Journal of Korea Multimedia Society Vol. 10, No. 8, August 2007(pp. 1052-1059)

통합 관리를 위한 정책 기반의 보안시스템 설계 및 구현

김용탁[†], 권오준[††], 이종민[†††], 김태석[††††]

요 약

현재 대규모 네트워크상에서 사용되는 네트워크 보안시스템은 자기도메인만을 보호하는 개별 보안시스템으로 구성되어있다. 개별 보안시스템의 문제점은 백본 네트워크를 보호할 수 없고, 체계적이며 실시간적인 대응이 힘들다는 것이다. 이 문제 해결을 위해 본 논문에서는 백본 네트워크의 접속점에 존재하는 라우터와 액세스포인터에 보안 기능을 추가한 보안시스템을 설계하였다. 제안한 보안시스템은 침입을 탐지하여 통합보안 관리시스템에 경보메시지를 보낸다. 통합보안 관리시스템에서 경보메시지의 내용을 분석하여 대응방안을 마련하고, 각 보안시스템에 배포함으로서 체계적이고, 즉각적인 대응을 할 수 있다. 본 논문에서는 제안한 보안시스템과 통합보안 관리시스템을 네트워크 시뮬레이션을 사용해 모델링하고, 기능 검증 및 성능을 분석하였다. 그 결과 체계적이고, 즉각적인 대응을 할 수 있는 통합 보안 관리시스템임을 확인 할 수 있었다.

Implementation and Design of Policy Based Security System for Integration Management

Yong-Tak Kim[†], Oh-Jun Kwon[††], JongMin Lee[†††], Tai-Suk Kim[††††]

ABSTRACT

Network security system used in the large scale network composes individual security system which protects only own domain. Problems of individual security system are not to protect the backbone network and to be hard to cope with in real-time. In this paper we proposed a security system which includes security function at the router, and the access point, which exist at the backbone network, to solve the problems. This security system sends the alert messages to an integrated security management system after detecting intrusions. The integrated security management system releases confrontation plan to each security system. Thus the systematic and immediate confrontation is possible. We analyzed function verification and efficiency by using the security system and the integrated security management system suggested in this paper. We confirmed this integrated security management system has a possibility of a systematic and immediate confrontation.

Key words: Intrusion Prevention System(침입방지시스템), Intrusion Detection System(침입탐지시스템), Firewall(방화벽), Security System(보안시스템)

※ 교신저자(Corresponding Author) : 권오준, 주소 : 부산시 부산진구 엄광로 995(614-714), 전화 : 051)890-1725, FAX : 051)890-1724, E-mail : ojkwon@deu.ac.kr
접수일 : 2007년 3월 6일, 완료일 : 2007년 7월 2일
[†] 준회원, (주)이지서티
(E-mail :ytkim@easycerti.com)
[††] 종신회원, 동의대학교 컴퓨터소프트웨어공학과
[†††] 정회원, 동의대학교 컴퓨터소프트웨어공학과
(E-mail : jongmin@deu.ac.kr)
[††††] 종신회원, 동의대학교 컴퓨터소프트웨어공학과
(E-mail : tskim@deu.ac.kr)
※ 이 논문은 2006년도 동의대학교 교내연구비(2006AA166)에 의하여 연구되었음.

1. 서 론

정보 통신 기술의 급속한 발전은 현대인의 삶 속에서 인터넷이 차지하는 비중을 증대시키고 있다. 이들은 각종 서비스를 지원하게 되었고, 이를 이용한 우리 사회는 새로운 정보화 사회로 빠르게 전환되고 있다. 그러나 이와 더불어 역기능인 정보시스템의 침해사고 및 네트워크 침해사고가 급증하고 있다. 이 때문에 우리 사회는 정보 보호의 필요성을 인식하고, 이를 보호할 수 있는 시스템들이 시장에 나오게 되었다[1].

현재 시장에서 상용화된 보안 시스템은 침입차단 시스템(Firewall), 침입탐지시스템(IDS: Intrusion Detection System), 가상 사설망(VPN: Virtual Private Network), 침입방지시스템(IPS: Intrusion Prevention System) 등이 있다. 하지만 침입의 유형이 매우 다양화 되면서, 보안시스템은 실시간 탐지를 통한 침해 대응이 어려워지고 있다. 그리고 개별 보안시스템 중심의 네트워크에서 보안 관리의 어려움이 중요한 문제로 대두되고 있다[2].

이 문제를 해결하기 위해 본 논문에서는 유·무선 네트워크로 유입되는 불법적인 침입 및 이상 징후를 보안 시스템에서 탐지하고, 경고 메시지를 알려 대응할 수 있도록 체계적인 정책기반 관리 모델의 통합보안 관리시스템을 설계하였다[3-6].

