韓國 컴퓨터情報學會 論文誌
第10卷 第6號, 2005. 12.

2005-10-6-1-2

퍼지인식도와 세션패턴 기반의 비정상 탐지 메커니즘

류 대 희*, 이 세 열**, 김 혁 진***, 송 영 덕****

Anomaly Detection Mechanism based on the Session Patterns and Fuzzy Cognitive Maps

Dae-Hee Ryu *, Se-Yul Lee **, Hyeock-Jin Kim ***, Young-Deog Song ****

요 약

최근 인터넷 이용자들이 급격하게 증가하고 있으며, 초보수준의 일반 네트워크 사용자들도 인터넷상의 공개된 해킹 도구들을 사용하여 고도의 기술을 요하는 침입이 가능하여 해킹 문제가 더욱 심각해지고 있다. 해커들이 침입하기 위하여 취약점을 알아내려고 의도하는 다양한 형태의 침입시도를 사전에 탐지하여 침입이 일어나는 것을 미리 방어할 수 있는 침입시도탐지가 적극적인 예방 차원에서 더욱 필요하다. 기존의 포트 스캔이나 네트워크 취약점 공격에 대응하기 위한 네트워크 기반의 비정상 침입시도 탐지 알고리즘은 침입시도탐지에 있어 몇 가지 한계점을 갖고 있다. 기존 알고리즘은 Slow Scan, Coordinated Scan을 할 경우 탐지할 수 없다는 것이다. 따라서 침입시도 유형에 제한을 받지 않고 침입시도에 관한 다양한 형태의 비정상 접속을 효과적으로 탐지할 수 있는 새로운 개념의 알고리즘이 요구된다. 본 논문에서는 세션 패턴과 탐지 오류율을 규칙기반으로 하는 침입시도 탐지알고리즘(Session patterns & FCM Anomaly Detector : SFAD)을 제안한다.

Abstract

Recently, since the number of internet users is increasing rapidly and, by using the public hacking tools, general network users can intrude computer systems easily, the hacking problem is getting more serious. In order to prevent the intrusion, it is needed to detect the sign in advance of intrusion in a positive prevention by detecting the various forms of hackers intrusion trials to know the vulnerability of systems. The existing network-based anomaly detection algorithms that cope with port-scanning and the network vulnerability scans have some weakness in intrusion detection. they can not detect slow scans and coordinated scans. therefore, the new concept of algorithm is needed to detect effectively the various. In this paper, we propose a detection algorithm for session patterns and FCM.

▸ Keyword : Intrusion detection, Pattern of service, Fuzzy Cognitive Maps

---

• 제1저자 : 류대희
• 접수일 : 2005.09.29, 심사완료일 : 2005.10.26
* 청운대학교 컴퓨터학과 교수, ** 청운대학교 컴퓨터학과 전임강사
*** 청운대학교 컴퓨터학과 부교수, **** 한서대학교 대학원 정보보호학과 박사과정

Ⅰ. 서 론

인터넷이 발달된 오늘날, 해킹 및 정보보호는 관심 있는 네트워크 분야중 하나이다. 이로 인하여 여러 자동화된 정보보호 대안들이 개발되고 있다. 그러나 1998년에서 2004년 동안 웹 서버로 많이 사용되는 마이크로소프트사의 인터넷정보서비스(Internet Information Server : IIS)의 침입 또는 취약점을 이용한 새로운 공격 기술 또한 100여 개 이상 발견되었다[1]. 이를 위한 방어 대책으로 최근 몇 년 동안 신경망, 데이터 마이닝, 패턴 인식, 퍼지 논리, 전문가 시스템 등을 적용한 네트워크 기반 탐지알고리즘이 연구되어지는 추세이다[2]. 퍼지 논리 및 전문가 시스템은 기존의 알고리즘위주의 문제해결 방식으로는 해결할 수 없었던 정성적인 정보(Qualitative Information)를 지식화하여 이를 문제해결 과정에 적극 활용할 수 있게 됨으로써 다양한 방법론적 연구가 이루어지게 되었다[3].

