대규모 백본망의 웜 바이러스와 분산서비스거부공격 탐지시스템 연구

이 명 선[†] · 이 재 광[††]

요 약

웜 바이러스 및 분산서비스거부 공격의 등장으로 침해사고의 공격대상 및 피해범위는 특정 시스템이나 서비스에서 벗어나 네트워크 자체의 장애 및 마비로 확대되고 있다. 이러한 공격 형태는 가장 강력하고 빈번하게 발생하고 있으며, 특히 공격의 경유지로 이용될 인터넷서비스제공사들은 심각한 피해를 입을 수 있다. 그러나 이러한 웜 바이러스 및 분산서비스거부 공격의 빠른 전파속도로 인해 다수의 시스템에서 동시에 발생하는 것이 일반적인 반면에 네트워크 자원의 대응은 네트워크 관리자에 의한 수동적으로 이루어져 대응 속도가 느리고 전체 발생량을 처리할 수 없는 형편이다. 이에 따라 본 논문에서는 웜 바이러스 및 분산서비스거부 공격 발생 여부 및 공격자(공격자 IP 주소)를 자동으로 탐지할 수 있는 방안을 제시한다.

A Study on Tools for Worm Virus & DDoS Detection

Myung-Sun Lee[†] · Jae-Kwang Lee[††]

ABSTRACT

As Worm Virus & DDoS attack appeares, the targets and damages of infringement accidents are extending from specific system or services to paralysis of the network itself. These attacks are expending very frequently and strongly, and ISP who will be used as the path of these attacks will face serious damages. But compare to Worm Virus & DDoS attack that generally occures in many Systems at one time with it's fast propagation velocity, network dimensional opposition is slow and disable to deal with the whole appearance for it is operated manually by the network manager. Therefore, this treatise present devices how to detect Worm Virus & DDoS attack's outbreak and the attacker(attacker IP adderss) automatically.

키워드 : 웜 바이러스(Worm Virus), 분산서비스거부공격(DDoS), 넷플로우(Netflow), 플로우스캔(Flowscan), 침입탐지(Intrustion Detection), Cflowd

1. 서 론

1.1 연구 배경

인터넷 사용인구의 폭발적인 증가와 더불어 악의적인 공격자들의 공격 또한 급증하고 있는 가운데, 2003년 1월 25일에 발생한 MS SQL 취약점을 이용한 웜 바이러스 공격은 우리나라 및 세계의 많은 네트워크를 마비시키는 인터넷대란을 초래하였다[1]. 이러한 웜 바이러스(Internet Worm)를 이용한 전파뿐만 아니라 분산서비스거부(DDos : Distributed Denial of Service)공격 등으로 인해 많은 임의의 공격대상이 심각한 보안위협에 노출되고 있다. 특히 최근에 등장한 웜 바이러스 및 분산서비스거부공격은 라우터, 스위치, 방화벽 그리고 침입탐지시스템 등과 같은 네트워크 자원이 고갈되어 정상적인 서비스가 불가능한 상태에 이르게 한다.

웜 바이러스 및 분산서비스거부공격은 악의적인 공격형태 중 가장 강력하고 빈번하게 발생하고 있으며 특히 공격의 경유지로 이용될 인터넷서비스제공자(ISP : Internet Service Provider)들은 심각한 피해를 입을 수 있다.

인터넷 이용기관의 경우는 방화벽이나 침입탐지시스템 그리고 저비용으로 고성능의 실시간 보안관제가 가능하지만 고속의 네트워크 백본을 운영하는 대형 인터넷서비스제공자들은 수십 기가 bps급의 고속 회선에서 보안 관제를 행해야 하기 때문에 기술적으로 매우 어려운 상황이며, 고성능의 보안탐지 및 대응장비를 구입해야하므로 실로 막대한 추가비용이 발생할 뿐만 아니라 고성능의 보안탐지 및 대응장비도 부족한 상태이다[2].

또한 개인의 프라이버시 및 기관의 주요 정보유출방지가 중시 되면서 대형 인터넷서비스제공자는 개인이나 기관의 동의 없이 전송되는 데이터를 분석하기 어려움으로 기존의 침입탐지시스템 등과 같은 패킷 데이터를 분석하는 보안장

※ 본 연구는 산업자원부에서 시행한 산업기술개발사업(2003 61 10009504)에 의해 지원되었음.
† 정 회 원 : 한국과학기술정보연구원 슈퍼컴퓨팅센터 책임연구원
†† 종신회원 : 한남대학교 컴퓨터공학과 교수
논문접수 : 2004년 8월 12일, 심사완료 : 2004년 8월 27일

비를 그대로 적용하기 어려운 상태이다.