보안 시스템은 Snort를 이용한 침입탐지 모듈과 탐지된 패킷을 규칙과 비교하여 차단하는 모듈로 나누어 설계하였다. 규칙은 정규화 표현식으로 구현하였으며, 일반 로그들은 데이터베이스에 저장되도록 하였다[7-9].

보안 시스템 및 통합보안 관리시스템의 모듈 검증을 위해 네트워크 시뮬레이터를 사용하였다. 테스트 환경은 유·무선 네트워크로 모델링하였으며, 접속점이 되는 노드에 보안기능을 가진 에이전트를 설정하여 기능 검증하였다. 본 논문에서는 알려지지 않은 공격 대신 할 수 있는 공격으로 분산 서비스 거부 공격(DDoS : Distributed Denial of Service)을 구현하였다. 분산 서비스거부 공격은 해커가 서비스 공격을 위한 도구들을 여러 노드에 심어놓고, 공격대상노드의 시스템이 처리할 수 없는 엄청난 분량의 패킷을 동시에 범람시켜 네트워크의 성능 저하나 시스템 마비시킨다.

본 논문에서 분산 서비스거부 공격을 사용하여 제안한 보안시스템과 통합보안 관리시스템의 기능을 검증하고, 알려지지 않은 공격에 대한 일반 보안시스템 환경과 제안 보안시스템이 설정된 환경에서의 성능을 비교 분석하였다[10-11].

본 논문의 구성은 다음과 같다. 2장에서 관련 연구에 대해 기술하고, 3장에서 보안 시스템모델링 및 설계에 대해 기술한다. 4장에서는 통합보안 관리시스템의 구성 요소에 대해 기능 검증 을 한다. 5장에서는 네트워크 시뮬레이터를 사용하여 제안 모델과 일반 모델의 네트워크 트래픽 성능을 비교 분석을 한다. 끝으로 6장에서 결론을 기술한다.

2. 관련 연구

2.1 침입탐지시스템(IDS: Intrusion Detection System)

침입탐지시스템은 기존에 발생했던 공격 패턴을 탐지하는 것으로 이전에 발생했던 다양한 공격유형 및 웜 바이러스, 서비스거부공격, 취약점 스캔 등을 탐지할 수 있는 장점을 가진다. 본 논문에서도 침입탐지시스템의 기본 모델이 되는 Snort 기본 메커니즘을 사용하였다. 그림 1은 Snort의 구조를 보여주고 있다.

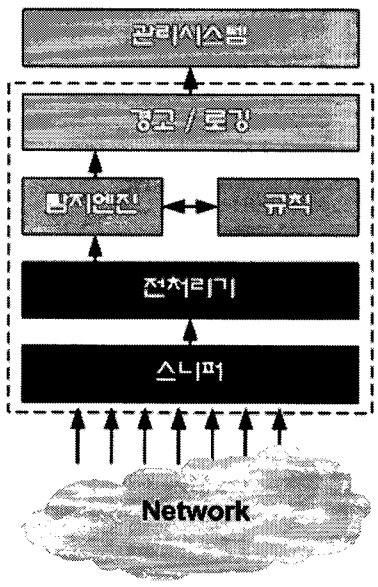

그림 1. Snort 구조

Snort은 스니퍼 기능을 사용하여 네트워크를 도청할 수 있다. 네트워크 스니퍼를 사용하면 어플리케이션 또는 하드웨어 장치에서 네트워크의 트래픽을 볼 수 있다. 인터넷의 대부분은 IP 트래픽이라 할 수 있다. 전처리기는 원본 패킷을 받아들여서 특정한 플러그-인으로 그 패킷을 보낸다. 이들 플러그-인은 패킷에서 특정한 종류의 행위를 찾는다. 패킷의 특정한 종류의 '행위'를 찾으면 그 패킷은 탐지 엔진으로 전송된다. 탐지 엔진은 전처리기와 플러그-인으로부터 오는 데이터를 받아서 여러 규칙과 비교한다. 만약 패킷과 일치하는 규칙이 있다면 그 패킷은 경고 처리기로 전달한다.

패킷에 대한 처리 방법에 대해서는 각 패킷에 대한 행동을 결정하는 데이터가 있어야 한다. Snort에서는 데이터베이스를 사용하여 특정 패킷에 대하여 규칙을 정의하였다. 표 1과 같이 규칙헤더와 규칙옵션으로 구성된다.

규칙헤더는 기본적으로 취할 행동(로그 또는 경고), 네트워크 패킷의 종류(TCP, UDP, ICMP 등), 출발지와 목적지 IP주소, 포트 등으로 이루어진다.