현재 침입탐지기술은 과거에 침입했던 형태의 규칙을 데이터베이스로 구축해 놓고, 네트워크 상에 이와 동일한 패턴이 나타나면 침입으로 간주하여 탐지한다. 침입탐지기술은 침입이 아닌데도 불구하고 침입으로 오인하고 수많은 네트워크 패킷을 탐지, 분석함으로써 시스템의 효율성을 저하시킬 뿐만이 아니라 막대한 비용손실을 초래하고 있다. 그러나 새로운 침입기술을 탐지하는 것은 쉬운 일은 아니다. 탐지기술은 이미 감사된 규칙기반과 비교하여 판단하므로 새롭고 다양한 침입탐지기술을 모두 규칙화하기에 어려움이 있기 때문이다[4]. 침입탐지시스템에서 침입(True Positive & False Positive)이라고 판단한 데이터를 분석한 결과, 실제 해킹은 불과 10% 미만이고, 90% 이상은 정상데이터이다. 바로 네트워크 상에 정상적인 패킷을 해킹으로 오 분류(False Positive Error)하거나 또는 실제 해킹이 일어났으나 정상적인 패킷으로 오 분류(False Negative Error)함으로써 보안 전문가 또는 분석가들이 최종 판단하는데 많은 시간과 비용을 소비하고 있다. 더구나 기존에 침입했던 패턴과 약간 변형된 패턴이나 새로운 패턴 또는 최신 침입 기술로 침입하면 피해를 당하기 전에는 사전에 탐지할 수 없는 오 분류 수치가 높아지는 치명적인 취약점을 가지고 있다.

포트 스캔이나 네트워크 취약점 검색 공격에 대응하기 위한 네트워크 기반의 비정상 침입시도 탐지 모델로는 Phrack magazine의 "Designing and Attacking Port Scan Detection Tools"에서 발표된 Scanlogd와 Silicon Defence에서 Snort의 preprocessor plug-in으로 만든 SPADE(Statistical Packet Anomaly Detection Engine) 등이 있다. 그러나 이러한 형태의 공개된 프로그램들은 침입시도탐지에 있어 몇 가지 한계점을 갖고 있다. Scanlogd는 일정시간 동안 정의된 임계값 이상의 연결 요청이 있을 경우 이를 침입시도로 탐지하기 때문에 일정시간보다 느리게 연결을 요청하는 Slow Scan을 탐지할 수 없다. 또한, 임의의 호스트가 아니라 여러 호스트에서 Coordinated Scan을 할 경우 탐지할 수 없다.

SPADE 알고리즘은 자주 접근되었던 포트를 대상으로 하는 스캔은 탐지할 수 없는 취약점을 갖고 있다. 평상시의 호스트별 포트들의 접근 빈도를 저장하여 두고 어떤 접근이 있을 경우 자주 접근하지 않던 곳이면 침입시도로 탐지를 하기 때문에 자주 접근되었던 포트를 대상으로 하는 스캔은 탐지할 수 없다.

현재 국내에 널리 알려진 Scanlogd와 SPADE 알고리즘은 탐지 가능한 침입시도 유형이 극히 제한적이기 때문에 침입시도 유형에 제한을 받지 않고 침입시도에 관한 다양한 형태의 비정상 접속을 효과적으로 탐지할 수 있는 새로운 개념의 알고리즘이 요구된다.

본 논문에서는 제 2장에서 본 논문의 기반 기술 및 관련 기능과 특징에 대하여 기술한다. 제 3장에서는 세션 패턴과 퍼지인식도(Fuzzy Cognitive Maps :FCM)을 이용한 알고리즘을 제안하고 제 4장에서 알고리즘을 통해 나온 결과에 대한 분석과 마지막으로 향후 연구되어야 할 부분에 대한 언급과 결론을 맺는다.

Ⅱ. 관련 연구 기반 기술

2.1 SPADE

SPADE은 Silicon Defence사에서 Snort의 Preprocessor plug-in으로 만든 네트워크 모니터링으로 비정상 이벤트를 Snort report 매커니즘을 통해 경보를 보낸다[5]. SPADE

는 Snort에 의해 수집된 패킷들 중에서 home-net 모드로 들어오는 Tcp_syn 만 찾아서 anomaly score를 가지고 비정상으로 결정된 패킷을 보고한다. anomaly score는 네트워크에서 미리 인지된 히스토리에 기반을 두고 결정한다. 이전에 발생한 이벤트의 수가 적은 패킷은 높은 anomaly score를 갖는다. anomaly score는 확률로부터 직접 계산되는데, 즉 주어진 IP와 Port 조합 x에 대해 해당 네트워크를 목적지로 하는 일반 트래픽의 패킷이 발생할 확률을 P(x)로 한다. 아래 수식과 같이 P(x)에 -log2를 취하여 그 패킷의 anomaly score A(x)를 구한다. A(x)가 설정된 임계값 보다 큰 x로의 패킷들을 침입시도로 탐지한다[5, 6].

