한국 퍼지 및 지능시스템 학회 2002, Vol. 13, No. 4, pp. 491-498

TCP 프로토콜을 사용하는 서비스거부공격 탐지를 위한 침입시도 방지 모델

A Probe Prevention Model for Detection of Denial of Service Attack on TCP Protocol

이세열 · 김용수
Se-Yul Lee, Yong-Soo Kim

대전대학교 컴퓨터공학부

요 약

진보된 컴퓨터 네트워크 기술은 개방형 네트워크 환경을 기반으로 이루어진다. 따라서, 네트워크를 위협하는 보안문제도 중요한 문제로 대두되고 있고 침입탐지 및 방지모델과 같은 기술이 필요하게 되었다. 본 논문에서는 퍼지인식도를 이용한 네트워크기반의 침입탐지 모델(SPuF, Syn flooding Preventer using FCM)을 제안하는데 이 방법은 패킷분석을 통하여 서비스거부공격을 탐지한다. 서비스거부공격은 침입시도 형태로 나타나며 대표적인 공격은 Syn Flooding이 있다.
SPuF 모델은 Syn flooding 공격을 탐지하기 위하여 패킷정보들을 캡처하여 분석하는 침입시도탐지 모델이다. 이 모델은 FCM을 적용한 판단모듈의 분석 결과를 토대로 서비스거부공격의 위험도 수준을 측정하고 공격에 대한 적절한 대응모듈을 적용한다. 연구실험을 위한 데이터로는 MIT Lincoln Lab의 KDD'99 데이터를 사용한다. SPuF 모델에서의 KDD'99 데이터로 모의실험한 결과, 97%이상의 침입시도탐지율을 나타내었다.

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 FCM(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 SPuF(Syn flooding Prevenrter using Fuzzy cognitive maps) model captures and analyzes the packet informations 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.
For the performance comparison, the "KDD'99 Competition Data Set" made by MIT Lincoln Labs was used. 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

1. 서 론

인터넷이 발달된 오늘날, 해킹 및 정보보호는 관심 있는 네트워크 분야중 하나이다. 이로 인하여 여러 자동화된 정보보호 솔루션이 개발되었다. 그러나, 1998년에서 2002년 동안 웹서버로 많이 사용되는 마이크로소프트사의 인터넷정보서버(Internet Information Server : IIS)에 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 침입탐지시스템이 연구되어지는 추세이다[2]. 퍼지 논리 및 전문가 시스템은 기존의 알고리즘위주의 문제해결 방식으로는 해결할 수 없었던 다양한 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, 네트워크상에 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)라고 판단한 데이터를 분석한 결과, 실제 해킹은 불

접수일자 : 2003년 4월 20일
완료일자 : 2003년 7월 30일

과 10% 미만이고, 90% 이상은 정상데이터이다. 바로 네트워크상에 정상적인 패킷을 해킹(False Positive Error)으로 오 분류하거나 또는 실제 해킹이 일어났으나 정상적인 패킷(False Negative Error)으로 오 분류함으로써 보안 전문가 또는 분석가들이 최종 판정하는데 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 False Negative Error의 수치가 높아지는 치명적인 취약점을 가지고 있다.

표 1은 기존의 침입탐지방법에서의 정상데이터를 해킹으로 오인(False Positive Error)하는 경우와 침입을 정상패킷으로 오인(False Negative Error)된 오류율 현황이다. 오류율 현황의 평가방법은 MIT Lincoln Lab에서 규정한 침입 시나리오 조건에 의한 타당성 있는 근거에 따라 상호 비교 결정한 자료이다[5, 6].

표 1. 침입탐지방법의 오류율
Table 1. Error Rates of Intrusion Detection Method

Intrusion Detection Method	Performance(Error Rates)	
	False Negative	False Positive
FSTC (Columbia Univ.)	22.65%	20.48%
Inductive Learning System	9.79%	9.10%
Case Based Reasoning	7.05%	13.05%
K-means (Average Value)	9.37%	20.45%
Fuzzy ART (ρ =0.9)	6.03%	38.73%

본 논문에서는 앞에서 언급했던 취약점을 이용한 공격형태 중 최근 2~3년 간에 발생빈도가 상당히 높으며 TCP/IP 프로토콜의 구조적인 결함으로 인하여 완벽한 해결방안이 없는 서비스 거부 공격(Denial of Service : DoS)에 대하여 침입이라는 관점에서 무작위로 탐지하고 무조건적인 대응방법 등으로 비정상사용자 뿐만 아니라 정상사용자에게 까지 피해를 끼치는 상황을 좀더 적응적으로 해결하는 방안을 제시한다. 본 본문에서 제시하는 방법은 기존의 탐지 방법과는 다른 접근방법으로 잘못 판단한 경고들(False Positive Error)을 포함하는 경고들이 발생된 상태에서 이를 분석하고 필요없는 경고에 대한 위험도를 결정 및 분석하여 시스템에 악영향을 미치는 가장 중요한 경고 요소들에 대하여 적응적으로 대응하는 방법이다.

본 논문에서는 제2장에서 본 논문의 기반 기술 및 관련 기능과 특징에 대하여 기술한다. 제3장에서는 퍼지인식도를 적용한 탐지 모델을 제안하고 이 모델을 기반으로 모의 실험과 모의 실험을 통하여 나온 결과에 대한 분석 및 실제 네트워크에서 테스트를 통하여 기존의 탐지 방법과 성능 비교분석을 하며 마지막으로 향후 연구되어야 할 부분에 대한 언급과 본 논문의 결론을 맺는다.