표 1. 규칙 헤더와 옵션 구조

RuleHeader		
Name	Description	
no	규칙 번호	
proto_no	프로토콜 번호	
name	프로토콜 명시	
action	이 패킷에 대한 행동 결정	
srcAddr	송신자 IP주소	
RuleHeader		
srcPort	송신자 포트번호	
destAddr	목적지 IP 주소	
destPort	목적지 포트번호	
flag	규칙 옵션 수행여부 결정	
Rule Option		
Type	Name	Description
TCP	tcp_falgs	SYN, FIN, ACK
	tcp_seq	시퀀스 번호
	tcp_ack	ACK의 번호
ICMP	icmp_type	메시지 형태
	icmp_code	메시지 코드
	icmp_id	메시지 ID
	icmp_seq	메시지 번호

규칙 옵션은 패킷이 규칙과 일치하기 위해 포함해야 하는 내용이다. IDS는 기본적으로 규칙 문법을 가지고 있으며, 규칙은 종류별로 묶여 정기적으로 갱신이 된다.

2.2 침입차단시스템(Firewall)

침입차단시스템의 기본 목표는 네트워크 사용자에게 가능한 투명성을 보장하면서 위협으로부터 보호해 줄 수 있는 보안 대책을 제공하는 것이다. 침입차단시스템은 외부네트워크와 내부 네트워크 사이의 트래픽을 제어하기 위해 구성된 시스템이다.

현재 방화벽의 작동원리는 크게 패킷 필터링구조와 서킷 레벨 방화벽으로 구분되어진다. 패킷 필터링은 OSI의 4 Layer에서 네트워크 패킷을 감시하는 방화벽 기술이다. 패킷의 방향성과 패킷의 IP나 TCP헤더에 있는 정보를 보고, 정해진 규칙에 의해 허용된다. 그림 2는 패킷 필터링 기반의 방화벽 구조이다.

서킷 레벨 방화벽은 상호 L4 계층 간에 연결에 대한 요청이나 데이터 패킷에 대한 인증을 해 주는 기능을 가지고 있다. 따라서 서킷 레벨 방화벽은 인가된 연결 설정인가를 조사하여 이 과정이 끝나기 전에는 데이터 패킷의 전송이 이루어지지 않도록 하는 것이다. 방화벽은 인가된 연결 테이블을 가지고 있고, 패킷이 테이블에 저장된 내용을 가지고 있을 경우에만 전송을 허용한다. 연결이 종료될 경우 테이블에서도 삭제가 된다.

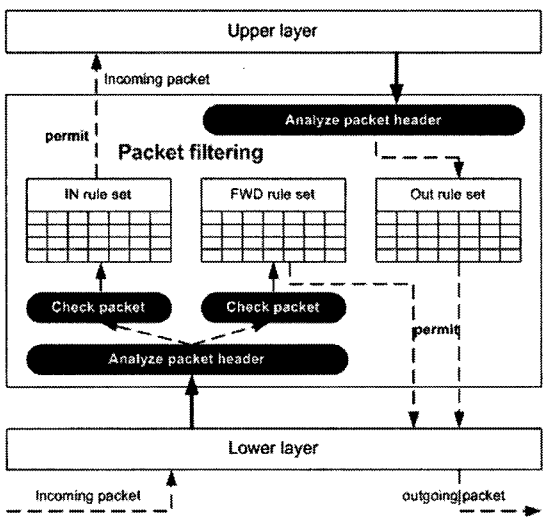

그림 2. 패킷 필터링 기반의 방화벽 구조

3. 제안 보안 시스템들 설계

본 논문에서 제안한 시스템은 크게 보안시스템과 통합보안 관리시스템으로 구분하고 있다. 그림 3은 일반 네트워크 접속점에 위치한 라우터와 액세스 포인터에 보안 기능을 추가한 시스템으로 설계된 보안 시스템들이다. 보안 시스템들은 이상 징후를 탐지하여 경보메시지를 통합보안 관리시스템에 전달한다. 통합 보안 관리시스템은 이상 징후를 분석하여 대응 정책을 보안 시스템들에게 전달하여 더 이상 백본 네트워크에 영향을 주지 않도록 설계하였다. 그림 3은 제안 시스템들의 전체 구성 개념도를 나타낸 것이다.

그림 3에서 설명한 유선 네트워크상의 제안한 라우터는 라우터의 기본 기능과 패킷 필터링 기능, 침입 탐지 및 차단기능을 가지고 있으며, 보안 라우터(SRS : Security Router Syetem) 라 명한다. 그림 4는 보안 라우터의 기본 구조를 나타낸 것이다.

