Journal of Knowledge Information Technology and Systems(JKITS), Vol. 9, No. 6, pp. 685~690, December 2014

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

An Improved Hybrid Probe Detection Model Based on Modules using Oriented Weight

Se-Yul Lee[*1], Jae-Hyeon An[2]

[1]*Department of Computer Science, Chungwoon University*
[2]*Department of Broadcast & Digital Media, Chungwoon University*

ABSTRACT

The rapid advances and spread of network-based technologies have managed in increasing network related attacks and threats which result in insecurity system and possibilities of malicious intrusions. Recently, a number of Detection System 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. Therefore, probe detection has become a major security protection technology to detection potential attacks. Probe detection needs to take into account a variety of factors and the relationship between the various factors to reduce false negative & positive error. It is necessary to develop new technology of probe detection that can find new pattern of probe. In this paper, we propose an improved hybrid probe detection based on 3-step modules. 3-step modules have session pattern analysis module, oriented weight module, and fuzzy cognitive map module. For the performance evaluation, the KDD CUP99 data made by MIT was used. Most of Detection System sensors provide less than 10% rate of false positives. The experiment results show that this approach can effectively reduce false positive rate and has a high detection rate.

KEYWORDS: Fuzzy cognitive maps, Oriented Weights, Improved hybrid probes, Session patterns, KDD Cup 1999 Data Sets

ARTICLE INFO: Received 20 October 2014, Revised 12 December 2014, Accepted 12 December 2014.

[*]Corresponding author is with the Department of Computer Science, Chungwoon University, 25 Daehak gil, Hongsung-Gun, Chungnam, 350-701, KOREA.

E-mail address: pirate@chungwoon.ac.kr

1. 서 론

오늘날 인터넷 응용 서비스가 매우 다양화됨에 따라 인터넷 서비스 이용자들이 기하급수적으로 증가하고 있으며 이와 동시에 네트워크에 대한 보안 및 개인정보유출 등의 정보보호의 심각성이 중요하게 여겨지고 있다. 과거에는 전문해커들에 의하여 해킹이나 네트워크 침입이 발생하였으나 오늘날에는 네트워크에 대한 초보적인 지식을 갖고 있는 일반인들까지도 인터넷상에 공개되어 있거나 또는 P2P 서비스 등을 통하여 쉽게 해킹도구를 접할 수 있으며 이를 통하여 너무나 쉽게 사용하여 고도의 기술을 요하는 침입까지 하고 있는 실정이다. 특히, 최근에는 개인정보 유출 및 서비스 거부 공격 형태의 침해사고는 매우 심각할 정도로 일반화 되어 가고 있는 추세이다[1]. 또한 스마트폰의 이용자는 증가하였으나 스마트폰 등과 같은 무선에 대한 보안의식은 너무나 낮은 편이여서 스마트폰 이용자들을 대상으로 하는 파밍(Pharming)공격 등 유·무선을 구별하지 않고 너무나 쉽게 해킹이 일어나고 있다. 이에, 본 논문에서는 다양한 형태의 침입시도탐지 기법을 개선하고 하이브리드형태로 재조립하고 성능향상 및 H/W의 가용성을 높이는 모델을 제안한다. 본 논문의 구성은 제 2장에서 3-step 모듈 및 모듈이 적용된 개선된 침입시도탐지모델을 알아보고 제 3장에서는 실험 및 평가를 통하여 기존의 알려진 탐지 알고리즘과의 결과를 비교 하고 결론을 기술한다.