2. Denial of Service Attack

전형적인 침입유형 가운데 가장 보편화된 서비스거부공격은 멀티프로세싱을 지원하는 운영체제에서 발생할 수 있는 공격방법으로서 구체적으로 한 프로세서가 시스템의 자원을 독점하거나, 모두 사용해 버리거나 또는 파괴하여서 그 시스템이 다른 프로세서들에게 올바른 서비스를 제공하지 못하도록 하는 공격을 말한다. 그러므로 시스템의 정상적인 수행에 문제를 발생시키는 모든 행위들을 서비스 거부공격이라고 부를 수 있다. 서비스 거부공격의 특징으로는 루트권한을 획득하는 공격이 아니며, 데이터를 파괴, 변조 또는 훔쳐 가는 것을 목적으로 하는 공격이 아니다. 서비스 거부 공격은 또한 공격의 원인이나 침입자를 추적하기 힘들며 다른 공격을 위한 사전 침입시도인 것이다. 이 공격유형의 방법은 다양하며 그 중 가장 대표적인 공격은 패킷 수준의 공격이다. 여기에 사용되는 종류는 ICMP, SMTP, Finger, Syn Flood 등이 있다. 이 종류들의 유사점은 운영체제의 TCP/IP 모듈에 의해서 정상적으로 만들어져 보내지는 패킷들이 아니라 임의적인 조작에 의해서 만들어지거나 또는 서로 관련이 없는 패킷을 아주 작은 단위로 단편화(fragment)하여 이루어진다는 것이다. 본 연구에서는 이러한 패킷 수준의 공격 중 TCP Syn Flooding에 대하여 다룬다.

2.1 TCP Syn Flooding

TCP Syn Flooding 공격은 TCP의 취약점을 이용한 공격형태이다. 일반적으로 TCP는 신뢰성 및 연결 지향적 서비스이므로 서버와 클라이언트간에 연결 설정하는 '3-way Handshake'라는 정상적 연결 흐름이 이루어진다. 여기서 그림 1과 같이 클라이언트가 SYN_x를 요청하고 서버로부터 SYN_y와 ACK_{x+1}을 받은 후 ACK_{y+1}을 보내지 않으면 서버에서는 클라이언트로부터 응답이 올 것을 기대하고 반쯤 열린 'Half Open State'가 된다.

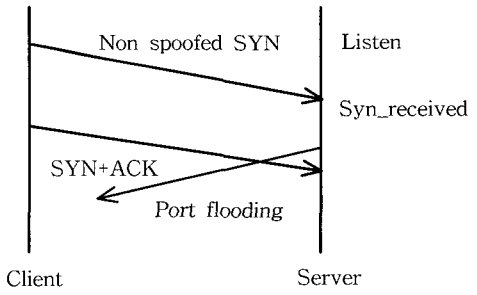


그림 1. Port Flooding 발생
Fig. 1. Port Flooding occurrence

물론 얼마간 이런 상태가 유지된 후 다음 요청이 오지 않으면 해당 연결을 리셋한다. 이때 리셋이 되기 전까지 메모리에는 그림 2와 같이 backlog queue가 계속 쌓이게 되는데 리셋이 되기 전에 지속적으로 이와 같은 요청이 아주 빠르게 이루어진다면 Syn Packet은 그림 3과 같이 backlog queue에 쌓이게 되어 결국 메모리 가용량(최대 연결 수)을 넘어서게 되고 마침내 해당 포드에 대한 연결을 받아들일 수 없는 서비스 거부 상태가 된다[7, 8, 9, 10, 11, 12].

실제로 TCP Syn Flooding 공격은 UDP Storm, Ping Flooding과 같은 다른 종류의 서비스 거부 공격과 같이 대량의 패킷을 보내지 않기에 공격이 노출되지 않는다. 또한 공

격자의 IP 주소를 임의의 주소로 만들어 보낼 수 있으므로 어디서 이러한 패킷이 오는지를 알아내기 매우 어렵다. backlog queue의 일반적인 가용량은 5~10정도의 연결 대기 상태가 가능하지만 실제 가용량은 운영체제에 따라서 또는 운영체제의 버전에 따라서 조금씩 차이가 있다.

그림 2, 그림3은 backlog queue가 쌓이면서 TCP Syn Flooding 공격이 일어나는 과정을 나타낸다.

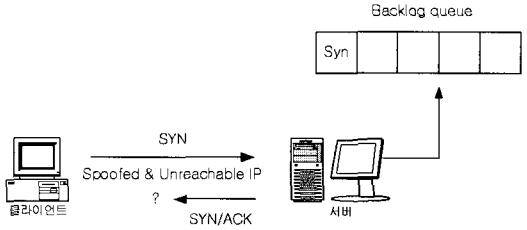


그림 2. TCP Syn Flooding 1 단계
Fig. 2. 1st Step of TCP Syn Flooding

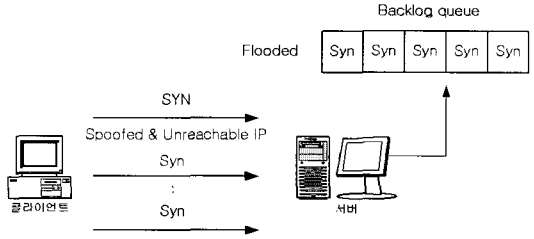


그림 3. TCP Syn Flooding 2 단계
Fig. 3. 2nd Step of TCP Syn Flooding

위의 그림에서 보듯이 Flooded 된 상태가 계속 지속되면 어떤 시스템도 생존할 가능성은 없다. Flooded 상태가 지속되지 않도록 하는 방법 또는 Flooded 되기 이전에 대처하는 방법 등이 필요하다.

