2003 International Symposium on Advanced Intelligent Systems
September 25-28, 2003, Jeju, Korea

An Adaptive Probe Detection Model using Fuzzy Cognitive Maps

Se-Yul Lee, Yong-Soo Kim
IS & IA Laboratory
Division of Computer Engineering
Daejeon University
96-3 Yongun-Dong, Dong-Gu, Daejeon, 300-716, Korea
E-mail : ailab@dju.ac.kr, kystj@dju.ac.kr

ABSTRACT – The advanced computer network technology enables connectivity of computers through an open network environment. There has been growing numbers of security threat to the networks. Therefore, it requires intrusion detection and prevention technologies. In this paper, we propose a network based intrusion detection model using Fuzzy Cognitive Maps(FCM) that can detect intrusion by the Denial of Service(DoS) attack detection method adopting the packet analyses. A DoS attack appears in the form of the Probe and Syn Flooding attack which is a typical example. The Syn flooding Preventer using Fuzzy cognitive maps(SPuF) model captures and analyzes the packet information to detect Syn flooding attack. Using the result of analysis of decision module, which utilized FCM, the decision module measures the degree of danger of the DoS and trains the response module to deal with attacks. The result of simulating the "KDD'99 Competition Data Set" in the SPuF model shows that the Probe detection rates were over 97 percentages.

Key words – Fuzzy Cognitive Maps, Probe Detection, Syn Flooding attack, Denial of Service, Intrusion Detection Systems

I. INTRODUCTION

The rapid growth of network in information systems has resulted in the continuous research of security. One of the researches is the Intrusion Detection Systems(IDS) that many companies have adopted to protect their information assets for several years. IDS is an area of increasing concerns in the Internet community. In response to this, many automated IDS have been developed. However, between 1999 and 2002, about 100 new attack techniques were created and published that 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. However, the techniques, which have been used in many systems, are useful only for the existing patterns of intrusion. But it can not detect new patterns of intrusion. Therefore, it is necessary to develop new technology of IDS that can find new pattern of intrusion[1].

A "false positive error" is that IDS sensor misinterprets one or more normal packets or activities as an attack. IDS operators spend too much time distinguishing events, which require immediate attention, from the other events, which have low priority or are normal events for a particular environment. Most of IDS sensors show less than a 10% rate of false positives. On the other hand, a "false negative error" is that attacker is misclassified as a normal user. It is difficult to distinguish between intruder and normal users. And it is difficult to predict all possible false negative error and false positive error due to the enormous variety and complexity of today's network. IDS operators rely on their experience to identify and resolve unexpected false error issues. Therefore, it is necessary to develop the methodology of new intrusion detection that can reduce the rate of false errors.

The main objective of this paper is to improve accuracy of intrusion detection by reducing false alarm rate and minimize the rate of false negative by detecting new attacks. In an open network environment, intrusion detection rate is rapidly improved by reducing a rate of false negative error more than a false positive error. We propose a network based intrusion detection model using Fuzzy Cognitive Maps that can detect intrusion by the DoS attack detection method adopting the packet analyses. 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 weak point 3-way handshake between the end-point of TCP, which is the connection-oriented transmission service and has the reliability[2, 3, 4].

The SPuF model captures and analyzes the packet information to detect Syn flooding attack. Using the result of analysis of decision module, which utilized FCM, the decision module measures the degree of danger of the DoS and trains the response module to deal with attacks[5, 6]. In section 2, the technical details of SPuF Detection Model and performance evaluation are described. In Section 3, we discuss the expected contribution of this paper and further research.

II. SPuF DETECTION MODEL

Syn flooding Preventer using FCM(SPuF) is a network based detection model. Therefore, it needs network data for the analysis of packet information. We used KDD'99 Data Set which consists of labeled data and Non-labeled data. The Label data mean Training Data which have syn flooding and normal data. The Non-labeled data mean Test Data in Test-bed network. TCP Syn Flooding Attack comes from abnormal packet. Thus, the detection of abnormal packet is the same as the detection of Syn flooding attack on TCP network.

