L4-Switch를 위한 SSFNet의 확장

*전형인° *한종현 **이은영 **김도환 *박승규
*아주대학교 정보통신전문대학원, **국가보안기술연구소 정보보증연구부
{gied80°, hanbell}@ajou.ac.kr {eylee, dkim}@etri.re.kr sparky@ajou.ac.kr

SSFNet Extension for L4-Switch

*Hyoung-in Jeon° *Jong-hyun Han **Eun Young Lee **Do Hwan Kim *Seung Kyu Park
*Graduated School of Information and Communication, Ajou University
**National Security Research Institute

요 약

규모가 방대한 네트워크상에서 네트워크의 침입과 방어의 효과와 유용성을 알아보기 위해, 실존하는 네트워크상에서 직접 침입과 방어를 테스트하는 것은 많은 노력과 비용이 든다. 이와 같은 문제점을 극복하기 위해 인터넷 침입의 표현에 필요한 네트워크 침입 시뮬레이션을 하기 위한 SSFNet 확장 연구가 진행되었다. 본 연구는 SSFNet에 새로이 추가된 L4-Switch 모듈을 이전 연구에서 만들어진 모듈들과 함께 대규모 네트워크 환경에서 네트워크 침입 시뮬레이션을 테스트하였다. 본 시뮬레이션은 L4-Switch와 http클라이언트, http서비스를 제공하는 호스트들을 설정하고, load balancing이 잘 되었는지를 살펴보았다.

1. 서 론

네트워크상에서 네트워크 침입이 서버나 클라이언트에 미치는 영향을 현존하는 네트워크상에서 연구하기에는 네트워크의 방대함과 또한 많은 비용 및 시간이 소모되기 때문에 어려움이 있다. 또한, 네트워크 침입과 방어로 인한 현상들의 효용과 유용성에 대한 정확한 자료도 산출하기 힘들다. 시뮬레이션은 이러한 단점을 극복하는 훌륭한 대안이며, 다양한 시뮬레이션 도구가 개발되었다. 이러한 네트워크 시뮬레이션을 수행하기 위한 툴로는 NS-2[1]와 SSFNet[2]등이 있으며, NS-2의 장점은 다른 시뮬레이션 툴과의 비교에서 멀티 캐스트를 지원한다는 것과, 지역적이기는 하나 무선 환경에서의 시뮬레이션을 할 수 있다는 점은 NS-2가 가진 큰 장점 중 하나이다. 그러나 100,000개 이상의 대규모 인터넷을 모델링하고, 이러한 환경에서 시뮬레이션 하기에는 적합하지 못하다.

SSFNet의 장점으로는 시뮬레이션 커널인 SSF의 소스는 공개되지 않았으나 그 중에서 네트워크의 시뮬레이션을 지원하는 SSFNet은 라우터, 링크, 네트워크 인터페이스 카드 등 대부분의 인터넷 서브 시스템들을 시뮬레이션 하는데 필요한 다양한 객체들이 Java로 구현되어 있어 시뮬레이션 특성에 맞추어 그들의 특성을 변경할 수 있다는 장점을 가지고 있다. 또한 SSFNet은 이를 기반으로 상위단계의 10만개 이상의 노드로 구성된 대규모 네트워크까지도 표현하도록 허용하고 있으며, 네트워크상의 실존하는 특정 행동을 따라 구현이 가능하다.

본 논문에서는 향후 네트워크 침입과 방어에 대한 시뮬레이션에서는 실제 네트워크 상황과 비슷한 정보를 얻기 위해 대규모 네트워크 환경이 필요하다고 판단하여, SSFNet을 시뮬레이션 툴로 사용하였고, 네트워크 침입과 방어에 관련된 시뮬레이션 중 L4-Switch를 구현하였다. L4-Switch는 서버 load balance를 기본 기능으로 한다. L4-Switch는 Round Robin 방식의 분산알고리즘을 사용하였고, SSFNet와 같이 java를 기반으로 작성되었다. SSFNet에 L4-Switch를 사용함으로써 다양한 보안 기능과 여러 프로토콜과 네트워크 환경에서의 서버 load balance를 시뮬레이션 할 수 있게 되었다

