情報保護學會論文誌
第11券 第5號, 2001. 10

신경회로망을 이용한 비정상적인 패킷탐지

이 장 헌*, 김 성 옥**

Detecting anomaly packet based on neural network

Jang-hun Lee*, Sung-Ok Kim**

요 약

21세기 정보화시대를 맞이하여 네트워크는 전산화의 기본적인 시설로 인식되고 있으나, 이러한 네트워크체계는 정보의 공유라는 본래의 취지에서 벗어나 자료의 불법 유출과 자료파괴의 도구로 사용될 수 있는 양면성을 지니고 있다.

최근에는 초보자들도 인터넷상에서 취약점 검색툴이나 여러 가지 해킹툴을 쉽게 구하고 사용할 수 있어 그 위협은 증대되고 있으며, 공격방법 또한 다양화 및 지능화 되고 있는 추세이다.

본 논문에서는 네트워크 공격을 위한 비정상적인 패킷을 탐지하는데 목적을 두고 있다. 이를 위해 네트워크 패킷을 수집하고 각 패킷의 확률특성을 이용하여 비정상적인 정도를 나타내주는 감사자료를 생성한 후 이를 신경회로망을 이용하여 침입여부를 판단한다.

ABSTRACT

As we live in the 21st century, so called the "Information Age", network has become a basic establishment. However, we have found the different face that it also has been used as a tool of a unauthorized outflow and destruction of information.

In recent years, beginner could easily get a hacking and weakness reference tools from internet. The menace of the situation has increased; the intellectual diverse offensive technique has become increasingly dangerous.

The purpose of the thesis is to detect a abnormal packet for networking offense. In order to detect the packet, it gathers the packets and create inspection information that tells abnormality by using probability of special quality, then decision of intrusion is made by using a neural network.

keyword : IDS, Neural Network

Ⅰ. 서 론

급속한 정보통신 기반구조의 확산에 따라, 정보화 서비스 또한 다양한 형태로 우리의 생활과 가까워지고 있다. 이러한 정보화의 발전이 진행될수록 그 역기능 또한 증가되어 정보보안에 대한 문제가 심각하게 대두되고 있다.

최근 세계 유명 사이트들이 연이어 침입을 당하여 많은 시스템 관리자들이 대응에 고심하고 있으며, 이제 해킹 문제는 사이버전쟁(Cyber War)이라는 표현까지 포함되면서 정보전의 심각한 문제로까지 진행되고 있는 것이 현실이다.

컴퓨터 보안은 차단(Prevention), 탐지(Detection), 대응(Response)의 3가지 형태가 필수적이다. 그러나, 지금까지의 보안의 개념은 외부 크래킹(Remote Attack)에 대한 방어의 개념의 차단에 중심을 두고 불균형적으로 운영되어 왔다. 이러한 보안기술의 불균형적인 발전에 비해 네트워크를 통한 외부 침입 가능성

* 한남대학교(jjangkma@skcc.com)
** 한남대학교(sokim@mail.hannam.ac.kr)

은 더욱 커졌고, 이로 인한 개인 및 기관의 정보유출 및 파괴의 위협이 가중되었다[1].

또한, 컴퓨터 시스템이나 전산망에 대한 공격은 더욱 기술적으로 발전하여 차단에 의한 접근 제어나 침입 차단시스템의 운영만으로는 다양한 보안 사양을 만족시키기 힘들게 되었다.

한국 정보보호진흥원의 01년도 7월 해킹사고 변화 [표 1]에 의하면 실질적인 통계가 이루어진 97년도부터 해킹사고가 매년 급격히 증가하고 있다는 것을 알 수 있다[2].

[표 1] 연도별 해킹사고 변화

년 도	96년	97년	98년	99년	00년	01년7월
해킹 사고	147	64	158	572	1,943	3,074
증가율 (%)	—	-44%	247%	362%	141%	272%

이러한 이유로, 침입을 즉각적으로 탐지하고, 대처하는 신기술을 채용해, 각종 침입행위를 능동적으로 탐지, 보고, 대응하는 보안 시스템인 침입탐지시스템의 필요성이 대두되었다. 침입탐지 시스템은 시스템과 네트워크를 감시해 이상한 사용자의 행동이나 네트워크 패킷 탐지를 수행하는 보안시스템이다.

본 논문은 신경회로망을 이용하여 비정상적인 네트워크 트래픽을 탐지할 수 있는 침입탐지시스템에 대한 연구를 중점으로 하고 있다. 정상적인 패킷에 대한 정보와 비정상적인 패킷의 정보로 신경회로망을 학습시켜서 탐지의 효율을 증대시키고 아울러 새로운 형태의 네트워크 공격에 대한 탐지능력을 가지도록 구성하였다.

신경회로망을 이용한 침입탐지시스템에 대한 연구는 1998년 James cannady가 발표한 "Artificial Neural Network for Misuse Detection"에서 발표된바 있으나, 그 적용방식이 침입탐지 시스템 분류 방법 중 오용탐지기법에 국한되어 본 논문과의 차이가 있으며, [표 2]와 같이 기존 신경회로망을 이용한 침입탐지기법에서는 단순히 패킷헤더의 정보를 입력 값으로 하고 있으나, 제안된 시스템에서는 패킷헤더의 확률적인 정보를 입력 값으로 하고 있다.

James cannady가 발표한 논문에 대해서 대략적으로 정리하면, 신경회로망의 입력부분이 패턴매칭의 침입탐지시스템에 입력부분으로 사용되는 패킷의 헤더정보(예, Protocol ID, Source Address/Port, Destination Address/Port, ICMP Type/Code등)를 직접 입력 값으로 사용하여 결과를 도출하였다. 이러한 방식을 사용했을 경우의 장점은 패턴매칭 시스템의 단점중의 하나인 Rule-Set의 유지관리를 쉽게 해주고, 보다 정확한 매칭방법을 제공한다는 것이다.

[표 2] 기존 신경회로망을 이용한 침입탐지시스템과 제안된 침입탐지시스템 비교

	기존의 시스템	제안된 시스템
방식	오용탐지방식	비정상탐지방식
입력	패킷헤더의 정보	패킷헤더의 확률적인 정보
신경회로망 구조	Feedforward	Feedforward

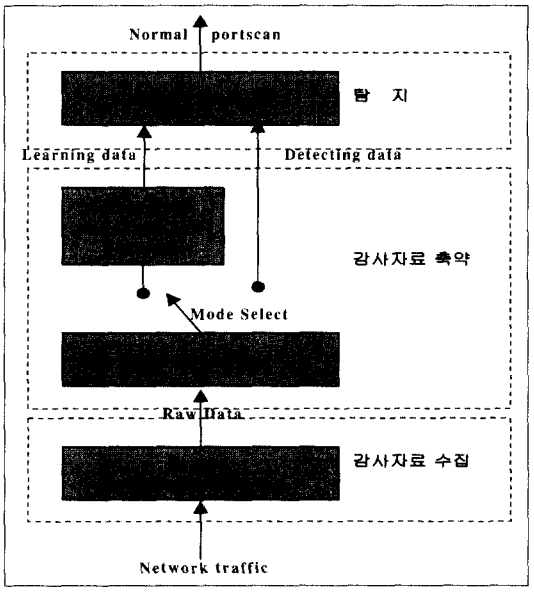
하지만, 신경회로망의 학습에 사용되는 데이터를 생성하기가 번거롭고, 구하기 힘들며, 변형된 공격형태의 경우 그 탐지의 성능을 보장받기 어렵다는 단점이 존재한다. 즉, 이러한 방식의 침입탐지시스템은 웹서버와 같이 사용자가 유동적인 환경에서는 효과적인 성능을 기대하기 어렵다.

