네트워크 공격 및 방어 시뮬레이션 프레임워크 제안

*권오철 **배성재 ***조재익 ****문종섭

고려대학교 정보경영공학대학원

*kwonoch@korea.ac.kr

Proposal of Network Attack/Defence Simulation Framework

*Kwon, Oh-Chul **Bae, Seong-Jae ***Cho, Jae-Ik ****Moon, Jong-Sub

Graduate School of Information management & Security, Korea University

요약

네트워크에서의 공격은 일반 사용자의 개인 정보 노출 및 국가 중요 네트워크에서의 불법 정보 노출 등 많은 위험 상황을 야기할 수 있다. 현재의 네트워크가 대규모화되고 고속화되고 있는 시점에서 기존의 저 수준의 공격이 아닌 다양한 기술이 접목된 네트워크 공격이 발생하고 있다. 이러한 공격의 영향을 실제 상황에서 분석하기에는 많은 어려움이 따르며 정확한 분석에 제약이 따르게 된다. 따라서 이러한 네트워크 공격을 모델링하고 침입탐지 및 차단을 모델링할 수 있는 시뮬레이션의 발달이 필요하다. 본 논문에서는 정상상태 모델, 공격 모델, 방어 모델로 이루어지는 네트워크 공격 및 방어 시뮬레이션 프레임워크를 제안하도록 하겠다.

1. 서론

2006년도의 사이버 침해사고 발생 원인을 살펴보면, 공격 유형이 다양해지고 고도화된 해킹 수법의 발달을 볼 수 있다. 아울러 웹 방화벽, PMS(Patch Management System), VMS(Virus Management System)등과 같은 최신 정보보호제품 구비미흡, 전문인력 부재, 정보보호에 대한 전반적인 투자부족 등이 간접적으로 영향을 미치는 것으로 파악되었다[1].

네트워크 공격으로 인한 피해증상과 피해정도에 대한 연구는 네트워크 공격과 방어를 연구하기 위한 기초단계이다. 하지만, 실제 네트워크의 방대함과 공격양상의 다양함이 정확한 분석을 어렵게 하여 아직까지 큰 연구 진전이 없는 분야이다. 네트워크 공격에 의한 증상과 피해정도를 파악하는 좋은 대안으로 시뮬레이터를 이용한 방법이 있다.

네트워크의 다양한 공격은 정확한 데이터의 수집이 가능한 범위에서는 모두 분석 할 수 있다. 하지만 실제 공격 실험은 실제 네트워크에서는 불가능하다. 공격 실험에 대한 법적인 문제가 있으며, 네트워크의 피해 정도를 예측하였더라도 실제 공격이 발생하였을 때의 행위에 대해 정확한 모델링이 불가능하기 때문이다. 이러한 실험을 정확하게 시도하기 위해서는 반드시 가상망으로 구성된 실험용 망이 구축되어야 하며, 실험용 망이 구축되기 위해서는 여러 가지 공격 모델링 방법과 모델링 된 공격 행위에 대한 표현 방법에 대해서 연구 되어야 한다.

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.

(IITA-2006-(C1090-0603-0025))

특히 악성 코드의 확산과 침해 사고의 발생은 중요한 정보 유출로 이어질 수 있는 문제이기 때문에 피해 정도 분석과 침입 탐지에 관한 연구를 위해 공격 및 방어에 관한 시뮬레이터는 반드시 연구되어야 한다.

하지만, 이전의 시뮬레이션 연구에서는 네트워크 공격 및 방어에 특화된 시뮬레이션을 제작하여 실험하기 보다는 기존의 시뮬레이터를 활용한 연구가 대부분이었다. 따라서 본 논문에서는 네트워크 공격 방어 시뮬레이션을 위한 프레임워크를 제안하고자 한다.

논문의 구성은 다음과 같다. 2장에서 기존에 사용되고 있는 네트워크 시뮬레이터에 대한 알아보고 3장에서 프레임워크 구성에 필요한 요소를 검토하고 4장에서 네트워크 공격 및 방어 시뮬레이션에 적합한 프레임워크를 제안하고 5장에서는 결론 및 향후연구를 기술한다.

2. 관련 연구

가. NS-2

현재 일반적으로 가장 널리 사용되고 있는 네트워크 시뮬레이터인 NS-2(Network Simulator-2)는 네트워킹의 성능분석을 목적으로 개발된 이벤트 기반(Event-driven)의 시뮬레이터이다. 이 시뮬레이터의 적용범위는 유선 네트워크의 경우 TCP/IP 프로토콜 패밀리와 각종 라우팅 프로토콜에 대한 시뮬레이션이 가능하며, 무선 네트워크에 경우에는 Ad Hoc 네트워크, WLAN, Mobile IP와 Cellular 네트워크 등의 시뮬레이션이 가능하다.