A. SPuF Detection Algorithm

Network Traffic can be classified into Normal Packets and Syn Packets. Every Packets consists of Time, Source IP, Source Port, Destination IP, Destination Port, Flag, Sequence Number, Window Size. Each packet is defined as 'p' and network traffic is the result of addition of every packet which is defined as 'T'. Thus, The following is a mathematical expressions of Packet and Traffic[6, 7].

$$p = (\text{time},\text{src\_ip},\text{src\_port},\text{dst\_ip},\text{dst\_port},\text{flag},\text{seq\_num},\text{window}) \quad (1)$$

$$T = \{\ p_1, p_2, p_3, \ldots\ldots\ldots\ ;\ \text{time}(p_i) \ \langle\ \text{time}(p_{i+1})\ \} \quad (2)$$

$$T = T\_norm + T\_syn \quad (3)$$

; T_norm : normal traffic, T_syn : Syn packet

$$\text{DETECT} : T \rightarrow D \quad (4)$$

$$D = P + N \quad (5)$$

; P : positive, N : normal, D : decision

$$P = T\_p + F\_p \quad (6)$$

$$;\ T\_p = \{\ p \mid p \in T\_syn,\ p \in P\ \}$$

$$;\ F\_p = \{\ p \mid p \in T\_norm,\ p \in P\ \}$$

$$N = T\_n + F\_n \quad (7)$$

$$;\ T\_n = \{\ p \mid p \in T\_norm,\ p \in N\ \}$$

$$;\ F\_n = \{\ p \mid p \in T\_syn,\ p \in N\ \}$$

B. Architecture of SPuF Detection Model

In this paper, we propose an Architecture of Network based Intrusion Detection and Monitoring Tool. It is depicted in Figure 1[4].

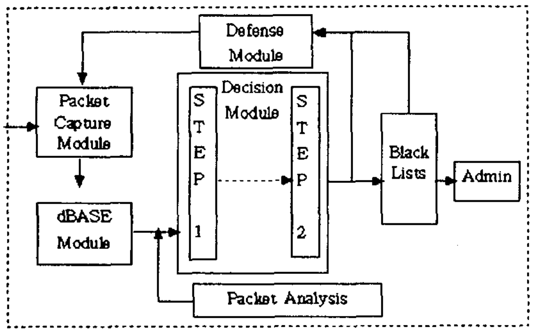


Figure 1. Architecture of Intrusion Detection Model

In the next figure, we described Decision Step of Syn Flooding. A Flowchart of Audit Record is shown in Figure 2.

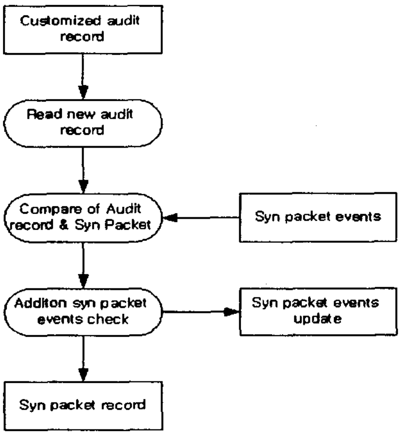


Figure 2. Flowchart of Audit Record Rule

The content in the box shows Half-Open State in Packet Capture Tables as shown in Figure 3. SYN & RST are the Flag of TCP Header. SYN changed Flag table(0→1 or 1→0) at the same time as RST in Three-Way Handshake of third connection setup fault which results in non-connection state.

Moreover, Sequence Number is changed abruptly in non-sequential order and Window Size is suddenly changed in Packet Data Tables. These are characteristics of Half-Open State[3, 4].

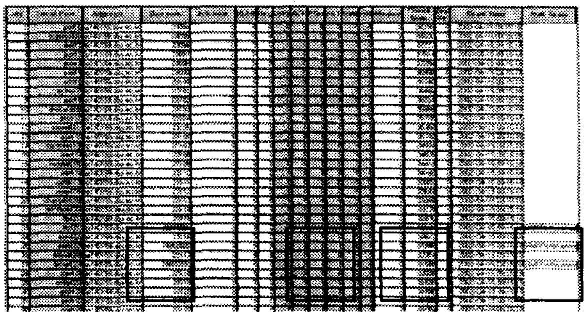


Figure 3. Detection Log Lists

C. Detection Module

Detection Module of SPuF is intelligent and uses Causal Knowledge Reason in FCM. Figure 4 shows the detection module utilizing variable events which hold mutual dependence. The weight value is the effect-value of path analysis which is calculated using Quantitative Micro Software's Eview version 3.1.