따라서 본 논문에서는 패킷의 특성을 확률적인 값으로 도출하여 직접적인 패킷정보를 통한 판단을 피하여 위의 문제점을 해결할 수 있는 방법을 제시하였다. 두 시스템과의 직접적인 비교는 그 방식의 차이로 인해 힘들지만, 상호 보완적인 측면을 지니고 있으며, 향후 두 시스템의 적절한 보완으로 그 성능향상을 기대할 수 있다고 판단된다.

본 논문은 우선 제안된 침입탐지시스템의 구조와 각 기능을 제시하고, 시스템의 핵심이 되는 감사자료 축약부와 신경회로망을 이용한 탐지부에 사용된 알고리즘을 중점적으로 연구하였다. 또한 실제 운영중인 네트워크에 제안된 침입탐지시스템을 설치하여 다양한 형태의 portscan과 네트워크 공격에 대하여 그 성능을 확인하고 신경회로망을 이용한 비정상패킷 탐지 및 여러 형태의 침입에 대한 탐지 가능성을 제시한다.

II. 제안된 침입탐지시스템

본 연구에서 사용된 비정상패킷 탐지기의 구성은 [그림 1]과 같다. 시스템의 구성은 감사자료 수집부, 감사자료 축약부, 탐지부로 구성된다. 감사자료 수집부는 network card를 promiscuous mode로



〔그림 1〕 제안된 비정상 패킷 탐지기의 구성도

설정하여 network 패킷을 수집하는 역할을 담당하고, 감사자료 축약부에서는 수집된 network 패킷의 특징을 구성하여 이를 탐지부로 넘겨준다.

〔그림 1〕과 같이 탐지부에서는 축약부에서 만들어진 network 패킷의 특징 값을 이용하여 학습 모드일 경우, 신경회로망이 정상 패킷 및 비정상 패킷을 학습한 후, 탐지모드로 전환되어 패킷의 비정상 여부를 판단하게 된다.

2.1 감사자료 수집

대부분의 운영체제에서는 application을 위한 datalink 계층에 접근할 수 있는 방법을 제공한다. 트래픽 데이터는 네트워크 tap을 promiscuous모드로 설정함으로써 모두 수집될 수 있으며, 본 논문에서는 패킷의 헤더부분만을 필요로 함으로 패킷의 몇 바이트만을 지정하여 수집하면 된다. 패킷필터 중 대표적인 것이 NIT(Network Interface Tap)와 BPF(BSD packet Filter)이다.

현재까지 알려진 가장 강력한 패킷필터인 BPF는 buffer read, promiscuous network 접근, packet waiting test를 제공한다. 또한 스택 기반구조 보다 20배 빠른 register구조를 기반으로 필터를 사용하며 non-shared buffer 모델을 사용함으로써 Sun-OS의 NIT보다 우수한 성능을 제공한다[6].

본 논문에서는 사용자 수준에서 시스템에 상관없이 패킷수집을 할 수 있는 libpcap을 사용하여 패킷을 수집하였다. 이것은 네트워크 통계치 수집, 보안 모니터링 등 다양한 프로그램에 사용되었고, BPF를 사용하므로 그 성능면에서도 우수하다.

libpcap은 패킷을 Network interface로부터 캡처하여 사용자가 접근할 수 있는 사용자 메모리에 복사한 Callback함수를 메모리에 복사된 패킷에 수행하도록 한다.

2.2 감사자료 축약

본 연구에서는 특별히 발신지 IP, 수신지 IP, 수신지 port, 수신지 Flag에 초점을 맞추었다. 우선 여기에서는 발신지 IP, 수신지 IP, 수신지 port간의 확률 값을 통해 신경회로망의 입력요소 하나를 생성하도록 하겠다.

두 개의 서버와 클라이언트사이의 서비스는 발신지 IP, 수신지 IP, 발신지 port, 수신지 port를 기본으로 이루어진다. 이 중 수신지 port는 두 서버와 클라이언트사이의 서비스를 판단할 수 있는 서비스 port이나 발신지 port는 네트워크 프로토콜의 수행 메커니즘에 의거 난수로 순차적으로 변경되므로 port의 번호가 그 의미를 갖지 않는다.

따라서 우리는 발신지 IP, 수신지 IP, 수신지 port에 초점을 맞추어 우선 이 들간의 상관관계를 통계적 자료의 축약 방법인 확률을 이용해 특성화하여 감사데이터를 축약하고자 한다.

소규모 네트워크에서 15,000여 개의 네트워크 패킷을 추출하여 이 패킷의 헤더데이터를 가지고 발신지 IP, 수신지 IP, 수신지 port 데이터를 추출하여 이들을 각각 개별적인 사건으로 가정하고, 사건들의 연계성을 판단하여 보았다.

위의 확률에서의 세 가지 사건의 상호 연계성의 판단은 세 가지 이상의 사건들간의 독립을 판단하는 사상의 판별 정리 중 각각의 쌍별로 독립을 판별(Pairwise Independent)하는 정리를 적용하여, 다음과 같이 나타낼 수 있다.

정리1. $P(Src_{IP} \cap Dst_{IP}) = P(Src_{IP})P(Dst_{IP})$
정리2. $P(Src_{IP} \cap Dst_{Port}) = P(Src_{IP})P(Dst_{Port})$
정리3. $P(Dst_{IP} \cap Dst_{Port}) = P(Dst_{IP})P(Dst_{Port})$

이를 각각 구하여 성립여부를 통해 세 가지 헤더데이터의 상관관계를 특성화하고 이에 해당하는 확

률법칙을 적용하여 이들 데이터의 통계적 특징을 특성화하려 한다.

패킷의 발신지IP, 수신지IP, 수신지port들의 개별 발생확률과 각 사건간의 독립판별을 위해 동시 발생 확률에 대한 검증을 위의 세 정리에 맞추어 〔표 3〕, 〔표 4〕, 〔표 5〕와 같이 나타낼 수 있다.

우선, 정리1의 확률관계는 〔표 3〕을 통해 검증사실을 나타냈다. 패킷의 헤더 데이터 중 발신지 IP, 수신지 IP를 개별 사건으로 간주하고 이 들간의 독립성여부를 판단하기 위해 위의 정리1을 각 패킷의 로그데이터에 적용하여 보았다. 결과는 〔표 3〕과 같이 얻을 수 있었다.

