A Probe Detection Model Using the Analysis of the Fuzzy Cognitive Maps

Se-Yul Lee[1], Yong-Soo Kim[2], Bong-Hwan Lee[3], Suk-Hoon Kang[2], and Chan-Hyun Youn[4]

[1] Department of Computer Science, Chungwoon University,
San 29 Namjang-Ri, Hongseong-Eup, Hongseong-Gun, Chungnam, 350-701 Korea
Pirate@cwunet.ac.kr
[2] Division of Computer Engineering, Daejeon University,
96-3 Yongun-Dong, Dong-Gu, Daejeon, 300-716 Korea
{kystj,shkang}@dju.ac.kr
[3] Department of Information & Communications Engineering, Daejeon University,
96-3 Yongun-Dong, Dong-Gu, Daejeon, 300-716 Korea
blee@dju.ac.kr
[4] School of Engineering, ICU,
119 Munjiro, Yuseung-Gu, Daejeon, 305-732 Korea
chyoun@icu.ac.kr

Abstract. The rapid growth of network-based information systems has resulted in continuous research of security issues. Intrusion Detection Systems (IDS) is an area of increasing concerns in the Internet community. Recently, a number of IDS schemes have been proposed based on various technologies. However, the techniques, which have been applied in many systems, are useful only for the existing patterns of intrusion. They can not detect new patterns of intrusion. Therefore, it is necessary to develop a new IDS technology that can find new patterns of intrusion. Most of IDS sensors provide less than 10% rate of false positives. In this paper, we proposed a new network-based probe detection model using the fuzzy cognitive maps that can detect intrusion by the Denial of Service (DoS) attack detection method utilizing the packet analyses. The probe detection systems using fuzzy cognitive maps (PDSuF) capture and analyze the packet information to detect SYN flooding attack. Using the results of the analysis of decision module, which adopts the fuzzy cognitive maps, the decision module measures the degree of risk of the DoS and trains the response module to deal with attacks. For the performance evaluation, the "IDS Evaluation Data Set" created by MIT was used. From the simulation we obtained the average true positive rate of 97.094% and the average false negative rate of 2.936%.

1 Introduction

The rapid growth of network in information systems has resulted in the continuous research of security issues. One of the research areas is IDS that many companies have adopted to protect their information assets for several years. In order to address the security problems, many automated IDS have been developed. However, between 2002 and 2004, more than 100 new attack techniques were created and published

O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3480, pp. 320 – 328, 2005.

which exploited Microsoft's Internet Information Server (IIS), one of the most widely used web servers. Recently, several IDS have been proposed based on various technologies. A "false positive error" is an error that IDS sensor misinterprets one or more normal packets or activities as an attack. IDS operators spend too much time on distinguishing events. On the other hand, a "false negative error" is an error resulting from 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. IDS operators rely on their experience to identify and resolve unexpected false error issues.

Recently, according to the CERT-CC (Computer Emergency Response Team Coordination Center), hacking is increasing about 300% each year. A variety of hacking techniques are known: DoS, Buffer Overflow Attack, Probe Attack, Vulnerability Scan Attack and others. Among them, Vulnerability Scan Attack and Probe Attack are the two most frequently used methods. Port scan or vulnerability of network as abnormality intrusion of network is based on anomaly probe detection algorithms such as s*canlogd* [14], RTSD (Real Time Scan Detector) [15], and Snort [16]. Such open source programs have some problems in invasion probe detection. That is, s*canlogd* and RTSD can not detect slow scan, while Snort does not provide open port scan. Therefore, a new algorithm that can provide slow scan and open port scan is required.