마지막으로 대형 인터넷서비스제공자에게 웜 바이러스 및 분산서비스거부 공격을 탐지하고 대응하는 것에 있어 또 다른 문제점은 대규모 백본망에서 탐지는 웜 바이러스 및 분산서비스거부공격 탐지 결과가 하루에도 수천 건에 이른다는 것이다. 이는 소수의 네트워크 관리자들을 중심으로 운영되고 있는 대부분은 인터넷서비스제공자들에게는 큰 부담일 수밖에 없다.

이에 따라 본 연구는 웜 바이러스 및 분산서비스거부 공격의 특징을 분석하고 이를 자동으로 탐지 및 통보할 수 있는 시스템을 설계하여 고속의 네트워크 백본을 운영하는 대형 인터넷서비스제공자의 관점에서 네트워크 보안을 강화할 수 있는 방안을 제시한다.

1.2 논문의 구성

2장에서는 침입탐지시스템(IDS, Intrusion Detec tion System), RTSD(Real Time Scan Detector), Flowscan/Flowcan+ 등 기존의 웜 바이러스 및 분산서비스거부공격을 탐지할 수 있는 탐지도구들을 중심으로 관련 연구를 기술하고, 3장에서는 웜 바이러스 및 분산서비스거부 공격기법들이 가지는 특징을 기술한다. 4장에서는 제안한 탐지 방법에 대한 설계 및 구현을 기술하고, 5장에서는 제안한 탐지 기법에 의한 실험 결과를 기술한다. 마지막으로 6장에서는 제안한 탐지 기법의 기능비교와 향후 발전방향을 언급한다.

2. 관련 연구

2.1 침입탐지시스템(IDS : Intrusion Detection System)

침입탐지시스템은 기존에 발생했던 공격 패턴을 탐지하는 것으로 이전에 발생했던 다양한 공격유형 즉, 해킹, 웜 바이러스, 분산서비스거부공격, 취약점 스캔 등을 탐지할 수 있다는 장점을 지닌다. 또한 패킷의 데이터 필드 값을 분석하여 데이터 필드에 포함된 악성코드를 탐지할 수 있다. 이러한 방식은 HTTP 프로토콜에 쉘 코드를 삽입한 공격 등을 탐지하는데 효율적이다.

그러나 침입탐지시스템은 데이터 필드 분석을 통한 보다 정교한 탐지가 가능한 장점을 가지나 이로 인한 기관 및 사용자 정보유출 가능성이 발생할 수 있다는 단점을 지닌다. 또한 침입탐지시스템은 대규모 백본 트래픽을 모니터링할 수 있는 처리 능력이 부족하여 다수의 침입탐지시스템을 병렬로 구축하는 것이 일반적이며, 이로 인해 막대한 구축비용이 소요된다. 침입탐지시스템의 또 다른 단점은 다수의 이벤트 발생으로 인해 관리자에 의한 재분석이 필요하다는 점과 공격탐지를 위한 장비로 자동 통보 및 차단능력이 미흡하다는 것이다. 물론 침입탐지시스템을 침입차단시스템(Firewall)과 연동하여 실시간 차단이 가능하나 그 기능은 극히 제한적이다.

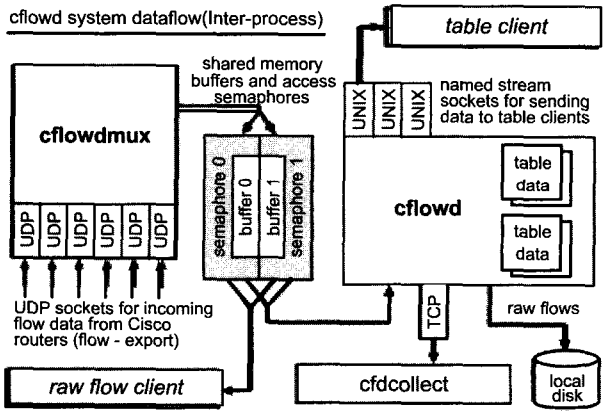
2.2 CFlowd

Cflowd는 Cisco의 Netflow를 이용한 스위칭 방법을 분석하기 위해 현재 사용되고 있는 플로우 분석 도구이다.[4] 수집, 저장, 기본적인 분석 모듈을 포함하고, ARTS++ 라이브러리를 이용하여 기본적인 분석 모듈을 만들어 사용한다.[5]

분석 패키지는 ISP나 네트워크 엔지니어가 Capacity Planning, Trends Analysis 그리고 네트워크 서비스 환경에서 Workload의 특성을 파악 할 수 있도록 데이터 수집과 분석 기능을 제공하고 있다.