2.2 Syn Flooding Attack에 대한 기존 방어

2.2.1 Backlog Queue 와 Half Open Time

실제 서비스 거부가 발생하는 원인은 backlog queue에 더 이상 받아들일 수 있는 조건이 되지 않기 때문이다. 따라서, 원천적으로 해결방안이라고는 할 수 없지만 공격에 대하여 어느 정도 경감시킬 수 있는 해결방안으로써 backlog queue 크기를 증가시켜주는 것과 half open 상태의 대기시간을 줄이는 방법을 적용할 수 있다. 그러나 H/W 및 OS마다 서로 다른 메모리 용량과 backlog queue 크기가 할당되어 있어 정확한 크기증가 선정이 어려워진다. 다음은 리눅스 시스템에서 설정한 예시이다[9].

```
# cat/proc/sys/net/ipv4/tcp_keepalive_time-->7200
# cat/proc/sys/net/ipv4/tcp_keepalive_probes-->9
# cat/proc/sys/net/ipv4/tcp_max_ka_probes-->5
```

위와 같이 설정을 하고 지속적인 공격 테스트를 해 본 결과 공격이 이루어지는 순간동안 아주 짧은 순간이나마 시스템이 다운되는 현상이 주기적 반복형태를 띄고 있는 결과를 나타내었다. 그리하여 추가적인 해결을 위하여 다음과 같이 추가조치를 하였다. 바로, tcp_max_syn_backlog와 syncookies의 수치를 조절하는 것으로서 tcp_max_syn_backlog의 기본값인 256을 1280으로 설정한다.

```
/sbin/sysctl -w net.ipv4.tcp_max_syn_backlog=1280
```

이는 socket queue의 크기를 높여주는 방법이다. 그러나, 이러한 대안은 지속적인 공격측면에서 볼 때 효율적이지 못하므로 적절한 대안이라 할 수 없지만 1차 방어측면에서 본다면 적절한 방어대안이라 할 수 있다.

2.2.2 Syncookies

syncookies에는 크게 Berkeley, Linux, Reset cookie가 있으며 '3-way handshake'에서 TCP 헤더의 Syn's sequence number, 소스 및 목적주소에 단방향 해쉬함수를 적용한 암호화 알고리즘을 이용한 방식으로 연결 설정이 정상적으로 이루어지지 않으면 더 이상 소스 경로를 따라 가지 않고 정상적 연결 요청에 대해서만 연결 설정을 하여 자원의 낭비를 줄이는 방법이다[8].

아래는 리눅스 시스템에서 공격 테스트를 위한 syncookies 설정 값으로써 공격시 시스템다운 현상을 어느 정도 차단하는 효과를 볼 수 있다.

```
/sbin/sysctl -w net.ipv4.tcp_syn_cookies=1
```

2.2.3 Packet Monitoring

라우터 및 게이트웨이를 통과한 후 시스템 접근에 앞서서 모니터링을 하는 방법으로써 들어오는 패킷을 잡아 분석하여 'half open state'를 요청하는 포트 및 IP address를 탐지하여 RST 등으로 연결 해제하는 방법이다. 본 논문에서는 제안하는 모니터링을 통한 탐지 또한 이 범주에 속한다. 이외에도 게이트웨이 또는 라우터를 수정하는 방법이 있다. 이는 기존의 방화벽에 새로운 기능을 추가한 것으로 Semi-transparent Router가 이에 해당한다. 그림 4와 같이 연결 설정 과정에 게이트웨이와 라우터가 중간 연결을 제어하는 방법으로 세부적으로는 임의의 라우팅 테이블을 변경하여 트래픽이 전달되지 못하도록 ICMP redirects를 허용하지 않는 방법과 IP source 라우팅을 사용하여 목적지의 경로를 지정하여 믿을 수 있는 IP address로 위장하지 못하도록 하는 source 라우팅 패킷 허용 불능법 등이 있다[9, 11].

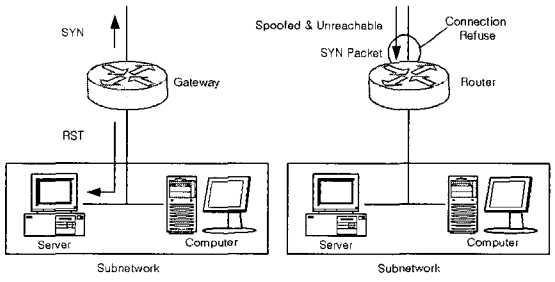


그림 4. Semi-transparent 라우터
Fig. 4. Semi-transparent Router

3. SPuF 탐지 모델

3.1 KDD'99 데이터

SPuF(Syn flooding Preventer using FCM)는 네트워크 기반의 탐지 방법을 사용하므로 분석 대상이 되는 네트워크 데이터가 필요하다. 공격자의 네트워크 행위는 패킷들로 나타난다. 패킷을 구성하는 데이터를 분석하고 어떤 데이터들의 속성이 TCP Syn Flooding 공격에 사용될 수 있는지 결정할 필요가 있다. 패킷 데이터 분석을 통해 SPuF에 이용될 속성들을 결정한다. 사용될 패킷의 종류는 TCP 패킷으로 1999년 KDD'99 Competition : Knowledge Discovery Contest에서 제공된 것을 활용한다. 침입과 정상데이터로 Label되어 있는 데이터를 Training Data로 사용하고 Label이 없는 데이터를 Test Data로 사용한다[9]. Training Data는 크게 DoS, R2L, U2R, Probing 4개의 공격 유형으로 구분된다. 본 실험은 네트워크 기반 탐지 기법이므로 Training Data 중에서 R2L, U2R은 호스트 기반 탐지기법이므로 제외하며, DoS와 Probing에 대하여 수행한다.