하지만 GUI가 부족하고 레이어 3이하에 관한 것들을 무시하고 있는 것과 .tcl로 이루어진 코딩이 처음 사용하는 사람들에게 문법적으로

나 표현적으로나 어려울 수 있다는 단점이 있다. 하지만 공개된 소스와 두터운 이용자층에 힘입어 널리 사용되고 있으며, 계속 발전하고 있는 시뮬레이터이다[2].

나. SSFNet

SSFNet은 자바기반의 인터넷 프로토콜과 네트워크 환경에 대한 모델링과 시뮬레이션 도구이다. SSFNet 모델들은 개별 클래스로 구성되어 각각의 설정과 상호 연결을 통해 웹환경에 대한 실질적이고 가용한 시뮬레이션을 가능하게 한다. 이 요소들에 대한 설정은 DML(Domain Modeling Language)을 통해 계층적이고, 간편하게 구성된다.

하지만 시뮬레이터의 주된 초점이 네트워크의 확장성과 프로토콜(라우팅 알고리즘) 표현에 치우쳐, 패킷레벨에서의 다양성과 애플리케이션 계층에 대한 고려가 미흡하고 시뮬레이션 과정/결과에 대한 그래픽 구현은 가능하나, 별도의 GUI 입력 및 사용자 인터페이스에 대한 고려가 부족하다는 단점이 있다[3].

다. QualNet

Qualnet은 상업용 네트워크 시뮬레이터이며, NS-2에 비해 향상된 GUI를 제공하고 있다. 또한, 다양한 Prototype을 제공하고 있어 빠른 초기설계가 가능하다. Qualnet의 가장 큰 장점은 이 기종간의 대규모 무선 네트워크를 대상으로 실시간 시뮬레이션을 수행하는 특징을 지니고 있다[4]. 하지만, 공격 및 방어 시뮬레이션에 대한 지원이 없으므로 모델링에 많은 시간과 인력을 투자해야한다는 단점이 있다.

라. OPNET

OPNET은 1986년 미국 국방부 전산망 프로젝트의 일환으로 추진된 네트워크 시뮬레이션 프로그램 개발에 의해 만들어진 프로그램이며, 개발 업체인 OPNET Technology사는 현재 세계 네트워크 시뮬레이션 시장의 80%를 점유하고 있는 네트워크/어플리케이션 관리 소프트웨어 업체이다. 상업목적의 시뮬레이터인 OPNET은 향상된 GUI와 강력한 고객지원 서비스로 네트워크 관리자에게 적합한 프로그램이다[5].

3. 프레임워크 구성을 위한 속성

사이버 공격 및 방어 체계에 대한 시뮬레이션 환경을 제공하기 위해서는 가상의 네트워크를 구축해야 하며, 이를 위해서는 가상 네트워크에 대한 모델링이 이루어져야한다. 모델링의 기초작업으로서 실제 네트워크를 구성하는 요소들을 분류하고, 네트워크 구성요소들이 실제 네트워크에서 수행하는 기능들에 대한 연구가 필요하다. 따라서 본 장에서는 네트워크 구성요소를 하드웨어와 소프트웨어적 구성요소로 구분하여 가상 네트워크 구성에 필요한 필수 요소를 선정하고 정상상태, 공격, 방어 데이터베이스에 필요한 구성요소도 연구하도록 하겠다.

가. 네트워크 구성요소

시뮬레이션에 필요한 네트워크의 기본구성요소는 우선 하드웨어와 소프트웨어로 나누어 생각할 수 있다. 표 1 은 하드웨어와 소프트웨어로 정리된 네트워크 구성요소를 나타낸다.

그림 1은 표 1 의 구성요소를 바탕으로 구성된 가상 네트워크이다. 가상망 모델링을 위해 기초적인 네트워크 구성을 하는데 사용할 수 있다.

표 1. 네트워크 구성요소

분 류	네트워크 구성요소 종류
하드웨어적 분류	네트워크 어댑터, 리피터, 허브, 스위치, 라우터, 게이트웨이, AP, UTP 케이블, 광섬유 케이블, WLAN
소프트웨어적 분류	서버, 클라이언트, 연결노드

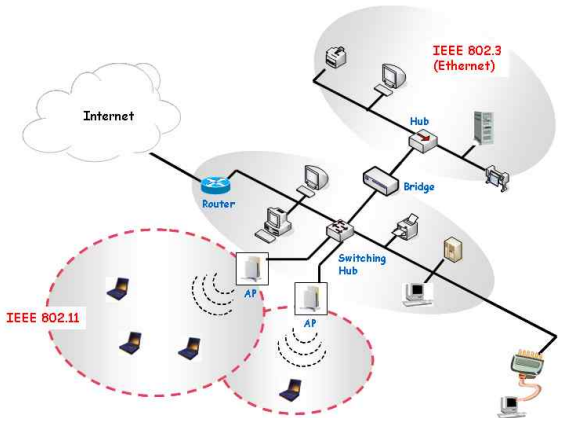

그림 1. 가상 네트워크 구성도

나. 데이터베이스 구성요소

표 2 는 시뮬레이션에서 사용할 데이터베이스 구성요소를 나타낸다. 각 데이터베이스 구성요소는 정상상태 모델링 DB를 구성하는데 사용되며, 공격모델과 방어모델이 시나리오에 따라 DB를 갱신하는 것으로 공격 및 방어행위를 표현하는데 사용된다.