2. 3-step 모듈 연구

2.1 세션분석모듈

개선된 Probe 탐지 모델의 첫 번째 모듈로써 <그림 1>과 같이 Session Classifier, Pattern Extractor, 그리고 Pattern Comparator로 구성되어 있다[2]. 패턴분류 에서는 입력된 패킷에서 Src(출발지)와 Dst(목적지)가 같은 세션으로 분류하는 역할을 한다. 출력된 세션은 실행 모드에 따라 패턴추출, 패턴 비교의 입력에 해당된다. 실행 모드는 학습모드와 탐지모드로 구분되며 세션분류에서는 출력된 세션은 학습모드인 경우 패턴추출로 들어가고 탐지모드인 경우 패턴비교로 들어간다. 패턴추출은 같은 Dst를 갖는 세션들을 모아 세션의 공통 패턴을 추출한다. 패턴은 2개의 feature로 구분되어 지며 한 쌍이 되어 패킷 추출의 출력이 된다. 패턴비교는 규칙기반으로 만들어 놓은 패턴과 침입 여부의 판단대상이 되는 패턴세션을 비교하여 세션이 패턴의 feature와의 유사성이 없는 것은 비정상 패턴으로 간주한다.

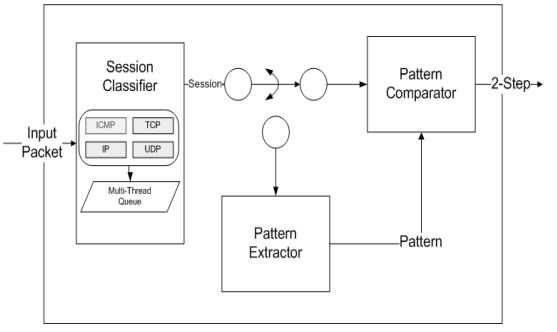

그림 1. 세션분석 모듈
Figure 1. Module of Session Analysis

2.2 퍼지인식도 및 방향성가중치 모듈

세션분석모듈을 통과한 비정상 패턴을 STEP 2와 STEP 3에 해당되는 퍼지인식도의 판단모듈과 방향성 가중치를 적용한다. 퍼지인식도는 주어진 문제영역내의 각 개념들 사이에 존재하는 CER(Cause-effect relationship)를 나타내는 방향성 그래프이다[3]. <그림 2>는 퍼지인식도를 표현한 것으로 각 노드와 노드사이의 가중치가 e_{xy}=0인 경우에는 각 노

드사이에는 아무런 관련이 없는 것을 의미하며 e_{xy} ≠0경우에는 노드에서 노드에 끼치는 원인에 대한 영향가치(Weight value)를 의미한다.

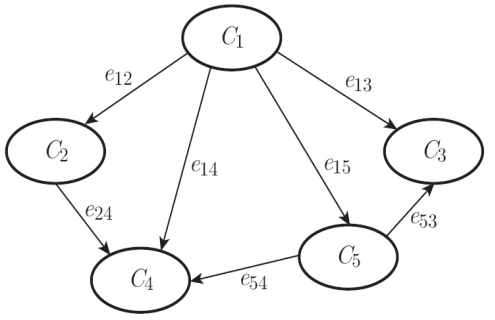

그림 2. 단순 퍼지인식도
Figure 2. A simple fuzzy cognitive maps

여기에 방향성가중치(Oriented Weight, OW)는 각 노드의 엔트로피에 대한 예상 최적치의 비선형에 대한 결과의 합이며 수식(1)과 같다[4, 5, 6].

$$A_{total}(x) = \omega_1 A_1 + \omega_2 A_2 + ... + \omega_n A_n = \sum_{i=1}^{n} \omega_i A_i \quad (1)$$

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

<그림 2>의 단순퍼지인식도에 STEP 1에서 원인을 일으키는 factor를 적용하면 <그림 3>과 같은 결과를 얻을 수 있다. 여기에 각 노드의 엔트로피에 대한 예상 최적치의 비선형인 방향성 가중치인 OW(Oriented Weight)를 적용하면 <그림 4>과 같은 결과를 얻을 수 있는데, <그림 3>과 <그림 4>에서 ω_{ij} 차이가 발생한다. 즉, 침입시도탐지에 대한 에러율(False positive/negative error)의 정확도가 높아졌다는 것이다. 이에 대한 객관적인 평가는 제 3장에서의 KDD 1999 데이터를 통하여 알 수 있을 것이다. 또한, 1에 가까울수록 실제 침입시도에 끼치는 영향도가 높다는 결과도 얻을 수 있다.