2. 관련연구

SSFNet은 인터넷 프로토콜과 네트워크의 모델링과 시뮬레이션을 위한 자바 기반의 컴포넌트 집합이다. 네트워크를 위한 DML 작성 시 호스트 범위를 이용하여 서브 네트워크 중심으로 네트워크를 구성할 수 있다. 또한 각 호스트 설정을 미리 정의한 템플릿으로 구성할 수 있게 하는 DICTIONARY를 이용하여 각 호스트에 대한 프로토콜의 설정을 손쉽게 할 수 있다[3]. 그러나 DNS나 FTP 서버 같은 모듈을 지원하고 있지 않아서 사용자가 직접 각 모듈을 구현하여 사용하여야 한다.

본 논문은 SSFNet의 ProtocolSession클래스를 확장한 L4-Switch 모듈 구현을 시도하고 있다.

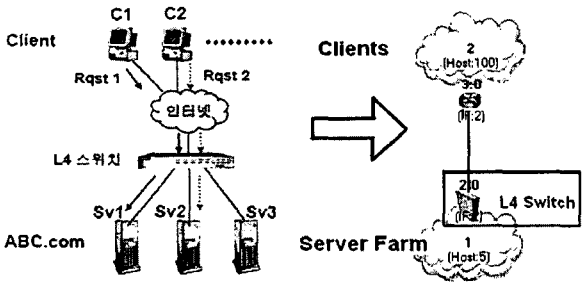
Switch는 하나의 Interface에서 또 다른 Interface로 Packet 전송 시 불필요한 Traffic은 제거하고 필요한 Traffic만을 선택적으로 전송하는 장비이다. 그러나 L4-Switch는 Packet만을 전송하는 것이 아니라 Packet의 Header를 검사하여, Server가 'Server Farm'을 구성할 경우 Packet을 Server에게 적절하게 분배하는 서버 load balancer역할도 한다. L4-Switch는 Server 앞 단에 위치하여 Server Farm의 서버들을 대신하여 클라이언트의 요청을 받아 packet을 서버에게 전송 한다. 이때 클

라이언트는 서버들의 주소로 직접 접근할 수 없고 Switch를 통해서만 접근이 가능하다.
Switch가 동작하는 방식에는 Proxy type과 Address Edit 방식이 있다. Proxy type은 서버와 Switch가 Connection을 수립하고, Switch와 서버와 별도의 Connection을 수립하는 방식이다. Address Edit은 클라이언트가 Switch의 주소로 패킷을 전송하면 Switch가 목적지 주소를 서비스할 서버의 주소로 변환하여 내보내는 방식이다.

L4-Switch의 가장 중요한 기능중의 하나는 서버 load balancing 알고리즘에는 Round Robin, Least Connection, Hash, Minimum Missies 등의 여러 방법이 있다. Round Robin 은 서버로 세션을 순차적으로 맺어주는 방식이고, Least Connection은 서버의 open 세션 수를 고려한 다음, 가장 적은 수의 open 세션을 가진 서버로 세션을 맺어주는 방식이다. Hash는 클라이언트와 서버 간에 한번 성립된 세션을 계속 유지해 주는 방식으로 특정 클라이언트는 특정 서버로만 접속하게 된다. Minimum Missies는 는 Hash 알고리즘과 거의 유사하나 Cache Redirection에 주로 사용한다.

3. L4-Switch Model

SSFNet에서는 실제 망의 구성을 그대로 적용하기에는 무리가 있다고 판단되어, 네트워크를 간략화 하여 서브넷의 호스트들이 'Server Farm'을 구성하는 서버라고 가정하였다. L4-Switch는 두 개의 인터페이스를 갖으며, 서버와 클라이언트를 연결한다.



