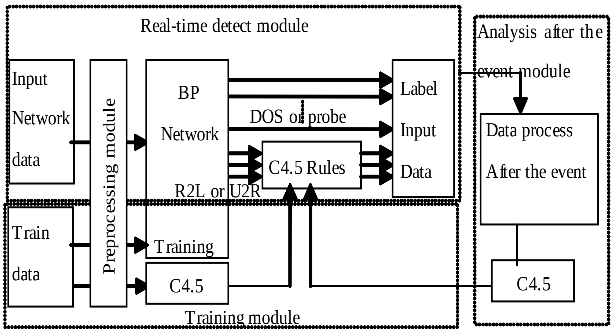

Figure 1 the hybrid Neural network and C4.5 model for IDS

C4.5 is a classic decision tree algorithm. Decision trees are structures used to classify data with common attributes. Each decision tree represents a rule which categorizes data according to these attributes. A decision tree consists of nodes, leaves, and edges. A node of a decision tree specifies an attribute by which the data is to be partitioned. Each node has a number of edges which are labeled according to a possible value of the attribute in the parent node. An edge connects either two nodes or a node and a leaf. Leaves are labeled with a decision value for categorization of the data. a set of C4.5 rules will be generated from each and from all trees produced by C4.5 together. The C4.5 rules can be used in misuse detection. These steps have been taken , the system can stop the learning phase and begin Real-time detection. We found that neural network and C4.5 have different classified abilities for different intrusions. Neural network have high performance to DOS and Probing attacks rather than to R2L and U2R attacks. on the contrast, C4.5 can detect the R2L and U2R more accurately than neural network. Therefore, Hybrid model will improve the performance to detect intrusions. In addition, the model also could be updated by accepting the C4.5rules mining from the after-the-event analysis module. This module works when the intrusion was happened after IDS misclassify the attacks as normal activities. The data of intrusion will be relabeled as the attack types by the network administrator. This data also be input the C4.5, then a set of rules extracted from built decision tree can be update the C4.5 rules set in real–time detect module.

5 Experimental Result

5.1 Dataset Description

The data in the experiment was acquired from the 1998 DARPA intrusion detection evaluation program[10].They set up an environment to acquire raw TCP/IP dump data for a local-area network(LAN) simulating a typical U.S.Air Force LAN. More than 200 instances of 58 attack types were launched against victim UNIX and Windows NT hosts in tree weeks of training data and two week of test data. For each TCP/IP connection, 41 various quantitative and qualitative features were extracted. Each connection is labeled as either normal, or as an attack, with exactly one specific attack type. Each connection record consists of about 100 bytes.

Attacks fall into four main categories:

DOS: denial of service

R2L: unauthorized access from a remote machine

U2R: unauthorized access to local super user(root) privileges

Probing: surveillance and other probing

We select normal dataset, Neptune attack(SYN flooding), Portsweep attack(port scanning), satan attack, buffer_overflow and guess_passwd datasets from [10] to train and test our IDS prototype. The complete description of features is found in [11].

Table 1 ATTACKS IN EXPERIMENT

Attack class	The selected attacks in our experimemt
DOS	Neptune
Probing	Portsweep,satan
U2L	Buffer_overflow
R2L	Guess_passwd

6 attack categories are numbered as follows:

(1-normal,2-neptune,3-satan,4-portsweep,5-buffer_overflow,6-guess_passwd)

We get 29313 train data patterns from 10% training set and 124,970 test data patterns from Test set which has attack patterns that are not present in the training data. Therefore Problem is more realistic. We divide test data patterns into 2sets, which each has 13112 (TESTSET ONE) and 111858 (TESTSET TWO)data patterns.

5.2 Training Neural Network

Multi-layer, feed-forward networks are used. In the study we use 3-layer network, consisting of 70 neurons in first hidden layer,14 neurons in second hidden layer and 6 neurons in the output layer, resulting to a 70-14-6 feed-forward neural network, as shown in Figure 2.

The training of the neural networks was conducted using feed forward back propagation algorithm using scaled conjugate gradient decent for learning. The network was set to train until the desired mean square error of 0.001 was met or 1500 epochs was reached. During the training process, the performance is 0.00157434 at 1500 epochs. Figure3 shows the training process.