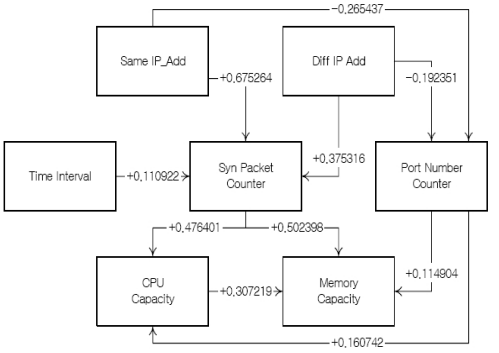

그림 3. OW가 적용안된 STEP 2의 퍼지인식도
Figure 3. FCM of STEP 2 without OW

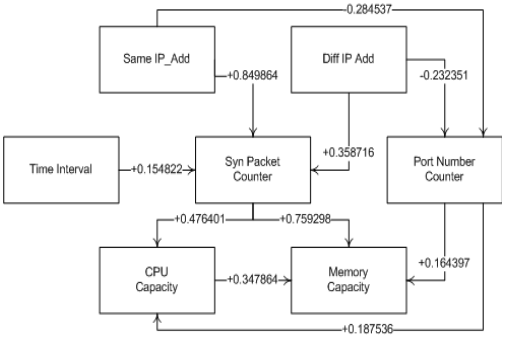

그림 4. OW가 적용된 STEP 3의 퍼지인식도
Figure 4. FCM of STEP 3 using OW

3. 실험 및 평가

실험의 평가는 공정성 있고 객관적 평가가 이루어질 수 있는 KDD CUP 1999 데이터를 이용하였으며 실험환경은 윈도우즈7, 인텔 i5프로세서, 4GB RAM의 환경에서 이루어졌다. <그림 5>는 3-STEP 모듈을 적용한 하이브리드형 침입시도 탐지모델이다.

2주간의 KDD 2000개의 데이터에서 DoS 공격(Smurf, Land, Pod), 정상패킷, Probe(Ipsweep, Nmap, Satan), U2R(buffer overflow, sqlattack, Rootkit), R2L(Guess-passwd, ftp, Phf)이 있으며 이를 정리하면 <표 1>과 같다. 여기에서의 관건은 false positive 에러율을 줄이는 것이다[7, 8, 9, 10].

표 1. KDD CUP 1999 데이터 리스트
Table 1. List of KDD CUP 1999 Data records

Attack category	Attack name	Records
Normal		1,000
DoS	Smurf	195
	Land	98
	Pod	78
Probe	Ipsweep	134
	Nmap	89
	Satan	75
U2R	buffer overflow	97
	sql-attack	86
	Rootkit	51
R2L	guess-passwd	42
	ftp write	30
	Phf	24

본 연구에서 제안한 FCM-OW는 <그림 6>에서 보듯이 기존의 KDD로 평가한 여러 가지 탐지알고리즘 중 초창기 탐지알고리즘으로 알려져 있으며 지금은 성능이 조금 떨어지는 K-Means, Fuzzy-ART와는 차이가 많이 발생하는 것을 알 수 있다. 그리고, 일반적으로 잘 알려진 Snort를 비교대상에서 제외시킨 이유는 Snort와 FCM의 성능평가 결과에서 FCM이 이미 월등하게 우수한 결과를 보여주고 있는 연구가 SCI(E), Scopus 논문으로 많이 나와 있기에 제외되었다.