$$A(x) = -\log_2(P(x))$$

2.2 Scanlogd

Scanlogd는 Phrack Magazine Vol.8에 있는 "Designing and Attacking Port Scan Detection Tools"에서 설명한 간단하고 신뢰성 있는 포트 스캔 탐지 모델이다. 이 모델은 Raw TCP Socket을 사용하여 Stealth를 포함하는 TCP Port Scan을 탐지하는 방식으로 포트 스캔 탐지 임계값은 아래와 같다.

포트 스캔으로 판단할 조건은 주어진 시간(Delay)동안 동일 접속 소스 주소로부터의 포트 접근 횟수(Count)를 설정한다. 이 두 가지 설정값들은 임의로 설정이 가능하다.

```
#define Scan_Count_Threshold 10
#define Scan_Delay_Threshold (Clk_Tck * 5)
```

Scanlogd는 포트 스캔에 대한 로그 데이터를 저장하고 소스 주소 데이터를 찾기 위하여 해쉬 테이블을 사용한다. 이 방식은 일반적으로 해쉬 테이블 크기가 충분히 크다면 제대로 잘 동작한다. 평균적으로 데이터를 찾는 시간은 이진 탐색(Binary search) 보다는 빠르다. 얼마나 많은 데이터를 유지하는가에 따라서 Scanlogd 프로그램이 제시간에 새로운 패킷 데이터를 가져올 수 있는지 없는지를 알 수 있게 된다. 이 문제는 해쉬 충돌 횟수를 제한함으로써 해결하였고, 같은 해쉬 테이블이 제약 사항에 도달하였을 때 같은 해쉬 값에 대한 데이터는 이전의 데이터를 버리는 방식을 취한다[7].

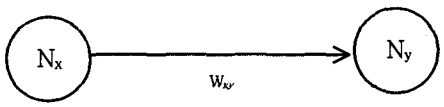
III. SFAD

3.1 SFAD의 기본원리

침입의도에 상관없이 사용자의 모든 이벤트는 패킷으로 나타나며 패킷이 모여 트래픽이 된다. 인터넷 서비스의 세션은 서버와 클라이언트간의 교환 패킷을 의미하며 소스의 위치에 따라 패킷은 서버 세션과 클라이언트 세션으로 구분된다. 서비스 주체인 서버와 클라이언트는 극 서비스의 프로토콜에 준하며 동일한 서비스의 세션은 일정한 패턴을 가지게 된다. 바로, 이 패턴에 준하는 정상적인 서비스와 비정상적인 서비스 패턴으로 구분하여 침입여부를 1차 판단할 수 있다.

서비스 프로토콜의 패턴으로 침입여부를 판단할 수 있으므로 각 서비스마다 프로토콜 패턴을 인지한 후 학습을 통하여 그 프로토콜 정상 서비스 패턴을 알아낼 수 있다. SFAD가 비정상을 탐지하기 위해 사용되는 패킷은 패킷의 데이터 분석을 통해 많은 패킷 데이터 중에서 선정된 목적지 IP(dst_ip), 목적지 포트번호(dst_port) 그리고 세션 패턴이다. 세션 패턴을 적용한 침입시도 탐지는 정상 서비스에서 서버와 클라이언트간의 세션을 dst_ip의 dst_port별로 규칙기반으로 하며, 이 규칙기반을 벗어나는 클라이언트의 접근 이벤트인 경우 이를 침입시도로 간주하는 것이다. 본 논문에서는 이 규칙기반 특징을 클라이언트와 서버가 주고받는 세션들의 길이, 즉 세션의 패킷수의 최소값을 하나의 특징으로 사용하며 이 중에서 처음 부분의 것을 특징으로 삼아 이와 다른 데이터 크기의 열을 갖는 세션은 비정상 세션으로 간주되어 침입시도로 탐지하게 된다. 이렇게 1차 탐지된 비정상 세션 패킷이 침입이라고 단정하는 것은 오탐지율이 높다는 것이 지금까지의 연구결과로 밝혀졌다. 본 연구에서는 탐지된 패킷에 퍼지인식도를 적용하여 오탐지율을 최소화 시키는 2차 탐지 모듈을 두는 것이다. 2차 탐지 모듈은 퍼지인식도(Fuzzy Cognitive Maps)의 Causal knowledge reason를 이용하여 지능적 판단모듈구조로 설계하였다. FCM은 주어진 문제영역내의 각 개념들 사이에 존재하는 인과관계(Cause-effect relationship)를 나타내는 유향성 그래프(Directed graph)이다. (그림 1)은 퍼지