정리2는 〔표 4〕를 통해 검증사실을 나타냈다. 패킷의 헤더 데이터 중 발신지 IP, 수신지 port를 개별 사건으로 간주하고, 이들간의 독립성 여부를 판단하기 위해 정리2를 각 패킷의 로그데이터에 적용

〔표 3〕 발신지 주소와 수신지 주소 사건의 상관관계 테이블

확률 / 패킷	$P(SRC_{IP})$	$P(DST_{IP})$	$P(SRC_{IP}) \times P(DST_{IP})$	$P(SRC_{IP} \cap DST_{IP})$
SRC_{IP1}, DST_{IP1}	0.64	0.53	0.3392	0.543
SRC_{IP2}, DST_{IP2}	0.22	0.3	0.066	0.221
SRC_{IP1}, DST_{IP3}	0.64	0.09	0.0576	0.009
SRC_{IP1}, DST_{IP4}	0.64	0.001	0.00064	0.001
SRC_{IP1}, DST_{IP5}	0.64	0.54	0.3456	0.543
			· · ·	
SRC_{IP1}, DST_{IP4}	0.64	0.001	0.00064	0.0013
SRC_{IP1}, DST_{IP4}	0.64	0.001	0.00064	0.0013
SRC_{IP1}, DST_{IP4}	0.64	0.001	0.00064	0.0013
SRC_{IP1}, DST_{IP5}	0.64	0.54	0.3456	0.543
SRC_{IP2}, DST_{IP2}	0.22	0.3	0.066	0.2216

〔표 4〕 발신지 IP와 수신지 포트 사건의 상관관계 테이블

확률 / 패킷	$P(SRC_{IP})$	$P(DST_{Port})$	$P(SRC_{IP}) \times P(DST_{Port})$	$P(SRC_{IP} \cap DST_{Port})$
SRC_{IP1}, DST_{PORT1}	0.64	0.005	0.0032	0.001
SRC_{IP2}, DST_{PORT2}	0.22	0.0003	0.00006	0.0003
SRC_{IP1}, DST_{PORT3}	0.64	0.09	0.0576	0.09
SRC_{IP1}, DST_{PORT4}	0.64	0.0016	0.001	0.0016
SRC_{IP1}, DST_{PORT4}	0.64	0.0016	0.001	0.0006
			· · ·	
SRC_{IP1}, DST_{PORT4}	0.64	0.0016	0.001	0.0016
SRC_{IP1}, DST_{PORT4}	0.64	0.0016	0.001	0.0016
SRC_{IP1}, DST_{PORT4}	0.64	0.0016	0.001	0.0016
SRC_{IP1}, DST_{PORT5}	0.64	0.0006	0.00038	0.0006
SRC_{IP2}, DST_{PORT6}	0.22	0.2216	0.0487	0.049

〔표 5〕 수신지 주소와 수신지 port 사건의 상관관계 테이블

확률 / 패킷	$P(SRC_{IP})$	$P(DST_{Port})$	$P(SRC_{IP}) \times P(DST_{Port})$	$P(SRC_{IP} \cap DST_{Port})$
DST_{IP1}, DST_{PORT1}	0.53	0.005	0.00265	0.001
DST_{IP2}, DST_{PORT2}	0.3	0.0003	0.00009	0.0003
DST_{IP3}, DST_{PORT3}	0.09	0.09	0.0081	0.09
DST_{IP4}, DST_{PORT4}	0.001	0.0016	0.0000016	0.0013
DST_{IP5}, DST_{PORT4}	0.54	0.0016	0.000864	0.0006
			· · ·	
DST_{IP4}, DST_{PORT4}	0.001	0.0016	0.0000016	0.0013
DST_{IP4}, DST_{PORT4}	0.001	0.0016	0.0000016	0.0013
DST_{IP4}, DST_{PORT4}	0.001	0.0016	0.0000016	0.0013
DST_{IP5}, DST_{PORT5}	0.54	0.0006	0.000864	0.0006
DST_{IP2}, DST_{PORT6}	0.3	0.2216	0.06648	0.2213

해 보았다. 결과는 〔표 4〕와 같이 얻을 수 있었다.

정리3 확율관계는 〔표 5〕를 통해 검증사실을 나타냈다. 패킷의 헤더 데이터중 발신지IP, 발신지 port를 개별 사건으로 간주하고 이들간의 독립성 여부를 판단하기 위해 정리3을 통해 검증사실을 나타냈다. 패킷의 헤더 데이터 중 발신지 IP, 발신지 port를 개별 사건으로 간주하고, 이들간의 독립성여부를 판단하기 위해 정리3을 각 패킷의 로그데이터에 적용하여 보았다. 결과 〔표 5〕와 같이 얻을 수 있었다.

위의 정리들을 통해 검증 한 결과 〔표 3〕, 〔표 4〕 〔표 5〕과 같은 결과를 얻을 수 있었다. 즉, 위의 표에 나타난 결과에서 보는 바와 같이 발신지 IP, 수신지 IP, 발신지 port 등 개별 사건사이에는 독립사상이 나타나지 않음을 알 수 있다. 즉, 세 가지 헤더 데이터는 연계성을 가지고 발생하는 사건으로 나타낼 수 있다. 따라서, 이 들간의 통계적 특성을 구하는 방법은 조건부 확률(Conditional probability)을 통해 구해질 수 있다.

따라서 이 들 사건이 이 모두 발생할 확률은

$$P(SRC_{IP}, DST_{IP}, DST_{Port}) = P(DST_{IP}, DST_{Port} | SRC_{IP}) \quad (1)$$

식 (1)로 구할 수 있다. 이러한 일반적인 확률적 접근을 통하여 패킷의 헤더데이터 간의 통계적 특성을 구하는 즉, 패킷의 헤더 데이터로 구성되는 감사자료를 헤더데이터의 각 요소간의 확률적 상관관계를 통해 이에 해당하는 확률법칙인 조건부 확률을 통해 특성화하여 축약할 수 있었다.[8]

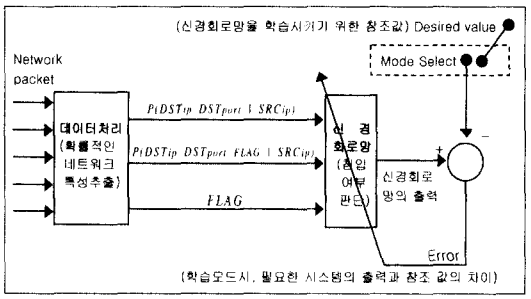
2.3 탐지

탐지부는 감사자료 축약부에서 만들어진 패킷의 특징자료를 통해 비정상 유무를 판단한다.

본 연구에서는 신경회로망을 사용하여 탐지부를 구성하였다. 감사자료 축약부에서 만들어진 데이터의 일부는 학습모드에 의해서 신경회로망의 학습에 사용되고, 학습이 완료된 후, 탐지모드부터는 실질적인 비정상 패킷을 판단할 때 사용된다.

신경회로망은 단순한 기능을 가진 많은 뉴런(neuron)들이 병렬 연결된 구조로 되어 있는데, 그 특징은 다음과 같다[10].

○ 각 뉴런은 다른 뉴런들과 독립된 기능을 갖는다.



〔그림 2〕 생성된 입력 값을 신경회로망 입력 후 학습과 탐지

즉 출력이 자신의 연결을 통하여 직접 전달되는 정보에만 의존한다. 따라서 병렬처리가 가능하다.

○ 뉴런들 사이의 연결이 매우 많다. 따라서 정보의 분산표현 및 처리가 가능하다. 또한 중복성(redundancy)이 커서 오류의 영향을 크게 받지 않으며, 연상 기억 특성을 갖는다.

○ 학습이나 훈련을 통해 연결강도(weight)를 조절함으로써 새로운 정보를 추가하거나 변경할 수 있는 적응 특성이 있다.

본 논문에서 신경회로망의 입력 값은 〔그림 2〕와 같으며, 비정상적인 패킷을 판별하는 과정을 정리하면 다음과 같다.

○ Network 패킷을 수집한다.

○ 수집된 패킷의 헤더정보를 바탕으로 이들 패킷사이의 특성을 확률적인 방법을 통해 구해낸다. 이렇게 구해진 데이터들은 네트워크의 특성을 확인할 수 있는데 도움을 준다.

○ 확률적인 방법으로 계산된 값을 신경회로망의 입력 값으로 사용한다.

○ 사용된 신경회로망은 감독학습법에 의해 연결강도가 갱신되므로, 학습모드와 탐지모드를 가지고 동작한다. 학습모드는 그림과 같이 신경회로망을 학습시키기 위해 참조 값이 존재한다. 이는 신경회로망의 연결강도를 결정하는 부분으로 실제 신경회로망의 출력과 참조 값의 차인 오차 값으로 연결강도를 오차역전파 알고리즘을 이용하여 갱신하게 된다.