KDD Data에서 데이터의 속성들은 서비스 거부 공격 유형에 대하여 분석하고 속성간의 연관성과 순차적인 의미를 찾아 기본속성, 시간 기반 트래픽 속성, 호스트 기반 트래픽 속성을 기반으로 탐지 형태를 구성한다[13]. 이러한 탐지 형태를 기반으로 규칙을 학습하고 생성하여, 네트워크 연결 패킷에서의 서비스 거부 공격 중 TCP Syn Flooding 공격을 탐지한다. 이러한 공격을 탐지하기 위하여 표 2와 같이 비정상적인 IP 패킷 특성 및 유사 특성을 기반으로 하는 탐지 모듈을 설계한다.

표 2. 비정상 패킷
Table 2. Abnormal Packets

종류	비정상적인 패킷 특성 및 유사 특성
IP Spoofing & Land	* 예약된 IP 주소로 지정된 경우 * 출발지 IP 주소 = 목적지 IP 주소 경우 * Incoming IP 주소 : 내부 IP 주소 패킷일 경우 * Outgoing IP 주소 : 외부 IP 주소 패킷일 경우
Flag	* SYN FIN 동시 수행된 경우 * SYN FIN [PSH/RST/RSTPSH] 동시 수행된 경우 * FIN 만 수행된 경우(Port Scan 해당) * Null 패킷인 경우
Reserved	* 예약 필드가 설정된 경우
Port Number	* 출발지/목적지 Port Number = 0 인 경우
ACK	* ACK 설정 = 0 인 경우
Target IP Address	* Broadcast Address(xxx.xxx.xxx.255) 인 경우
Sequence Number	* 순차적에서 갑자기 비순차적일 경우
Netstat Command	* SYN_RECV의 발생 빈도가 높은 경우

TCP Syn Flooding 공격은 비정상 패킷을 이용한 공격형태이다. 그러므로, 비정상패킷을 탐지하는 것은 바로 TCP Syn Flooding 공격을 탐지하는 것이다. 결과적으로 네트워크 기반의 침입 탐지 시스템에서는 패킷을 분석하기 위한 전처리 단계로써 패킷 모니터링이 상당히 중요한 부분을 차지하게 된다. 여기서 간과해서는 안되는 점은 패킷 모니터링에서 패킷 캡쳐기능의 효율정도에 따라 탐지 효율도 함께 비례한다는 점이다. 기존의 침입 탐지 시스템에서는 싱글 시스템에서 패킷 캡쳐 기능과 탐지 기능을 동시에 수행하는 관계로 하드웨어의 리소스를 충분히 고려하지 않아 패킷 캡쳐를 놓치는 경우가 발생한다. 본 실험에서는 이러한 점을 보완하기 위하여 하드웨어장치로써 프로토콜 분석기를 두어 패킷 캡쳐 효율을 높인다.

3.2 SPuF 탐지 알고리즘

네트워크의 모든 트래픽은 정상 패킷(Normal Packet)과 비정상패킷(Syn Packet)으로 구분된다. 네트워크 상의 모든 패킷은 Time, Source IP, Source Port, Destination IP, Destination Port, Flag, Sequence Number, Window size 등으로 구성된다. 각 패킷을 p 라고 정의하고 패킷들이 합한 네트워크 트래픽을 T 라고 정의하면 패킷과 트래픽은 아래의 식과 같이 표현된다[14, 15].

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

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

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

; T_norm : 정상 트래픽, T_syn : 비정상 트래픽(Syn packet)

$$DETECT : T \rightarrow D \quad (4)$$

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

; P : 침입 결정, N : 정상 결정, D : 판단 결정

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

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

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

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

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

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

이러한 네트워크의 패킷 수준의 알고리즘을 비정상 패킷의 특성을 나타내는 표 2와 비교, 판단하여 1차 Syn Flooding 공격임을 탐지하여 연결 상태가 Half-open state인지를 판단한다. 이 방법은 정상패킷과 Syn 패킷을 탐지하는 기존의 침입 탐지 시스템과 똑같은 효과를 낸다. 그러나,

표 3. SPuF 위험도 형태
Table 3. Vulnerability Type of SPuF

그룹	분류 형태	설 명
high (대응영역)	attack_event_rate	탐지 이벤트 수에 대한 실제 공격 비율이 40%이상인 경우
	new_vulnerabilities	새로운 취약점을 이용한 경우
	60% < mem_cpu_cap	메모리/CPU가용률이 전체 리소스 60%이상를 점유
medium (경고영역)	dst_port_list	동일 Destination port 목록
	dst_ip_list	동일 Destination IP 목록
	40%< mem_cpu_cap < 60%	메모리/CPU가용률이 전체 리소스 40%이상, 60%이하 점유
low (경계영역)	src_port_list	공격자의 동일 Port 목록
	src_ip_list	공격자의 동일 Source IP 목록
	mem_cpu_cap < 40%	메모리/CPU가용률이 전체 리소스 40%이하를 점유
	network_scan	네트워크 스캔 탐지

이러한 방법에 의한 탐지에는 한계점이 있다. 일반적으로 침입자는 침입 대상이 되는 네트워크의 정보를 알아내기 위한 목적으로 침입 시도를 한다. 그러나, 단순한 스캔 같은 공격을 침입시도라고 판단하여 그때마다 시스템 관리자에게 경보를 알리게 되면 실제 네트워크 모니터링에서는 계속된 경고음이 발생한다. 그러므로, 침입 판정에 있어서 시스템에 위험도를 주는 공격 위험도 측정이 필요하다. 일반적으로 공격 위험도 측정은 시스템의 취약성 위험도에 따라 측정되며 본 논문에서는 시스템 보안 취약성 맵(Security Vulnerability Map : SVM)을 사용한다. SPuF에서 위험도 평가 방법은 시그니쳐를 위험도별로 그룹화하는 방법으로 이는 퍼지인식도에 의하여 각각의 이벤트 항목에서 다음 항목에 영향을 주는 가중치를 부여하며 표 3과 같이 세 그룹으로 나누어 구분한다.

