International Journal of Fuzzy Logic and Intelligent Systems, vol. 6, no. 2, June 2006 pp.173-177

The network model for Detection Systems based on data mining and the false errors

Se-Yul Lee* · · ong-Soo Kim**

*** Department of Computer Science, Chungwoon University,**
San29 Namjang-Ri, Hongseong-Eup, Hongseong-Gun, Chungnam, 350-701, Korea
E-mail: {pirate, jbc66}@cwunet.ac.kr
**** Department of Computer Engineering, Daejeon University,**
96-3 Yongun-Dong, Dong-Gu, Daejeon, 300-716, Korea
E-mail : kystj@dju.ac.kr

Abstract

This paper investigates the asymmetric costs of false errors to enhance the detection systems performance. The proposed method utilizes the network model to consider the cost ratio of false errors. By comparing false positive errors with false negative errors, this scheme achieved better performance on the view point of both security and system performance objectives. The results of our empirical experiment show that the network model provides high accuracy in detection. In addition, the simulation results show that effectiveness of probe detection is enhanced by considering the costs of false errors.

Key Words : Detection Systems, False Errors, Data Mining, Session Patterns

1. Introduction

The rapid growth of network in information systems has resulted in the continuous research of security issues. One of key research areas is detection system which many companies have adopted to protect their information assets for several years. In order to address the security problems, many automated detection systems have been developed. However, between 2002-2005, more than 200 new attack techniques were created and published which exploited Microsoft's Internet Information Server (IIS), one of the most widely used web servers. Recently, several detection systems have been proposed based on various technologies. A "false positive error" is an error that detection system sensor misinterprets one or more normal packets or activities as attack. The detection system operators spend too much time on distinguishing events. On the other hand, a "false negative error" is an error resulting from that attacker is misclassified as a normal user. It is quite difficult to distinguish intruders from normal users. It is also hard to predict all possible false negative errors and false positive errors due to the enormous varieties and complexities of today's networks. The detection system operators rely on their experience to identify and resolve unexpected false error issues. This paper proposes a method to analyze and reduce the total costs based on the asymmetric costs of errors in the detection system. This method adopts the model which has shown successful results for detecting and identifying unauthorized or abnormal activities from the networks [1].

The proposed method is to minimize the loss for an organization under an open network environment. This study employs the network model for detection. Furthermore, this study analyzes the cost effectiveness of the false error levels and presents experimental results for the validation of our detection model.

The section 2 presents the introduction of detection systems and the studies of data mining approaches for detection systems. This research model is addressed in detail in Section 3. In Section 4, the asymmetric costs of false negative errors and false positive errors are validated by experimental results. Finally, this paper is concluded with the summary, contributions, and limitations.

2. Detection Systems

An intrusion is an unauthorized access or usage of the resources of a computer system [2]. Intrusion Detection System (IDS) is the software with the functions of detecting, identifying and responding to unauthorized or abnormal activities on a target system [3, 4]. The goal of IDS is to provide a mechanism for the detection of security violations either in real-time or batch-mode [5, 6]. These violations are initiated either by outsiders attempting to break into a system, or by insiders attempting to misuse their privileges [7]. IDS

Manuscript received Feb. 24, 2006; revised May. 24, 2006.
This research was supported by the Chungwoon University Research Grant in 2005.

collects information from a variety of systems and network sources, and then analyzes the information for signs of intrusion and misuse [8]. The major functions performed by IDS are monitoring and analyzing user and system activity, assessing the integrity of critical system and data files, recognizing activity patterns reflecting known attacks, responding automatically to detected activity, and reporting the outcome of the detection process.

Intrusion detection is broadly divided into two categories based on the detection method: misuse detection and anomaly detection. Misuse detection works by searching for the traces or patterns of well-known port attacks. Clearly, only known attacks, which leave characteristic traces, can be detected this way. This model of the normal user or system behavior is commonly known as the user of system profile. A major strength of anomaly detection is its ability to detect previously unknown attacks.

The IDS is categorized according to the kind of audit source location which they analyze. The IDS is classified as either a network-based intrusion detection or a host-based intrusion detection approach for recognizing deflecting attacks. When IDS looks for these patterns in the network traffic, it is classified as network based intrusion detection. When IDS looks for attack signatures in the log files, it is classified as host based intrusion detection. In either case, these products look for attack signatures and specific patterns that usually indicate malicious or suspicious intent. Host based IDS analyzes host bound audit sources such as operating system audit trails, system logs, and application logs. Network based IDS analyzes network packets that are captured on a network.