인식도를 도식화 한 것으로써 각 노드와 노드사이의 가중치가 Wxy=0인 경우에는 각 노드사이에 아무런 관련이 없는 것을 의미하며, Wxy≠0 경우에는 (그림 1)과 같은 의미를 부여한다. 단순한 퍼지 인식도에서는 인과관계 값을 {-1, 0, 1}로 취할 수 있다. 따라서 이경우의 인과관계는 최대 또는 최소의 정도로 발생한 것을 의미한다{8,9,10}.



$W_{xy}>0$: N_x 수치 증가로 인한 N_y 수치 증가인 경우
$W_{xy}<0$: N_x 수치 증가로 인한 N_y 수치 감소인 경우

그림 1. 퍼지인식도
Fig. 1. Fuzzy Cognitive Maps

2차 탐지모듈에서 여러 가변 요소 중 어떤 요소에 의존성을 부여함으로써 가장 최적의 탐지를 할 수 있는 것이 가장 큰 관건이다{11,12,13}. 그 뿐만 아니라 탐지한 IP address를 침입으로 최종 결정할 수 있는 것이다. 퍼지 인식도는 이러한 여러 가변 요소를 적용하여 최적의 판단을 내리게 한다. 본 논문에서 사용된 가변 요소는 패킷 필터링에서 캡쳐된 소스/목적지 주소, 침입시간 간격, Syn 패킷 수, Port number, windows size 등이 된다.

3.2 SFAD 탐지 모델

SFAD는 (그림 2)와 같이 세션 분류기, 패턴 추출기, 패턴비교기로 되어있는 STEP1 그리고 (그림 3)과 같이 퍼지 인식도 가변판단모듈을 적용한 STEP2로 구성된 SFAD 탐지모델 (그림 4)로 이루어져 있다.

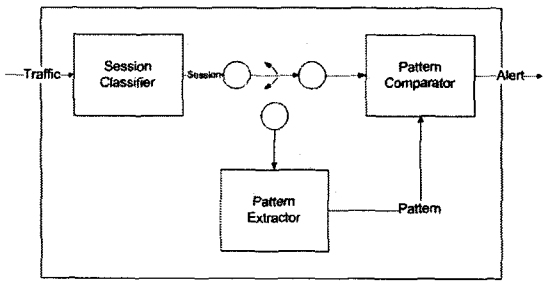


그림 2. SFAD 탐지의 STEP1
Fig. 2. STEP1 of SFAD Detection

STEP1에서 세션 분류기는 트래픽의 패킷들을 읽어서 출발지와 목적지가 같은 세션으로 분류하는 역할을 한다. 세션의 종류마다 패킷 저장 버퍼가 있으며 패킷들이 모두 모이면 그 버퍼의 모든 패킷이 하나의 세션으로 출력된다. 출력된 세션은 실행 모드에 따라 패턴 추출기, 패턴 비교기의 입력에 해당된다. 실행 모드는 학습모드와 탐지모드가 있다. 세션 분류기에서 출력된 세션은 학습모드인 경우 패턴 추출기로 들어가고 탐지 모드인 경우 패턴 비교기로 들어간다.

패턴 추출기는 같은 목적지를 갖는 세션들을 모아 그 세션의 공통 패턴을 추출하여 출력한다. 패턴은 두 가지의 feature로 구분된다. 첫 번째는 세션을 이루는 패킷들의 데이터 크기를 패킷 시간 순서로 나열했을 때 동일 목적지 주소를 갖는 세션들의 공통부분이 처음 부분인 경우이다. 두 번째는 동일 목적를 갖는 세션들의 최소 길이 이다. 여기서 세션의 길이는 세션을 이루는 패킷들의 수가되며 이 두가지 feature는 한 쌍이 되어 패턴 추출기의 출력이 된다.