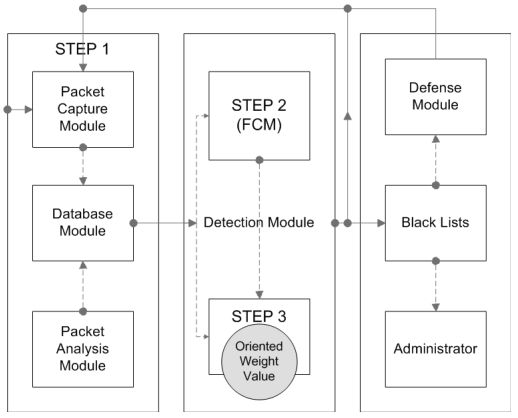

그림 5. 3-STEP 모듈 기반형 하이브리드 침입시도탐지
Figure 5. Hybrid Probe Detection based on 3-STEP Modules

실험 및 평가에서는 탐지능력이 인정된 SVM (Support Vector Machine), FCM(Fuzzy Cognitive Maps)과도 차이가 발생하였고, False positive 에러율은 기존의 여러 가지 탐지알고리즘에 비하여 월등히 성능이 우수함을 알 수 있으며 저자가 이전에 연구한 FCM을 적용한 Probe 탐지방법보다 전반적으로 개선되었음을 확인할 수 있다.

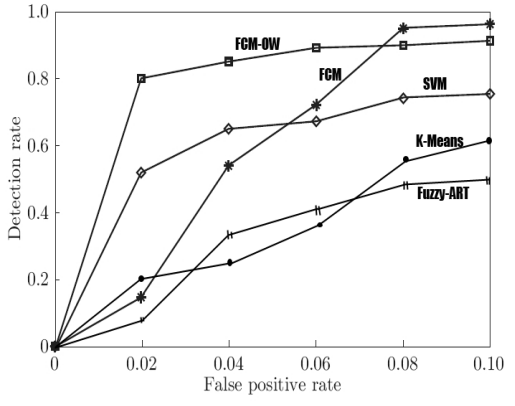

그림 6. 정상탐지율 및 오탐지율 비교
Figure 6. Camparison of Detection rate & False positive rate

4. 결 론

본 논문에서는 공격자가 침입을 하기 전에 미리 시도해 보는 시도탐지를 포함한 기존의 여러 가지 침입시도탐지 및 침입탐지방법 중 탐지율과 오탐지율이 가장 우수한 탐지방법을 모듈화하여 하이브리드형으로 재설계하였다. 이 모델은 저자가 이미 발표하여 우수한 탐지방법으로 인정된 FCM에 전처리과정으로 1단계의 패킷분석모듈과 후처리과정인 3단계의 방향성가중치를 추가하여 개선한 Probe 탐지모델이다. 본 논문에서 제안된 FCM-OW 탐지모델의 성능 분석을 위해 성능 평가 데이터로 사용되는 MIT의 'KDD IDS Evaluation Data Set'을 이용하여 수행하였고 성능결과는 SVM 보다 월등히 우수하였으며 본 저자가 이전에 발표한 FCM 보다도 전반적으로 우수한 성능 결과를 얻을 수 있었다. 향후 연구과제로는 최근 모든 네트워크환경이 클라우드 및 스마트폰환경으로 변화하고 있으므로 클라우드 및 스마트폰 기반을 탐지하는 모델로의 개발하여 확장 모듈을 추가 개발·보완하는데 있다.

References

[1] M. Jazzar, and A. Jantan, *Towards real-time intrusion detection using fuzzy cognitive maps modeling and simulation,* International Symposium on Information Technology. Vol. 2, pp. 1-6, 2008.

[2] M. Jazzar, and A. Jantan, *Using fuzzy cognitive maps to reduce false alerts in SOM-based intrusion detection sensors*, Asia Internation Conference on Modeling and Simulation, Vol. 2, pp. 1054-1060, 2008.

[3] M. Stula, and D. Stipanicev, *Fuzzy cognitive map for decision support in image post-processing*, 18th International Conference on Systems, Signals and Image Processing, Vol. 11, pp. 1-4, 2011.

[4] I. Gul, and M. Hussain, *Distributed cloud intrusion detection model*, International Journal of Advanced Science and Technology, Vol. 34, pp. 451-460, 2011.