The current IDS has contributed to identifying attacks using historical patterns. But they have difficulty in identifying attacks using a new pattern or with no pattern[9]. Previous studies have utilized a rule based approach such as USTAT, NADIR, and W&S [10-12]. They lack flexibility in the rule to audit record representation. Slight variations in an attack sequence can affect the activity rule comparison to a degree that intrusion is not detected by the intrusion detection mechanism. While increasing the level of abstraction of the rule base does provide a partial solution, it also reduces the granularity of the intrusion detection device. These limitations in rule based systems can be summarized as follows: the lack of flexibility and maintainability in the acquisition process of rules, the lack of predictive capability, the lack of automatic learning capability, a high rate of false alarms or missing alarms, and difficulty in applying organizational security policies.

Many recent approaches of IDS have utilized data mining techniques. For example, the Computer Misuse Detection System (CMDS), the Intrusion Detection Expert System (IDES), and the Multics Intrusion Detection and Alerting System (MIDAS) using neural networks. These approaches build detection models by applying data mining techniques to large data sets of an audit trail collected by a system [13]. Data mining based IDS collects data from sensors which monitor several aspects of a system. Sensors may monitor network activity, system calls used by user processes, and file system accesses. They extract predictive features from the raw data stream being monitored to produce formatted data that can be used for detection. Data gathered by sensors are evaluated by a detector using a detection technique. Table 1 shows the researches of data mining applications to IDS.

Table 1. List of data mining applications in IDS [4-10]

Detection method	Data mining methods
Misuse	CBR of Esmaili NN of Endler NN of Cannady GA of Balajinath
Anomaly	NN of Kumar NN of Endler NN of Bonifacio GA of Sinclair
Network based	CBR of Esmaili NN of Heatley GA of Balajinath

3. Cost of errors for Detection Systems

3.1 Network models for Detection Systems

The model consists of network based detection model and monitoring tool(Fig. 1) [14]. The model adopts the problem solving methodology which uses previous problem solving situations to solve new problems. The model does preprocessing by packet analysis module and packet capture module. The packet capture module captures and controls packet. The packet capture module does real-time capturing and packet filtering by using the monitoring tool of Detector4win Ver. 1.2 [15]. In the packet filtering process, packets are stored according to the features which distinguish normal packets from abnormal packets. The packet analysis module stores data and analyzes half-open state. After storing packets, the packets, which are extracted by audit record rules in the packet analysis module, are sent to the detection module.

The input and the output of detection module, namely STEP 1, is traffic and alert, respectively. The traffic is an audit packet and the alert is generated when an intrusion is detected. The detection module consists of session classifier, pattern extractor, and pattern comparator. The session classifier takes packet of the traffic and checks whether or not the source is the same as the destination. There is a buffer for the specific session to be stored. And, if the next packet is arrived, it is stored in the correspond buffer. If all packets of the corresponding buffer are collected, all packets of the corresponding buffer are output on session. The output session becomes an input to the pattern extractor or pattern comparator according to action mode. The action mode consists of learning mode and pre-detection mode. The output session from the session classifier is sent to the pattern extractor in the learning mode and to the pattern comparator

in the pre-detection mode. Fig. 2 is the block diagram of the STEP 1.

The pattern extractor collects the sessions, which have the same destination, and extracts common pattern. Each extractor has two features. The first feature is a head part which appears in common sessions, which have the same destination, when sessions are arranged by size packets using the time sequence. The second feature is the minimum length of the sessions which have the same destination. The length of session is the number of packets of session.