○ 일정기간의 학습기간을 거치면 시스템은 실제적인 출력 값을 생성하는 탐지모드로 동작하게 된다. 시스템이 탐지모드로 동작하면 학습모드에서 사용하는 참조 값은 필요가 없어지며, 신경회로망의 연결강도의 갱신 없이 입력으로 들어오는

패킷의 확률적인 값을 이용하여 탐지결과를 생성한다.

2.3.1 탐지에 사용된 신경회로망

본 연구에서 사용된 신경회로망은 순방향 신경회로망(Feedforward Neural Network, FNN)을 사용하고 있다. [그림 3]는 탐지엔진을 사용된 순방향 신경망(FNN) 구조를 보여주고 있다. 이 구조는 3개의 층, 즉, 입력층(Input Layer), 히든층(Hidden Layer), 그리고 출력층(Output Layer)으로 구성되어 있으며 이를 각 각 i, j, k로 표기하고, 입력층과 히든층과의 연결강도(Weight)를 w_{ji}로, 히든층과 출력층간의 연결강도를 w_{kj}로 표기되어 있다.

연결강도는 오차 역전파 알고리즘(Error back-propagation algorithm)에 의해 오차가 최소가 되도록 갱신된다[11].

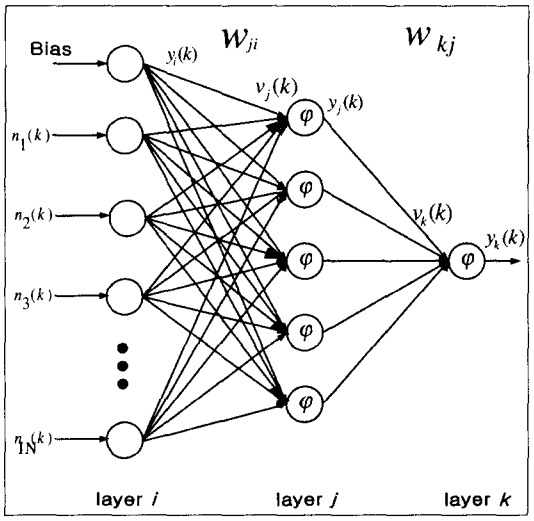
신경망의 입력층은 감사자료 축약부에 의해 생성된 패킷의 특징값 $n_i(k)$와 Bias로 구성된다.

$$y_i(k)=\begin{cases} Bias \\ n_i(k), \end{cases} \qquad i=1,2,3,\cdots,IN$$

여기서 IN은 입력층 뉴런수를 나타낸다.

히든층은 입력신호를 그대로 받아들이며 출력은 다음과 같다

$$y_j(k)=\varphi(v_j(k))=\frac{1}{1+e^{-s\cdot v_j(k)}} \tag{2}$$



[그림 3] 판단부에 사용된 신경회로망

$$v_j(k)=\sum_{i=1}^{L} w_{ji}(k)y_i(k) \tag{3}$$

$$L=BIAS+IN+HN$$

여기서, $v_j(k)$는 히든층의 입력으로 식(3)과 같고, $\varphi(\cdot)$는 비선형함수로 시그모이드(sigmoid)함수를 사용하였으며, s는 시그모이드 함수의 기울기이다.

시그모이드 함수는 다음과 같은 장점으로 인해 뉴런의 활성 함수로 많이 이용되는 함수이다.

- 역치함수와 선형함수의 특성을 모두 가지고 있다는 점이다. 시그모이드 함수의 기울기 s값과 BIAS값을 적절히 조절함으로써 역치 함수와 선형 함수의 특성을 얻어낼 수 있다.
- 시그모이드 함수가 비선형 함수라는 점이다. 다층 신경망이 가치를 가지기 위해서는 뉴런의 활성함수가 비선형일 필요가 있다.
- 시그모이드 함수가 미분 가능한 함수라는 점이다. 연결 가중치를 구하기 위해 필요한 델타는 활성 함수의 미분 과정을 필요로 하기 때문에 활성 함수로서 미분 가능한 함수만을 사용할 수 있다.
- 시그모이드 함수가 S형을 갖는다는 점이다. 시그모이드 함수는 그 함수 값의 범위가 0과 1사이이다. 이것은 아무리 큰 입력이나 작은 입력이 주어지더라도 항상 0과 1사이의 값을 나타낸다. 이것은 신경망의 어느 하나의 뉴런이 신경회로망의 전체 동작을 지배하게 되는 문제를 해결해 준다.

신경회로망의 최종 출력 및 내부상태는 식(4), (5)와 같이 나타난다.

$$y_k(k)=\varphi(v_k(k))=\frac{1}{1+e^{-s\cdot v_k(k)}} \tag{4}$$

$$v_k(k)=\sum_{j=1}^{HN} w_{kj}(k)y_j(k) \tag{5}$$

2.3.2 신경회로망의 학습법칙.

신경회로망에 학습의 종류는 기준에 따라서 여러 가지로 분류될 수 있다. 가장 일반적인 것으로는 감독학습(Supervised learning)과 무감독 학습(Unsupervised learning)이 있다.

감독학습은 학습 중에 주어진 입력에 대하여 올바른 출력이 어떤 것이어야 하는지를 제공해 주는 학습법이다. 즉 입력 패턴에 대한 신경회로망의 출력

패턴형태를 지시해 주는 목적 패턴을 갖는 것으로 입력 패턴과 목적패턴의 쌍들로 이루어진 학습 패턴이 사용된다.

본 논문에 사용한 신경회로망의 각각의 연결강도에 대한 학습법칙은 오차 역전파 학습 알고리즘을 사용하였다.

오차 역전파 알고리즘은 감독 학습 방법 중 델타 학습 법칙의 일종으로 볼 수 있는데, 델타 학습 법칙의 기본은 현재 주어진 연결 강도로 생성되는 오차 값을 구하여 이를 감소시키는 방향으로 연결 강도의 값을 조정하는 것으로 이때 오차 값의 계산을 위해 각 노드의 올바른 출력 값을 제공해 주어야 한다. 하지만 간단한 XOR 문제도 해결하지 못하는 단점을 지녔다. 따라서 오차 역전파 알고리즘은 이러한 문제를 해결하기 위한 방법의 일종으로 다층의 신경회로망을 학습시키는데 적합하도록 제안되었다. 오차 역전파 알고리즘은 일반화된 델타규칙(Generalized Delta Rule)이라고도 하며 1986년 룸멜하트(David E. Rumelhart)에 의해 만들어진 학습규칙으로 오늘날 가장 유명해진 신경회로망 학습규칙 중 하나이다.

오차 역전파 알고리즘의 학습 규칙은 만일 어떤 뉴런의 활성이 다른 뉴런에 의해 잘못된 출력에 영향을 주었다면 두 뉴런의 연결 가중치를 그것에 비례하여 조절해 주어야 한다는 것이다. 그리고 그러한 과정은 그 아래 단에 있는 뉴런들까지 계속된다.