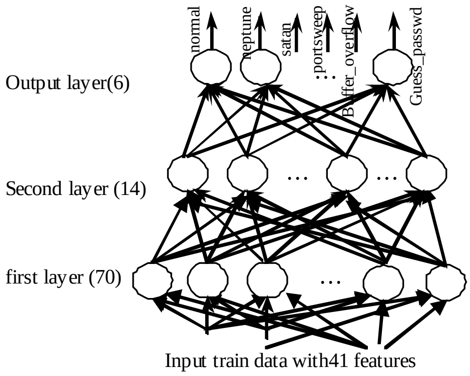

Figure 2 BP network structure for IDS

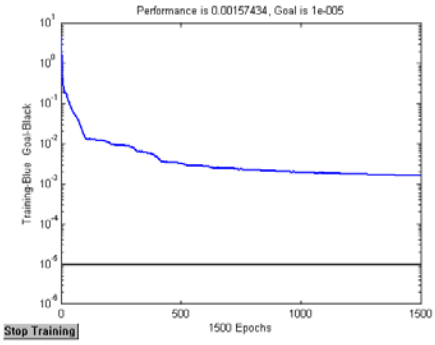

Figure 3 BP training on KDD intrusion detection data-subset

5.3 Test Neural Network

The TESTSET ONE consists of 13112 data patterns with 41features. The classified results, the false positive and detect rate are obtained in confusion matrix Shown in the following Table2:

Table 2 The confusion matrix obtained by BP network

Predicted actual	1	2	3	4	5	6	%correct
1	**6038**	**0**	**20**	**1**	**0**	**0**	**99.6**
2	**1**	**3834**	**22**	**9**	**0**	**0**	**99.1**
3	**2**	**19**	**795**	**0**	**0**	**0**	**97.4**
4	**0**	**9**	**3**	**165**	**0**	**0**	**93.2**
5	**11**	**0**	**0**	**0**	**0**	**0**	**0**
6	**2183**	**0**	**0**	**0**	**0**	**0**	**0**
%correct	**73.3**	**99.2**	**94.6**	**94.2**	**0**	**0**	

(1-normal,2-neptune,3-satan,4-portsweep,5-buffer_overflow,6-guess_passwd)

The top-left entry in the confusion matrix shows that 6038 of the actual "normal" test examples were predicted to be normal by this entry. The last column indicates that in total 99.6% of the actual "normal" examples were recongnized correctly. The bottom row shows that 73.3% of test examples said to be "normal" were indeed "normal" in reality. From the last column, we can obtain the average detect rate of 64.9%. the false positive rate is 26.7%(1-73.3%).According to the table, we can see the BP network can't detect the buffer_overflow and guess_passwd attacks.

5.4 C4.5 rules

C4.5rules read the decision tree produced by C4.5 and generates a set of production rules from each and from all trees together. Single C4.5 acquires pruned decision tree with 117 nodes on train data. Total classification error rate is 47%. However, we found that C4.5 has high classification capability for buffer_overflow and guess_passwd. Following results is a part of C4.5 rules for buffer_overflow and guess_passwd on given 29313 training patterns .

Rule 1: num_failed_logins > 0
dst_host_same_srv_rate > 0
-> class guess_passwd
Rule 2: hot > 2
root_shell > 0
-> class buffer_overflow
Rule 3: src_bytes <= 70
dst_bytes > 5006
dst_host_same_src_port_rate > 0
-> class buffer_overflow

We put the above rules into the C4.5 rules in the real-time detect module. The TESTSET ONE, as before, is tested by using hybrid model. The classified results, the false positive and detect rate was obtained in confusion matrix Shown in the following Table3:

Table 3 The confusion matrix of hybrid BP and C4.5

predicted actual	1	2	3	4	5	6	%correct
1	6032	0	20	1	5	1	99.5
2	1	3834	22	9	0	0	99.1
3	2	19	795	0	0	0	97.4
4	0	9	3	165	0	0	93.2
5	3	0	0	0	8	0	72.7
6	1473	0	0	0	0	710	48.2
%correct	80.3	99.2	94.6	94.3	61.5	99.8	

From the right last column, we can obtain the average detect rate of 85.01%. the false positive rate is 19.7%(1-80.3%).According to the table, we can see the hybrid model obtain detect rate 72.7% for buffer_overflow and 48.2% for guess_passwd attacks. In contrast with 0% in TABLE2, it has made a great improvement.