(그림 1)과 같이 각 Cisco 라우터는 Flow-export 패킷을 cflowdmux와 cflowd를 실행하고 있는 호스트에 보낸다. 호스트의 cflowdmux는 UDP 데이터그램인 Flowd-export 패킷을 수신하여 공유메모리 버퍼에 쓰고, 호스트의 cflowd는 공유메모리 버퍼에 쓰여진 패킷을 읽어서 로컬테이블에 저장한다. 최종 데이터 수집은 호스트의 cfdcollect에 의해서 수행 되는데, cfdcollect는 주기적으로 한번에 하나의 cflowd와 TCP 연결을 맺고 cflowd의 로컬 테이블로부터 테이블 데이터를 수집하여 ARTS라는 바이너리 파일로 저장한다.

ARTS++ 유틸리티를 통하여 ARTS 파일로부터 AS matrix와 Net matrix같은 여러 가지 통계정보를 얻을 수 있는데, 이 통계정보를 가지고 데이터를 수집한 네트워크의 Protocol별로 트래픽 량을 알고 싶을때, artsprotos 유틸리티를 이용하면 cfdcollect가 저장한 ARTS 파일을 읽어 5분단위로 Protocol별 트래픽을 보여준다. 이러한 네트워크의 트래픽 종류와 트래픽 량을 파악하여 Network management, Billing, Network Planning 그리고 Network Monitoring 등에 활용할 수 있다.



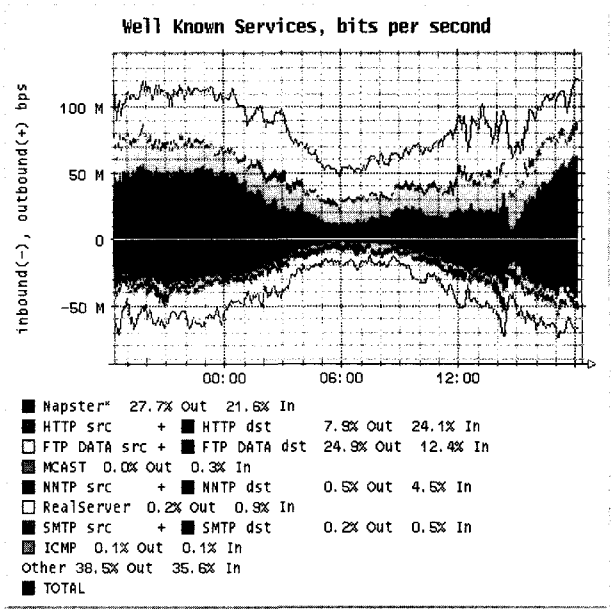
(그림 1) CFlowd data flow detail

2.3 FlowScan/FlowScan+

Flowscan은 시스코 라우터에서 보내는 플로우 데이터를 분석하여 유용한 정보를 얻을 수 있게하는 분석 도구로 Dave Flonka에 의해 개발되었다. FlowScan은 라우터의 트래픽을 실시간 모니터링해 보여주며 이는 그래프로 표현되어 트래픽의 추이를 한눈에 파악할 수 있게 해 준다[7].

Flowscan은 네트워크의 트래픽을 측정하여 실시간에 거의 근접하게(5분 단위) 그래프를 아래 (그림 2)와 같이 만들어 준다.

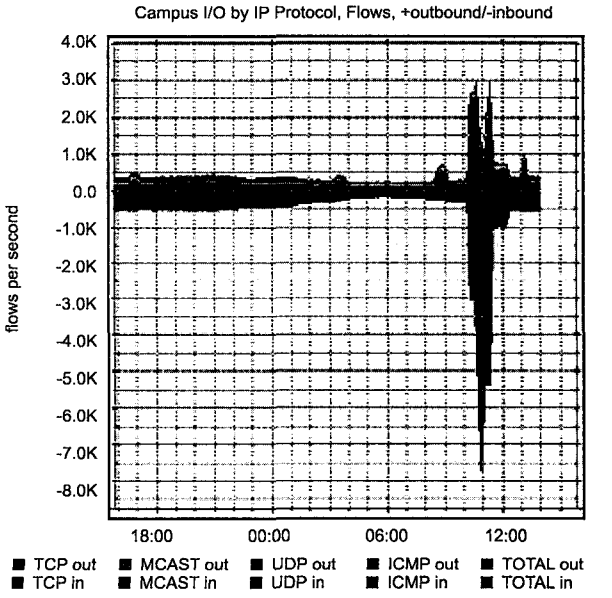
Flowscan을 사용하기 위해선 Netflow 버전 5가 전송(export) 가능한 시스코 라우터가 필수적으로 필요하다. Flowscan 분석 시스템은 특별한 플랫폼을 요구하지는 않으며 대부분의 플랫폼에서 무리 없이 설치 가능하다.