표 2. 데이터베이스 구성요소

대분류	상세 분류
서버	파일서버, 메일서버, 웹서버, DNS서버, DB서버, 텔넷 서버, 기타
클라이언트	웹 브라우저, P2P 프로그램, 메신저, 기타
네트워크	스위치, 라우터, AP, 연결노드

4. 프레임워크 구성

가. 정상상태 모델링

정상상태 모델링은 가상망의 구성을 바탕으로 데이터베이스 구성요소의 관계를 설정하게 된다. 그림 2 는 TTA 표준활용맵[6]을 바탕으로 한 가상네트워크 토폴로지를 나타낸다. 가상네트워크 토폴로지에 따라 각 노드간의 기본 트래픽을 설정하여 정상상태로 모델링하게 된다. 위치정보와 인접정보가 노드간의 트래픽을 결정하는 중요한 요소

로 작용하게 된다.

세부적인 네트워크 트래픽은 검증된 데이터셋을 사용하도록 한다. 대표적인 데이터셋으로는 MIT/LL 데이터셋이 있으며 자체 제작된 데이터셋을 사용할 수도 있다.

정상상태 DB의 데이터에 따라 공격모델의 공격 성공 여부를 판별하게 된다. 예를 들어 OS 취약점을 이용한 웜 공격 모델의 경우 정상상태 DB의 취약점 공개일과 패치 생성일을 바탕으로 공격성공 여부와 방어성공 여부가 판별되게 된다.

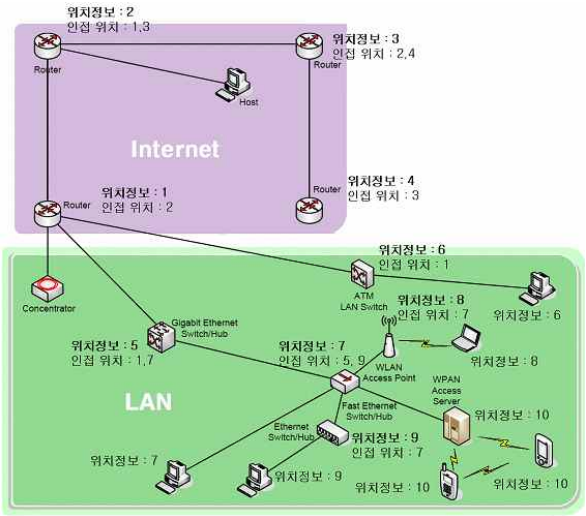

그림 2. TTA 표준활용맵을 바탕으로 한 가상네트워크 토폴로지

나. 공격 모델링

공격 모델링은 Petri-net[7]을 기반으로 한 공격모델을 구성하게 된다. 각 공격을 Petri-net을 표현기법을 이용하여 공격DB 구성하게 되며 각 공격 단계별로 정상상태 DB와 연관된 DB를 갱신하는 작업을 수행함으로 공격이 수행되게 된다.

그림 3 은 공격대상 호스트에서 Shell 사용권한을 획득하는 절차를 Petri-net을 이용하여 표현한 것이다.

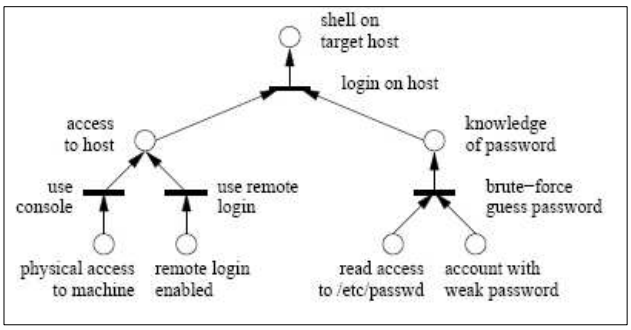

그림 3. Petri-net 기반의 Attack net 모델링 기법 예제

공격 DB는 각 공격의 단계별 세부단계를 저장하게 되며 연관된 정상상태 DB 요소를 기술하게된다. 따라서 세부적인 공격 표현을 하기위해서는 각 공격단계를 세부적으로 분석한 공격 절차 데이터를 사용해야한다. 대표적인 공격 유형이나 악성코드의 특성은 대표적인 Anti-virus 회사에서 제공하는 분석보고서를 활용할 수 있으며, 시뮬레이션 목적에 따라 논리적인 공격 모델을 별도로 생성할 수 있다.