The main objective of this paper is to improve the accuracy of intrusion detection by reducing false alarm rate and minimize the rate of false negative by detecting unexpected attacks. In an open network environment, intrusion detection rate is rapidly improved by reducing false negative errors rather than false positive errors. We propose a network based probe detection model using the fuzzy cognitive maps that can detect intrusion by the DoS attack detection method. A DoS attack appears in the form of the probe and SYN flooding attack, which is a typical example. The SYN flooding attack takes advantage of the vulnerable three-way handshake between the end-points of TCP [3-5, 7]. The proposed PDSuF [13] captures and analyzes the packet information to detect SYN flooding attack. Using the results of detection module, which utilizes the fuzzy cognitive maps, the detection module measures the degree of risk of the DoS and trains the response module to deal with attacks [6, 7].

The rest of this paper is organized as follows. The background and related work is summarized in Section 2. Section 3 describes the proposed new PDSuF model. Section 4 illustrates the performance evaluation of the proposed probe detection model. Conclusions and future work are presented in Section 5.

2 Related Work

Previous studies of DoS attack detection can be divided into three categories: attack prevention, attack source trace-back and attack identification, and attack detection and filtering. Attack prevention obviously provides avoidance of DoS attacks. With this method, server system may be securely protected from malicious packet flooding attack. There are indeed known scanning procedures to detect them based on real experience [1-2]. Attack source trace-back and identification is to identify the actual

source of packet sent across network without replying to the source in the packets [8]. Attack detection and filtering are responsible for identifying DoS attacks and filtering by classifying packets and dropping them [10]. The performance of most of DoS detection is evaluated based on false positive error and false negative error. The detection procedure utilizes the victim's identities such as IP address and port number. Packet filtering usually drops attack packets as well as normal packets since both packets have the same features. Effectiveness of this scheme can be measured by the rate of the normal packet which is survived in the packet filtering. Among these schemes, attack prevention has to recognize how DoS attack is performed and detect attack pattern using predefined features [12]. Therefore, when a new attack detection tools are developed, new features that detect the pattern of attack needs to be defined. Current IP trace-back solutions are not always able to trace the source of the packets. Moreover, even though the attack sources are successfully traced, stopping them from sending attack packets is another very difficult task.

DoS attacked traffic is quite difficult to distinguish from legitimate traffic since packet rates from individual flood source are usually too low to catch warning by local administrator. Thus, it is efficient to use inductive learning scheme utilizing the Quinlan's C4.5 algorithm approach to detect DoS attack [11]. Inductive learning systems have been successfully applied to the intrusion detection. Induction is formalized by inductive learning using decision tree algorithm which provides a mechanism for detecting intrusion. The key idea of this approach is to reduce the rate of false errors. The false error rates of the known intrusion detection schemes are summarized in Table 1.

As shown in Table 1, FSTC (False Scan Tool and Clustering) provides the largest false negative error, while the Fuzzy ART scheme provides the smallest false negative errors and the largest false positive error. In the meantime, Inductive Learning System provides moderate false negative and false positive error on the average. From the above results, it is highly recommended to develop a new DoS detection scheme based on fuzzy cognition.

Table 1. False errors of IDS [2]

Methodology	False Negative Error	False Positive Error
FSTC	22.65%	20.48%
Inductive Learning System	9.79%	9.10%
K-Means (Average Value)	9.37%	20.45%
Fuzzy ART (ρ= 0.9)	6.03%	38.73%

3 PDSuF Model

3.1 PDSuF Algorithm

The PDSuF model is a network-based detection scheme that utilizes network data to analyze packet information. Based on the analysis of each packet, probe detection is performed. In order to determine intrusion detection, various features of packet is

utilized including source IP address, source port number, destination IP address, destination port number, flags, data size, timestamp, and session pattern as given by (1).

Packet X = (src_ip, src_port, dst_ip, dst_port, flag, data, timestamp, pattern,…) (1)

Now it is needed to quantize each feature parameter based on comparison criterion to determine attack detection. The procedure to assign effect values can be summarized as follows.