(그림 2) Flowscan의 트래픽 추이 그래프

Flowscan+는 Flowscan에 DB 쿼리(Query)기능을 추가한 것으로 KAIST와 KISTI에서 공동 개발한 것이다. 이러한 Flowscan/Flowscan+는 트래픽 추이 분석을 통해 이상 트래픽 발생유무를 가시적으로 명확히 표현할 수 있다는 장점을 지닌다. 이를 통해 기존의 공격유형을 탐지할 수 있을 뿐만 아니라 아래의 (그림 3)에서 볼 수 있듯이 대량의 플로우를 발생시키는 새로운 공격유형의 등장을 효과적으로 탐지할 수 있다.

그러나 Flowscan/Flowscan+는 트래픽 추이 분석을 통해 이상 트래픽의 발생 유무만 탐지할 뿐 실제 어느 IP의 어떤 포트번호에서 문제가 발생하는지는 관리자가 수동으로 Netflow 정보를 분석하거나 DB 쿼리를 통해 조사하여야 한다.



(그림 3) 분산서비스거부 공격시 Flowscan 그래프 변화

3. 웜 바이러스 및 분산서비스거부공격 특징

백본망에서 많이 사용하는 시스코 라우터의 Netflow에서 전송되어지는 플로우 정보의 분석을 통해 DB로 구축하고, 이를 통계와 유형정보를 이용한 이상탐지 알고리즘으로 구성된 분석탐지 모듈이 실시간으로 분석하여 관리자에게 통보함으로써 관리자가 즉시 대응 할 수 있는 분석탐지 모델을 개발하고자 한다. 본 장에서는 탐지되어지는 웜 바이러스 및 분산서비스거부 공격이 네트워크에 미치는 특성을 살펴보도록 한다.

3.1 웜 바이러스

웜 바이러스는 네트워크를 통해 전파되는 과정에서 다음과 같은 특징을 지닌다.

3.1.1 브로드캐스트 또는 플로우 수의 급격한 증가

웜 바이러스는 공격대상을 찾기 위해 임의의 네트워크 블록으로 브로드캐스트를 하거나 임의의 다수의 IP로 연결을 시도한다. 이를 통해 현재 부팅되어 실행되고 있는 시스템의 존재를 파악하고, 해당 시스템에 대한 공격을 시도하는 것이다.

3.1.2 대량의 트래픽 발생

또한 희생자를 찾기 위해 무차별적인 트래픽을 유발함으로써 대역폭을 낭비시켜 네트워크 장비의 처리용량의 한계에 이르게 한다.

3.1.3 취약점을 공격(특정 Port 공격)

최근 웜 바이러스에 의한 공격방법은 대부분 네트워크를 통해 시스템이 가지는 취약점을 공격하는 것이 일반적이다. 예를 들어 Sasser 웜의 경우 MS04-011 LSASS 취약점을 공격하여 전파되는 웜으로 445번 포트의 접근을 시도한다.

〈표 1〉 웜 바이러스에 따른 공격 포트

바이러스명	프로토콜	공격포트
Agobot	TCP	80, 135, 445
LoveSan	TCP	135
ScanBot	TCP	139, 445
Deloder	TCP	445
MulDrop	TCP	1133, 7648
MyDoom	TCP	3127
Raleka	TCP	6667
Slammer	UDP	1434

3.1.4 이메일을 통한 전파

최근에는 이메일의 스크립트 또는 첨부파일을 통해 전파되는 웜 바이러스가 증가하고 있는 추세이다. Netflow에서는 패킷 데이터를 분석할 수는 없으므로 특별한 네트워크 징후 없이 이메일을 통해 전파되는 웜 바이러스의 경우 제안한 탐지 방법으로 탐지하기 어렵다.

3.2 분산서비스거부공격

분산서비스거부 공격은 인터넷상에서 다수의 시스템이 협력하여 하나의 목표 시스템을 공격함으로 서비스 장애를 일으키게 만드는 것을 말한다. 목표 시스템은 대량의 메시지

들로 인해 결국 시스템 가동이 멈추어지게 되어, 선의의 사용자들은 정작 그 시스템으로부터 서비스를 받지 못하는 일이 벌어지게 된다[8, 9].

이러한 분산서비스거부 공격은 공격 과정에서 다음과 같은 특징을 지닌다.