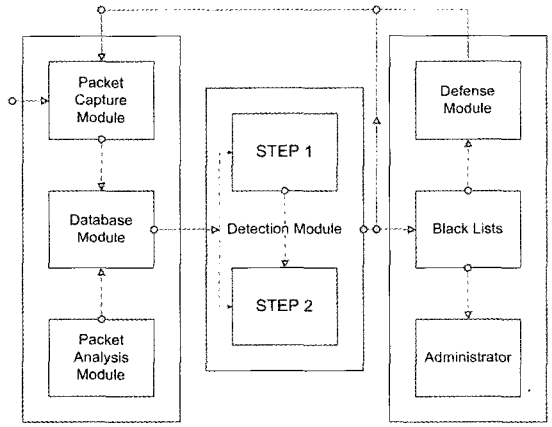

Fig. 1. Architecture of model

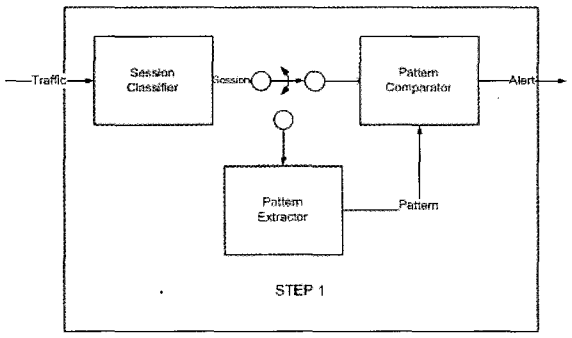

Fig. 2. A Block Diagram of STEP 1

The pattern comparator compares packets with the rule based pattern. If the probe packets and the rule based pattern do not correspond, the pattern comparator considers the probe packets as the abnormal session and generates an alert signal. Thus, the pattern comparator receives a session and the rule based pattern as an input. From the input session the data size and the length of session are extracted. If there is a mismatch in one of two features, the pattern comparator considers a session as the abnormal session. What we must consider for the pattern extraction is whether we extract the pattern continuously or we extract the pattern periodically. We generally call the former the real-time pattern extraction and the latter the off-line pattern extraction. The real-time pattern extraction is better than off-line pattern extraction in the viewpoint of updating the recently changed pattern. But, it is difficult to update the pattern when probes occur. For the pattern, if possible, normal traffic becomes a rule-based patterns. Otherwise, an abnormal traffic sometimes becomes a rule-based pattern. And an abnormal intrusion traffic is considered as an normal traffic. It is called false negative error. The model uses detection module, namely STEP 2, to compensate the false negative error by using fuzzy cognitive maps. The detection module of model is intelligent and uses causal knowledge reason utilizing variable events which hold mutual dependences. When CPU capacity increases because syn packet increases, the weight of a node, W_{ik}, has the value of range from 0 to 1. The total weighted value of a node depends on path between nodes and iteration number. It is expressed as the following equation.

$$N_k(t_{n+1}) = \sum_{i=1}^{n} W_{ik}(t_n) N_i(t_n)$$

Nk(tn) : the value of the node k at the iteration number tn
tn : iteration number
Wik(tn) : weight between the node i and the node k at the iteration number tn

On the above equation, the sign of weight between the node *i* and the node *k* depends on the effect from the source node to the destination node.

3.2 Analysis for costs of errors

The analysis of costs of errors are presented in the Fig. 3. The purpose of Fig. 3 is to analyze the relationship between the total costs and detection system errors and to find the optimal threshold of network model that minimizes `the total costs for intrusion detection. The solution provides the weights of errors while the weights can be adjusted to enhance the effectiveness of intrusion detection according to the threshold value of the activation function. The activation function produces the level of excitation by comparing the sum of these weighted inputs with the threshold value. This value is entered into the activation function, for example the sigmoid function, to derive the output from the node.

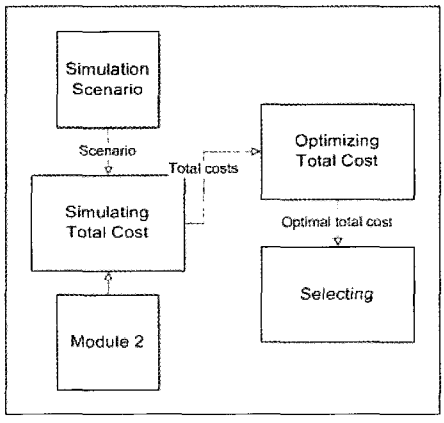

Fig. 3. A Block Diagram of Error's Cost

The cost of attacks or errors has received attention in designing IDS [16]. The cost of a false negative error is much higher than that of a false positive error because an

organization may suffer from various security incidents compromising confidentiality, integrity, and availability when IDS does not detecting real attacks. This paper introduces the concept of the asymmetric costs of errors to calculate overall misclassification costs. The performance of detection system is optimized when the total costs are minimized.

