Design of Hybrid Network Probe Intrusion Detector using FCM

Chang-Su Kim*, **Se-Yul Lee****, *Member, KIMICS*

Abstract— The advanced computer network and Internet technology enables connectivity of computers through an open network environment. Despite the growing numbers of security threats to networks, most intrusion detection identifies security attacks mainly by detecting misuse using a set of rules based on past hacking patterns. This pattern matching has a high rate of false positives and can not detect new hacking patterns, making it vulnerable to previously unidentified attack patterns and variations in attack and increasing false negatives. Intrusion detection and prevention technologies are thus required. We proposed a network based hybrid Probe Intrusion Detection model using Fuzzy cognitive maps (PIDuF) that detects intrusion by DoS (DDoS and PDoS) attack detection using packet analysis. A DoS attack typically appears as a probe and SYN flooding attack. SYN flooding using FCM model captures and analyzes packet information to detect SYN flooding attacks. Using the result of decision module analysis, which used FCM, the decision module measures the degree of danger 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 max-average true positive rate of 97.064% and the max-average false negative rate of 2.936%. The true positive error rate of the PIDuF is similar to that of Bernhard's true positive error rate.

Index Terms— Fuzzy Cognitive Maps, Probe Detection, SYN Flooding, DDoS and PDoS, Intrusion Detection.

Manuscript received January 9, 2009; revised March 3, 2009. *Chang-Su Kim is with the Department of Internet, Chungwoon University, Chungnam, 350-701, Korea (Tel: +82-41-630-3153, Fax:+82-41-634-8700, Email: ddoja@chungwoon.ac.kr)** Corresponding Author: Se-Yul Lee (Email: pirate@chungwoon.ac.kr)

I. INTRODUCTION

The rapid growth of network in information systems has resulted in continuous security research, including intrusion detection system (IDS) that many companies have adopted to protect their information assets. IDS are an area of increasing concern in the Internet community, and many automated IDS have been developed. Between 2007 and 2008, some 200 new attack techniques were created and published that exploited Server and Workstation, one of the most widely used web servers.

Detection system techniques in many systems are useful only against existing patterns of intrusion and can not detect new patterns of intrusion, making it necessary to develop new detection system that find new patterns of intrusion [1].

In "false positives" Detection system sensors misinterpret one or more normal packets or activities as an attack. Detection system operators thus spend much time distinguishing events that require immediate attention from other events that are low-priority or normal in a particular environment.

Most detection system sensors have fewer than 10% false positives. A "false negative" occurs when an attacker is misclassified as a normal user. It is difficult to distinguish between cracker and normal users and difficult to predict all possible false negatives and false positives due to the enormous variety and complexity of today's network. Detection system operators rely on experience to identify and resolve unexpected false errors. Our main objective is to improve detection system accuracy by reducing false alarms and minimizing false negatives by detecting new attacks. In an open network environment, intrusion detection is rapidly improved by reducing false negatives more than false positives.

We propose a network based hybrid probe intrusion detection model using fuzzy cognitive maps (PIDuF) that detects intrusion by denial of service detection using packet analysis. A DoS attack typically appears as a probe and SYN flooding attack. The SYN flooding attack takes advantage of the vulnerable three way handshake between the end-point of TCP layer, which is connection-oriented transmission service [2, 3].

The PIDuF model captures and analyzes packet information to detect SYN flooding attacks. Using results of decision module analysis, which uses FCM, the decision module measures the degree of DoS danger and trains the response module to deal with attacks [4, 5, 6].

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 PIDuF model. Section 4 illustrates the performance evaluation of the proposed probe intrusion detection model. Conclusion and future work presented in Section 5.

II. RELATED WORK

Previous studies of denial of service detection can be divided into three categories: attack prevention, attack source trace-back and identification, and attack detection and filtering. Attack prevention obviously provides avoidance of DoS. 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 [7, 8].

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 [9]. Attack detection and filtering are responsible for identifying DoS 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 [11].

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.

A denial of service 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. It is efficient to use inductive learning scheme utilizing the Quinlan's C4.5 algorithm approach to detect DoS [12]. 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.

Table 1 False error of Detection Systems [2]

Methodology	False Negative Errors (%)	False Positive Errors (%)
False Scan Tool and Clustering	22.65	20.48
Inductive Learning System	22.65	9.10
K-Means	22.65	20.45
Fuzzy ART ($\rho = 0.9$)	22.65	38.73

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.

III. PIDuF MODEL

A. PIDuF Algorithm

The PIDuF 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, time-stamp, and session pattern as given by (1).

Packet X = (sr_ip, sr_pt, ds_ip, ds_pt, flag, data, timestamp, pattern, etc).....(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).