<그림 1. 간략화한 네트워크>

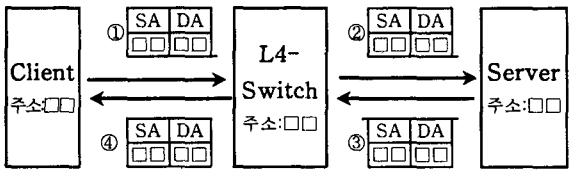
<그림 1>은 간략화 한 네트워크의 형태를 실제 네트워크와 비교하여 보여준다. L4-Switch 내부의 서브넷을 'Server Farm', 호스트들을 서버라 설정하였다.
본 논문에서 구현한 L4-Switch는 Switch의 형식으로는 L4-Switch가 Server Farm의 서버들을 대신하여 클라이언트의 요청을 받기위해 L4-Switch의 주소를 서버로 등록하여, 외부의 호스트들이 서버로 인식하고 접속하도록 하는 Proxy type 방법을 사용하였다. 서버 load balancing 알고리즘은 클라이언트의 요청을 각 서버들에게 순차적으로 분배하는 Round Robin 알고리즘을 사용하였다.

4. L4-Switch 설계 및 구현

구현된 L4-Switch는 주요기능인 패킷 전달을 위해서 Proxy type의 Switching을 한다. 그리고 부가적인 기능인 load balancing을 위해서 클라이언트의 요청을 각 서버에 분배하는 load balance와 Server Farm의 서버리스트를 관리하는 Server Table을 갖는다.

4.1 Proxy Type Switching

Proxy Type Switch는 Server Farm의 서버들을 대신하여 클라이언트의 서비스 요청을 받기 때문에 L4-Switch가 서버로 간주되도록 서버로 등록하여야 한다. 또한 Switch뒤 Server Farm의 서버들이 클라이언트와 직접통신하지 못하도록 등록된 서버 목록에서 Server Farm의 서버들을 제거한다. 따라서 클라이언트와 서버간의 통신은 중간에 L4-Switch가 중계하여 통신한다.

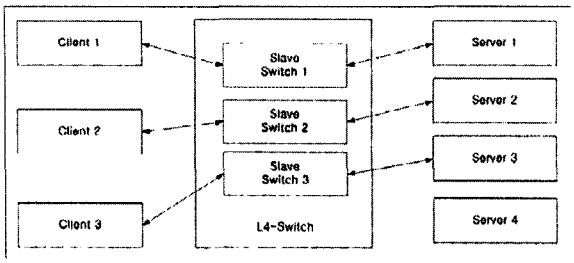


<그림 2. Proxy type L4-Switch>

<그림 2>는 Proxy type L4-Switch의 동작을 보여준다. ①클라이언트가 L4-Switch를 서버로 인식하고 Source IP address(SA)를 자신의 주소로 Destination IP address(DA)를 L4-Switch의 주소로 서비스 요청패킷을 보낸다. ②클라이언트로부터 패킷이 L4-Switch로 들어오면, L4-Switch는 load balance 정책에 의해 서비스할 서버를 선택하고, Source IP를 자신의 IP로 변경하고 Destination IP를 Server의 IP로 변경하여 내보낸다. ③서버는 L4-Switch에게 응답 패킷을 보낸다. ④L4-Switch는 서버로부터 패킷을 받으면, 그 패킷의 Source IP를 자신의 IP로 변경하고 Destination IP를 요청패킷을 보낸 클라이언트 IP로 변경하여 내보낸다.

4.1 Load balance

Load balance는 클라이언트의 서비스 요청이 들어오면, Server Farm의 서버 중 적절한 서버에 서비스 요청 패킷을 전달하는 기능이다. L4-Switch는 클라이언트의 요청을 Server Farm의 서버들에게 효율적으로 분배하기 위해 Round Robin 알고리즘을 사용, Server Table의 서버를 순차적으로 선택하여 연결을 시킨다.
L4-Switch에는 각각의 서버와 클라이언트를 연결시켜주는 Slave Switch가 존재한다. Slave Switch는 서비스를 요청하는 하나의 클라이언트에 대응하여 Connection을 맺고, 또 클라이언트의 서비스 요청을 수용하는 서버와 Connection을 맺어 서버와 클라이언트를 중계한다.



<그림 3. Round Robin 정책을 이용한 Load balance>

<그림 3>은 Slave Switch양단에 각각의 클라이언트와 서버가 연결된 예를 보여준다. Slave Switch는 클라이언트로부터 요청을 받으면 Round Robin 정책으로 적절한 서버를 선택하여 Slave Switch 양단에 서버와 클라이언트와의 세션을 유지한다. 새로운 클라이언트로부터 서버로의 요청이 들어오면 L4-Switch는 새로운 Slave Switch를 만들어 적절한 서버와 연결을 한다.