오차함수 $J(k)$ 는 신경회로망의 출력 $y(k)$ 와 원하는 출력 $d(k)$ 차로 정의된다.

$$J(k)=\frac{1}{2}[e(k)]^2=\frac{1}{2}[d(k)-y(k)]^2 \quad (6)$$

오차함수크기를 최소화하는 연결강도 갱신은 오차함수를 각 층의 연결강도 w_{kj}에 대하여 편미분함으로서 구할 수 있다.

$$\frac{\partial J(k)}{\partial w_{kj}(k)}=\frac{\partial J(k)}{\partial y_k(k)}\cdot\frac{\partial y_k(k)}{\partial v_k(k)}\cdot\frac{\partial v_k(k)}{\partial w_{kj}(k)} \quad (7)$$

히든층과 입력층의 연결강도에 대한 오차함수의 편미분은 다음과 같다.

$$\frac{\partial J(k)}{\partial w_{ji}(k)}=\frac{\partial J(k)}{\partial y_k(k)}\cdot\frac{\partial y_k(k)}{\partial v_k(k)}\cdot\frac{\partial v_k(k)}{\partial y_j(k)}\cdot\frac{\partial y_j(k)}{\partial v_j(k)}\cdot\frac{\partial v_j(k)}{\partial w_{ji}(k)} \quad (8)$$

앞에서 정리한 식을 요약하면 신경회로망의 연결강도는 다음과 같이 갱신된다.

식 (9)는 출력층과 히든층의 연결강도에 대한 것이고, 식 (10)은 히든층과 입력층의 연결강도에 대한 것이다.

$$w_{kj}(k+1)=w_{kj}(k)-\eta\frac{\partial J(k)}{\partial w_{kj}(k)}+\alpha\triangle w_{kj}(k-1) \quad (9)$$

$$w_{ji}(k+1)=w_{ji}(k)-\eta\frac{\partial J(k)}{\partial w_{ji}(k)}+\alpha\triangle w_{ji}(k-1) \quad (10)$$

위 식에서 $w_{kj}(k)$, $w_{ji}(k)$는 현재의 연결강도이고, $w_{kj}(k+1)$, $w_{ji}(k+1)$은 갱신될 연결강도이다.

$\frac{\partial J(k)}{\partial w_{kj}(k)}$ 와 $\frac{\partial J(k)}{\partial w_{ji}(k)}$는 현재의 연결강도의 변화분을 의미하고, $\triangle w$는 연결강도의 이전 변화분을 의미한다. 그리고, η는 신경망의 학습률(learning rate), α는 모멘텀률(momentum rate)이다.

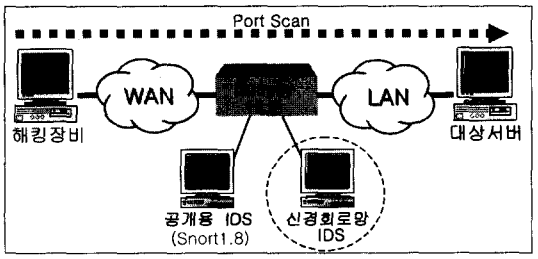
학습률은 시스템의 학습속도 및 수렴정도에 관계하는 인자로, 너무 큰값의 학습률은 알고리즘의 불안정을 야기할 수 있고, 너무 작은 값의 학습률은 수렴속도가 느려져서 많은 학습횟수를 필요로 하게된다.

모멘텀은 신경회로망의 연결강도 조절식에 관성을 줌으로써 학습 시간을 단축하고 학습 성능의 향상을 위해 고안된 것이다. 모멘텀은 현재의 연결강도와 그 이전 연결강도의 차이에 의해 계산된다. 따라서 모멘텀을 구하기 위해서는 이전의 연결강도를 저장하고 있어야 한다. 모멘텀은 연결강도 변화에 관성을 줌으로써 연결강도가 아주 얕은 지역의 극(local minima)에 빠지는 것을 어느 정도 해결해 줄 수 있으며, 신경회로망의 학습속도를 향상시킬 수 있다. 모멘텀률은 신경회로망의 학습률과 마찬가지로 적절히 속도 및 안정성의 조건에 따라 적당히 조절해 주어야 한다[12].

Ⅲ. 실험결과

[그림 4]는 본 논문에서 사용된 실험환경을 보여주고 있다. 여기서는 본 논문에서 사용된 신경회로망을 이용한 침입탐지시스템 외에 이의 성능을 검증하기 위해 공개용 침입탐지시스템인 Snort와 상용 침입탐지시스템인 Siren을 사용하였다.

먼저, 제안된 시스템의 탐지성능을 확인하기 위해 portscan을 하였다.



〔그림 4〕 논문에서 사용된 실험환경

Port scanner는 관리자나 침입자 모두에게 유용한 도구이다. 관리자의 측면에서는 관리 시스템의 보안 취약점을 확인할 수 있는 과정에서 사용되는 반면, 침입자의 경우 침입하려는 실질적인 침입 이전 사용할 수 있는 시스템의 취약지점을 찾을 때 사용된다. 여기서는 portscan은 후자의 악의적인 목적으로 사용되는 경우로 정의한다.

본 논문에서는 공격 호스트에서 NMAP을 이용하여 대상호스트로의 portscan공격에 대한 탐지성능을 실험하였다.

NMAP은 Fyodor에 의해 개발되고 유지되는 자유로운 배포가 가능한 Port scanner이다. 이것은 Linux, FreeBSD, Open BSD, Solaris 그리고 NT등의 다양한 운영체제에서 동작된다. NMAP은 인터넷에서 자유롭게 이용할 수 있는 가장 인기 있는 scanner이다[7].

이것은 여러 가지 방화벽이나 침입탐지시스템의 탐지를 피하기 위해 여러 가지 옵션을 가지고 동작한다.

〔표 6〕은 공격호스트에서 사용된 NMAP port scaner의 scan방식과 그에 따른 Flag특성, 그리고 이러한 패킷을 받은 대상호스트의 port상태에 따른 그 응답특성을 기술한 것이다.

TCP connect scan과 TCP half scan은 일반적으로 사용되는 scan방식으로 보통 이를 SYN-Flag scan이라고 한다. 이러한 형태의 패킷을 받은 대상호스트의 경우 RFC(Request for Comments)793에정의된 것과 같이 port가 열려 있으면 SYN/ACK로 응답하고, 닫힌 port의 경우 RST/ACK flag로 응답하게 된다. 따라서 공격자는 이러한 특징을 이용하여 대상 호스트가 열려있는지, 닫혀있는 지를 판단하게 된다.

또 다른 방식으로는 Non-SYN-Flag scan인데 이는 stealth, Xmas Tree, NULL scan으로 나누어진다. 이것 또한 〔표 6〕에 나타난 바와 같이 대상

〔표 6〕 공격호스트에서 사용된 NMAP portscaner의 scan방식과 대상호스트의 응답특성

방 식	Flag	열린 port	닫힌 port
TCP connect	SYN	SYN/ACK	RST/ACK
TCP half connect	SYN (then RST)	SYN/ACK	RST/ACK
stealth	FIN	-	RST/ACK
Xmas Tree	URG/PSH/ FIN	-	RST/ACK
NULL	No Flags	-	RST/ACK

호스트에서 열려진 port의 경우 그 패킷이 무시되고, 닫혀진 port에 대해서는 RST/ACK로 응답하게 된다[7].

3.1 SYN-scan에 대한 탐지

먼저 SYN-scan에 대한 제안된 침입탐지시스템의 탐지여부를 알아보았다.

데이터를 25,000개 단위로 수집하여 데이터 추출 방법에서 정의한 확률 값과 flag값을 생성하여 탐지부인신경회로망의 입력 값으로 전달한다.

먼저, 25,000개 중 10,000개의 패킷 특성 값을 학습모드에서 사용하였으며, 나머지 15,000개에 대해서 portscan 유·무를 판별하도록 하였다.