그림 4의 보안 라우터의 기능은 다음과 같다. Packet Forwarding은 IP 패킷을 다음 노드로 전달

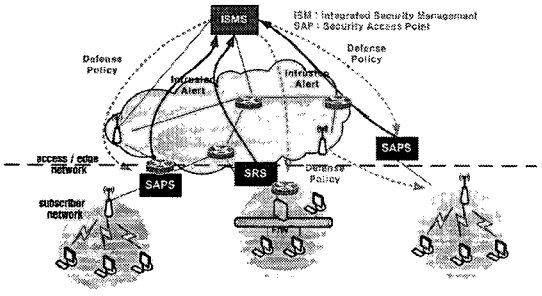

그림 3. 통합보안 관리시스템 전체구성도

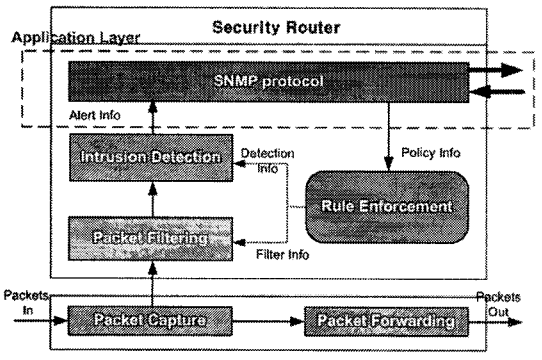

그림 4. 보안라우터의 구조

하는 목적을 가진다. Packet Capture는 패킷을 가로채는 기능을 가지고 있으며, Packet Filtering은 패킷의 흐름을 차단하기 위해 만든 모듈이다. Rule Enforcement에서는 ISMS (Integration Security Manager System)에게 정책을 배포 받아 패킷 필터링과 침입 탐지에 대한 차단을 한다. Intrusion Detection는 Filtering으로부터 전달 받은 패킷의 유해 여부를 판단하여 통합관리 보안시스템에 SNMP을 사용해서 경보 정보를 보낸다.

무선 네트워크상의 접속점으로 사용되는 보안 액세스포인트 시스템도 보안 라우터시스템과 같은 구조를 가진다. 그림 5는 보안 액세스포인터 시스템의 기본구조를 설계한 것이다.

NAT는 L3의 보안 구성을 위해 필요하며, 내부 네트워크에서 외부 네트워크로 유해패킷이 전송될 경우 일차적으로 필터링을 해 줌으로서 보안성을 높이고 있다. 통합보안 관리시스템은 보안 관리자가 직접 관리하는 모델이다. 세부적인 정책설정 과정이나 인위적인 다른 조치가 보안 사고의 처리에 개입 될 필요가 있는 경우에 대해 사용할 수 있도록 설계하였다. 그림 6은 통합보안 관리시스템의 기본구조를 나타낸 것이다.

통합보안 관리시스템은 경보 메시지를 보안 관리자에게 알리며, 보안 관리자는 경보 메시지의 로그 패턴을 분석하여 적절한 대응 정책을 수립하여 보안 정책을 만들게 된다. 통합보안 관리시스템은 보안 정책을 보안 시스템들에게 정책메시지를 통해 전달하게 된다. Alert Analyzer는 보안 시스템들로부터 받은 경보 정보를 Alert-Table에 저장한 후, 전체 네트워크의 현 상태를 확인하고, 로그를 통해 침입이 있

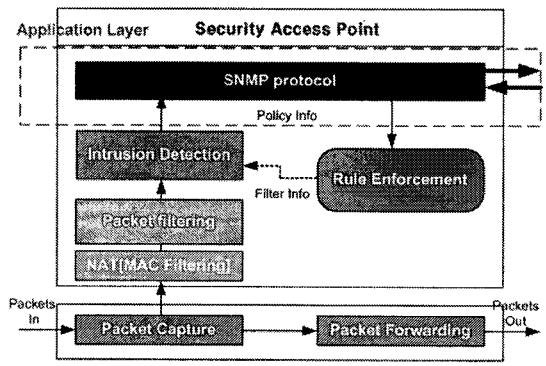

그림 5. 보안 액세스 포인트 구조

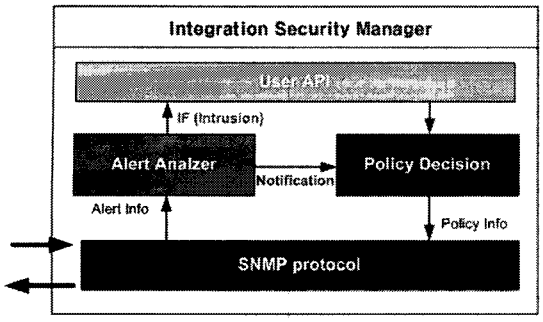

그림 6. 통합보안 관리시스템의 구조

는지를 판단할 수 있도록 관리자에게 전달하게 된다. 만약 침입이라고 판단되면, 보안 관리자들에 의해 Policy Decision에서 정책을 결정하게 된다. Policy Decision은 보안 에이전트와 통신을 통해 보안 에이전트에 보안 정책을 전달한다. 또한 보안 에이전트로부터 정책 요구를 받으면 그 보안 에이전트에 해당하는 Filtering 정보나 Detection 정보를 찾아서 정책을 전달한다.