3.2.1 대역폭/처리량 공격

무차별적인 트래픽을 유발함으로써 대역폭을 낭비시키는 대역폭 공격과 많은 수의 소규모 패킷을 고속으로 전송함으로써 서버나 네트워크 장비의 처리용량의 한계를 경험하게 하는 공격으로 PPS 공격 등이 존재한다.

3.2.2 프로토콜 공격

TCP, UDP 그리고 ICMP 프로토콜과 같은 프로토콜의 기대되는 행위를 이용하는 것으로 SYN Flood 등이 이에 포함된다.

3.2.3 소프트웨어 취약점 공격

네트워크 소프트웨어의 취약점을 이용한 것으로, www 공격 등이 이에 포함된다. Netflow에서는 패킷 데이터를 분석할 수는 없으므로 소프트웨어 취약점 공격하는 분산서비스거부 공격의 경우 제안한 탐지 방법으로 탐지가 어렵다.

4. 설계 및 구현

본 장에서는 웜 바이러스 및 분산서비스거부공격 탐지를 위한 분석방법에 대하여 설명한다. 기존의 웜 바이러스 탐지 방법들은 공격시 일어나는 플로우 수의 급증 현상, 플로우당 데이터량이나 패킷량의 이상 현상 등을 탐지하여 왔다.

본 장에서 제안하는 방법은 전체적인 네트워크에 있어서 좀 더 정확한 탐지를 위해 Netflow 정보 중 비정상이라 탐지되는 플로우를 탐지하고, 탐지된 정보를 이용해 정확한 이상 판단을 하게 된다.

4.1 Netflow 트래픽 분석

Netflow는 Cisco 라우터가 각 네트워크 인터페이스를 통해 지나가는 트래픽의 플로우 정보를 제공하는 기능으로, 네트워크 서비스 이용 과금이나 모니터링에 주로 이용된다. Netflow에 이용되는 기본 단위는 플로우이다. 플로우란 송신자에서 수신자로의 일련의 단방향성 패킷의 흐름으로 정의된다. 각 플로우는 송신자/수신자 IP 주소, 송신자/수신자 포트번호, 3계층 프로토콜 타입, ToS(Type of Service), 그리고 Input interface identifier도 같이 사용하면서 정보를 제공한다. 또한, 포트별 플로우수, 패킷 수, 패킷 크기(바이트)를 알 수 있다[10].

따라서 약 5분마다 오는 Netflow정보를 이용해 실시간으로 플로우별로 정보들을 확인할 수 있다. 이러한 정보들을 이용하여 현재 네트워크상의 이상 트래픽이라 여겨지는 브로드캐스트, 핑 스캔, 싱크 플러드(Sync Flood) 등의 플로우 정보를 묶어 파일화 및 데이터베이스화를 하게 된다.

4.2 웜 바이러스 탐지

Netflow 트래픽 분석을 통해 얻어진 자료를 통해 웜 바이러스를 탐지한다. 일반적인 웜 바이러스 패턴은 여러 네트워크에 브로드캐스트를 하여 자신의 복제 및 유포를 위한 대상을 찾게 된다. 이렇게 찾아진 대상의 취약점을 이용하여 비교적 짧은 길이의 웜 바이러스 코드를 단기간 내에 여러 대상에게 유포하게 되는 것이다.

이러한 웜 바이러스의 특징을 이용하여 다음과 같은 경우를 탐지하게 된다.

- 송신자 IP에서 x.x.x.x/26 이상으로 브로드캐스트하는 경우
- 송신자 IP에서 32개 이상의 플로우 증가
- 사용하지 않는 수신자 IP 사용 유무
- 웜 바이러스로 사용되는 포트로의 연결시도
- 15분 동안 3개 이상의 대역에 브로드캐스팅

브로드캐스트 하는 송신자 IP를 블랙리스트 데이터베이스에 저장 후 모니터링 한다. 사설 IP, 루프백 IP, 멀티캐스트 IP, 실험용 IP의 경우 수신자의 IP가 될 수 없으므로 이러한 경우 아래의 <표 2>와 같이 모니터링의 대상이 된다.

〈표 2〉 네트워크에서 사용되지 않는 IP 목록

구 분	IP 대역
사설 IP 주소	10.0.0.0 - 10.255.255.255 172.16.0.0 - 172.31.255.255 192.168.0.0 - 192.168.255.255
루프백 IP 주소	127.0.0.0 - 127.255.255.255
멀티캐스트 IP 주소	224.0.0.0 - 239.255.255.255
실험용 IP 주소	240.0.0.0 - 255.255.255.255

또한, 보통 웜 바이러스로 이용되는 포트인 135, 139, 445 포트등과 사건/사고가 발생하였을 경우 추가적인 작업을 통해 이용되는 포트를 추가함으로 탐지한다. 마지막으로 한계임계치 값을 두어, 약 5분 동안 일어날 수 있는 플로우를 정의함으로써 이상이 있는 플로우를 탐지한다.