3.3 SPuF 탐지 모델 구조

본 논문에서 제안하는 네트워크 기반의 침입 탐지 및 감시 도구의 전체적인 구조는 그림 5와 같다.

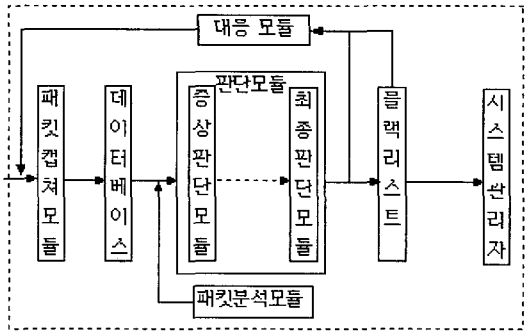


그림 5. 침입탐지 모델 구조
Fig. 5. Architecture of Intrusion Detection Model

각 모듈로 구성된 탐지 모델의 전체 구조는 들어오는 패킷을 이용하여 패킷을 분석하고 제어하는 모듈과 데이터를 저장하고 Half-open 상태를 판단하는 판단모듈로 되어 있으며 추가로 대응모듈이 있다. 여기서 패킷캡쳐모듈은 promiscuous mode에서 데이터 링크층의 패킷을 캡쳐하며 이를 프로토콜별 패킷을 받아서 세션별로 저장한다. 여기서 세션이란 Source IP와 Destination IP 그리고 프로토콜 종류가 같은 세션들끼리 모아서 데이터저장 테이블에 저장하는 동시에 패킷들을 판단모듈로 보낸다. 패킷은 파싱(Parsing)되어 여러 항목들로 저장되고 패킷분석모듈을 통하여 Syn 패킷과 정상패킷으로 구분하여 1차 Half-open 상태를 탐지한다. 탐지된 IP 주소는 퍼지인식도를 활용한 최종판단 모듈을 통하여 결정되며 침입으로 판정된 후, 블랙리스트 dBase에 저장되고 시스템관리자에게 통보된다. 이러한 일련의 과정을 통하여 재차 공격 시에는 블랙리스트 dBase와 각 패킷의 구성요소 항목 비교 알고리즘을 통하여 공격을 탐지하고 대응모듈을 가동하게 된다. 그림 6은 감사 기록 규칙에 의하여 True Negative(Syn Flooding 공격)으로 판정되는 과정을 나타낸다.

패킷캡쳐모듈은 Detector4win ver 1.2 모니터링 프로그램에 해당된다. 실시간 캡쳐와 동시에 데이터링크계층과 네트워크계층 그리고 전송계층 등을 파싱(Parsing)하는 패킷 필터링 과정에서 정상패킷과 비정상패킷으로 구분하기 위한 특성 항목에 맞게 저장한 후 패킷 분석 모듈에서 audit record rule에 의하여 True Positive가 결정되며 그림 7에서 □으로 표시한 부분과 같이 Half-open 상태로 나타난다.

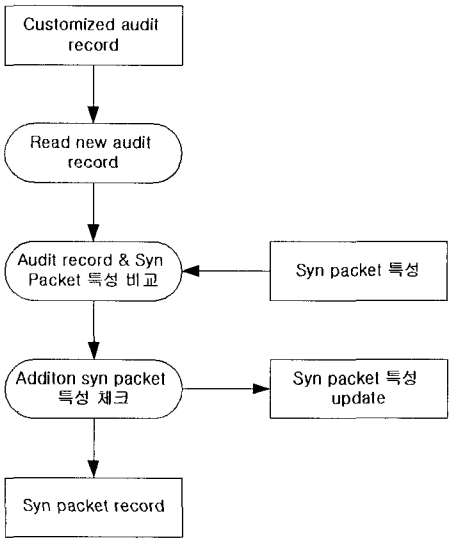


그림 6. 감사 기록 규칙의 흐름도
Fig. 6. Flowchart of Audit Record Rule

SYN과 RST는 연결제어와 관련된 TCP 헤더의 Flag부분으로, 각각의 수치가 0 -> 1 또는 1 -> 0으로 변경된 영역은 '3-way handshake'에서 3번째 연결설정부분을 수행하지 않은 경우에 해당되어 Half-open 상태가 된 경우이다. 또한, TCP의 순서적 전달인 Sequence Number가 비순서적으로 도착한다. 이는 외부의 비정상적인 연결설정을 의미한다. 아울러, 흐름제어영역인 Window 크기가 순간적으로 변경된다. 이 역시 Half-open 상태에 나타나는 특징들 중 하나이다.