학습모드에서 사용된 데이터에서 사용된 패킷 특성 10,000개중 상용 및 공개용 침입탐지시스템에서 정상적인 패킷이라 판별된 것은 9,700 개이고, 나머지 300개는 portscan이라고 판별된 패킷이다.

신경회로망에서 사용된 입력층, 히든층, 출력층의 개수는 3×6×1을 이루며, 학습률 η는 0.3, 모멘텀률(momentum rate)을 α는 0.7을 사용하여 학습모드에서 학습을 수행하였다.

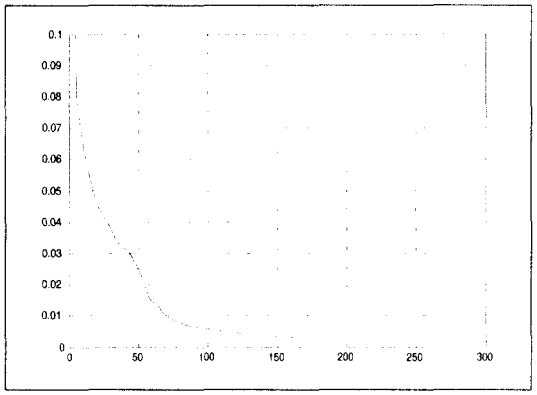
〔그림 5〕는 사용된 신경회로망에서 학습횟수에 따른 오차의 변화를 보여준다.

여기서 X축의 값은 학습의 반복 수를 나타내며 Y축의 값은 그때마다의 error값을 나타낸다.

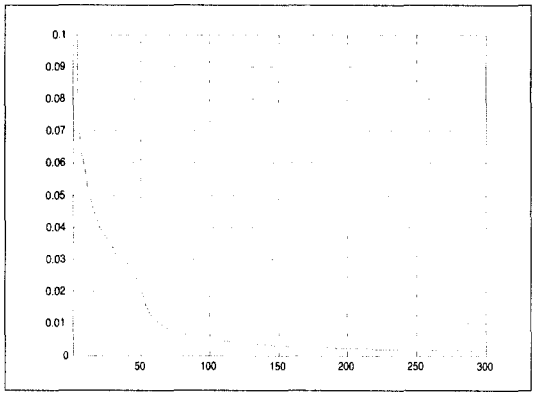
다음 그림에서 알 수 있듯이 초기의 신경회로망이 iteration수가 증가함에 따라 0의 값으로 error값이 감소하다가 200번째부터 일정한 값의 error로 수렴하는 것을 알 수 있다.

학습의 대한 결과 값은 〔표 7〕에 나타나 있다.

학습된 신경회로망 탐지부에 대해 15,000개의 패킷을 적용시켜, 그 탐지결과를 산출했다. 3,000개의



〔그림 5〕 SYN-scan의 학습에 대한 오차



〔그림 6〕 FIN-scan의 학습에 대한오차

〔표 7〕 SYN-scan에 대한 제안된 시스템의 결과

	탐지	false positive/negative
normal 패킷의수	11,470	0
portscan 패킷의수	3,530	0

〔표 8〕 Non-SYN-scan에 대한 제안된 시스템의 결과

	탐지	false positive/negative
normal 패킷의수	16,932	0
FIN-scan 패킷의수	414	0
XMAS-scan 패킷의 수	1,536	0

데이터 중 정상적인 패킷의 수는 11,470개이고, portscan을 위해 사용된 패킷은 3,530개가 포함되어 있음을 공개 침입탐지 시스템으로 확인하였다.

〔표 7〕에서 나타난 바와 같이 제안된 신경회로망을 사용한 portscan 탐지기의 경우 false positive나 false negative 없이 정확하게 정상 패킷과 portscan 패킷을 판별해 냈다.

3.2 Non-SYN-scan에 대한 탐지

다음으로 Non-SYN-packet scan에 대한 제안된 시스템으로 결과를 확인하였다.

위 실험에서는 본 연구에서 제안된 시스템이 학습에 사용된 패킷 특성과 다른 형태의 scan 패킷이 들어왔을 때 탐지효과를 알아보기 위해 학습모드에서 FIN-scan에 대해 시스템을 학습시키고, 탐지모드에서 각각 FIN, XMAS scan에 대한 탐지가 효과적으로 이루어지는지를 알아보았다.

학습모드에서 사용된 데이터는 5000개이고, 여기에 정상적인 패킷은 3,882개이고 FIN-scan관련 패킷은 1,118개이다.

탐지부에 사용된 신경회로망의 입력, 히든, 출력층의 구성 및 학습 파라메터들은 위의 실험1에서 사용된 구성과 동일하다.

탐지모드에서 사용된 데이터는 총 18,882개로, 이중 정상적인 패킷은 16,932개이고 FIN-scan관련 패킷은 414개, 그리고 학습된 scan방식과 다른 형태인 XMAS-scan관련 패킷은 1536개이다.

〔표 8〕에는 본 연구에서 제안된 시스템에 대한 Non-SYN-scan에 대한 실험결과를 나타내었다.

실험결과에서 나타난 바와 같이 학습모드에서 학습이 이루어진 FIN-scan 패킷뿐만 아니라, XMAS-scan에서도 오탐 없이 정확한 탐지성능을 보여주었다. 이러한 실험결과에서 알 수 있듯이 앞으로 새롭게 개발될 Flag 조작형태의 portscan에서 좋은 성능을 기대할 수 있다고 판단된다.

3.3 SYN-Flooding을 이용한 DOS의 탐지

DOS(Denial Of Service)공격이란 다중작업(Multi-tasking)을 지원하는 운영체제에서 발생할 수 있는 공격 방법으로서 구체적으로 한 프로세스가 시스템의 리소스를 독점하거나, 모두 사용해 버리거나 또는 파괴하여서 그 시스템이 다른 프로세스들에게 올바른 서비스를 제공하지 못하도록 하는 공격을 말한다.

DOS공격은 그 정의 자체가 매우 광범위하기 때문에 이를 위한 공격 또한 매우 다양한 방법들이 존재할 수 있다. 시스템의 올바른 서비스 수행을 못하게

하는 공격 특성에 의해서 이 공격은 시스템에서의 루트 권한 획득 또는 시스템, 사용자 데이터의 파괴나 변조 등을 행하지는 못하나 시스템의 정상적인 수행 즉, 네트워크나 시스템 서비스 등의 마비를 야기함으로써 사용자들에게 많은 불편을 주게된다.

이러한 DOS공격 방식 중에서 Syn-Flooding의 공격방식은 패킷수준의 DOS 공격방식의 대표적인 예로써 유명한 Kevin Mitnick이 사용한 IP spoofing 공격에 이용되기도 했던 DOS 공격으로써 시스템 자체를 마비시키지는 않으나 시스템의 특정 서비스 기능을 눈치채지 못하게 마비시켜 버리기 때문에 다른 공격을 위한 사전 공격으로 이용될 확률이 매우 높은 공격이다.