4.3 분산서비스거부공격 탐지

분산서비스거부공격의 경우 어떤 특정한 포트 혹은 방법이 정해져 있는 것이 아니라 탐지가 힘들다는 문제점이 있다. 보통의 분산서비스거부공격의 경우 Netflow의 정보를 한 번 더 가공함으로써 수신자 IP에 대한 정보로 바꿀 수 있다.

분산서비스거부공격의 경우 다음과 같은 특징의 경우를 탐지하게 된다.

- 수신자 IP별로 임계치 이상의 플로우의 경우
- 사용하지 않는 송신자 IP 사용 유무
- 패킷당 평균 크기 확인

분산서비스거부공격의 경우 여러 송신자가 하나의 수신자에게 공격을 하게 되기 때문에, 수신자 IP의 플로우가 급증하는 현상이 발생할 수 있다. 그로인해 패킷당 평균 데이터량이 정상일 경우보다 감소하게 될 것이다.

또한, 송신자 IP 변조를 통해 사용하지 않는 IP를 이용하는 경우를 탐지할 수 있다.

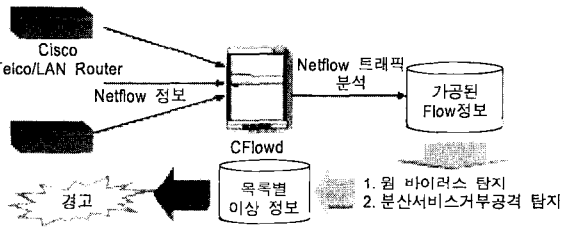
4.4 처리 메커니즘

본 논문에서 제안된 전체시스템의 처리 플로우는 아래

의 (그림 4)와 같이 시스코라우터에 설정된 클라이언트에 Netflow 정보를 보내게 된다. 클라이언트의 CFlowd는 라우터에서 보내어진 Netflow 정보를 약 5분마다 한번씩 파일로 내보내게 된다. 파일이 내보내지게 되면, 이 파일에 담겨있는 플로우 정보중 필요한 필드만을 추출하여, '가공된 Flow 정보 데이터베이스'에 저장을 하게 된다. 데이터 베이스를 이용하는 이유는, 5분동안 받아진 플로우 정보일지라 하더라도 여러 라우터에서 보내어 지는 플로우 정보이기 때문에 상당히 커다란 파일이 되고, 이 파일을 메모리에 유지하기 하기란 상당히 힘들고, 필드값의 조합으로 필요한 정보를 찾기가 힘들기 때문에, 데이터베이스를 이용한다.

'가공된 Flow 데이터베이스'에 있는 값을 분석하여, 3.1장에서 언급한 브로드 캐스트, 플로우 수의 급격한 증가, 대량의 트래픽, 특정 포트의 공격에 대한 웜 바이러스 탐지 및 하나의 호스트에 집중되는 대역폭/처리량 및 프로토콜 공격의 분산서비스거부 공격을 탐지해 '목록별 이상정보 데이터베이스'에 추가하게 된다.

마지막으로 '목록별 이상정보 데이터베이스'의 정보를 분석해, 정의되어진 임계치 이상의 값이 탐지되면, 탐지된 결과에 대한 경고를 보여주게 된다.



(그림 4) 제안시스템 처리 메커니즘

5. 실험결과 및 고찰

5.1 실험 환경

실제 네트워크의 트래픽을 관리하기 위해 설치된 Netflow를 이용하여 네트워크 트래픽 정보를 수집하였다. 2004년 6월 1일의 플로우 정보를 바탕으로 실험하였다.

본 실험의 구현 및 환경은 아래의 <표 3>과 같다.

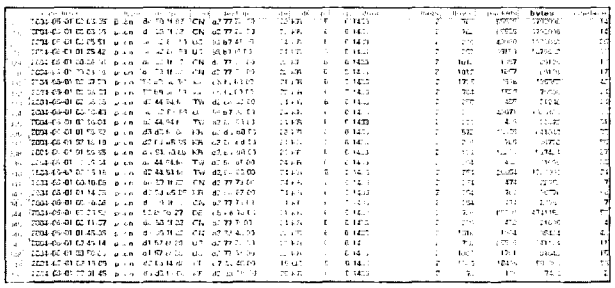
<표 3> 실험 환경

구 성 요 소	개 발 환 경
CFlowd 시스템	◦ 운영체제 : RedHat Linux 9.0 ◦ 시스템 : Pentium 2.6 Zeon Dual
Netflow 트래픽 분석 모듈	◦ 운영체제 : RedHat Linux 9.0 ◦ 개발언어 : Perl DBMS : MySQL
이상 탐지 모듈	◦ 운영체제 : RedHat Linux 9.0 개발언어 : C/C++ ◦ DBMS : MySQL