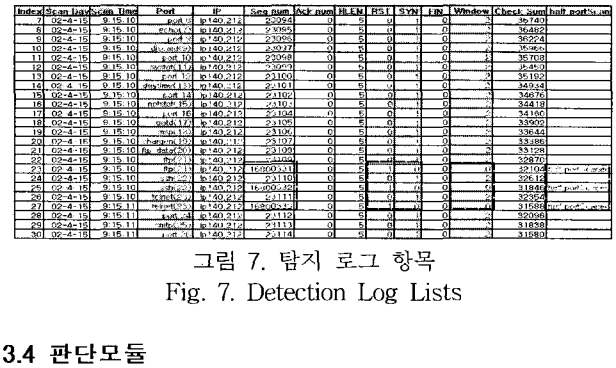
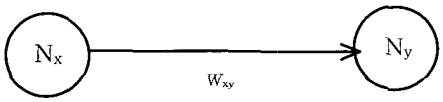


그림 7. 탐지 로그 항목
Fig. 7. Detection Log Lists

3.4 판단모듈

판단 모듈은 퍼지 인식도(FCM)의 Causal knowledge reason을 이용하여 지능적 판단모듈구조를 설계하였다. FCM은 주어진 문제영역내의 각 개념들 사이에 존재하는 인과관계(Cause-effect relationship)를 나타내는 유향성 그래프(Directed graph)이다. 그림 8는 퍼지 인식도를 표현한 것으로써 각 노드와 노드사이의 가중치(링크)가 W_{xy}=0인 경우에는 각 노드사이에는 아무런 관련이 없는 것을 의미하며 $W_{xy}\neq 0$ 경우에는 그림 8와 같은 의미를 부여한다. 단순한 FCM에서는 인과관계 값을 {-1, 0, 1}로 취할 수 있다. 따라서 이경우의 인과관계는 최대 또는 최소의 정도로 발생한 것을 의미한다.



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

그림 8. 퍼지인식도
Fig. 8. Fuzzy Cognitive Maps

판단모듈에서 여러 가변 요소 중 어떤 요소에 의존성을 부여함으로써 가장 최적의 탐지를 할 수 있는 것이 가장 큰 관건이다. 그뿐만 아니라 탐지한 IP address를 침입시도로 간주하고 블랙리스트 DB에 저장하여야 하는지도 결정하여야 한다. 퍼지인식도는 이러한 여러 가변 요소를 적용하여 최적의 판단을 내리게 한다[11, 15].

그림 9은 가변요소를 적용한 판단모듈의 퍼지인식도를 나타낸 것으로써, 판단모듈에 의존성을 갖는 가변요소로 IP address의 동일성 여부와 Half-open 상태의 시간간격 그리고 각 프로세서의 CPU가용율과 메모리가용율 및 판단모듈 후 재차 공격시 대응모듈의 처리로 인한 공격성 IP address에 대한 syn 패킷 조절을 둘 수 있다.

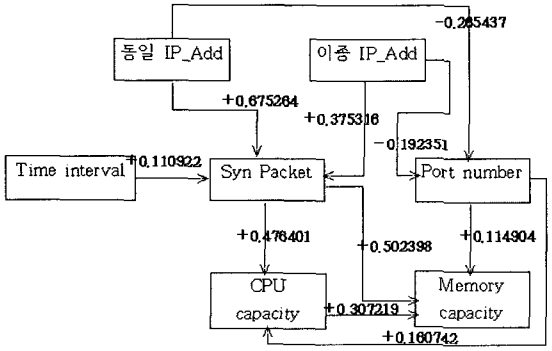


그림 9. 퍼지인식도가 적용된 판단모듈
Fig. 9. Decision Module Using FCM

가변요소를 노드(N_x)와 다음 노드(N_y)에 두고 두 노드의 링크인 가중치(W_{xy})를 적용하는 것이다. 예를 들면, Syn Packet과 CPU가용율에서는 Syn Packet의 용량이 증가할수록 CPU가용율이 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.

$$N_k(t_{n+1}) = \sum_{i=1}^{n} W_{ik}(t_n) N_i(t_n) \tag{8}$$

단, 가중치(Wxy)의 증감부호는 다음 노드에 미치는 영향에 따라서 결정을 내렸으며 수치는 규칙기반에 의한 통계적 누적수치를 정하기 위해 Quantitative Micro Software Ltd. 의 Eview ver 3.1을 이용하여 경로분석의 효과계수를 SPuF의 가중치로 사용하였다.

3.5 대응모듈

대응모듈은 그림 10과 같이 과거의 Unreachable한 패킷의 데이터를 저장하여 임의의 패킷과 비교해서 동일여부에 따라서 접근을 통제하는 방법으로 네트워크의 접근통제를 기본으로 하였으며 제안하는 모듈은 공격자 접근통제 알고리즘을 이용한다[12].

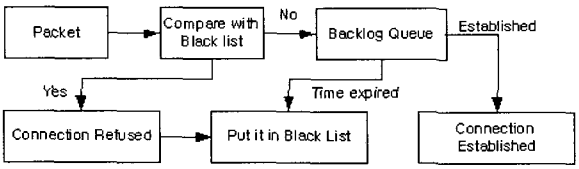


그림 10. 대응 모듈 흐름도
Fig. 10. Flowchart of Defense Module

사용자의 접근통제 정보로는 데이터링크 계층에서의 Source MAC Address와 Destination MAC Address, 네트워크 계층에서는 TTL(Time to Live) 정보와 Source IP address, Destination IP address 그리고 전송 계층에서는 TCP Source Port와 TCP Destination Port가 필요하다.

3.6 성능 평가

SPuF의 DoS 및 Probing의 탐지율은 표 2를 기반으로 하는 SPuF 흐름도에서 1차 탐지된다. 그림 11은 SPuF의 최적 탐지율 및 오경보율이다. 여기서 계수는 패킷수가 아니고 connection records로 계산한다.