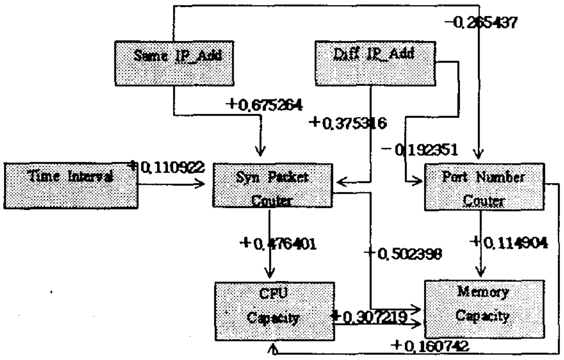
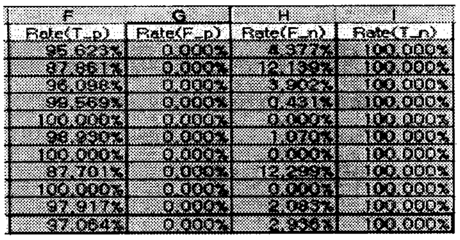


Figure 4. Detection Module using FCM

D. Performance Evaluation

The best detection rate and false error rate(Figure 5.) is the result of simulation of connection records of DoS attack in 2 weeks. Thus, the rate(T_p) is measured as 97.064%. In the KDD'99 competition, the winner, Dr. Bernhard's true positive rate(T_p) is 97.1%. We compare Dr. Bernhard's true positive rate with that of SPuF and come to know that the result of SPuF is as good as Dr. Bernard's result. The 0% rate(F_p) means the limitation of Data Set which has the DoS and Probe attack Lists among Test Data.



F	G	H	I
Rate(T_p)	Rate(F_p)	Rate(F_n)	Rate(T_n)
95.623%	0.000%	4.377%	100.000%
87.861%	0.000%	12.139%	100.000%
96.098%	0.000%	3.902%	100.000%
99.569%	0.000%	0.431%	100.000%
100.000%	0.000%	0.000%	100.000%
98.930%	0.000%	1.070%	100.000%
100.000%	0.000%	0.000%	100.000%
87.701%	0.000%	12.299%	100.000%
100.000%	0.000%	0.000%	100.000%
97.917%	0.000%	2.083%	100.000%
97.064%	0.000%	2.936%	100.000%

Figure 5. The Best Detection Rates & Error Rates

From the result of simulation and the aspect of resource capacity, we can see the influence of attack counts on the vulnerability of Hardware Capacity when the number of counts was increased from 0 to 70,000.

In figure 6, we set the Bandwidth ranged from 40% to 60% for the hardware capacity limitation, the probe detection, and the deadline in the probe attack. This value is the average when we consider the real-time defense and DDoS on network.

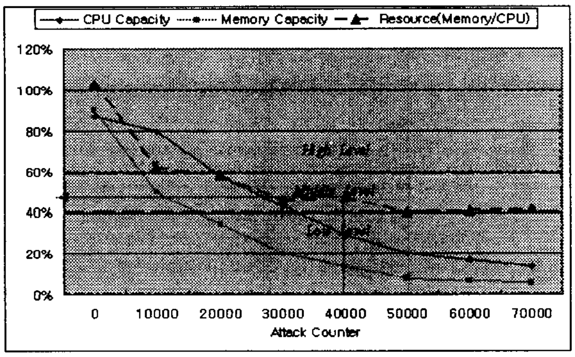


Figure 6. Attack Counter vs. Hardware Resource Capacity on Testbed Network

III. CONCLUSIONS

This paper presented an adaptive probe detection model using Fuzzy Cognitive Maps, called SPuF. For the performance evaluation, the "KDD'99 Competition Data Set" made by MIT Lincoln Labs was used. As a result of simulating the KDD in the SPuF, the probe detection rates were over 97 percentages.

Because probe detection system has always put an emphasis on detection rate, this paper has considered the aspect of cost ratio between false positive error and false negative error for information security, which can be used to decide the performance of adaptive intrusion detection and security policy of the system. Therefore, further research is needed to develop and fortify an integrated intrusion prevention system by incorporating separate modules, which can be applied to any type of probe detection system.

REFERENCES

[1] A. Siraj, S. M Bridges, R. B. Vaughn, Fuzzy cognitive maps for decision support in an intelligent intrusion detection system, IFSA World Congress and 20th NAFIPS International Conference, Vol. 4, pp. 2165-2170, 2001.

[2] D. J Joo, The Design and Analysis of Intrusion Detection Systems using Data Mining, Ph. D. Dissertation, KAIST, 2003.

[3] C. L. Schuba, I. V. Krsul, M. G. Khun, E. H. Spaford, A. Sundram, and D. Zamboni, Analysis of a denial of service attack on tcp, IEEE Symposium on security and Privacy, 1997.

[4] S. Y. Lee, Y. S. Kim, A RTSD Mechanism for Detection of DoS Attack on TCP Network, Proceedings of KFIS 2002 Spring Conference, pp. 252-255, 2002.

[5] 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, 1999.

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

[7] S. J. Park, A Probe Detection Model using the Analysis of the Session Patterns on the Internet Service, Ph. D. Dissertation, Daejeon University, 2003.