5.2 실험 결과

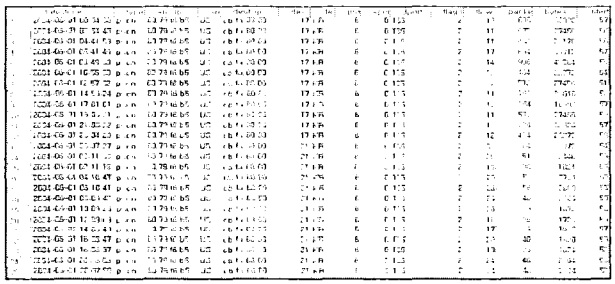
공격이 일어난 경우 기본적으로 평소보다 많은 플로우 수와 패킷수 그리고 플로우 당 데이터량이 작음이 관찰된다. 또한, 약 3~4시간 안에 비슷한 유형의 플로우가 발생하고 이러한 유형이 반복되는 것을 관찰할 수 있다.

(그림 5)에서는 Netflow 트래픽 분석 모듈에 의해 가공되어진 플로우 정보를 보여준다. 대부분의 플로우 정보들의 특징이 많은 개수의 flow를 가지고 있음을 볼 수 있고, 비교적 작은 패킷당 바이트 크기를 관찰할 수 있다.



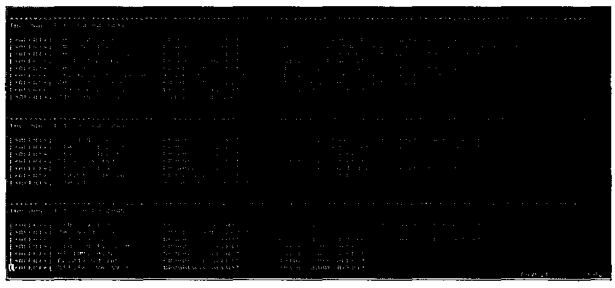
(그림 5) 가공된 Flow 정보

(그림 6)에서와 같이 비슷한 유형의 이상이 있는 플로우가 반복되는 유형을 관찰 할 수 있다. 또한, 이와 같이 확실한 공격이라 의심할 수 있는 플로우 정보의 경우, 약 50byte 크기의 작은 패킷당 바이트 수를 관찰할 수 있다.



(그림 6) 공격이 의심되는 Flow 정보

그리고 이러한 공격 유형을 분석해 실시간으로 (그림 7)과 같이 관리자에게 이상을 통보한다.



(그림 7) 이상탐지 화면

5.3 실제 침해현황 보고와의 비교

플로우 정보를 얻은 기관에서의 침해사항 보고서와 본 논문에서 제안한 분석방법을 통한 방법과의 비교를 한 <표 4>를 보게 되면 침해사항 보고서와 비교해 상당히 많은 문제점을 보고한다. 실제 침해사항 보고서에 기록되어 있는 정보와 정확히 일치 하는 개수는 431개로서 문제가 되는 대부분의 정보와 일치한다고 할 수 있다. 대부분의 정보와 일치한다고 가정할 수 있는 이유는, 하루동안의 데이터를 이용

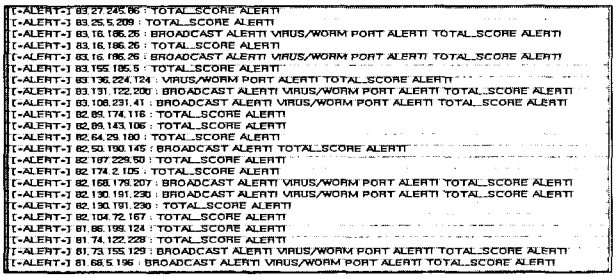
하였기 때문에, 사전에 저장되어진 '목록별 이상정보 데이터베이스'의 내용이 없어 임계치에 모자라 탐지가 되지 않을 수 있기 때문이다. 또한, 하루만의 정보만을 이용하였기 때문에 현재까지는 임계치에 도달하지 못하였을지라도, 후의 정보를 이용하게 되면 탐지 가능한 경우일 것이기 때문이다.

그리고 침해사항 보고서에는 기록되지 않았으나, 추가로 문제가 되는 정보는 66개 정도로 실제 보고서와 비교해 좀 더 높은 문제를 탐지할 수 있음을 나타낸다.

