通信情報保護學會論文誌
第 10 券 第 4 號, 2000. 12

네트워크 상에서의 침입차단시스템 영향력 분석

정 선 이*, 박 정 은*, 유 수 연*, 장 성 은*, 채 기 준*, 노 병 규**

Analysis on Effects of The Firewall on Networks

Sunnie Chung*, Jeong-eun Park*, Soo-yeon Yoo*,
Sung-eun Jang*, Ki-joon Chae*, Byung-gyu No**

요 약

정보유출, 파괴, 위·변조, 바이러스와 같은 정보화 역기능으로부터 정보시스템과 통신망을 보호하기 위하여 침입차단시스템에 대한 요구가 증대되고 있다. 실제로 침입차단시스템을 사용하기 위해서는 그것이 네트워크에 미치는 영향에 대해서 보안 관리자가 알고 분석할 수 있어야 한다. 그러나 현재 침입차단시스템의 성능에 대해서 의문을 갖게 될 때 이를 평가할 수 있는 마땅한 도구가 없기에 침입차단시스템이 네트워크에 미치는 영향에 대한 연구가 필요하다. 본 논문에서는 침입차단시스템이 네트워크에 미치는 영향을 파악하기 위하여 실제 네트워크에 다양한 트래픽을 적용해 봄으로써 분석하였다. 또한 COMNET-III를 이용하여 침입차단시스템이 없는 경우와 있는 경우의 네트워크를 모델링하여 다양한 침입차단시스템의 운영환경 및 네트워크 환경 변화에 따른 영향을 분석하였다.

ABSTRACT

The Firewall is needed in order to protect communication networks from ill effects of informatization such as information leakage, destruction, forgery and virus. To take an advantage of the firewall, the security manager must understand the effects that it can have on the network. There are, however, no tools available to evaluate the performance of the firewall. In this paper, we study the effect of the firewall by putting various kinds of traffic into the actual network. Also, using COMNET-III, we model two networks with and without the firewall. And we analyze the effects under the various network environments.

keyword : *Firewall, Performance, network, modeling, evaluation*

Ⅰ. 서 론

급변하는 정보화 사회에서 컴퓨터 사용이 증가하면서 네트워크를 이용한 정보교환이 증가함에 따라 그 정보전달 속도와 신뢰성이 점점 더 중요해 지고 있다. 그러나 이러한 정보통신 기술의 발달과 급속한 정보화는 정보유출, 파괴, 위·변조, 바이러스, 서비스 방해, 불건전 정보 유통, 해킹 등의 컴퓨터 범죄 등과 같은 정보화 역기능을 확산시키는 계기가 되었다. 따라서 이러한 정보화 역기능으로부터 정보시스템과 통신망을 보호하고, 정보 자원에 대한 각종 위협이 존재하는 정보통신 환경에서 야기되는 여러 문제점들을 예방할 수 있는 침입차단시스템이 요구되고 있다.

* 이화여대 컴퓨터학과
** 한국정보보호센터

실제로 침입차단시스템을 사용하기 위해서는 그것이 네트워크에 미치는 영향에 대해서 보안 관리자가 알아야 하고 분석할 수 있어야 한다. 또한, 침입차단시스템을 설치했을 때 네트워크의 성능이 저하된 경우 그 원인이 네트워크 자체에 있는지 혹은 침입차단시스템에 있는지를 파악할 수 있어야 한다. 그러나 현재까지는 침입차단시스템 자체에 대한 개념 소개나 침입차단의 정확도, 침입차단시스템 자체에 대한 성능 평가에 대한 연구가 대부분이었다[1]. 즉, 침입차단시스템이 네트워크에 미치는 영향에 대한 의문을 갖게 될 때 이를 평가할 수 있는 마땅한 도구가 없기에 본 연구는 필요하다.

본 연구에서는 침입차단시스템이 네트워크에 미치는 영향을 파악하기 위해 먼저 실제 네트워크에 다양한 종류의 트래픽을 적용해본 후, 트래픽 종류에 따른 네트워크의 성능을 비교 분석하였다. 특히 네트워크에 장애가 발생하였을 때 그 장애 원인을 분석하였다. 그 다음에는 네트워크 모델링 도구인 COMNET-III를 사용하여 침입차단시스템이 설치된 경우와 그렇지 않은 경우를 모델링한 후, 그 결과를 분석하였다.

본 논문의 구성은 다음과 같다. 2장에서는 침입차단시스템에 대하여 소개하고, 3장에서는 본 논문에서 사용할 네트워크 분석툴들에 대해 소개한다. 4장에서는 실제 네트워크에 침입차단시스템을 설치하고 그것이 있을 때와 없을 때의 네트워크 상태를 트래픽별로 분석해 본다. 5장에서는 모델링된 네트워크 상에서 침입차단시스템이 미치는 영향을 비교 분석한다. 마지막으로 6장에서는 결론과 향후계획에 대해 기술한다.

II. 침입차단시스템 소개

2.1 정의

침입차단시스템(방화벽 혹은 firewall)은 외부로부터의 불법적인 접근이나 해커의 공격으로부터 내부 네트워크를 방어하기 위해 내부 인트라넷과 외부 인터넷 사이에 유일한 통로에 설치하여 두 네트워크간에 이루어지는 접근을 제어하는 장치이다. 침입차단시스템을 양방향 트래픽의 병목점에 설치함으로써 내부 네트워크의 취약한 부분이 외부에 노출될 위험을 감소시킬 수 있다. 침입차단시스템의 기본 목표는 네트워크 사용자에게 가능한 한 투명성을 보장하면서 위험 지대를 줄이고자 하는 적극적인 보안 대책을 제공하는 것이다[2~5].