4. 제안 보안시스템들 구현

4.1 시뮬레이션 환경

통합보안 관리시스템과 보안시스템들의 테스트 환경은 네트워크 시뮬레이션인 NS-2를 사용하여 그림 7과 같은 네트워크 형태로 구성하였다. 그림 7은 유선 네트워크와 무선 네트워크로 구성되어 있으며, 일반 보안 시스템인 IDS 에이전트와 제안 보안시스템을 설치하여 성능을 비교할 수 있도록 구성하였다. NS-2 시뮬레이션은 라우터와 호스트의 구분이 없고, 하나의 부모 노드 클래스를 상속받아 제안 보안시스템 첨부하여 구현하였다. 본 논문에서는 제안 보안시스템의 기능 및 성능과 일반 보안시스템과 비교하여 성능을 분석하였다. 시나리오 구성은 4.2절의 방법으로 검증하였다.

4.2 제안 보안 시스템 검증 방법

그림 8은 본 논문에서 제안한 보안 시스템을 설치하여 통합 관리 할 수 있도록 검증하기 위한 시뮬레이션 환경을 나타낸 것이다.

시나리오 구성은 DDoS의 공격 유형 중 하나인 Smurf 공격을 통해 제안 보안 시스템과 일반 보안시

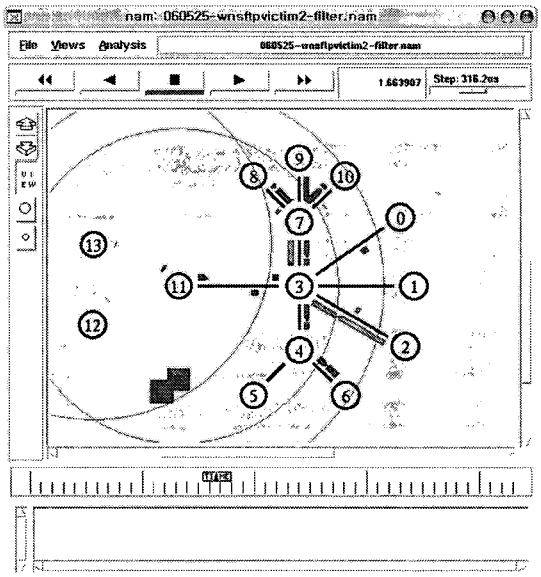

그림 7. NS-2 시뮬레이션 환경

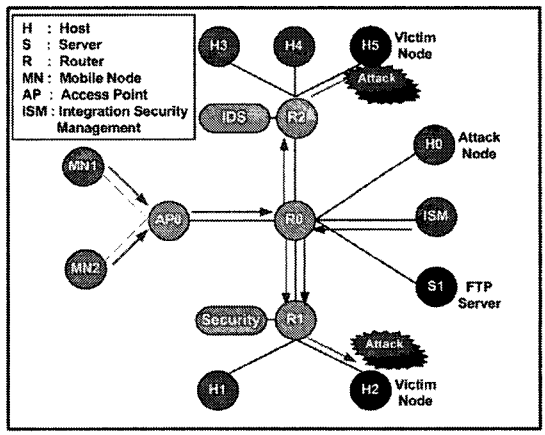

그림 8. 시나리오 구성도

스템의 보안성 검증을 하였다. 일반 보안 시스템의 경우, Smurf 공격에 대한 대응책이 없다고 가정한다. 공격 노드인 H0는 해킹을 통해 MN1, MN2의 시스템 내에 Daemon을 설치하였다. 희생노드인 H2와 H5는 S1로부터 파일 서비스를 받는다. H2가 속한 네트워크의 R1 라우터에는 보안 에이전트가 설치된 상태이며, 무선 네트워크 AP0에도 보안 에이전트를 설치하였다. H5는 IP 헤더의 Source IP 주소를 공격하고자 하는 Target IP로 변경한 다음 IP 헤더 뒤에 ICMP 메시지를 붙여서 ICMP Ping Request를 Daemon에 전송하게 된다. ICMP Ping Request를 받은 Daemon

이 설치된 노드는 ICMP Ping Reply를 희생 노드에 되돌려 보낸다. 본 논문에서는 ICMP 메시지의 사이즈를 조작하여 희생노드의 FTP 와 CBR 서비스를 방해했다.