그림 11은 2주 동안의 2백만 이상의 connection records 중에서 서비스 거부 공격의 connection records에 대하여 모

	A	B	C	D	E	F	G	H	I
1	week_day	n(T_p)	n(F_p)	n(F_n)	n(T_n)	Rate(T_p)	Rate(F_p)	Rate(F_n)	Rate(T_n)
2	1_1	284	0	13	93,948	95.623%	0.000%	4.377%	100.000%
3	1_2	152	0	21	70,482	87.861%	0.000%	12.139%	100.000%
4	1_3	197	0	8	90,811	96.098%	0.000%	3.902%	100.000%
5	1_4	231	0	1	85,569	99.569%	0.000%	0.431%	100.000%
6	1_5	93	0	0	54,721	100.000%	0.000%	0.000%	100.000%
7	2_1	185	0	2	53,092	98.930%	0.000%	1.070%	100.000%
8	2_2	341	0	0	2,829	100.000%	0.000%	0.000%	100.000%
9	2_3	164	0	23	9,547	87.701%	0.000%	12.299%	100.000%
10	2_4	531	0	0	85,782	100.000%	0.000%	0.000%	100.000%
11	2_5	235	0	5	51,091	97.917%	0.000%	2.083%	100.000%
12	SUM	2413	0	73	597,372	97.064%	0.000%	2.936%	100.000%

그림 11. 최적 탐지율과 오경보율
Fig. 11. The Best Detection Rates & Error Rates

의 실험한 결과이다. 여기서, Rate(T_p)가 97.064%로 나온 것은 KDD'99 CUP 99년도 우승자인 Dr. Bernhard의 Winning Rate(T_p)가 97.1%인 것과 비교하면 모의 실험의 탐지 성능도 우수함을 입증한다. 아울러, Rate(F_p)가 0%의 의미는 Test Data 중에서 DoS와 Probing 공격에 대한 connection records의 세부유형을 포함하는 SVM을 근거로 하는 SPuF의 실시간 업데이트 규칙기반 탐지에 의한 제한적 상황에서 모의 실험한 결과이다. Rate(F_n)이 2.936%는 MIT Lincoln Labs에서 공격리스트(Syn list)에 입력하지 않은 것을 탐지한 것으로, 정상 패킷을 침입으로 잘못 오경보한 것(False Negative)은 아니며 이를 확인하기 위하여 tcpdump에서 직접 Test Data의 connection records를 살펴본 결과, MIT Lincoln Labs에서 공격 리스트에 입력을 하지 않은 비정상 패킷이였다.

하드웨어 리소스 가용율 측면에서 테스트를 한 결과, 공격횟수 0~70,000번으로 공격이 증가할수록 하드웨어가용율(CPU와 메모리)이 최종적으로 시스템부하로 적용되며 시스템부하율의 변화추이로 최대침입시도 공격시 시스템 위험도를 확인할 수 있게 된다.

그림 12에서 침입시도 공격시 하드웨어 가용율의 임계값 및 침입시도 판단 및 결정하는 데드라인으로 40% 가용율영역대를 설정하고 60% 가용율영역대를 시스템관리자에게 통보하는 임계값으로 설정한다. 이는 실시간 대응처리를 고려한 수치와 시험망이 아닌 네트워크에서 분산 서비스 거부공격(DDoS)을 위해 감안한 수치이며 반복적 테스트에 의한 평균값을 적용하였다[11].

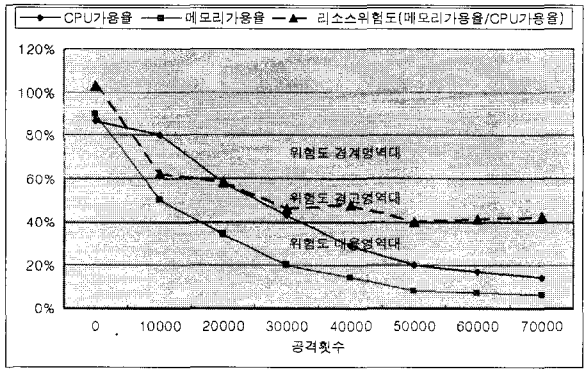


그림 12. 시험망에서의 공격횟수에 대한 하드웨어 가용율
Fig. 12. Attack Numbers vs. Hardware Capacity on Testbed Network

그림 13에서 공격횟수가 40,000번 이상인 경우 시스템의 부하율이 50% 이하로 떨어진다. 그러나 실제 네트워크에서는 그림 14에 나타나듯이 테스트결과보다 더 낮은 공격횟수에서 발생하며, 초당 21,000번 이상으로 interval을 불규칙적으로 발생한 경우 시스템 부하율이 50%보다 낮은 수치를 보인다. 이런 결과는 실제 네트워크에서 발생할 수 있는 여러 가능 요소인 트래픽(UDP Syn flooding 공격 제외), 전파지연시간 그리고 hop count를 무한루프로 돌리는 비정상 분할된 정상패킷 등에 대한 고려사항을 감안하지 않은 결과이다[15].

실제 네트워크상의 테스트는 2002년 9월, 12월 그리고 2003년 2월에 매월 3주 동안의 결과를 평균하여 표시하고 100Mbps 카테고리 5의 이더넷환경에서의 인텔 펜티엄4 2GHz, DDR 512M 시스템과 Cisco 라우터 1750시리즈, RADcom Ltd.의 RC-88WL High-performance WAN/LAN 프로토콜 분석기에서 측정하였다.