2.2 필요성

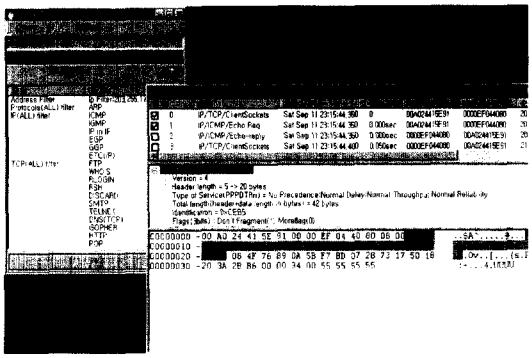
침입차단시스템이 없는 환경에서 네트워크의 보안은 전적으로 호스트 시스템의 보안에 의존하게 되는데, 이에 대한 책임은 네트워크에 연결된 모든 호스트가 일정하게 분담해야 한다. 그러므로 네트워크가 커질수록 보안의 통제는 매우 어려워진다. 이 때 방화벽을 사용함으로써 전체 네트워크의 보안 수준을 높이고 네트워크 공격에 적절히 대처할 수 있다. 침입차단시스템은 한 도메인 내의 네트워크 보안을 위한 최선의 해결책을 제공한다. 물론 침입차단시스템이 완전한 해결책이라고는 할 수 없지만, 가장 효과적이고 비교적 비용 적게드는 방법이다.

2.3 종류

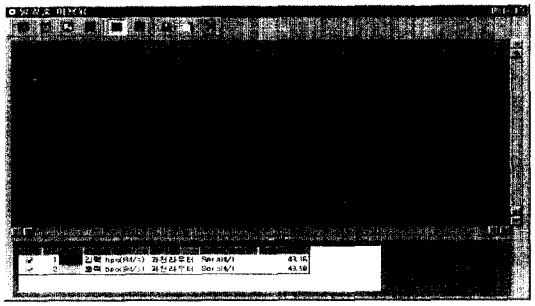
침입차단시스템은 크게 두 가지로 분류할 수 있다. 침입차단시스템이 사용하는 기술에 따라 분류할 수 있고, 침입차단시스템의 구성에 따라 분류할 수도 있다. 침입차단시스템을 사용하는 기술에 따라 분류하면 패킷 필터링 게이트웨이(Packet Filtering Gateway), 회로 레벨 게이트웨이(Circuit Level Gateway), 응용 게이트웨이(Application Gateway), 혼합형 게이트웨이(Hybrid Gateway), 상태정밀검사 방식(Stateful Packet Inspection)으로 분류할 수 있고[5], 구성에 따라 분류하면 스크리닝 라우터(Screening Router), 배스천 호스트(Bastion Host), 이중 네트워크(Dual Homed Hosts), 스크린 호스트 게이트웨이(Screen Host Gateway), 스크린 서브넷 게이트웨이(Screen Subnet Gateway)로 나눌 수 있다[6~10].

III. 네트워크 분석 툴과 시뮬레이션 툴 소개

3 장에서는 본 논문에서 사용한 네트워크 분석 툴과 시뮬레이션 툴에 대해 간단히 소개하고자 한다. 네트워크 분석 툴로는 e-Watch와 MonaLisa를 사용하였고, 시뮬레이션 툴로는 COMNET-III를 사용하였다. e-Watch는 트래픽을 모니터링하여 분석할 수 있게 해주는 소프트웨어이다. [그림 1]은 e-Watch를 통해 패킷을 수집한 그림이다. e-Watch에서는 그 외에도 패킷을 종류별로 만들어 네트워크를 통해 전송할 수 있다. 이 때 패킷의 종류 및 개수와 전송 시나리오를 선택할 수 있다. 트래픽을 모니터링한



〔그림 1〕 패킷 수집/분석의 예

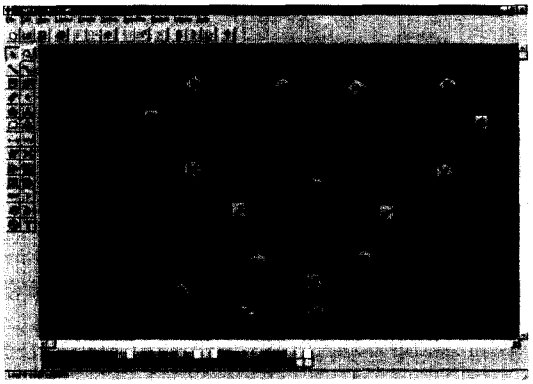


〔그림 2〕 일중 이용률의 예

결과는 프레임 분포율, 링크 사용효율, 장애율 등으로 표현되는데, 이 정보들은 실시간 그래프로 보여진다[11].

MonaLisa는 WAN/LAN으로 구성된 네트워크 장치 및 트래픽에 대한 감시 및 분석 기능이 있는 시스템이다. 분석하고자 하는 대상과 항목을 설정해주면 네트워크의 상황을 실시간 또는 주기적으로 분석한다. MonaLisa에서는 장애율 분석과 성능 분석을 수행할 수 있다. 장애율 분석항목에서는 전체기간 장애율, 일일중 장애율, 장애율 분포, 실시간 장애 정보를 제공한다. 이는 실시간 그래프나 보고서로 제공된다. 〔그림 2〕는 입출력 이용률을 동시에 보여주는 화면이다.

COMNET-Ⅲ는 CACI 사에서 개발한 네트워크 모델링 툴로서 설계한 네트워크에 대한 성능을 평가 및 분석할 수 있게 해주는 툴이다. COMNET-Ⅲ는 ATM, Frame Relay, TCP/IP, point-to-point, Token Ring, FDDI 등의 네트워킹 기술을 제공한다. 시뮬레이션은 입력받은 값을 가지고 수행된다. 이 때 애니메이션 기능을 설정해 줄 수 있어서 사용자들의 이해를 도울 수 있다. 결과는 로그파일과 실시간 그래프로 볼 수 있는데 이때 세부항목들은 설정가능하다. 〔그림 3〕에서는 COMNET-Ⅲ를 이용하여 모델링한 화면을 보여준다[12].