패턴 비교기는 규칙기반으로 만들어 놓은 패턴과 침입여부의 판단의 대상이 되는 패턴 세션을 비교하여 세션이 패턴과 다르면 비정상 패턴으로 간주하여 경보를 출력한다. 즉, 패턴 비교기는 세션과 패턴의 두 개의 입력을 받으며 입력된 세션은 패턴 추출 때와 비슷하게 두 가지 feature가 추출된다. 추출된 feature과 규칙기반 feature을 비교하여 세션의 두 feature 중 유사성이 없는 것은 비정상 세션으로 정보를 출력한다.

STEP2에서 (그림 3)은 가변요소를 적용한 판단모듈의 퍼지 인식도를 나타낸 것으로써, 판단모듈에 의존성을 갖는 가변요소를 적용한 것이다.

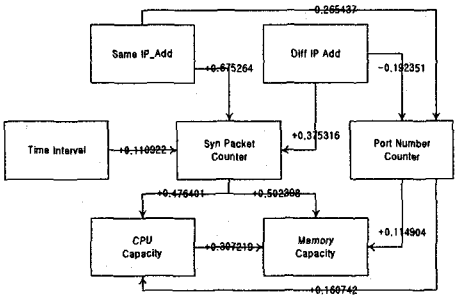


그림 3. SFAD 탐지의 STEP2
Fig. 3. STEP2 of SFAD Detection

가변요소를 노드(Nx)와 다음 노드(Ny)에 두고 두 노드의 링크인 가중치(Wxy)를 적용하는 것이다. 예를 들면, Syn packet과 CPU 가용율에서는 Syn packet의 용량이 증가할수록 CPU 가용율이 증가하므로 이때 가중치는 0보다 크게 된다. 이때 임의의 노드에 가해지는 수치는 노드와 가중치를 연결한 네트워크를 통과할수록, 그리고 반복횟수에 따라서 달라지게 된다. 이를 수식화 하면 아래와 같다.

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

단, 가중치(Wxy)의 증감부호는 다음 노드에 미치는 영향에 따라서 결정이 되며 수치는 규칙기반에 의하 통계적 누적수치를 정하기 위해 Quantitative Micro Software Ltd.의 Eview ver 3.1을 이용하여 경로분석의 효과계수를 가중치로 사용한다.

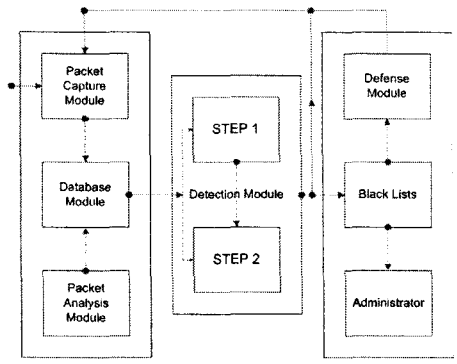


그림 4. SFAD 모델 구조
Fig. 4. Architecture of SFAD Model

IV. 구현 결과 분석

SFAD 모델 평가의 신빙성을 위해서 DARPA 프로젝트로써 MIT Lincoln 연구소에서 만든 침입탐지 평가 데이터 중에 1999년 데이터 집합을 이용하여 테스트 하였다. IDS 평가 데이터에는 5주 분량의 패킷들이 수집되어 있으며 이 중 1,2,3주는 평상시 데이터이고, 4,5주는 공격이 들어있는 데이터이다. SFAD는 세션 패턴 추출로 1,3주 데이터를 사용하였고, 4주 데이터를 테스트 데이터로 사용하여 탐지율과 오경보율을 얻었다. 4,5 주 데이터에는 〈표 1〉과 같이 5개의 크게 분류된 침입 공격들이 있으며 이중 침입시도 공격인 Probe만을 탐지율로 평가했다.

〈표 1〉 공격 유형
Table 1 Attack Types

유형	종류
DoS	Apache2, Arppoison, Back, Crashiis, Dosnuke, Land, Mailbomb, Syn Flood, Ping of Death, Process Table, selfping, Smurf, sshprocesstable, Syslogd, tcpreset, Teardrop, Udpstorm
U2R	anypw, casesen, Eject, Ffbconfig, Loadmodule, ntfsdos, Perl, Ps, sechole, Xterm, yaga
R2L	Dictionary, Ftpwrite, Guest, Httptunnel, Imap, Named, ncftp, netbus, netcat, Phf, ppmacro, Sendmail, sshtrojan, Xlock, Xsnoop
Probe	insidesniffer, Ipsweep, Is_domain, Mscan, NTinfoscan, Nmap, resetscan, Saint, Satan
Data	Secret