[state 1] *Feature Equality*

$$FE(x) = \begin{Bmatrix} 0(x \neq a) \\ 1(x = a) \end{Bmatrix}$$

a: standard, *x*: comparison

[state 2] *Feature Proximity*

$$FP(x) = \frac{k}{|x - a|}$$

a: standard, *x*: comparison, *k*: constant

[state 3] *Feature Separation*

$$FS(x) = k|x - a|$$

a: standard, *x*: comparison, *k*: constant

[state 4] *Feature Covariance*

$$FC(x, y) = |\mathrm{cov}(x(t), y(t))|$$

x, y: comparison, *t*: time, cov(): degree of dispersion

[state 5] *Feature Frequency*

$$FF(x) = \log_2 \frac{1}{\Pr(x)}$$

Pr(x) : *x*'s probability

Using the above state variables, the total degree of abnormality for a packet can be calculated as in (2).

$$\begin{aligned} A_{total}(x) &= \omega_1 A_1 + \omega_2 A_2 + \ldots\ldots + \omega_n A_n \\ &= \sum_{i=1}^{n} \omega_i A_i \end{aligned} \quad (2)$$

$A_{total}(x)$: Abnormality per packet
ω_i : Weight value of packet
A_i : Abnormality of packet
n : Total feature number of abnormality

If the total degree of abnormality for a packet is greater than the threshold of attack attempt, the associated packet is classified as abnormal.

3.2 PDSuF Architecture

The PDSuF architecture consists of network-based intrusion detection system and monitoring tool as shown in Fig. 1 [5, 9]. As monitoring tool, a protocol analyzer is used, whereas the detection system is directly connected to the router, which interconnects LANs. The PDSuF algorithm is obviously implemented on the detection system.

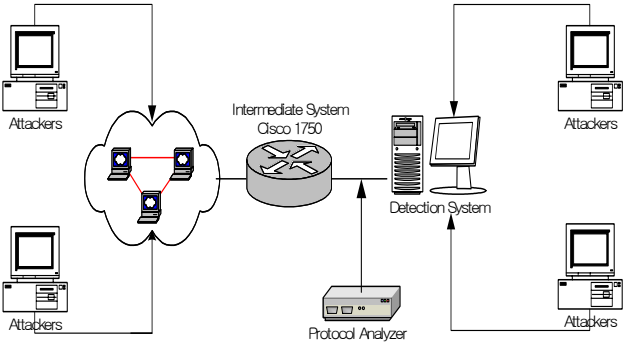

Fig. 1. PDSuF architecture

The detection module of the PDSuF is intelligent and uses causal knowledge reason in fuzzy cognitive maps. Fig. 2 shows the detection module using variable events that are mutually dependent. In detection module of Fig. 2, an optimal detection is