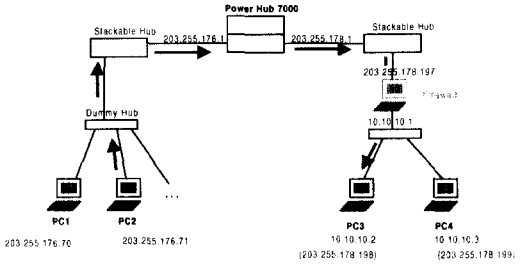
〔그림 3〕 COMNET-Ⅲ를 이용한 모델링의 예

Ⅳ. 실제 네트워크 성능 분석

이 장에서는 네트워크의 성능을 분석하기 위해 설정한 실제 네트워크에 여러 종류의 트래픽을 전송해 봄으로써 침입차단시스템이 설치되었을 때와 설치되지 않았을 때의 네트워크 상황을 비교 분석해 보았다. 이 때 전송한 트래픽은 크게 두 종류인데, 하나는 FTP 트래픽이고 다른 하나는 Telnet 트래픽이다. 이 두 종류의 트래픽은 패킷의 크기와 포트(port) 번호를 달리하여 구별하였는데, 패킷의 크기는 실제 전송되는 패킷을 수집하여 평균값을 도출한 값을 이용하였다. FTP 패킷의 경우는 최대 전송 단위(MTU)에 가까운 크기로 전송되고 Telnet 패킷의 경우는 매우 크기의 패킷이 전송됨을 확인할 수 있었다. 실제 네트워크의 대부분을 차지하는 HTTP 트래픽은 실제로 수집해본 결과 웹 콘텐트, 전송 방향, 패킷의 성격에 따라 그 크기가 매우 다양하였다. 따라서 HTTP 트래픽을 전송하였을 때의 성능은 FTP 트래픽과 Telnet 트래픽을 전송해본 결과로 커버할 수 있다고 판단되어 본 논문에서는 생략하였다.

4.1 환경설정

네트워크를 분석하기 위한 환경은 〔그림 4〕와 같이 Power Hub인 Fore7000에 연결되어 있는 203.255.176.1과 203.255.178.1의 두 개의 10BASE-T Ethernet 망으로 구성된다. 그 중 203.255.178.1에 연결된 PC3과 PC4는 침입차단시스템에 의해 보호된다. 이때 침입차단시스템에서는 NAT 기능이 있어 사설망 10.10.10.0으로 구성된 침입차단시스템 내부 네트워크가 외부로 나갈 때에는 공개주소로 변환되어 나가게 된다. PC3의 경우 침입차단시스템



〔그림 4〕 침입차단시스템 설치시 실제 네트워크 분석 환경

내부의 사설망에서의 주소는 10.10.10.2이지만 침입차단시스템 외부로 나갈 때에는 203.255.178.198이라는 공개 주소로 나간다. PC4의 경우도 마찬가지로 침입차단시스템 내부망에서는 10.10.10.3 주소를 가지고 있으며 외부로 나갈 때에는 203.255.178.199로 나간다. 송신자인 203.255.176.1의 PC2가 트래픽을 발생시키면 Fore7000을 통해 203.255.178.1의 침입차단시스템을 통해 수신자의 PC3으로 전송된다. 트래픽의 종류로는 FTP, TELNET, HTTP, FTP와 TELNET의 혼합 트래픽을 사용한다. 이때 203.255.176.1망과 203.255.178.1망에 어떤 영향을 미치는지 알아보고 Fore7000에 어떤 영향을 미치는지 알아보고자 한다. 네트워크 분석도구로는 e-Watch를 사용하였다.

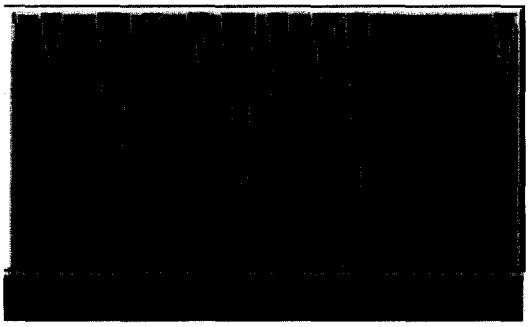
4.2 FTP 트래픽

FTP는 대역폭에 민감한 응용프로그램으로 처리율이 중요하다. 아래 성능 평가 테스트에서는 13Mbytes의 FTP 트래픽을 전송하였을 때, 처리율을 중심으로 침입차단시스템이 있는 경우와 없는 경우를 비교하였다. 테스트결과 침입차단시스템이 있는 경우에는 평균 2.5-3.0Mbytes의 전송률을 보인데 반해, 침입차단시스템이 없는 경우에는 5.6-6.0Mbytes로 높아 침입차단시스템이 없는 경우의 전송 속도가 더 빠름을 알 수 있었다. 침입차단시스템이 있는 경우에는 패킷 헤더를 검사해서 통과여부를 결정하므로 전송이 오래 걸린 것으로 분석된다.

4.2.1 상황판

e-Watch를 통해 실시간으로 사용률을 프레임/초, 바이트/초 값으로 각각 관찰할 수 있다. 〔그림 5〕와 〔그림 6〕은 203.255.176.71의 상황판으로 침입차단시스템이 있는 경우와 없는 경우의 사용률을 프레임/초, 바이트/초 단위로 관찰한 화면인데, 침입차

〔그림 5〕 침입차단시스템이 있는 경우



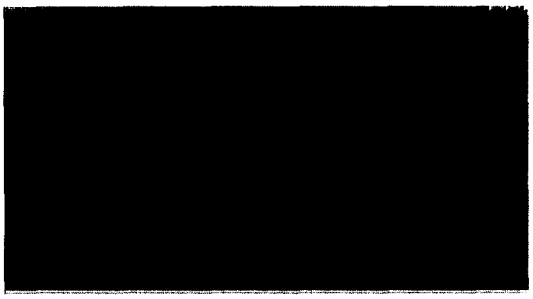
〔그림 6〕 침입차단시스템이 없는 경우

단시스템이 있는 경우의 사용률이 침입차단시스템이 없는 경우보다 낮아짐을 볼 수 있다. 이는 침입차단시스템이 지나가는 패킷들을 통과시켜도 되는 패킷인지 검사하기 위한 프로세싱을 하기 때문으로 볼 수 있다.