5.5 The analysis after the event module

After some buffer_overflow and guess_passwd intrusions are misclassified as normal activities, intruders could attacks the network. After this intrusion was occurred, the administrator must analyze and relabel those records as corresponding intrusion labels in the dataset after-the-event. We build a decision Tree with C4.5, and extract rules for update the C4.5 rules set in real–time detect module. In our experiment, we utilize the C4.5 on the TESTSET ONE and get a set of production rules. the extractive rules is :

Rule 4: protocol_type = 6
duration > 2
src_bytes > 20
src_bytes <= 39
->class guess_passwd

We use the TESTSET TWO consisting of 111858 data patterns with 41 features. The classified results, the false positive and detect rate was obtained in confusion matrix. Shown in the following Table4:

From the last column, we can obtain the average detect rate of 93.28%. the false positive rate is 0.2%(1-99.8%).According to the table, we can see the hybrid model obtain detect rate 72.7% for buffer_overflow and 100% for guess_passwd attacks. It is much high detect rate comparing with 48.2% in TABLE3.

Table 4 The confusion matrix obtained by hybrid model after the event

Predicted actual	1	2	3	4	5	6	%correct
1	54307	12	111	83	17	4	99.5
2	80	52654	428	972	0	0	97.3
3	5	33	779	0	0	0	95.3
4	0	8	1	168	0	0	94.9
5	1	0	0	0	8	2	72.7
6	0	0	0	0	0	2184	100
%correct	99.8	99.9	59	79.5	32	99.9	

6 Conclusion

In this paper, we proposed a hybrid neural network and C4.5 model for misuse detection. Neural network have high performance to DOS and Probing attacks rather than to R2L and U2R attacks. On the contrast, C4.5 can detect the R2L and U2R more accurately than neural network. The model we proposed lets them work together in their each strong point. Our actual experiments show that it has made a great improvement by using hybrid model. Our future work will address the remaining issues in the development of a complete IDS based the neural network and decision tree for detecting more types of intrusions.

References

[1] Quinlan J. C4.5:programs for machine learning. San Mateo: Morgan Kaufmann,1993

[2] Cunningham R, Lippmann R. Improving Intrusion Detection performance using Keyword selection and Neural Networks. MIT Lincoln University (http://www.ll.mit.Edu/ IST/pubs.html)

[3] Ryan J, Lin M, and Mikkulainen R. Intrusion Detection with Neural Networks. Advances in Neural Information Processing Systems, vol. 10, MIT Press

[4] Ghosh A, Schwartzbard A, and Shatz M. Learning Program Behavior Profiles for Intrusion Detection. in Proceedings First USENIX Workshop on Intrusion Detection and Network Monitoring. Santa Clara. California, April 1999

[5] Girardin L, and Brodbeck D. A Visual Approach or Monitoring Logs. In Proceedings of the 12th System Administration Conference (LISA'98). pp. 299-308.Boston, MA, Dec.1998

[6] S.C. Lee, D.V. Heinbuch. Training a Neural- Network Based Intrusion Detector to Recognize Novel Attacks. Information Assurance and Security. pp.40-46, 2000

[7] W. Lee and S.J. Stolfo. Data mining approaches for intrusion detection. In Proceedings of Very Large Data Bases,1994

[8] Cannady J. Artificial Neural Networks for Misuse Detection. Proceedings, National Information Systems Security Conference (NISSC'98).Arlington.VA.pp. 443-456,Oct.1998

[9] Dorothy E Denning. An Intrusion Detection Model. In IEEE Transactions on Software Engineering. Number 2, page 222, Feb. 1987

[10] S.J. Stolfo, et al. "KDD cup 1999 dataset". UCI KDD repository. http://kdd.ics.uci.edu

[11] Task description of Kddcup'99. http://kdd.ics.uci. edu/databases/ kddcup99/task.html