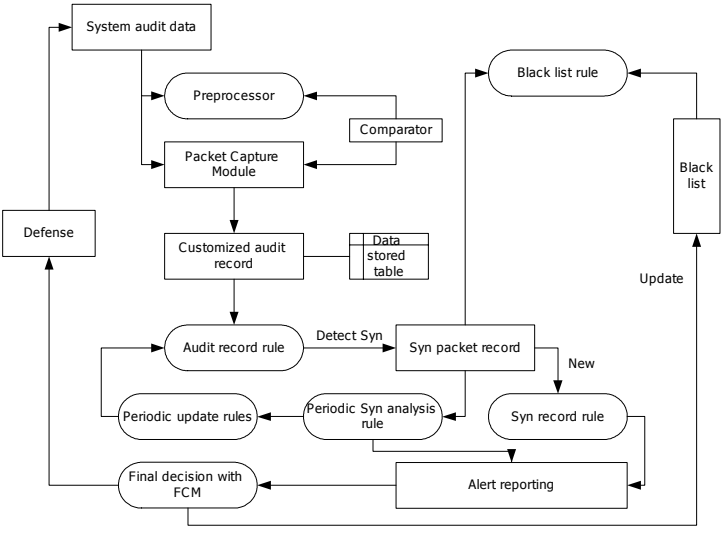

Fig. 2. Flowchart of detection module

provided by giving dependency to some events among several variable events. In addition, regarding the detected IP address as a probe, the detection module decides whether to save the IP address to the black list or not. The weight is the effect value of path analysis calculated using quantitative Micro Software's Eview Ver. 3.1. Fig. 3 shows the details of fuzzy cognitive maps (FCM) in Fig. 2. As the variable events dependent on the detection module, we can set the identity of IP address, the time interval of half-open state, the rate of CPU usability, the rate of memory, and SYN packet. For example, the weight between the two nodes is bigger than 0 since the rate of CPU usability increases in proportion to the size of SYN packet. In Fig. 3, each rectangular box represents feature event, while each number denotes effect value in FCM.

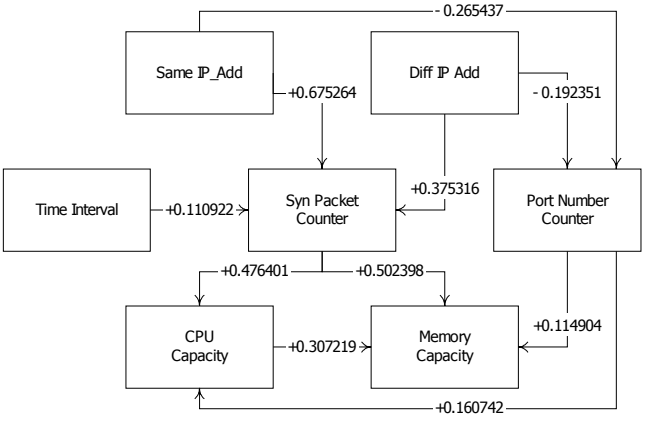

Fig. 3. Path model of the FCM

4 Performance Evaluation

For the performance evaluation of the proposed PDSuF model, we have used the KDD data set (Knowledge Discovery Contest Data) by MIT Lincoln Lab, which consists of labeled data (training data having SYN flooding and normal data) and non-labeled data (test data). Since the TCP SYN flooding attacks come from abnormal packets, detection of abnormal packets is similar to detection of SYN flooding attacks in TCP networks.

The best detection and false error rates are summarized in Table 2. The simulation results for the connection records of DoS attacks are collected for 10 days. The average rate of true positive is measured of 97.064%. According to the KDD'99 competition results, the best rate of the Bernhard's true positive is known as 97.1% [11]. Comparing Bernhard's true positive rate with that of PDSuF, we realized that the result of PDSuF is as good as Bernard's. In addition, the false negative rate of the proposed scheme, 2.936%, is considerably smaller than that of the Bernhard's, 3.91%.

Table 2. Best detection and error rates

Day	True Positive	False Positive	True Negative	False Negative
Day 1	95.623%	0.000%	100.000%	4.377%
Day 2	87.861%	0.000%	100.000%	12.139%
Day 3	96.098%	0.001%	99.999%	3.902%
Day 4	99.569%	0.000%	100.000%	0.431%
Day 5	100.000%	0.000%	100.000%	0.000%
Day 6	98.930%	0.000%	100.000%	1.070%
Day 7	100.000%	0.001%	99.999%	0.000%
Day 8	87.701%	0.000%	100.000%	12.299%
Day 9	100.000%	0.000%	100.000%	0.000%
Day 10	97.917%	0.000%	100.000%	2.083%
Average	97.064%	0.000%	99.999%	2.936%

Fig. 4. illustrates the performance of four different detection algorithms for both DoS and probing. The key difference between PDSuF and the others is that the former is resource based probe detection algorithm, whereas the latters are basically rule-based detection algorithms. Thus, the proposed algorithm is able to detect probe regardless of input patterns and the number of features. The key advantage of the PDSuF over the other alogorithms is the ability of real-time update of effect values in FCM. Therefore, as shown in Fig. 4, the proposed PDSuF algorithm outperforms the other algorithms in both DoS and probe.