4.2.2 바이트/초

〔그림 7〕은 침입차단시스템이 있는 경우 203.255.176.71의 초당 전송된 바이트 수로써 〔그림 8〕의 침입차단시스템이 없는 경우보다 전송기간이 길고 전송률도 낮음을 보여준다. 침입차단시스템이 있는 경우에는 패킷 헤더 조사와 어플리케이션에 따른 침입차단시스템의 프로세싱으로 인하여 전송이 오래 걸린 것으로 분석된다.

〔그림 7〕 침입차단시스템이 있는 경우



〔그림 8〕 침입차단시스템이 없는 경우

4.2.3 복수 Collision

MonaLisa를 통해 복수 collision을 분석한 화면이다. 203.255.176.1에서의 복수 collision을 보면 〔그림 9〕는 침입차단시스템이 있는 경우로서 복수 collision이 40% 내외를 기록되는데 반해 침입차단시스템이 없는 경우인 〔그림 10〕은 복수 collision이 30% 내외를 기록한다. 침입차단시스템에서는 패킷 통과 여부를 결정하기 위해 프로세싱하는 시간이 걸리기 때문에 침입차단시스템으로 들어가기 위한 외부 네트워크 203.255.176.1에서의 collision이 높아졌다.

4.3 TELNET 트래픽

테스트를 위해 11개의 TELNET 접속이 이루어졌다. TELNET 패킷의 사이즈는 64 bytes이다.

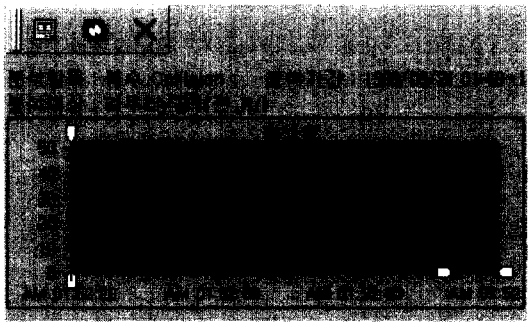
〔그림 11〕과 〔그림 12〕를 비교해 보면 차이가 거의 없음을 알 수 있다. TELNET 트래픽은 low-bandwidth 응용프로그램이기 때문에 침입차단시스템으로 인한 처리율 저하가 거의 보이지 않는다. TELNET 트래픽은 특성상 interactive하기 때문에 처리율은 깊이 고려해야 할 사항이 아니라고 판단된다. TELNET에서는 오히려 다수의 사용자가 동시에 접속하여 프로세스를 수행하였을 때의 성능저하가 평가요소이다.

4.4 FTP와 TELNET 트래픽 혼합

FTP 트래픽 50 Mbyte와 TELNET 트래픽을 11개 동시에 연결하여 복수 collision과 침입차단시스템의 CPU, 메모리 사용률을 알아보았다.