4.1 Session Classifier

세션 분류기는 네트워크에서 패킷을 캡쳐하기 위하여 tcpdump를 이용한다. tcpdump에 의해 캡쳐된 파일은 오프라인으로 세션 분류기의 입력으로 사용되고, 세션 분류기는 세션별로 분류하여 세션 데이터 파일을 출력한다. 세션 데이터 파일은 여러 개의 동일한 형식의 행으로 구성되며 각 행은 클라이언트 또는 서버 세션으로 쌍을 이룬다. 각 행의 처음 부분에는 그 세션을 구성하는 패킷들의 공통된 정보가 기록되고 그 뒤로 각 패킷의 크기 순서대로 오게 된다. 각 필드는 세션이 시작된 시각으로서 첫 패킷을 최초 송, 수신된 Time, 패킷의 출발지 또는 목적지의 IP주소와 포트번호인 src_ip, dst_ip, src_port, dst_port을 의미하며 세션의 패킷들의 크기인 size 등으로 구성되어있다.

4.2 Pattern Extractor

4.2.1 정상 세션 패턴

정상 세션 패턴이란 정상적인 클라이언트가 정상적인 서비스를 서버로부터 받을 때 사용된 세션들의 공통된 패턴을 의미한다. FTP, 텔넷 등 여러 서비스 중 (그림 5)는 텔넷

서비스의 한 호스트에 대한 정상 세션 패턴을 보여주는 그래프이다. 패턴 추출기는 각 호스트들의 포트별로 패턴에 사용되는 공통 경로와 최소 세션 길이를 추출하여 세션 패턴 파일로 보낸다.

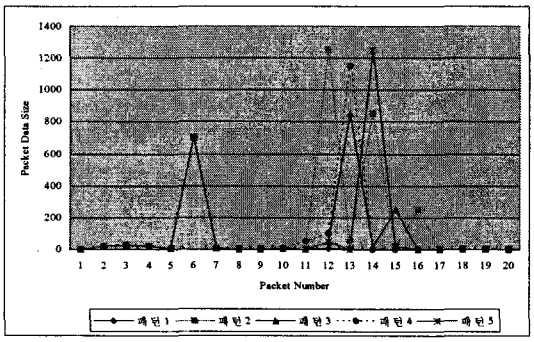


그림 5. 텔넷 서비스의 정상 세션 그래프
Fig. 5. Normal Session Graph of Telnet

4.2.2 비정상 세션 패턴

비정상 세션은 두 가지 형태의 비정상 패턴을 가진다. 그 중 첫번째는 서비스 프로토콜을 위반하는 패턴형태이다. Portsweep와 같은 침입시도인 경우 서비스를 받지 않고 자신의 목적지 호스트의 상태 확인 후 바로 프로토콜을 종료하는 방식으로 정상 세션 패턴을 따르지 않는다. 이러한 비정상 세션은 패턴길이가 매우 짧고 데이터의 송, 수신이 거의 없다는 게 특징이다.

(그림 6)은 텔넷 서비스 프로토콜을 위반하는 비정상 세션 데이터 그래프이다.

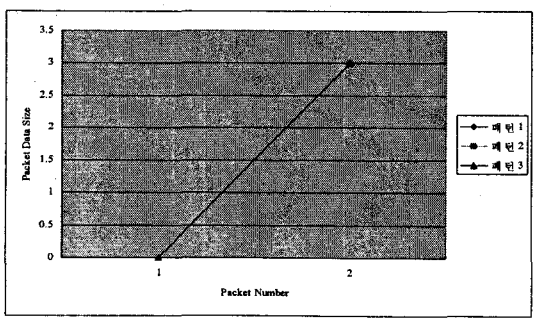


그림 6. 텔넷 서비스의 비정상 세션 그래프
Fig. 6. Anomaly Session Graph of Telnet

두 번째는 서비스 프로토콜을 준수하는 비정상 세션 패턴이다. 이러한 종류는 텔넷서비스의 SATAN등이 있으며 일단 접속해서 서비스를 즉시 Reset하지 않고 취약점 검색을 위해 정상적인 서비스를 한다는 것이 정상 서비스 세션과 동일하여 구분하기 어려운 특징을 갖는다.

(그림 7)은 텔넷에서 SATAN 인 경우의 세션 그래프이다.