5. 성능 분석

본 논문에서 제안한 통합보안 관리시스템과 일반 보안 시스템에 대해 성능 분석하였다. 그림 9는 NS-2 시뮬레이션을 통해 검증에 필요한 환경 변수를 나타낸 것이다.

모든 노드의 링크 특성은 양방향 링크(Duplex-Link)로 연결하였으며, 전송 지연 시간은 10ms로 설정하였다. 그리고 Smurf 공격인 ICMP Redirect에 사용되는 Ping 패킷 사이즈를 1024byte로 생성하여 전송한다. 패킷이 저장되는 큐의 형태는 Drop Tail 방식을 채택 하였고, 패킷 전송 간격 시간은 0.05 sec로 하였다. 전송 계층 프로토콜은 TCP를 사용하였고, 응용 계층의 프로토콜은 FTP를 사용하였다. FTP의 서비스는 1.0초에서 시작하여 5.0초까지 트래픽을 전송하며, ICMP redirect 공격은 1.5초가 지나면 공격 노드에서 Daemon에 패킷을 전송하여 각 희생노드에 공격을 하도록 구성하였다.

그림 10은 일반 보안시스템이 설치된 경우이며, H0에서 Smurf 공격을 가할 경우, 대응할 수 없는 보안시스템이다. 이와 같이 알려지지 않은 공격이나 이상 징후에 따른 대응을 할 수 없는 일반 보안시스템인 경우를 가정하였다. H0에서는 Smurf 공격을 통해 Daemon 프로그램이 설치된 MN1과 MN2에 공격 패킷을 전송하였다. 그리고 H5는 S1으로부터 CBR 트래픽과 FTP 트래픽을 받고 있고 있다. 이때 희생노드의 수신된 패킷의 수를 나타낸 것이다.