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

$$= \sum_{i=1}^{n} \omega_i A_i \quad \cdots\cdots (2)$$

$A_{total}(x)$: *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.

B. Architecture

The PIDuF architecture consists of network based intrusion detection system and monitoring tool as shown in Fig. 1 [8]. As monitoring tools, a protocol analyzer is used, whereas the detection system is directly connected to the router, which interconnects LANs. The PIDuF algorithm is obviously implemented on the detection system.

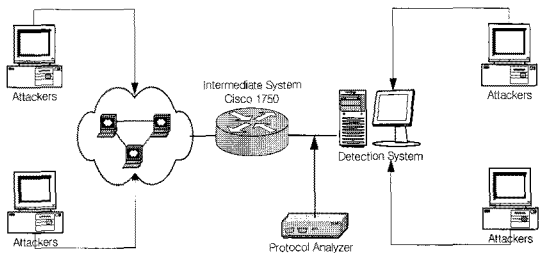


Fig. 1 Architecture of PIDuF

The detection module of the PIDuF 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 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 in Fig. 2.

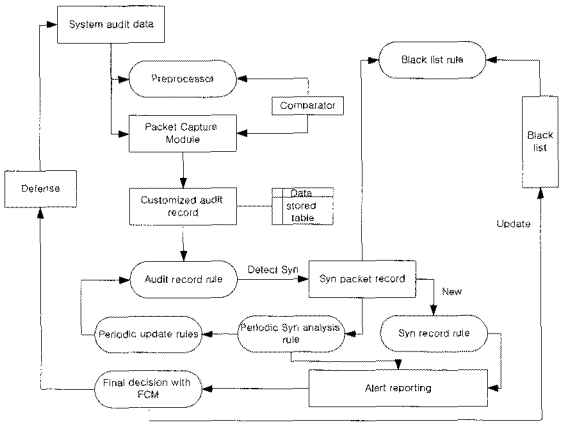


Fig. 2 Flowchart of Hybrid Detection Module Rules

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.

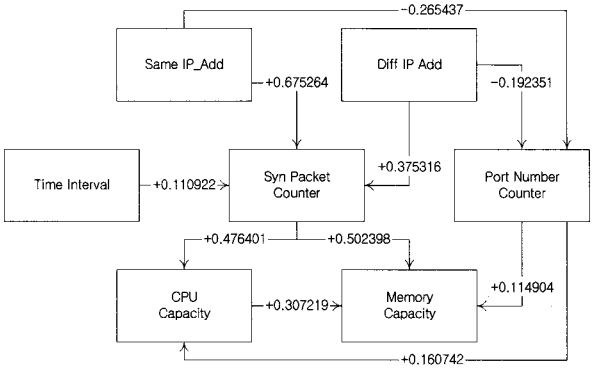


Fig. 3 Weight values of Detection using FCM

IV. PERFORMANCE EVALUATION

For the performance evaluation of the proposed PIDuF model, we have used 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.

Table 2 Best Detection and Error rates

Week_Day	True Positive	False Positive	False Negative	True Negative
1_1	95.623%	0.000%	4.377%	100.000%
1_2	87.861%	0.000%	12.139%	100.000%
1_3	96.098%	0.000%	3.902%	100.000%
1_4	99.569%	0.000%	0.431%	100.000%
1_5	100.000%	0.000%	0.000%	100.000%
2_1	98.930%	0.000%	1.070%	100.000%
2_2	100.000%	0.000%	0.000%	100.000%
2_3	87.701%	0.000%	12.299%	100.000%
2_4	100.000%	0.000%	0.000%	100.000%
2_5	97.917%	0.000%	2.083%	100.000%
SUM	97.064%	0.000%	2.936%	100.000%

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 2 weeks. 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 97.10% [13]. Comparing Bernhard's true positive rate with that of PIDuF, we realized that the result of PIDuF is as good as Bernard's. In addition, the false negative rate of proposed scheme, 2.0336%, is considerably smaller than that of Bernhard's, 2.91%.

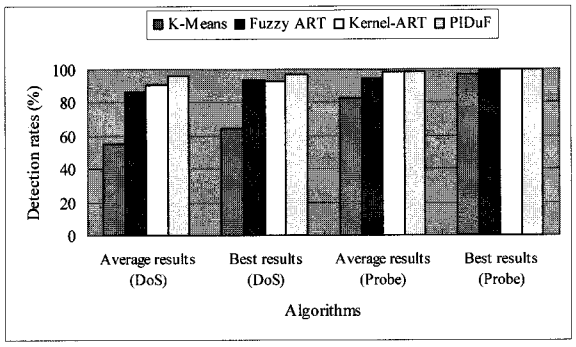


Fig. 4 Detection rate of DoS vs. Probe

Fig. 4 illustrates the performance of four different detection algorithms for both DoS and probing. The key difference between PIDuF and the others is that the former is resource based probe detection algorithm, whereas the latter 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 PIDuF over the other algorithms is the ability of real-time update of effect values in FCM. Therefore, as shown in Fig. 4, the proposed PIDuF algorithm outperforms the other algorithms in both DoS and probe.