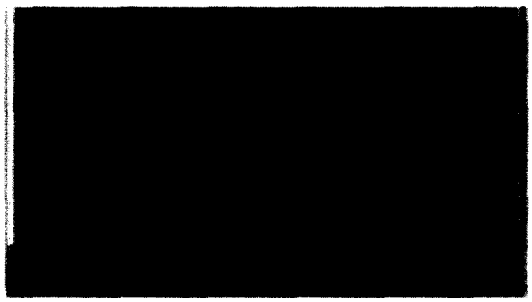
4.4.1 침입차단시스템이 있는 경우

침입차단시스템이 있는 경우 203.255.176.1에서의 collision을 MonaLisa를 통해 살펴보면 〔그림 13〕,



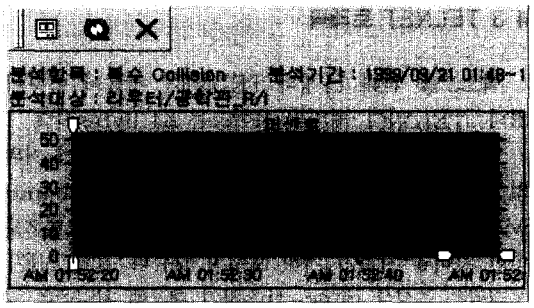
〔그림 9〕 침입차단시스템이 있는 경우

〔그림 10〕 침입차단시스템이 없는 경우

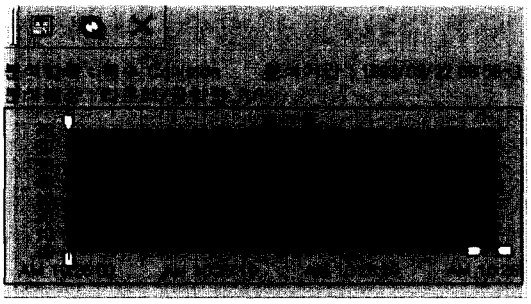


〔그림 11〕 침입차단시스템이 있는 경우

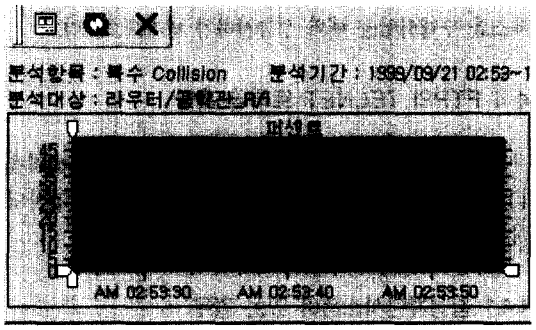
〔그림 12〕 침입차단시스템이 없는 경우



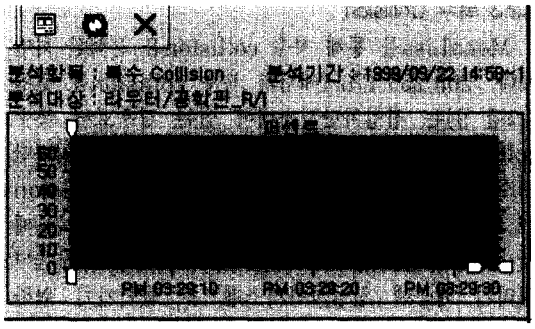
〔그림 13〕 FTP만을 보낸 경우



〔그림 14〕 FTP와 TELNET을 보낸 경우



〔그림 15〕 FTP만을 보낸 경우



〔그림 16〕 FTP와 TELNET을 보낸 경우

〔그림 14〕와 같다. 〔그림 13〕의 FTP만 보낸 경우에는 〔그림 14〕의 FTP와 TELNET을 같이 보낸 경우보다 복수 collision이 높다. FTP만 전송할 경우, 대부분의 전송 프레임이 1514 bytes로 긴 것으로 bandwidth를 완전히 사용하였고, FTP와 TELNET을 동시에 사용할 경우에는 1514 bytes의 긴 FTP 프레임과 함께 64 bytes의 짧은 TELNET 트래픽이 동시에 전송되어 그만큼 bandwidth에 여유가 생겨 충돌률이 줄어든 것이다. 203.255.178.1에서도 같은 현상을 보인다.

4.4.2 침입차단시스템이 없는 경우

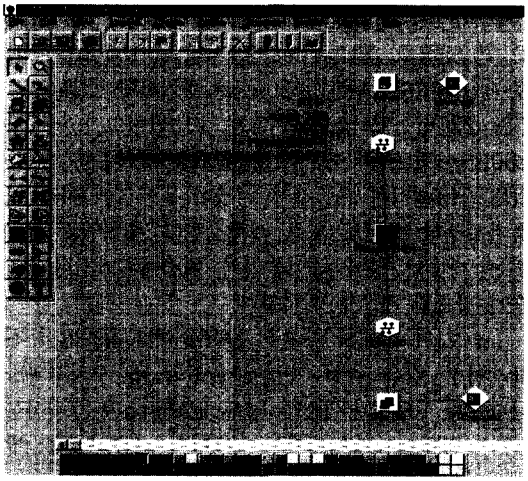
침입차단시스템이 없는 경우 203.255.176.1을 살펴보면 FTP만 보내는 경우인 그림 15보다 FTP와 TELNET을 혼합하여 보낸 〔그림 16〕의 경우에 복수 collision의 차이가 뚜렷함을 알 수 있다. 트래픽을 섞어서 보낼 경우에는 복수 collision이 급격히 줄어들었다. 침입차단시스템이 있는 경우에는 패킷을 검사하는 시간이 길어지기 때문에 다른 크기의 트래픽이 주는 영향이 줄어들었던 것이다. 그러나 여기서와 같이 침입차단시스템이 없는 경우에는 트래픽의 크기에 따라 현저하게 차이가 난다.

V. 네트워크 모델링 구현 및 결과 분석

4장에서는 실제 네트워크에서 침입탐지시스템이 네트워크에 주는 영향을 분석하였는데 이 장에서는 모델링된 네트워크의 경우를 좀 더 자세히 분석해보고자 한다.

5.1 모델링 구현

본 논문에서 모델링 하고자 하는 네트워크 구성도는 〔그림 17〕과 같다. 하나의 FTP 서버는 Fore7000이라는 라우터에 연결되어 있고, 그 라우터의 맞은편에는 여러 컴퓨터들이 하나의 컴퓨터 그룹을 형성하고 있다. FTP 서버에는 'Server app'라는 애플리케이션 소스가 연결되어 있는데, 이는 실제적인 서버의 역할을 제어하는 기능을 한다. 컴퓨터 그룹에도 'FTP request'라는 애플리케이션 소스가 붙어 있다. 컴퓨터 그룹에서 FTP를 요청하는 메시지를 서버에게 보내면 서버는 임의의 크기의 메시지를 다시 컴퓨터 그룹에게 보내주게 되는데, 침입차단시스템은 Fore7000 라우터 위에 설치하였다. 서버와 라우터간의 링크는 IEEE 802.3 CSMA/CD 10Base_T



〔그림 17〕 침입차단시스템을 설치한 망 모델링

로 설정하였고, delay, collision, utilization 등은 실시간 그래프로 관찰하였다.

5.2 모델링 결과 분석

모델링한 네트워크의 시뮬레이션 결과를 분석하는 데는 COMNET-Ⅲ에서 제공하는 리포트 파일을 사용하였다. 리포트 파일은 시뮬레이션 동안의 결과값을 통계적 수치로 보여주므로 실시간 그래프보다 정확한 값을 얻을 수 있기 때문이다. 앞으로 결과를 분석할 때 사용될 IAT(Inter Arrival Time)는 컴퓨터 그룹에서 FTP request를 보내는 간격을 나타내는 용어이고 IAT 5sec는 지수분포의 형태로 평균값이 5.0sec인 분포임을 의미한다. 사용자가 변할 때의 결과값을 비교 분석하기 위해서 IAT를 5sec로 고정시키고 사용자수를 10명, 50명, 100명으로 증가시켰다. 또, IAT가 변할 때의 결과값을 비교 분석하기 위해서는 사용자수를 50명으로 고정시키고 IAT를 10, 30, 50sec로 변화시켜가면서 모델링하였다. 침입차단시스템은 패킷을 검사하고 통과시키는데 처리 시간을 필요로 한다. 침입차단시스템별로 이 처리시간은 모두 다른데, 이를 위해 APT (Additional Processing Time)를 변화시켜보았다[5].

5.2.1 프레임 및 패킷 지연시간

COMNET-Ⅲ에서는 리포트 파일에서 패킷 지연시간을 보여준다. 패킷 지연시간은 전송 계층을 거쳐 응용 계층에서 지연된 시간까지 포함하므로 여러 파라미터 변화에 따른 결과를 명확히 볼 수 있어 패킷

〔표 1〕 패킷 지연시간

분류 \ 항목	사용자/IAT/APT	packet delay: send back(ms)	packet delay: FTP request(ms)	생성된 packet 수
사용자가 변할 때	10명	18	25	1,283
	50명	18	15481	5,449
	100명	18	62591	5,449
APT가 변할 때	10ms	68	59796	5,450
	50ms	201797	199081	1,620
	100ms	229023	245037	635
IAT가 변할 때	10sec	18	57	3,020
	30sec	18	22	981
	50sec	18	18	630

지연시간을 분석할 수 있다[7].