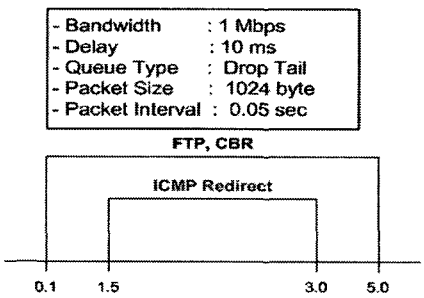

그림 9. 시뮬레이션에 대한 환경 변수

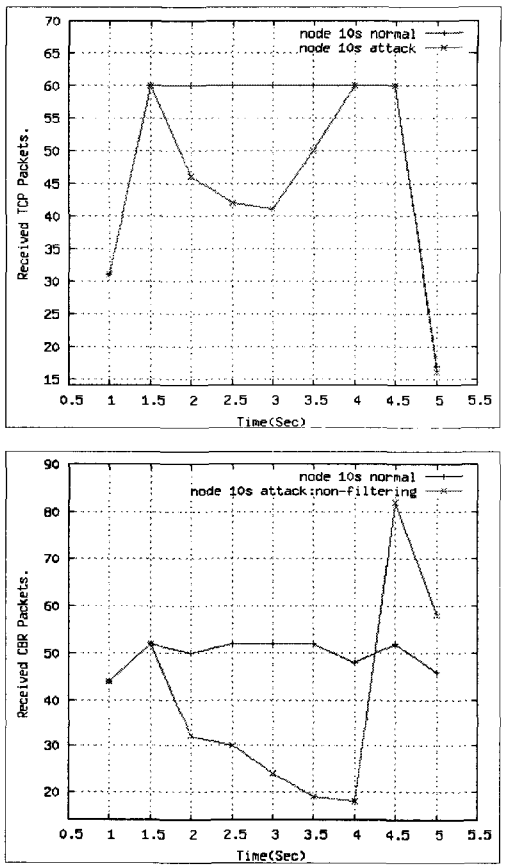

그림 10. 일반 보안시스템이 적용된 H5의 패킷 수신율

그림 10의 왼쪽은 FTP 서비스에 따른 패킷 수신율을 나타낸 것이고, 오른쪽은 CBR 트래픽의 패킷 수신율을 나타낸 것이다. 각 그래프는 정상적인 패킷의 수신율과 ICMP redirect 공격을 했을 때의 수신된 패킷 수를 나타낸 것이다. 그림 10의 각 그래프는 1초에서 1.5초 사이 두 수신 패킷수가 일치하는 것을 알 수 있다. 실제 1.5초에서 4.5초 사이의 패킷수가 최대 수신 패킷 수이다. FTP 트래픽과 CBR 트래픽은 1.0초에서 생성하여 5.0초까지 계속 서비스를 하였다. 1.5초에서 갑자기 패킷의 수가 감소된 것은 공격 노드에서 ICMP redirect 공격을 통해 패킷을 수신하는 노드가 공격을 받기 때문이다. 1.5초에서 3.0초까지 0.05초 간격으로 공격 패킷을 전송하였다. 이 경우 희생 노드는 정상적인 FTP 서비스를 받을 수 없다는 것을 그림 10의 attack 선을 통해 확인 할 수 있다. 특히 2.5초에서 4.0초까지 패킷 수신율은 Ping 공격으로 인해 정상적인 패킷을 수신할 수 없으며, 급속

한 네트워크 성능 저하가 온 것을 그림 10을 통해 알 수 있다.

그림 11은 제안한 보안 시스템을 적용했을 때 수신된 패킷의 수를 나타낸 것이다. H0에서는 Smurf 공격을 통해 Daemon 프로그램이 설치된 M1와 M2에 공격 패킷을 전송하였다. 그리고 H2는 S1으로부터 CBR 트래픽과 FTP 트래픽을 받고 있고 있다. S1 노드에서 H2 노드로 1.0초에서 5.0초까지 FTP 트래픽과 CBR 트래픽을 전송하였다. H0의 Smruf 공격을1.5초에서 3.0초까지 0.05초 간격으로 MN1과 MN2에게 전송하였다. 이 경우, 제안한 보안 시스템에서는 공격 패킷을 감지하여 ISM 노드에 경보메시지를 전송하게 된다. 경보 메시지를 전송 받은 ISM은 정책 메시지를 전송하여 제안한 보안시스템이 공격 패킷을 차단하도록 메시지를 전송하게 된다. 그림 11의 1.5초에서 2초사이의 공격 패킷에 의해 왼쪽의 FTP 트래픽의 수신된 패킷 수와 왼쪽의 CBR 트래픽의 수신된 패킷 수가 감소된 것을 알 수 있다.

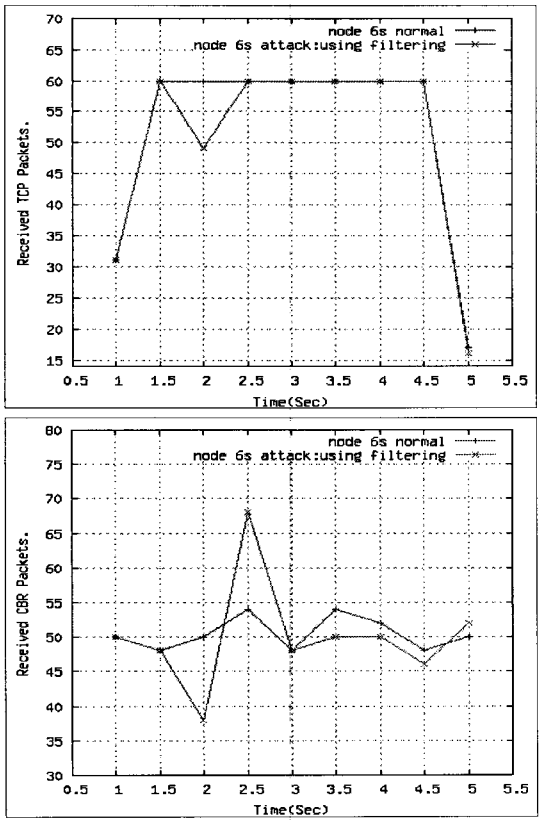

그림 11. 제안 보안 시스템이 적용된 H2의 패킷 수신율

하지만 2.5초에서 보안 정책이 적용된 후 정상적인 패킷의 수가 수신된 것을 그림 11을 통해 알 수 있다.

본 논문에서 제안한 보안 시스템은 알려지지 않은 공격의 경우, 일반 보안 시스템과는 달리 효과적인 대응을 할 수 있다는 것을 성능 분석을 통해 확인할 수 있었다.

6. 결 론

현재 대부분의 개별 보안시스템의 경우, 네트워크 접속점에 위치하여 자기 도메인에 대한 보안만을 담당하기 때문에 2003년 1.25 인터넷 대란에서 나타난 백본 네트워크를 보호할 수 없는 단점을 가지고 있다.