[5] S. Y. Lee, Y. S. Kim, and B. H. Lee, *A probe detection model using the analysis of the fuzzy cognitive maps,* International Conference Cyber and Security, Vol. 3480, pp. 320-328, 2005.

[6] J. S. Park, M. H. Park, and S. H. Jung, *A whitelist-based scheme for detecting and preventing unauthorized AP acess using mobile device*, Journal of The Korea Information Communications Society. Vol. 10, No. 3. pp. 632-640, 2012.

[7] W. Xiang, H. Zhang, and H. Wang, *Application of BP neural network with L-M algorithm in power transformer fault diagnosis*, International Power System Protection and Control, pp. 100-104, 2011.

[8] S. J. Park, *A probe detection model using the analysis of the session patterns on the internet service*, 1Ph. D. Dissertation, Daejeon University, 2003.

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

[10] B. Kosko, *Fuzzy engineering*, Englewood Cliffs, NJ: Prentice-hall, 1996.

방향성 가중치가 적용된 모듈기반의 개선된 하이브리드 침입시도탐지모델

이세열[1], 안재현[2]
[1] *청운대학교 컴퓨터학과*
[2] *청운대학교 방송영상학과*

요 약

급작스런 성장이 이루어진 네트워크 기반의 기술들로 인하여 오늘날 우리는 보안의 위협에 살고 있으며 보안의 위협 또한 증가하게 되었다. 최근에는 수많은 침입탐지시스템에서 다양한 기술들을 제안하고 있다. 그러나, 이러한 기술들은 침입의 패턴이 많이 알려진 형태의 많은 시스템에 적용되었다. 이에, 침입시도탐지는 이러한 보안 위협의 잠재적인 공격에 대응할 수 있는 중요한 핵심으로 자리를 잡게 되었다.. 침입시도탐지에는 오탐지율과 비정상탐지율을 감소할 수 있는 여러 가지 요소들이 있으며 이들 간의 관계가 에러율을 크게 좌우하게 된다. 또한 침입시도탐지는 전혀 새로운 패턴의 침입시도를 탐지할 수 있는 기술 또한 계속적으로 요구되어 지고 있다. 이에, 본 논문에서는 3단계 모듈을 기반으로 하는 개선형 하이브리드 침입시도탐지모델을 제안한다. 3단계 모듈은 세션패턴분석, 방향성 가중치 모듈, 퍼지인식도 모듈이다. 실험평가를 위하여 MIT에서 만들어놓은 KDD CUP 1999 데이터를 사용하였다. 대부분의 기존 탐지 시스템은 10%내외의 오탐지를 제공하고 있다. 그러나, 실험 결과, 이 방법은 오탐지율을 감소시켜주는 효과가 있으며 높은 정상탐지율을 나타낸다.

감사의 글

본 논문은 청운대학교의 2011학년도 학술연구조성비를 지원 받음.

Se-Yul Lee received the M.S. degree in Department of Information & Communications Engineering and the Ph.D. degree in the Department of Computer Engineering from Daejeon University in 1999 and 2003, respectively. From 1998 to 2001, he was a researcher at ETRI & Insopack Co. From 2004 to present, he is a professor in the Department of Computer Science at Chungwoon University. His current research interests include Network Security Intrusion Detection & Prevention, System Security, Fuzzy-neural Networks. He is a life member of the KKITS.

E-mail address: pirate@chungwoon.ac.kr

Jae-Hyeon An received the bachelor's degree in the Department of Germany Language & Literature from the SoongSil University in 1987. He received the Ph.D. degree in the Department of Communications from Westfaelische Wilhelms-Universitaet (Germany) in 1997. He is a professor in the Department of Broadcasting & Digital Media at Chungwoon University since 2008. His current research interests include communication, culture contents & Broadcasting. He is a member of the KKITS.

E-mail address: jahan@chungwoon.ac.kr