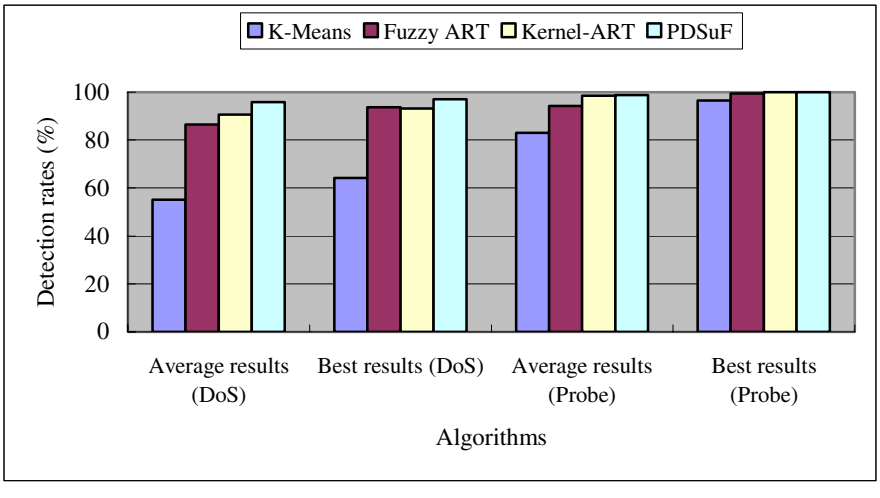

Fig. 4. Detection rates of DoS vs Probe

In order to evaluate the performance from the viewpoint of resource usage, system resource usage of the PDSuF is compared to that of Synkill, which is a well-known SYN flood attack detection tool developed by Purdue University[17]. Fig. 5 shows the system resource usage of both Synkill and PDSuF when DoS attack is applied at 100 seconds and the two detection tools are activated at 200 seconds. Both PDSuF and Synkill take care of the attack from 200 seconds to 350 seconds. In Fig. 5, we can see that resource usage of PDSuF drops drastically at about 250 seconds, while resource usage of Synkill drops rapidly at around 300 seconds. This results from the fact that the attack detection tools detect the attack and discard abnormal packets. Also, Fig. 5 illustrates that the proposed PDSuF outperforms Synkill using less system resources. The main reason that the PDSuF performs better than Synkill is that PDSuF is basically a probe detection scheme which is activated in advance for false errors, whereas Synkill is in operation after the attack, which results in longer time delay.

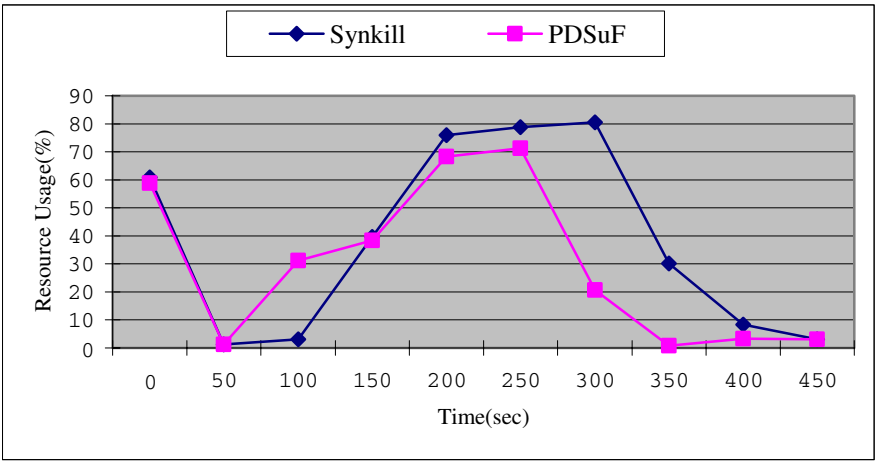

Fig. 5. Comparison of system resource usage

5 Conclusions

In this paper, we proposed a network based intrusion detection model using fuzzy cognitive maps which can detect intrusion by DoS attack. A DoS attack appears in the form of the intrusion attempt. The SYN flooding attack takes advantage of the weak point of three way handshake between the end points of TCP connections. The PDSuF model captures and analyzes the packet information to detect SYN flooding attack. Using the results of the FCM detection module, the detection module measures the degree of risk of the DoS and trains the response module to deal with attacks.