본 논문에서는 유·무선 네트워크에서 사용되고 있는 네트워크 장비에 보안 기능을 추가하였다. 그리고 추가된 보안 기능을 가진 보안시스템과 통합보안 관리시스템이 실시간 통신을 통해 침해에 대응할 수 있도록 설계하였다. 보안 시스템과 통합보안 관리시스템의 기능 검증을 위해 네트워크 시뮬레이터인 NS-2를 사용하였다. 실 네트워크와 유사한 환경을 모델링하기 위해 공격 패턴을 분석하여 분산 서비스 거부 공격인 ICMP Redirect 공격을 구현하였다.

검증 결과 제안한 보안 시스템의 모듈이 침해를 탐지하고, 경보 메시지를 통합보안 관리시스템에 전달하였다. 통합보안 관리시스템에서 침해에 따른 대응정책을 각 시스템에 배포함으로서 이후 계속적인 침해에 대응할 수 있었다.

본 논문에서 제안한 보안 시스템을 실 네트워크에 적용할 경우, 알려지지 않은 공격의 확산을 보다 체계적이고, 효과적으로 차단할 수 있는 장점을 가지고 있으며, 가장 중용한 것은 백본 네트워크의 안전성을 높일 수 있을 것으로 기대된다.

참 고 문 헌

[1] 전자통신연구소 기술정보센터, "인터넷 침입차단 시스템의 기술 및 시장 동향," 주간기술동향 통권 891호 1994.

[2] 다이구지 이사오 외 편저, "통신 네트워크 시큐리티," 도서출판 동서, 1998.

[3] S.Kumar and E.Spafford, "A pattern -matching model for misuse intrusion detection," *National Computer Security Conference*, Vol. 17 pp. 11-21, 1994.
[4] Paul Reeder, "Intrusion Detection, the next generation," *IEEE*, 2001.
[5] Biswanath Mukherjee, L.Told Heberlein, and Karl N. Levitt, "Network Intrusion Detection," *IEEE*, 1994.
[6] James H. Cowie, Editor "Scalable Simulation Framework API Reference Manual," *version 1.0, Documentation draft*, 1999.
[7] Paul Reeder, "Intrusion Detection, the next generation," *IEEE*, 2001.
[8] R. Durst, T.Champion, B. Witten, E. Miller, and L. Spagnuolo. "Testing and Eva-luating Computer Intrusion Detection System." *CACM*, Vol. 7, No. 42, pp. 53-61, 1999.
[9] Jae-Hyuk Lee, Eul Gyu Im, Joo Beom Yun, and Seung-Kyu Park, "Network Intrusion and defense simulation framework based on SSFNet," *International Conference*, Vol. 1, No. 6, 2004.
[10] 이영석 , 나중찬 "통합 보안 관리를 위한 이기종 보안 시스템 연동" 한국정보보호학회지 정보보호학회지, Vol. 13, No. 1, 2003.
[11] 최현희, 정태명 "통합보안관리시스템을 위한 보안정책 일반화에 관한 연구" 한국 정보처리학회논문지C, Vol. 9, No. 6, 2002.

김 용 탁

1998년 동의대학교 공과대학 컴퓨터공학과 학사
2003년 동의대학교 공과대학 컴퓨터공학과 석사
2006년 동의대학교 공과대학 컴퓨터응용공학과 박사수료
관심분야 : 모바일 프로토콜, 무선 네트워크, 네트워크 보안, 인터넷 QoS

권 오 준

1986년 경북대학교 전자공학과 (공학사)
1992년 충남대학교 전산학과 (이학석사)
1998년 포항공대 전자계산학과 (공학박사)
1986년~2002년 한국전자통신연구원 선임연구원
2000년~2002년 동의대학교 전산통계학과
2002년~현재 동의대학교 컴퓨터소프트웨어공학과 부교수
관심분야 : 컴퓨터네트워크, 정보보호, 인공신경망

이 종 민

1992년 경북대학교 컴퓨터공학과(공학사)
1994년 한국과학기술원 전산학과(공학석사)
2000년 한국과학기술원 전자전산학과(공학박사)
1997년~2002년 삼성전자 무선사업부 책임연구원
2005년 University of California at Santa Cruz, Research Associate
2002년~현재 동의대학교 컴퓨터소프트웨어공학과 조교수
관심분야 : 모바일 컴퓨팅, 라우팅, 센서 네트워크

김 태 석

1992년 일본 KEIO대학 이공학부 계산기과학전공 졸업
1992년 일본 KEIO대학 이공학부 객원연구원
1993년~현재 동의대학교 컴퓨터소프트웨어공학과 교수
2000년~2003년 동의대학교 전산정보원장
2000년~2003년 (재)부산테크노파크 운영위원
2003년~2005년 동의대학교 교무처장
관심분야 : 인터넷응용, 원격강의, 자연어처리