다. 방어 모델링

방어모델링은 공격을 사전 차단하는 탐지모듈과 공격당한 네트워크 요소를 복구하는 치료모듈로 구성되게 된다.

탐지모듈은 방화벽, IDS, IPS의 공격탐지 및 차단을 구성하는 모듈로서 각 보안 장비의 성능에 따라 공격모델의 공격 수행시 공격을 차단할 것인지 허용할 것인지를 결정하게 된다. 이를 위해서 방어모델 DB에서는 각 보안장비의 탐지기능과 탐지율이 중요한 요소로 작용하게 된다.

치료모듈은 공격당한 네트워크 요소들을 복구하는 모듈로서 취약성 패치시기와 치료백신 배포시기 그리고 통합 패치시스템 구성여부를 바탕으로 감염된 호스트를 어느 시점에 정상상태로 복구시키는 지를 결정하는 부분이다. 방어모델 DB에는 복구행위에 해당되는 요소를 저장하게 되며 공격당한 일부 요소는 복구되지 않을 수도 있다.

표 3 은 방어모델 구성표를 나타낸 것으로 웜확산을 기반으로 하고 있다. 따라서 공격모델에 따라 구성요소가 추가될 수 있다.

표 3. 방어모델 구성표

분류	중요요소	
탐지모듈	Signature 기반	공격 Signature 보유여부, 탐지율
	Anomaly 기반	이상특성 탐지율
치료모듈	패치속도, 패치율, 중단율, 통합패치시스템 유무, 보안 정책변경시기, 네트워크 차단시기	

라. 모델링별 동작 구성

그림 4 는 각 모델링의 동작 구성을 나타낸다. 각 데이터베이스의 네트워크 구성요소들은 각 모델링의 작동에 따라 갱신되게 된다. 3개의 모델링들의 행위가 통합적으로 작동하는 것이 공격방어 시뮬레이터의 핵심이라고 할 수 있다.

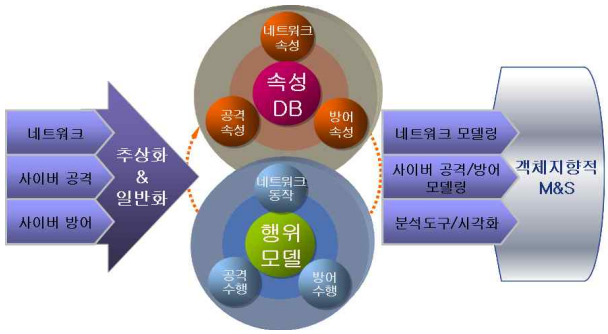

그림 4. 모델링별 동작 구성

또한, 네트워크 동장상태와 공격 및 방어 진행사항을 시각화하는 모듈과 공격 및 방어 결과를 통계적으로 분석하는 모듈도 추가할 수 있겠다.

5. 결론

지금까지 공격 및 방어 시뮬레이션을 위한 프레임워크를 제안하였다. 정상상태, 공격, 방어 모델링은 서로 유기적으로 영향을 주면서 시뮬레이션을 동작시킨다. 각 모델링의 상호작용이 각각 DB를 갱신시

키며 네트워크 상태를 나타내는 것이 이 프레임워크의 핵심이라고 할 수 있다. 본 논문에서 제안한 프레임워크가 전문적인 공격 및 방어 시뮬레이션 구현의 기본들을 제공할 것이라고 판단한다.

향후 연구로는 정상상태를 모델링하기 위한 효과적인 데이터셋을 구성하는 방법과 트래픽 표현방법 및 네트워크 상태에 대한 효과적인 시각화에 대한 연구가 있겠다.

참 고 문 헌

[1] 국가사이버안전센터, “2006년도 사이버 침해사고 사례집”, http://www.ncsc.go.kr/, 2007.5.

[2] 배성수, 한종수, “네트워크 시뮬레이터(NS2 기초와 활용)”, 세화, 2005. 2.

[3] 김용탁, 김태석, 권오준, “SSFNet 환경에서 보안시스템 시뮬레이션을 위한 IDS 모델링 및 구현”, 한국시뮬레이션학회논문지 제15권 1호, pp. 87~95. 2006. 3.

[4] QualNet 공식 웹사이트, http://www.scalable-networks.com

[5] OPNet 공식 웹사이트, http://www.opnet.com/

[6] 한국통신기술협회 웹사이트, http://www.tta.or.kr/

[7] Ronald W. Ritchey, Paul Ammann, "Using Model Checking to Analyze Vulnerabilities", IEEE, 2000