A false negative error, which is the cost of not detecting an attack, is occurred when the detection system does not function properly and mistakenly ignores an attack. This means that the attack will succeed and the target resource will be damaged. Thus, a false negative error should take a higher weight than a false positive error. The false negative errors are therefore described as the damage cost of the attack. The cost function for detection system can be defined as follows:

$$A_{total}(x) = \omega_1 A_1 + \omega_2 A_2 + ... + \omega_n A_n$$

$$= \sum_{i=1}^{n} \omega_i A_i$$

$A_{total}(x)$: Total cost

ω_i : Weight for each cost A_i

A_i : Cost for each error i

To measure each cost, we used the errors that are the misclassified by our detection methods. The cost ratio of a false positive error and a false negative error varies depending on the characteristics of the organization. Thus, we found out the minimal total costs by the simulation of adjusting the weights one hundred times. The threshold values can be searched to minimize the total costs for a specific cost ratio of false negative errors to false positive errors.

4. Performance Evaluation

For the performance evaluation of the proposed model, we used the KDD (Knowledge Discovery Contest Data) data set by MIT Lincoln Lab, which consists of labeled data (training data having syn and normal data) and non-labeled data (test data). We utilize a network model to apply the proposed method for the above data. Three-layer feedforward network is used to detect an intrusion. Logistic activation function is utilized in the output layer. The number of hidden nodes is selected through experiment with n/2, n, and 2n of nodes (n is the sum of input nodes) by fixing the input and output nodes. A series of experiments was conducted to analyze the effects of varying the value of the threshold values of false negative errors and false positive errors (Fig. 4).

As the threshold value increases, false positive errors increase while false negative errors decrease. After the ratio of false negative errors over false positive errors is given, the threshold value that minimizes the total cost can be determined. Let us suppose that the cost of false negative error is equal to that of false positive error. We can find that the optimal point of the threshold is 0.12 from Fig. 4. When the output is larger than the threshold value, the output is interpreted as an attack, and normal vice versa.

The performance of networks is calculated by the function of cost, which consists of false positive errors and false negative errors (Table 2). The performance of network model is measured in the output sample data. The total costs of the network model is 15.32% when the threshold value is 0.5 which is a general value without considering costs of errors. When the optimal point of threshold of 0.12 is applied to the network model from Fig. 4, the cost is 15.95%. The cost decreases and the performance of the intrusion detection model is sensitive according to the threshold. A false negative error is more important in detection system as mentioned in the previous section. We need to concentrate on the decrease of false negative errors according to the change of the threshold value. The decreases in the false negative errors is 1.17% from 9.01 to 7.84%. The change in the total cost would be greater if weights are added to the negative false errors.

Table 2. The performance of network models

Threshold value	Sample	False positive errors(%)	False negative errors(%)	Cost(%)
0.5	Input	24.63	9.23	16.93
	Output	21.63	9.01	15.32
	Total	23.13	9.12	16.13
0.12	Input	25.49	8.45	16.97
	Output	24.06	7.84	15.95
	Total	24.78	8.15	16.46

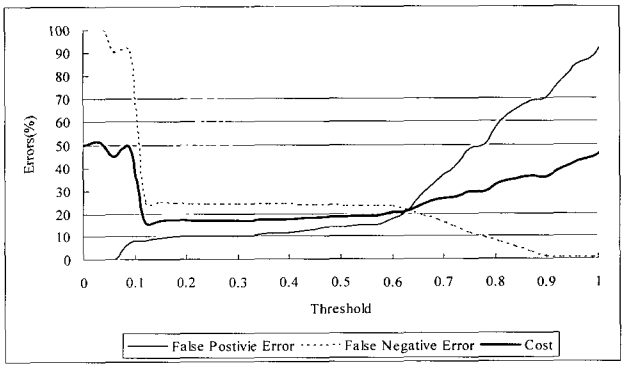

Fig. 4. The performance of a model with cost of errors

5. Conclusion

There has been a variety of researches and systems designed to detect intrusion by using data mining approaches. However, most researches addressed the measure of system performance as providing prediction accuracy without considering the costs of errors in intrusion detection. In this paper, we proposed a network model based on costs of false positive errors and false negative errors. The first diagram of this research develops a network model for intrusion detection. The second diagram analyzes the system performance based on costs of errors.