〔표 1〕에서는 다양한 환경에서의 패킷 지연시간을 보여준다. 먼저 사용자가 10명에서 50명, 100명으로 증가한 경우 컴퓨터 그룹에서 FTP 서버로 전송하는 FTP request 메시지의 지연시간은 25ms, 15481ms, 62591ms로 급격히 증가함을 볼 수 있다. 이는 사용자가 증가함에 따라 서버로 전송하는 메시지가 증가하게 되고 그에 따라 collision도 증가하게 되어 서버로 전송하기까지 지연시간이 길어진 것이다. 반면에 서버에서 컴퓨터 그룹으로 전송하는 send back 메시지의 지연시간은 사용자가 증가하여도 그리 큰 차이를 보이지 않음을 볼 수 있다. 그 이유는 많은 지연시간을 가지고 서버로 전송된 FTP request 메시지와는 달리 서버에서는 하나씩 차례대로 처리한 send back 메시지를 전송하기 때문이다.

APT를 변화시켜 본 경우, APT가 10ms인 경우 send back 패킷의 지연시간은 68ms을 나타내었다. 그러나 APT가 50ms인 경우는 201797ms로 급격하게 증가하였다. ATP가 100ms인 경우에도 계속 증가하였는데, 이는 침입차단시스템의 처리시간이 길어질수록 처리되어야 할 패킷이 지연되고 지연시간도 길어지게 된 것이다. 그런데 send back 메시지의 경우 FTP request 메시지보다 지연시간의 증가폭이 큰 것은 send back 메시지의 크기가 FTP request 메시지보다 크기 때문에 APT의 증가에 영향을 많이 받았기 때문으로 분석할 수 있다. IAT를 변화시켰을 때의 결과도 같은 맥락에서 해석할 수 있다. 패킷의 생성 간격이 짧을수록 전송하고자 하는 패킷이 증가하게 되고 그로 인해 collision이 증가하게 된다. 따라서 패킷의 전송 지연시간도 길어지게 된다. 사용자 수

를 증가시켰을 때와 같은 이유로 send back 메시지의 지연시간의 감소폭이 더 큼을 볼 수 있다.

5.2.2 프레임 collisions

〔표 2〕를 보면 사용자 수가 증가함에 따라 프레임 collision의 수도 크게 증가한다. 이는 사용자측에서 메시지를 많이 전송하면 Ethernet망을 통과하려는 경쟁 트래픽들이 많아지게 됨에 따라 발생한다. 동시에 전송을 시도하는 프레임들은 collision을 일으키게 되는 것이다. Collision episodes 수치를 보면 사용자 수가 10에서 50으로 변할 때는 collision수가 약 40배정도 증가함을 알 수 있다. 즉, 사용자가 50명 정도 되었을 경우에는 다음 리포트인 노드 프로세서 이용률에서도 볼 수 있듯이 이 망의 트래픽 처리한계에 거의 도달하였다고 보여진다. 이와 같은 망이 실제로 구축되었다고 가정할 때, 50여명의 사용자가 한꺼번에 패킷전송을 시도한다면 collision으로 인해 상당한 성능저하를 가져올 것으로 예상된다.

마지막 100명의 사용자가 지수분포 5sec로 FTP 트래픽을 요청할 때, 침입차단시스템의 APT의 변화에 따른 노드 이용률을 보여준다. 리포트를 보면 APT가 증가함에 따라 collision이 감소함을 알 수 있다. 먼저 Fore7000과 비교하여 보면 Ethernet 1에서 collision이 823번, Ethernet 2에서의 collision은 770번 발생하였다. 여기서 Ethernet 1은 FTP 요청을 하는 사용자 100명과 Fore7000 또는 침입차단시스템 IRX-211 사이에 위치하는 망이며 Ethernet 2는 Fore 7000 또는 IRX-211과 FTP 서버 사이에 위치하는 망이다. IRX-211이 설치된 경우 APT가 5 ms이면 Ethernet 1에서의 collision은 799번으로, Ethernet 2에서의 collision은 751로 감소하였다. APT가 50ms로 증가하면 Ethernet 1은 227번, Ethernet 2는 113번이고, APT가 100ms이면 각각 87번, 25번으로 줄어든다. 이는 IRX-211에서의 프로세싱 시간이 길어짐에 따라 사용자로부터 서버로 또는 서버로부터 사용자로 전송되는 패킷의 양이 줄어들었기 때문에 collision의 수가 감소한 것으로 해석된다.

〔표 2〕의 마지막 부분은 IAT를 변화시키면서 시뮬레이션 했을 때의 프레임 collision 수치결과를 나타낸다. IAT가 10인 경우 Ethernet 1에서는 75번, Ethernet 2에서는 125번의 collision이 발생하였다. 그러나 IAT가 30인 경우는 IAT가 10인 경우보다 FTP request 메시지의 발생 빈도가 작으므로 트래픽 양도 적어져서 collision이 상당히 감소하였다. 또한, IAT를 50으로 증가시켰을 경우에는 Ethernet 1에서는 1번, Ethernet 2에서는 4번으로 매우 적은 collision이 발생했음을 알 수 있다. 따라서, 사용자가 50명 정도일 경우 IAT가 50이상이 된다면 collision으로 인해 발생할 문제는 거의 없다고 생각해도 좋을 것이다.