이 공격방식은 TCP 자체의 결함을 이용한다. TCP에서 서버와 클라이언트의 연결은 위에서도 언급한 바와 같이 'Three way hand shaking'이라는 규칙은 이용하는데, 이 연결과정의 마지막 단계에서 계속해서 ACK를 보내지 않는다면 서버는 half-open 상태에 머물러 있게 된다. TCP에 대한 명세(specification)를 하고 있는 문서에서는 이 상황에서 어떻게 해야 할 것인가에 대한 내용이 정의되어있지 않고 그 운영체제를 설계한 사람의 마음에 달려있는 것이다. 알려진 바에 의하면 대부분의 운영체제의 TCP모듈은 half-open 상태에서 TCP 연결을 위해서 백로그 큐(backlog queue)에 연결상태를 유지하기 위한 정보를 저장하고서 half-open 상태로 계속 머무르게 되다가 정해진 일정시간이 지나도 ACK 패킷이 오지 않게 되면 다시 정상적인 상태로 돌아오게 구현되어 있다고 한다. 그런데 만일 백로그 큐의 크기가 정적으로 할당되어 있으며 특정포트에 대해서 이러한 일이 계속적으로 발생하여 시스템이 일정시간 후에 백로그 큐에서 연결 정보를 삭제하는 것보다 더 빠르게 일어난다면 백로그 큐는 항상 가득 차게 될 것이다. 그러면 이 이후에 이 포트에 대한 TCP 연결요청을 모두 거부할 수밖에 없게 되는 것이다. 많은 경우 이러한 상황에서는 공격받는 특정 포트의 서비스만이 정상적이지 못하지만 운영체제의 구현에 따라서는 시스템의 마비를 유발할 수 도 있는 것으로 알려져 알려져 있다.

다음은 SYN-Flood를 이용한 시스템 공격시 나타나는 패킷의 일부를 TCPdump로 캡쳐해서 나타내었다.

이러한 패킷상의 특징은 공격자는 네트워크상에 존재하지 않는 조작된 IP 주소를 사용하기 때문에

```
04:37:19 10.10.10.10.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.11.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.12.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.13.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.14.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.15.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.16.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.17.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.18.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.19.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.20.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.21.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.22.41508 > target.23: S 3935335593:3935335593(0)
04:37:19 10.10.10.23.41508 > target.23: S 3935335593:3935335593(0)
...
```

위의 그림에서 나타난 패킷을 받은 시스템은 SYN-ACK패킷을 보내게 되지만 조작된 IP 주소이므로 ACK 패킷을 받지 못할게 될 것이다. 이러한 방식으로 공격이 이루어지게 된다.

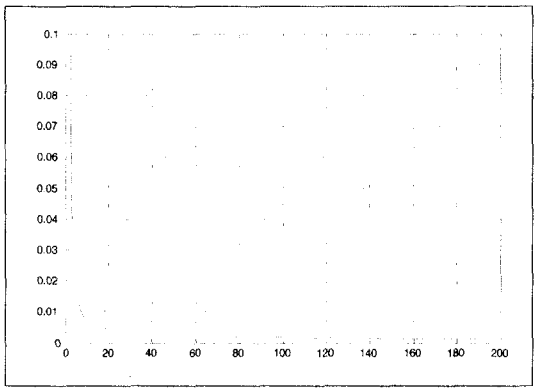
본 논문에서 제안된 시스템의 DOS 공격의 일종인 SYN-Flood공격에 대한 탐지성능을 확인하기 위하여 다음과 같은 단계를 사용하였다.

먼저, 대상호스트의 서비스가 있는 port를 알아내기 위해 공격자의 호스트에서 대상 호스트로의 portscan을 수행하였다. 대상호스트의 열려진 port를 통해 Syn-flood를 통해 서비스를 방해하였다. 실험에 사용된 시스템구성은 이전의 실험과 동일하고, 5000개의 패킷단위로 저장된 데이터를 이용하여 실험하였다.

사용된 신경회로망의 구조는 이전에 portscan의 탐지 때와 같은 값을 가지고, 각 층의 뉴런을 연결하는 연결강도(weight)는 위의 실험에서 사용된 값으로 초기화하였다. 먼저, 학습모드에서 5000개의 SYN-Flood 패킷 및 Normal 패킷을 학습시키고, 이후에 학습된 신경회로망 판단엔진을 이용하여 그 탐지성능을 확인해 보기 위해 목적지 시스템의 23번을 portscan한 후, 23번 포트에 대해 SYN-Flood공격을 시행하였다.

여기에서 수집된 15,000개의 데이터에 대해 성능을 확인하였다. 이 15,000개의 패킷중 정상적인 패킷은 14,165개이고, 나머지는 portscan과 SYN-Flood 공격에 대한 패킷으로 구성되어 있다.

〔그림 7〕은 SYN-Flood 탐지에 사용된 신경회로망의 학습곡선을 나타낸 것이다. 그림에서 알 수 있듯이 이전에 portscan 탐지시 학습곡선과 비교하였을 때 빠른 수렴특성을 나타낸다는 것을 알 수 있다.



〔그림 7〕 SYN-Flood에 대한 학습곡선

이는 사용된 신경회로망의 초기 연결강도의 값을 random한 값을 사용하지 않고, portscan탐지시의 학습된 연결강도를 유지하고, 이에 추가적인 SYN-Flood에 대한 학습정보를 제공함으로써, 이전 실험에서 사용된 신경회로망보다 더 빠르게 학습해 나간다는 것으로 판단된다.

다음의 〔표 9〕에 나타난 바와 같이 제안된 시스템은 portscan패킷과 Syn-Flood패킷을 오탐 없이 정확하게 탐지해 냈다.

〔표 9〕 SYN-Flood에 대한 제안된 시스템의 결과

	탐지	false positive/negative
Normal 패킷의수	14,165	0
portscan 패킷의수	20	0
Syn-Flood 패킷의 수	835	0

본 실험결과를 통해서 제안된 시스템이 portscan뿐만 아니라, 비정상적인 트래픽이나 패킷조작에 의한 DOS 공격의 탐지에서도 좋은 성능을 낼 수 있을 것으로 기대된다. 또한, 추가적인 비정상패킷의 정보를 학습을 통한 지속적인 성능향상을 유지할 수 있을 것으로 판단된다.

3.4 변형된 portscan의 탐지와 성능비교

본 실험에서는 침입탐지시스템의 탐지를 피하기 위해 변형된 portscan방법을 사용하였다. 일반적으로 해커들은 공격 초기에 portscan을 이용하여 공격대상의 port정보수집, network mapping을 수행한다. 그러나 이미 제시된 portscan방식을 그대로 사용할 경우 쉽게 침입탐지시스템에 감지되기 때문에 해커들은 좀 더 은밀한 방법으로 정보를 수집하려고 노력한다. 이러한 침입탐지시스템의 감지를 피하기 위해서 기존 portscan탐지 알고리즘의 취약점을 이용하는 경우가 많은데, 대표적인 탐지 알고리즘의 경우 source IP로부터 M초 이내에 N만큼의 다른 port/IP 조합의 패킷이 탐지되면 이를 portscan으로 탐지하는 것이다. 이러한 알고리즘은 느린 형태의 portscan공격에 대해서는 탐지 할 수 없는 취약점을 지니고 있다. 느린 형태의 portscan은 패킷자체는 위의 실험에서 보여준 네트워크 패킷과 유사한 형태이지만, portscan에 사용되는 패킷의 간격이 길어 찾아내기가 어렵기 때문에 공격자들은 이러한 방식을 이용하여 오랜 시간 동안 공격대상 시스템에 대한 정보를 수집하게 된다.

본 실험에서는 이러한 느린 형태의 portscan공격에 대한 탐지성능을 기존의 Snort와 비교하였다.