〈표 4〉 실제 침해사고 현황 보고와 제안한 방법 비교 결과

	침해사항 보고서	제안한 분석방법
총 문제 보고	477	497개
일치하는 보고	431개	
일치하지 않는 보고	46개	66개

(그림 8)과 같이 침해사항 보고서에는 없는 이상탐지 목록을 확인할 수 있다.



(그림 8) 추가적으로 발견된 이상탐지

6. 결론 및 향후 계획

제안된 시스템은 대규모 백본망의 인터넷서비스제공자의 입장에서 적은 비용으로 편리하게 웜 바이러스 및 분산서비스거부 공격을 탐지하기 위한 Netflow기반의 탐지 도구를 설명하였다.

제안된 시스템은 <표 5>에서 보는 바와 같이 플로우 분석을 통한 이상징후 탐지, 웜 바이러스 및 분산서비스거부 공격 탐지, 탐지 결과 통보 기능면에서 뛰어난 성능을 보이고 있다.

그러나 제안된 시스템은 Netflow를 기반으로 개발되어 Netflow가 가지는 기본적인 한계적, 즉 데이터 필드를 분석하지 못함으로 인해 발생하는 정교한 공격유형 탐지, 이메일 등 기본 서비스를 이용한 공격을 탐지하기 힘들다는 문제점을 지닌다.

〈표 5〉 기존 시스템과 제안된 시스템 기능 비교

	IDS	RTSD	Flow Scan/+	제안 시스템
트래픽 이상징후 탐지	-	-	○	○
웜/DDoS 탐지	○	-	-	○
해킹 사전활동 탐지	○	○	-	△
탐지결과 통보	△	-	-	○
정교한 공격 유형 분석 (패킷 데이터 분석)	○	○	-	-

향후에는 호스트 단의 문제점 뿐 아니라, 전체 네트워크에서의 트래픽 이상징후를 탐지하여, 문제가 되어진다고 생각되는 포트및 이상 패턴을 이상탐지 알고리즘의 자료로 추가하여 좀더 탐지율을 높이게 하고, 관리자 및 공격자 IP를 관리하는 기관의 보안 담당자들에게 자동으로 탐지 결과를 통보할 수 있는 자동 통보시스템을 추가할 계획이다.

참 고 문 헌

[1] CERTCC-KR, KISA, "MS-SQL 슬래머(Slammer) 공격 테스트 및 사고대응", http://www.certcc.or.kr, Jan., 2003.
[2] 김승해, "서비스거부공격 자동탐지시스템 설계 및 구현", Aug., 2003.
[3] 최우형, "침입자 추적 대응 기술 - Netflow를 통한 탐지 기법", 2004.
[4] CAIDA, http://caida.org/tools/measurement/cflowd.
[5] CAIDA, http://www.caida.org/tools/utilities/arts.
[6] KrCERT, http://www.krcert.or.kr/.
[7] Flowscan+, http://flowscan.kreonet2.net/.
[8] Arno Wagner, Thomas Dübendorfer, ETH Zürich, "DDoS Attack Detection based on Netflow Logs, Feb., 2003.
[9] K. J. Houle, G. M. Weaver, CERT, "Trends in Denial of Service Attack Technology," http://www.cert.org/archive/pdf/DoS_trends.pdf, Oct., 2001.
[10] 정재훈, 이승윤, 김용진, 인터넷 트래픽 수동적 측정 도구 Cflowd의 설치 및 설정 방법, 2001.
[11] 정현철, 변대용, KISA, "트래픽 분석을 통한 서비스거부공격 추적", http://www.kisa.or.kr, Jan., 2003.

이 명 선

e-mail : mslee@kisti.re.kr
1982년 아주대학교 전자공학과(공학사)
1996년 한남대학교 대학원 컴퓨터공학과 (공학석사)
2001년~현재 한남대학교 대학원 컴퓨터 공학과 박사과정 수료
1983년~1992년 시스템공학연구소 선임연구원
1993년~2000년 연구개발정보센터 연구전산망 실장
2001년~현재 한국과학기술정보연구원 슈퍼컴퓨팅센터 책임연구원
관심분야 : 컴퓨터시스템 & 네트워크, 정보통신보안

이 재 광

e-mail : jklee@netwk.hannam.ac.kr
1984년 광운대학교 전자계산학과(학사)
1986년 광운대학교 대학원 전자계산학과 (석사)
1993년 광운대학교 대학원 전자계산학과 (박사)
1986년~1993년 군산전문대학 전자계산 학과 부교수
1997년~1998년 University of Alabama 객원교수
1993년~현재 한남대학교 컴퓨터공학과 교수
관심분야 : 컴퓨터 네트워크, 정보통신, 정보보호