5.2.3 노드 프로세서 이용률

노드 프로세서의 이용률이란 도착한 패킷을 입력버퍼에 받은 다음 프로세서가 차례대로 입력버퍼에 있는 패킷들을 처리하는 비율을 의미한다. 프로세서에 의해 처리된 패킷들은 내부 버스를 통해 출력버퍼로 전달되고, 출력버퍼에서는 다음으로 전송될 노드의 입력버퍼로 전달되기 위해 기다리게 된다. 〔표 3〕

〔표 2〕 프레임 collisions

분류 \ 항목	사용자/IAT/APT	Ethernet1 collision /collided frames	Ethernet2 collision /collided frames
사용자가 변할 때	10명	14/28	11/22
	50명	442/886	353/706
	100명	823/1,661	770/1,540
APT가 변할 때	5ms	799/1,609	751/1,502
	50ms	227/456	113/226
	100ms	87/174	25/50
IAT가 변할 때	10sec	75/150	125/250
	30sec	7/14	19/38
	50sec	1/2	4/8

〔표 3〕 노드 프로세서 이용률

분류 \ 항목	사용자/IAT/APT	서버	Fore7000 or IRX-211
사용자가 변할 때	10명	23.54	.0049
	50명	99.99	.0223
	100명	99.99	.0333
APT가 변할 때	5ms	100	32.15
	10ms	100	63.96
	50ms	79.99	100
	100ms	54.07	100
IAT가 변할 때	10sec	55.42	.0116
	30sec	18.01	.0037
	50sec	11.56	.0024

은 사용자수에 따른 노드 프로세서 이용률의 변화를 보여준다.

사용자가 10명인 경우의 서버노드의 프로세서 이용률은 약 23.5%를 보이고 있다. 그러나 사용자가 50명인 경우는 거의 100%에 가까운 이용률을 보이고 있는데 이는 사용자가 50명 이상이 될 경우 서버에서 트래픽을 처리할 수 있는 한계에 도달했음을 의미한다. 그러므로 사용자가 100명으로 증가한 경우 서버노드의 프로세서 이용률은 변화가 없다. 반면에 Fore7000의 프로세서 이용률은 사용자수가 증가함에 따라 조금씩 증가하고 있다. 여기서 Fore7000 노드의 프로세서 이용률이 서버노드에 비해 상당히 낮음을 볼 수 있는데, 이는 침입차단시스템이 설치되지 않은 라우터를 모델링할 때 라우터의 트래픽 처리 시간을 거의 0에 가깝게 주었기 때문이다. 이는 침입차단시스템이 설치된 IRX-211 모델과 비교시 유용하다.

[표 3]에서 두 번째 분류는 사용자가 100명인 경우 IAT가 지수분포로 5sec일 경우를 보여준다. 침입차단시스템에서 패킷 필터링 등을 위해 필요한 추가 프로세싱 시간은 5ms, 10ms, 50ms, 100ms인 경우를 모델링하였다.

IRX-211의 프로세서 이용률은 APT가 5ms로 증가하면 프로세서 이용률이 32.15%, 10ms이면 63.96%로 점차 증가하다가 50 ms이상 100ms까지는 프로세서를 100% 사용하였다. 이것은 Fore7000 스위치가 사용되었을 때 0.03%를 사용한 것과 비교하여 IRX-211에 APT가 추가됨에 따라 프로세서 사용이 지속적으로 증가함을 보여준다. 50ms 이후로는 급격하게 높은 프로세서 이용률을 보여 프로세서를 완전히 사용하게 되었다. 침입차단시스템에서는 패킷이 들어오면 각각 패킷필터링을 하기 위하여 패킷의 헤더를 검사하고 침입차단시스템의 종류에 따라 응용 계층까지 패킷을 끌어올려 검사하기 때문에 프로세싱 시간이 오래 걸리고 이 작업을 수행하는 프로세서가 바빠지게 된다[5].

이에 반해 FTP 요청을 받아들이고 파일을 전송해주는 서버의 경우는 Fore7000이나 IRX-211에 APT가 5ms, 10ms 추가되었을 때에는 100%의 프로세서 이용률을 보여주다가 50ms, 100ms가 추가로 수행되었을 때에는 FTP 요청 수가 줄어들어 서버 프로세서 이용률이 반대로 79.99%, 54.07%로 감소한다.

표의 마지막 부분을 보면 IAT가 증가하는 경우도 사용자수가 증가하는 경우와 유사한 모습을 나타낸다. 트래픽이 감소함에 따라 서버의 프로세서 이용률도 점점 감소하고 있다. IAT가 10인 경우 서버 프로세서 이용률은 55.42%를 나타내고, IAT가 30인 경우는 18.01%, IAT가 50인 경우는 11.56%를 나타내고 있다. 즉, IAT가 50인 경우는 서버의 프로세서가 request 메시지를 받고 특정파일의 일정 부분을 읽어서 다시 전송해 주는 작업을 프로세서의 11.56%만을 사용하여 처리할 수 있는 것이다. 프로세서를 모두 사용하지 않으므로 이 작업 외의 다른 작업도 병행할 수 있는 여건이 된다. Fore7000의 프로세서 이용률도 트래픽 감소에 의해 점차 감소하였다.

[표 4] 시스템별 FTP 요청수

시스템 \ 항목	FTP 요청수
Fore7000	5,449
IRX-211 APT 50ms	4,360
IRX-211 APT 100ms	2,946

서버에서의 프로세서 이용률이 떨어진 것은 FTP 요청에 따라 디스크 읽는 작업이 감소한 면과 일관성을 가진다. [표 4]는 사용자가 100명이고 IAT가 5sec인 경우 서버로 들어온 디스크 읽기 요청을 허락한 숫자를 보여준다.

Fore7000의 경우 5,449번 디스크 요청을 허락하였고 IRX-211에 APT가 5ms, 10ms 걸릴 때에도 평균 5,440번으로 비슷하게 디스크를 읽어왔으나, APT가 50ms, 100ms로 증가함에 따라 4,360, 2,946번으로 줄어들었다. 즉, 침입차단시스템에서의 프로세싱 시간이 증가하여 침입차단시스템에서 머무르는 시간이 증가하였고, 이에 따라 전체적인 FTP 요청이 줄어들었다. FTP 요청수의 감소는 서버에서의 프로세서 이용률 감소를 뒷받침한다.