In order to evaluate the performance from the viewpoint of resource usage, system resource usage of the PIDuF is compared to that of Synkill, which is a well-known SYN flood attack detection tool developed by Purdue University [11]. Fig. 5 shows the system resource usage of both Synkill and PIDuF when DoS attack is applied at 100 seconds and the two detection tools are activated at 200 seconds. Both PIDuF and Synkill take care of the attack from 200 seconds to 350 seconds.

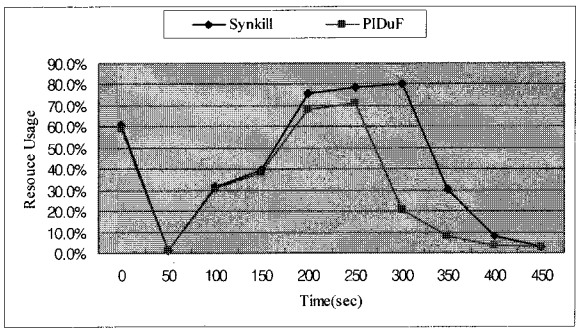


Fig. 5 Comparison of system resource usage

In Fig. 5, we can see that resource usage of PIDuF 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 PIDuF outperforms Synkill using less system resources. The main reason that the PIDuF performs better than Synkill is that PIDuF 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.

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

REFERENCES

[1] Solar, "Designing and Attacking Port Scan Detection Tools," Phrack Magazine, Vol. 8, Issue 53, pp. 13-18, 1998.

[2] "Real-Time Scan Detector in real time network," http://www.krcert.or.kr

[3] S. Staniford, J. A. Hoagland, and J. M. Mcalerney, "Practical Automated Detection of Stealthy Portscans," http://silicondefense.com/software/spice/index.html.

[4] R. Axelrod, "Structure of Decision: The cognitive maps of Political Elites," Princeton, NJ:Princeton University Press, 1976.

[5] J. Cannady, "Applying Neural Networks to Misuse Detection," In Proceedings of the 21st National Information System Security Conference, 1998.

[6] STRC, Intrusion Detection System and Detection Rates Report, KISA, 2008.

[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. Y. Lee, "An Adaptive Probe Detection Model using Fuzzy Cognitive Maps," Ph. D. Dissertation, Daejeon University, 2003.

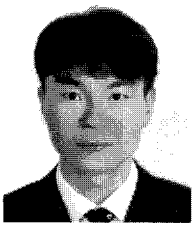
[9] S. Gibson, "The Strange Tale of the Denial of Service Attacks Agent GRC.COM," http://grc.com/dos/grcdos.htm.

[10] 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.

[11] S. Y. Lee, C. S. Kim, and H. K. Jung, "A Study of a Secure Mobile Agent Services Based on Grid Proxy Gateway," Journal of KIMICS, Vol. 6, No. 3, Dec. 2008.

[12] S. Savage, D. Wetherall, A. Karlin, "Pratical Network Support for IP Trace back," In Proceedings of ACM/SIG COMM, 2000.

[13] S. Y. Lee and Y. S. Kim, "Design and analysis of probe detection systems for TCP networks," International Journal of Advanced Computational Intelligence and Intelligent Informatics, Vol. 8, pp. 368-380, 2004.



Chang-Su Kim

He received the B.S., M.S. and Ph. D. degrees in Computer Engineering from Paichai University, in 1996, 1998 and 2002, respectively. From 2001 to 2004, he has a lecturer of Paichai University, IT Education Center. Since 2005, he has worked as a Full-time lecture in Department of Internet at Chungwoon University. His current research interests include Document Information Processing, Web Service, and Mobile Internet Service.

Se-Yul Lee

He received the B.S. degree in Department of Electronic- Physics, the M.S. degree in Department of Information and Communications Engineering and Ph. D. degree in Department of Computer Engineering from Daejeon University, in 1996 and 2003, respectively. He was a researcher at Insopack Ltd and ETRI from 1998 to 2001. Since 2004 he has been an Assistant Professor in Department of Computer Science at Chungwoon University. His current research interests include Network Security, Grid middleware, and Fuzzy Neural Networks.