4.2. Server Table

Server Table은 Server Farm의 서버들의 주소를 관리하는 Table이다. Round Robin 정책으로 Load balancing을 하기위해서는 서버들의 리스트가 필요로 하게 된다. Server Table은 인덱스와 각 서버의 IP주소로 테이블을 구성하며, L4-Switch의 초기화 과정에서 테이블의 내용이 채워진다. SSFNet에서는 서버의 IP주소를 직접적으로 얻을수 없기 때문에 NH주소(Network Host Interface address)를 IP 주소로 변환시켜 Server_Table에 저장을 한다.

Index	IP address
0	Server IP address 1
1	Server IP address 2
2	Server IP address 3

< 표 1. Server Table 의 예 >

<표1>은 Server Table의 예를 보여준다. 각 서버의 IP주소에 Index를 두어 Round Robin정책을 수행할 수 있도록 한다.

5. 시뮬레이션

구현된 L4-Switch를 시뮬레이션 테스트를 하기위하여 1개의 L4-Switch, 25개의 Server, 6개의 router와 5400개의 host로 구성된 네트워크 환경에서 200초 동안 시뮬레이션 하였다. 25개의 서버는 L4-Switch의 내부에서 Server Farm을 구성하고 있고, 6개의 router는 각각 900개의 호스트을 가지고 있다. 1개의 L4-Switch는 각 호스트에서 들어오는 요청을 Server Farm 안의 서버들에게 순차적으로 연결 시켜 Round Robin 정책을 통한 Load blanace을 시뮬레이션 하였다.

```
[L4Switch] 요청이 들어왔음. [76]번째 패킷
[L4Switch] 1번 서버와 연결 성공 [76]번째 패킷
[L4Switch] 요청이 들어왔음. [77]번째 패킷
[L4Switch] 2번 서버와 연결 성공 [77]번째 패킷
                    .
                    .
[L4Switch] 요청이 들어왔음. [100]번째 패킷
[L4Switch] 25번 서버와 연결 성공 [100]번째 패킷
[L4Switch] 요청이 들어왔음. [101]번째 패킷
[L4Switch] 1번 서버와 연결 성공 [101]번째 패킷
                    .
                    .
```

<그림 4. L4-Switch가 행해지는 과정>

<그림 4 >는 L4-Switch가 클라이언트로부터 요청을 받았을 때 서버로 연결을 하고 있는 과정을 보여준다. 클라이언트로부터 L4-Switch에 서비스 요청의 들어올 경우 L4-Switch는 25개의 서버를 순차적으로 연결시키는 것을 확인할 수 있다.

6. 결론 및 향후 과제

본 논문에서는 L4-Switch에 필요한 모듈의 구현과 향후 연구할 네트워크 공격과 방어에 관련된 설정과 그에 따른 반응을 구현을 위해 SSFNet을 확장하여 대규모 인터넷에서 L4-Switch의 시뮬레이션이 가능한 기반을 구축하고, 그의 정상적 구동을 확인하였다. 앞으로 본 연구결과와 네트워크 공격과 방어 시뮬레이션에 더 필요한 모듈들을 응용하여, 대규모 네트워크 환경에서 네트워크 공격과 방어에 관련된 시뮬레이션을 수행 할 것이다.

7. 참고문헌

[1] "NS-2 The Network Simulator", http://www.isi.edu.nsnam/ns/
[2] "SSF Simulator implementation", http://www.ssfnet.org/ssfImplementation.html
[3] James H. Cowie, "Scalable Simulation Framework API Reference Manual", Version 1.0, Documentation Draft-Revision, March 1999.
[4] 한종현, 윤주범, 이은영, 박승규 "Domain Name Service를 위한 SSFNet의 확장", 한국통신학회 추계종합학술발표회 논문집, p104, 2003,11
[5] 조규찬, 장해권, 박승규, 최경희 "확장된 SSFNet 시뮬레이션에 의한 Web Proxy Server 특성 분석", 한국통신학회 하계종합학술발표회논문집, Vol. 25, p279, 2002.7.
[6] http://tunelinux.pe.kr/tune/l4/l4.html