For the performance evaluation of the proposed model, the average rates of the true positive and false negative errors are measured. The true positive error rate of the PDSuF is similar to that of Bernhard's true positive error rate. However, the false negative rate of the proposed scheme is considerably smaller than that of the Bernhard's.

In addition, system resource usage of the PDSuF is compared to that of Synkill, which is a wellc-known SYN flood attack detection. The proposed PDSuF outperforms Synkill in system resource usage and time delay. The better performance results from the fact that the PDSuF is basically a probe detection scheme which is activated in advance for false errors. For further research, the PDSuF detection method needs to be extended to general purpose intrusion detection system.

Acknowledgements

This work was supported by University IT Research Center Project. It is also supported in part by KOSEF under grant No.(R05-2002-000-01008-0).

References

1. S. Gibson, "The Strange Tale of the Denial of Service Attacks Agent GRC.COM" http://grc.com/dos/grcdos.htm
2. S. A. Hofmeyr, S. Forrest, and A. Somayaji, "Intrusion detection using sequences of system calls," Journal of Computer Security, Vol. 6, pp.151-180, 1998.
3. R. Axelrod, "Structure of Decision: The Cognitive Maps of Political Elites," Princeton, NJ: Princeton University Press, 1976.
4. J. Cannady, "Applying Neural Networks to Misuse Detection," In Proceedings of the 21st National Information System Security Conference, 1998.
5. Hongik Univ., STRC, Intrusion Detection System and Detection Rates Report, KISA, 1999.
6. H. S. Lee, Y. H. Im, "Adaptive Intrusion Detection System Based on SVM and Clustering", Journal of Fuzzy Logic and Intelligent Systems, Vol. 13, No. 2, pp.237-242, 2003.
7. L. Feinstein, D. Schnackenberg, R. Balupari, D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response", DARPA Information Survivability Conference and Exposition, 2003.
8. S. Savage., D. Wetherall, A. Karlin., "Practical Network Support for IP Trace-back," In Proceedings of ACM SIGCOMM, 2000.
9. A. Garg, A. L. Narasimha, "Policy Based end Server Resource Regulation," IEEE/ACM Transactions on Networking , Vol. 8, No.2, pp. 146-157, 2000.
10. P. Ferguson, D. Sene, "Network Igress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," RFC 2827, 2000.
11. W. Lee, S. J. Stolfo., "A Framework for Constructing Features and Models for Intrusion Detection Systems," In Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2000.
12. K.C Chang, "Defending against Flooding-Based Distributed Denial of Service A Tutorial," IEEE Communications Magazine, 2002.
13. S. Y. Lee, "An Adaptive Probe Detection Model using Fuzzy Cognitive Maps", Ph. D. Dissertation, Daejeon University, 2003.
14. Solar, "Designing and Attacking Port Scan Detection Tools", Phrack Magazine, Vol. 8, Issue 53, pp. 13 – 15, 1998.
15. "Real-Time Scan Detector in real time networks," http://www.krcert.or.kr
16. S. Staniford, J. A. Hoagland, and J. M. Mcalerney, "Practical Automated Detection of Stealthy Portscans", http://silicondefense.com/software/spice/index.htm
17. C. L. Schuba, I. V. krsul, M. G. Kuhn., "Analysis of a Denial of Service Attack on TCP, " Proceedings of IEEE Symposium on Security and Privacy, pp. 208 – 223, 1997.