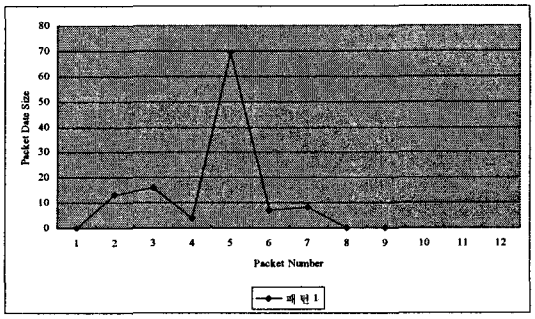


그림 7. SATAN의 텔넷서비스 침입시도 그래프
Fig. 7. Probe Graph of Telnet on SATAN

4.3 Pattern Comparator

패턴 비교기는 이미 만들어 놓은 패턴과 침입 시도 여부의 판단 대상이 되는 세션을 비교하여 정상 유무를 간주하여 경보를 출력한다. 패턴 비교기는 세션과 패턴의 두 개의 입력을 받아 입력된 세션은 패턴 추출 때와 같이 패킷의 크기와 세션 길이를 추출한다. 이들과 추출된 패턴을 각각 비교하여 세션의 특징 중 한 가지라도 다르면 비정상 세션으로 경보를 출력한다.

올바른 판단을 얻기 위해서 정상적인 패턴과 비정상 패턴 사이에 뚜렷한 차이가 있어야 한다. (그림 8)과 (그림 9는 정상 서비스 세션과 침입시도 세션의 패턴차이와, 침입시도 세션의 서비스 프로토콜 준수 여부에 따라 두 가지로 나누어 설명한다. 첫째, 정상 서비스 세션과 서비스 프로토콜을 위반하는 침입시도 세션의 패턴 비교이다.

(그림 8)은 텔넷 서비스에 대해 침입시도와 정상 세션의 뚜렷한 패턴 차이를 보여주며 이러한 침입시도는 탐지가 가능하다.

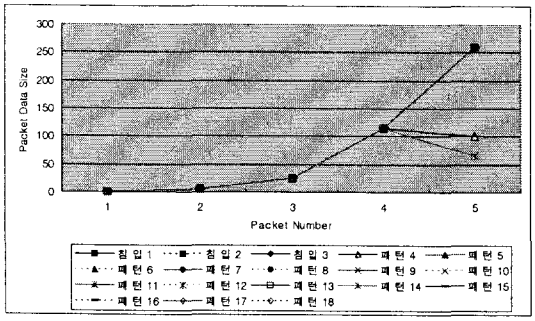


그림 8. 텔넷 서비스 프로토콜을 위반하는 침입시도와 정상 세션의 패턴 비교
Fig. 8. Probe vs Normal Session Patterns of Anomaly Telnet Service Protocol

둘째, 정상 서비스 세션과 서비스 프로토콜을 준수하는 침입시도 세션의 패턴 비교이다. 위에서 설명한 첫 번째 보다 더 정상 세션에 가까운 패턴을 보이지만, 세션의 길이나 모양이 정상 세션과 차이를 보이므로 탐지가 가능하다. (그림 9)는 텔넷 서비스에 대한 정상 세션과 침입시도 세션의 패턴 비교를 보여준다.

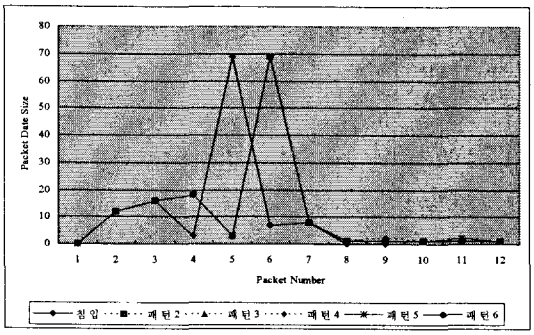


그림 9. 텔넷 서비스 프로토콜을 준수하는 침입시도와 정상 세션의 패턴 비교
Fig. 9. Probe vs Normal Session Patterns of Normal Telnet Service Protocol

분석 결과와 같이 침입시도가 정상 세션의 패턴과 다르면 서비스 프로토콜을 준수하는지 위반하는지의 여부에 상관없이 탐지가 가능함을 보여준다.