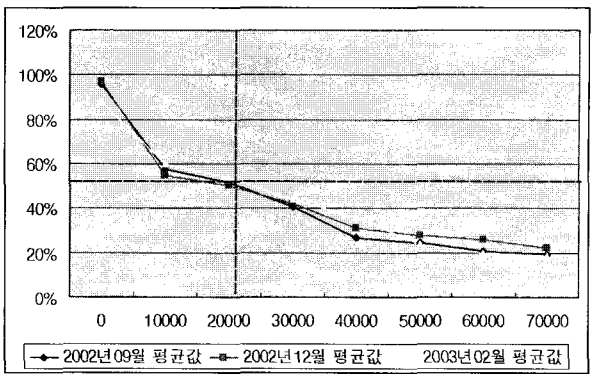


그림 13. 실시간 네트워크에서의 공격횟수에 대한 하드웨어 가용율
Fig. 13. Attack Number vs. Hardware Capacity on Real Time Network

4. 결 론

본 논문에서는 현재 침입탐지시스템에서 침입으로 판단된 데이터에서 False Positive Error와 False Negative Error와 같은 오경보율을 감소시키는 SPuF 모델을 제안하였다. SPuF 모델은 데이터링크계층의 패킷을 캡쳐 및 분석하여 침입시도탐지기능을 수행하는 네트워크 기반 침입시도탐지 모델이다. 이 모델의 가장 큰 특징은 탐지성능을 좌우하는 요소들간의 상호 관계로부터 퍼지인식도를 이용한 침입시도 여부를 판단한다는 것이며 이때, 퍼지인식도에서 가장 중요한 가중치를 결정하는 수치는 경로분석을 통한 방법론을 취하여 실험하였다.

침입시도 여부를 판단하는 하드웨어 가용용량 구역대를 정확히 선정하기 위하여 실시간 처리 가능한 데드라인 시간과 초당 발생하는 Flow 임계값을 설정하여 침입여부를 결정하는 방법에선 3단계의 SVM 시스템 취약성 위험도를 고려하는 방법을 취하였다. KDD'99 Data Set으로 실험한 결과, 해킹 침입시도 탐지 성공률이 97% 이상 되었다. 특히, 퍼지인식도를 이용하여 현재까지 알려지지 않은 새로운 해킹 기법을 포함하는 기존의 비정상 패킷에 대하여 실제 시스템의 리소스 가용율에 끼치지 않는 패킷들로 처리함으로써 False Positive Error를 감소시킬 수 있었다.

본 논문에서 제안한 FCM를 적용한 탐지 기법은 현재로는 서비스 거부 공격에만 적용된 단계이다. 이 기법을 더 세분화하여 분리 가능한 모듈로 구성하여 기존의 어떠한 침입 탐지 시스템 또는 침입 시도 탐지 시스템에 적용이 가능하도록 하고 대응모듈을 더욱 강화한 침입 방지 시스템으로 개발, 보완 발전시키는 것이 향후의 과제이다.

참 고 문 헌

[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 system 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] 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] Computer Emergency Response Team, "TCP Syn Flooding and IP Spoofing Attacks," CERT Advisory: CA, 96-121, 1996.
[8] Syncookies mailing list.
ftp://koobera.math.uic.edu/pub/docs/syncookies-archive, 1996.
[9] S. Y. Lee and Y. S. Kim, "A RTSD Mechanism for Detection of DoS Attack on TCP Network," Proceedings of KFIS 2002 Spring Conference, pp. 252-255, 2002.
[10] Amang Garg and A. L. Narasimha Reddy, "Policy Based end Server Resource Regulation," IEEE/ACM Transactions on Networking , Vol. 8, No.2, pp. 146-157, 2000.
[11] K. B. Sim , J. W. Yang, D. W. Lee, S. Y. Lee, Y. S. Kim, et al., "Intrusion Detection System of Network Based on Biological Immune System," Journal of Fuzzy Logic And Intelligent Systems, Vol. 12, No. 5, pp. 411-416, 2002.
[12] E. J. Lee. " A Study on Intrusion Detection System through Network," Master Thesis, Inchon University, pp. 56-60, 2001.
[13] W. Lee and 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.
[14] S. J. Park, "A Probe Detection Model using the Analysis of the Session Patterns on the Internet Service", Ph. D. Dissertation, Daejeon University, 2003.
[15] S. Y. Lee, "An Adaptive Probe Detection Model using Fuzzy Cognitive Maps", Ph. D. Dissertation, Daejeon University, 2003.

저 자 소 개

이세열(Se-Yul Lee)
1996년 : 대전대학교 전자물리학과 이학사
1999년 : 동 대학원 정보통신공학과 공학석사
2000년 : (주)인소팩 부설기술연구소 연구원
2003년 : 동 대학원 컴퓨터공학과 공학박사

관심분야 : 침입탐지, 정보보호, 네트워크 보안, 퍼지 논리 등
Phone : +82-42-280-2540
Fax : +82-42-284-0109
E-mail : ailab@dju.ac.kr

김용수(Yong-Soo Kim)
1981년 : 연세대학교 전기공학과 공학사
1983년 : KAIST 전기 및 전자공학과 공학석사
1986년 : 삼성전자 종합연구소 주임연구원
1993년 : Texas Tech Univ. 공학박사
1995년~현재 : 대전대학교 컴퓨터공학부 부교수

관심분야 : 신경회로망, 퍼지 논리, 패턴인식, 영상처리, 침입탐지 등
Phone : +82-42-280-2547
Fax : +82-42-284-0109
E-mail : kystj@dju.ac.kr