The results of the empirical experiment indicate that the network model provides very high performance for the

accuracy of intrusion detection. The cost of false negative errors must be much higher than that of the false positive errors to an organization. The total cost of errors is minimized by adjusting the threshold value for the specific cost ratio of false negative errors to false positive errors.

This study provides insights into the multi-facetted method of evaluating IDS performance in terms of false negative and false positive errors as well as detection accuracy. Our study will help organizations to employ IDS effectively by reducing the total costs due to the inevitable IDS errors.

Reference

[1] Lee, W., Stolfo, S. J., "A data mining framework for building intrusion detection models," *IEEE Symposium on Security and Privacy*, pp. 209-220, 1999.

[2] Safavi-Naini, R., Balachadran, B., "Case-based reasoning for intrusion detection," 12th Annual Computer Security Application Conference, pp. 214-223, 1996.

[3] Denning, D. E., "An intrusion detection model," *IEEE Trans. S. E.*, SE-13(2), pp. 222-232, 1987.

[4] Richards, K., "Network based intrusion detection: a review of technologies," *Computer and Security*, pp. 671-682, 1999.

[5] Debar, H., Dacier, M., "Towards a taxonomy of intrusion detection systems," *Computer Networks*, pp. 805-822, 1989.

[6] Debar, H., Becker, M., "A neural network component for an intrusion detection system," *IEEE Computer Society Symposium Research in Security and Privacy*, pp. 240-250, 1992.

[7] Weber, R., "Information Systems Control and Audit," *IEEE Symposium on Security and Privacy*, pp. 120-128, 1999.

[8] Lippmann, R. P., "Improving intrusion detection performance using keyword selection and neural networks," *Computer Networks*, Vol. 24, pp. 597-603, 2000.

[9] Jasper, R. J., Huang, M. Y., "A large scale distributed intrusion detection framework based on attack strategy analysis," *Computer Networks*, Vol. 31, pp. 2465-2475, 1999.

[10] Ilgun, K., Kemmerer, R. A., "Ustat: a real time intrusion system for UNIX," *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pp. 16-28, 1993.

[11] Hubbards, B., Haley, T., McAuliffe, L., Schaefer, L., Kelem, N., Walcott, D., Feiertag, R., Schaefer, M., "Computer system intrusion detection," *Computer Networks*, pp. 120-128, 1990.

[12] Vaccaro, H. S., "Detection of anomalous computer session activity," *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pp. 280-289, 1989.

[13] Helman, P., "Statistical foundations of audit trail analysis for the detection of computer misuse," *IEEE Transactions on software engineering*, Vol. 19, pp. 861-901, 1993.

[14] Lee, S. Y. and Kim, Y. S., "Design and analysis of probe detection systems for TCP networks," *International Journal of Advanced Computational Intelligence & Intelligent Informatics*, Vol. 8, pp. 369-372, 2004.

[15] Lee, S. Y., *An Adaptive probe detection model using fuzzy cognitive maps*, Ph. D. Dissertation, Daejeon University, 2003.

[16] Maxion, R. A., "Masquerade detection truncated command lines," *International Conference on Dependable Systems and Networks*, pp. 219-228, 2002.

Se-Yul Lee

He received the M. S. Degree in Department of Information & Communications Engineering and Ph. D. degree in Department of Computer Engineering from Daejeon University, in 1999 and 2003, respectively. He was a Researcher at Insopack Co. from 2000 to 2001. From 2004 to present, he is Professor of Chungwoon University and his research area is Network Security, Intrusion Detection & Prevention, System Security, Fuzzy-neural Networks.

Byoung-Chan Chun

He received the Ph.D degree in information Technology, Soonchunhyang University in 2001. from 2002 to present , he is Professor of chungwoon University. he is interested Computer Architecture, Homenetwork, Microprossor, Mobile Network.

Yong-Soo Kim

He received the B. S. degree from Yonsei University, and M. S. degree from Korea Advanced Institute of Science and Technology(KAIST) in 1981 and 1983, respectively. He received the Ph. D. degree in the Department of Electrical Engineering from Texas Tech University in 1993. He was a Researcher at Samsung Electronics Co. from 1983 to 1986. He is currently an Associate Professor in the Department of Computer Engineering, Daejeon University. His research interests include neural networks, fuzzy logic, image processing, pattern recognition, intrusion detection systems.