〔표 10〕 느린 형태의 scan에 대한 실험결과

	전체 실험 패킷 (13,000개)		false positive	false negative
	패킷구분	패킷수		
Snort	Normal	11,044	0	1,178
	Scan	778		
제안된 시스템	Normal	11,044	0	0
	Scan	1,956		

〔표 10〕와 같이, Snort의 경우 정상적인 패킷과 scan패킷이 각각 11,044개와 1,956개로 구성된 패킷중 778개에 대해서만 탐지하고 나머지 1,198개는 탐지해 내지 못했다. 이것은 Snort가 위에서 설명한 portscan탐지 알고리즘을 사용하고 있기 때문이다. 제안된 시스템의 경우 일반적인 SYN-scan에 사용된 파라메터와 동일하게 구성하여 탐지를 하였고, 탐지결과〔표 10〕에 나타난 바와 같이 오탐 없이 효율적인 성능을 유지함을 알 수 있다.

따라서 본 논문에서는 기존의 portscan 방식과 변형된 방식들에 대해 효과적으로 탐지됨을 알 수 있다. 또한 제안된 확률적인 방법에 의한 네트워크 특성추출이 적절하다는 것을 본 실험을 통해서 알 수 있었다.

Ⅳ. 결 론

급속한 정보 통신 기술의 발달로 인터넷을 포함한

정보 인프라는 날로 발전하고 있으나 역기능적인 해킹/트래킹 등 비정상적인 사용자의 급증으로 정보보안기술의 혁신이 요구되고 있다. 지금까지 많은 보안관련 업체에서 새로운 기법을 이용하여 더 좋은 보안시스템을 개발하고 있으나 해커들 또한 새로운 기법을 연구하고 적용하는 사례가 빈번한 실정이다.

본 연구에서는 네트워크상 패킷의 다양한 성격을 통계학적으로 수집하여 이를 신경회로망에 학습시키고 비정상적인 패킷을 탐지할 수 있는 시스템을 제안하였다.

실험환경에서는 정상적인 패킷에 비정상적인 패킷을 조합하여 공격대상 호스트의 Port 정보를 수집하기 위해 NMAP이라는 portscan 툴을 사용했으며, 제안된 시스템에 적용하여 정상적인 트래픽 중에서 portscan을 위해 사용된 비정상적인 패킷을 적절하게 탐지하는가를 확인하였다.

제안된 침입탐지시스템의 실험 결과를 정리하면 다음과 같다.

- 학습시킨 침입에 대하여 정확히 탐지한다.(SYN-scan의 학습과 탐지)
- 기존의 학습된 데이터를 바탕으로 학습시키지 않은 다른 특성의 침입을 탐지한다.(FIN-scan의 학습과 XMAS-scan의 탐지)
- 기존 학습에서 얻어진 연결강도를 사용함으로써 새로운 침입에 대하여 빠르고 효율적인 학습과 탐지가 가능하다.(SYN-Flooding을 이용한 DOS 공격 탐지)
- 변형된 침입 형태에 대한 탐지에서 우수한 성능을 가진다.(시간 주기를 느리게 한 portscan의 탐지)

이러한 결과로 비추어 볼 때 제안된 시스템은 새롭게 개발된 취약점 검색이나 portscan 방식이 나오더라도 적절히 찾아내고 대처할 수 있는 가능성을 제시했으며, 또한 최근 많이 활용되고 있는 해킹 기술인 DOS공격 방법 중 SYN-Flood 공격에 대해서도 만족할 만한 성능을 확인하였다. 그리고 기존 침입탐지시스템에서 false negative가 많이 발생되는 침입에 대한 효과적인 탐지를 수행함으로써 본 시스템은 지능형 침입탐지가 가능하다는 것을 입증하였다.

따라서 본 논문에서 제안된 시스템은 기존의 상용 및 공개용 네트워크 침입탐지 시스템과 상호 연동시 관리자에게는 침입행위에 대한 다양한 정보를 제공할 수 있으며, 공격자들이 Insert/Evasion 기법 등으로 시스템 탐지를 시도한다 하더라도 성공 가능성을 최소화시킬 수 있게 되었다. 하지만 시스템 환경에 따라 학습모드와 탐지모드의 적절한 선택기준과 감사자료 축약부에서 생성되는 자료에 따라 신경회로망의 탐지능력이 좌우되므로, 관리자는 네트워크 상황과 시스템 환경에 맞는 적절한 모드 전환시점 및 감사 자료의 선택을 신중히 할 필요가 있으며, 속도 및 탐지성능을 만족시킬 수 있는 다양한 학습 알고리즘을 개발하여 이를 적용시킬 수 있는 방법에 대한 연구도 필요할 것이다.

향후에 패킷헤더의 정보를 이용하여 다양한 통계적 특성을 정의하고 특징을 추출해 내는 Data Mining에 대한 보다 수준 높은 연구가 병행되었을 때 신경회로망 침입탐지시스템은 학습속도 및 신뢰성을 더욱 향상시켜 강력한 지능형 침입탐지시스템으로 개선될 수 있을 것으로 기대된다.

참 고 문 헌

[1] Proctor, *Practical Intrusion Detection*, Prentice Hall, 2000.

[2] 한국정보보호센터, *"2001년 7월 국내외 해킹현황"*,2001

[3] Kumar. S, *"Classification and Detection of Computer Intrusions,"* Ph.D. Thesis, Department of Computer Sciences, Purdue University, W.Lafayette, 1995.

[4] K.A. Jackson, D.H. DuBois and C.A. Stalling, *"An Expert System Application for Network Intrusion Detection"*, Proceeding of the 14th National Computer Security Conferfence. pp. 215~225, October 1991.

[5] Koral Ilgaun, Richard A. Kemmerer and Phillip A. Porras, *"State Transition Analysis: A Rule-Based Intrusion Detection Approach"*, IEEE transactions on software engineering. 21(3):181-199, Mar 1995.

[6] McCanne, S., Jacobson, V. *"The BSD Packet Filter: A New Architecture for User-Level Packet Capture"*, Proceedings of the 1993 Winter USENIX Conference, pp. 259~269, 1993.

[7] Fyodor, *"The Art of Port Scanning"*, Phrack Magazine Volume 7, article 11, Issue 51, September, 1997.
[8] Garsia, *"Probability and Random Process for Electrical Engineering"*, Addison Wesley, 1994.
[9] S. Staniford, J.A. Hoagland, J. M. Mc Alerney *"Pracrical Automated Detection of Stealthy portscans"*, Silicon Defense
[10] S. Haykin, *"Neural Network"*, Prentice-Hall, 1995.
[11] B. Kosko, *"Neural Networks for Signal processing"* Prentice-Hall Inc. 1992.
[12] Hagan, M. T., H. B.Demuth, and M. H. Beale, *"Neural Network Design"*, PWS Publishing.

〈著者紹介〉

이 장 헌 (Jang-Hun Lee) 정회원
1970년 3월~1974년 3월 : 육군사관학교 토목공학 이공학사 졸업
1984년 7월~1986년 6월 : 미 해군 대학원 전산과학 석사 졸업
1998년 3월~현재 : 한남대 대학원 컴퓨터공학 박사과정
1998년11월~2000년11월 : 육군전산소 소장
2000년11월~2001년 5월 : 육본 지휘통신참모부 정보체계관리 처장
2001년 9월~현재 : SK C&C 기술자문위원
〈관심분야〉 전자공학, 통신공학, 정보보호

김 성 옥 (Sung-Ok Kim) 정회원
1962년 3월~1966년 3월 : 연세대학교 수학과 이학사 졸업
1973년 9월~1976년 6월 : 미 미네소타주립대 전자계산학석사 졸업
1986년 3월~1989년 2월 : 연세대학교 대학원 이학박사
1970년 3월~1983년 2월 : 국방과학연구소(ADD) 수석연구원
1983년 3월~ 현재 : 한남대학교 컴퓨터공학과 교수
〈관심분야〉 시뮬레이션, 수치해석, 교육공학, 정보보호