Ⅵ. 결론 및 향후 연구 방향

본 논문에서는 침입차단시스템이 네트워크에 미치는 영향을 연구하기 위하여 실제 네트워크에 여러 트래픽을 적용하여 트래픽별 특성을 분석하였으며, 침입차단시스템을 설치한 후 같은 과정을 되풀이하였다. 또한 네트워크 시뮬레이션 도구를 이용하여 침입차단시스템이 있는 네트워크를 모델링하였고 다양한 트래픽을 전송해보았다.

실제 네트워크에 침입차단시스템을 설치한 후 e-Watch와 같은 망 관리 도구를 사용하여 네트워크를 분석해 본 결과, 침입차단시스템에서의 트래픽에 대한 처리시간으로 인해 지연이 발생하여 전송속도가 저하되고 충돌률이 높아짐을 그래프를 통해 알 수 있었다.

한편, 침입차단시스템이 있는 망을 모델링한 경우도 실제 네트워크의 경우와 비슷한 모습을 보였다. 즉, 패킷 지연시간, 패킷 충돌률, 노드 프로세싱 시간 등을 중심으로 살펴보았을 때, 침입차단시스템이 없는 경우보다 네트워크의 현저한 성능저하가 발생하였다.

본 논문에서는 수치적으로 결과를 분석하지는 않았지만, 침입차단시스템의 처리 속도가 지연되거나 처리해야할 트래픽이 많아질수록 네트워크에도 심각한 영향을 줄 수 있다는 것을 확인할 수 있었다. 따라서, 침입차단시스템을 설계하거나 사용할 때에도 침입차단시스템이 네트워크에 미치는 영향은 고려해야할 요인이 된다. 본 논문에서 수행한 침입차단시스템이 네트워크에 미치는 영향에 대한 연구는 요즘과 같이 네트워크의 보안이 요구되는 상황에 특히 유용하게 사용될 수 있다. 즉, 여러 가지 공격으로부터 네트워크를 보호하기 위하여 침입차단시스템을 설치할 경우 보안 서비스가 제공되는 장점은 있으나 네트워크의 성능을 저하시킬 수 있다는 단점이 있었다. 침입차단시스템을 설치하려 할 때 본 논문의 연구결과를 고려하여 상황에 적합한 조치를 취할 수 있을 것이다.

여기서는 침입차단시스템에 대해서만 그 영향을 분석하였으나, 향후에는 침입탐지시스템이나 백신시스템 등 포괄적인 의미의 정보보호시스템이 네트워크에 미치는 영향에 대해서 연구하려 한다. 이에 덧붙여 최적의 침입차단시스템을 설계하기 위한 파라미터 도출과 수학적인 분석에 관한 연구도 수행할 수 있을 것이다.

참 고 문 헌

[1] David Newman, "Super Firewalls," Data Communications, 1999. 5.

[2] D. Brent Chapman, "인터넷 방화벽 구축하기", 한빛미디어, 1998.

[3] Karanjit Siyank, "인터넷 방화벽과 네트워크 보안", 이한출판사, 1996.

[4] "정보보호동향 정보서비스", http://twister.kisa.or.kr

[5] "가디안 소개 및 보안 세미나", http://guardian.syds.com

[6] "인터넷 보안 방화벽(Firewall) 시스템", http://esperosun.chungnam.ac.kr:8080/firewall/abstract.html

[7] "인터넷 보안: 가상사설망, 방화벽 그리고 침입탐지시스템"

[8] "인터넷-보안/방화벽", http://www.postech.ac.kr/~pack/Infotree/Internet/Security/security.html

[9] "인터넷 방화벽과 보안", http://myhome.shinbiro.com/~net/up1/peace1.htm

[10] "방화벽", http://athena.chonnam.ac.kr/~shlee/study/study.html

[11] e-Watch manual, (주)하늘소프트.

[12] COMNET III Reference Guide, CACI, 1998.

[13] "MonaLisa homepage", http://www.monalisa.co.kr

〈著者紹介〉

정 선 이 (Sunnie Chung)

1998년 2월 : 이화여자대학교 국어국문학과 졸업
2000년 8월 : 이화여자대학교 컴퓨터학과 석사
2000년 9월~현재: Lucent Technologies
〈관심분야〉 이동통신, 네크워크 보안, XML

박 정 은 (Jeong-eun Park)
1999년 2월 : 이화여자대학교 컴퓨터학과 졸업
1999년 3월~현재 : 이화여자대학교 컴퓨터학과 석사과정
〈관심분야〉 이동통신, IMT-2000, 네트워크 보안

유 수 연 (Soo-yeon Yoo)
1999년 2월 : 이화여자대학교 컴퓨터학과 졸업
1999년 3월~현재 : 이화여자대학교 컴퓨터학과 석사과정
〈관심분야〉 멀티미디어, IP QoS, 네트워크 보안

장 성 은 (Sung-eun Jang)
1999년 8월 : 한신대학교 수학과 졸업
1999년 9월~현재 : 이화여자대학교 컴퓨터학과 석사과정
〈관심분야〉 네트워크 보안, 침입탐지시스템, 액티브 네트워크

채 기 준 (Ki-joon Chae) 종신회원
1982년 2월 : 연세대학교 수학과 졸업
1984년 5월 : 미국 시라큐즈대학교 컴퓨터과학과 석사
1990년 5월 : 미국 노스캐롤라이나 주립대학교 컴퓨터공학과 박사
1990년 8월~1992년 2월: 미국 해군 사관학교 전자계산학과 조교수
1992년 3월~현재: 이화여자대학교 컴퓨터학과 부교수
〈관심분야〉 네트워크 보안, 액티브 네트워크, 망관리, 성능분석

노 병 규 (Byung-gyu No) 정회원
1988년 2월 : 충남대학교 계산통계학과 졸업
1995년 2월 : 충남대학교 전산학과 석사
1988년 2월~1997년 1월 : 한국전자통신연구원 선임연구원
1997년 1월~현재 : 한국정보보호센터 평가2팀 팀장
〈관심분야〉 네트워크, 정보보호, 시스템 평가