V. 결 론

본 논문에서는 공격자가 침입을 하기 전에 미리 시도해 보는 포트스캔이나 네트워크 취약점 검색 공격을 탐지하기 위하여 일반적인 인터넷 서비스의 정상적인 서비스 패턴과 퍼지인식도를 이용하여 비정상적인 침입시도의 탐지하는 SFAD를 제안하였다. SFAD는 침입시도 판단의 단서로 사용자가 서비스를 실제로 이용하고 있는지 아닌지 여부에 초점을 맞추고 있다. 평상시 정상적인 서비스 패턴을 추출하여 기억시키고, 그 패턴과 다른 비정상 서비스 패턴이 보이면 이를 탐지한다. SFAD의 성능 분석을 위해 성능 평가 데이터로 사용되는 MIT에서 만든 "IDS Evaluation Data Set"을 이용하여 수행하였고, True Positive 97.0%와 False Positive 9.5%의 성능을 얻었다. 이 결과는 99년 우승자의 True Positive 97.1%와 False Positive 9.2%와 유사한 성능을 보인다. 성능 분석 결과는 기존의 탐지 알고리즘인 Scanlogd에서 탐지하지 못했던 Slow Scan과 Coordinated Scan을 정상 및 정상을 위반하는 세션패턴을 찾아냄으로써 탐지 할 수 있었으며 2차 탐지모듈을 추가 적용하여 True Positive 정확도를 높여 오판단율을 최소화 시켰다.

향후 연구과제로는 본 논문에서 제안한 SFAD 모델 구조의 방어모듈과 퍼지 인식도에 의한 2차 탐지모듈의 정확도를 향상시켜 구현하여 더욱 강화된 침입 방지 모델을 개발 및 보완 발전하는데 있다.

참고문헌

[1] Franklin L., "Protection the Web server and Application," Computer and Security, No.20, pp.31-35, 2001.

[2] Hofmeyr, S. A., Forrest, S., and Somayaji, A., "Intrusion detection using sequences of systems

calls," Journal of Computer Security, Vol.6, pp.151-180, 1998.
[3] Axelrod, R., "Structure of Decision : The Cognitive Maps of Political Elites," Princeton, NJ : Princeton University Press, 1976.
[4] Cannady, J., "Applying Neural Networks to Misuse Detection," In Proceedings of the 21st National Information System Security Conference, 1998.
[5] Stuart Staniford, James A. Hoagland and Joseph M. Mcalerney, "Practical Automated Detection of Stealthy Portscans," http://www.silicondefense.com.
[6] James A. Hoagland and Stuart Staniford, "Viewing IDS alerts : Lessons from SnortSnart," IEEE, 2001.
[7] "Designing and Attacking Port Scan Detection Tools," Phrack Magazine, Vol.8 Issue 53, July, 1998.
[8] S. Y. Lee, An Adaptive Probe Detection Model using Fuzzy Cognitive Maps, Ph. D. Dissertation, Daejeon University, 2003.
[9] K. A. Kang, "Performance Analysis of Optimal Neural Network structural BPN based on character value of hidden node," KSCI, Vol. 5, No. 2, pp. 11-16, 2000.
[10] S. Y. Lee, "A Probe Detection Model Using the Analysis of the Fuzzy Cognitive Maps," ICCSA 2005, LNCS 3480, pp. 320-328, 2005.
[11] S. J. Park, A Probe Detection Model using the Analysis of the Session Patterns on the Internet Service, Ph. D. Dissertation Daejeon University, 2003.
[12] B. S. Ko, Y. R. Choi, "A Design of Secure Audit/Trace Module to Support Computer Forensics," KSCI, Vol. 9, No. 1, pp. 79-86, 2004.
[13] Y. S. Park, Y. R. Choi, "A Study on the Active Traceback Scheme Responding to a Security Incident," KSCI, Vol. 10, No. 1, pp. 27-33, 2005.

저 자 소 개

류 대 희
원광대학교 대학원 이학박사
1995~현재 청운대학교 컴퓨터학과 교수
〈관심분야〉 알고리즘, 퍼지이론, 확률응용 등

이 세 열
대전대학교 대학원 컴퓨터공학과 공학박사
2004~현재 청운대학교 컴퓨터학과 전임강사
〈관심분야〉 IDS, 네트워크보안 등

김 혁 진
아주대학교 대학원 컴퓨터공학과 공학박사
1997~현재 청운대학교 컴퓨터학과 부교수
〈관심분야〉 CG, CAGD, 웹기술등

송 영 덕
한서대학교 대학원 정보보호학과 박사과정
〈관심분야〉 정보보호 등