DEVS 모델링을 통한 교육용 DDoS 시뮬레이터의 구현

서희석*, 임기영*, 이승재**

요약

본 논문은 DEVS 모델링을 통한 교육용 DDoS 시뮬레이터를 구현하는데 목적이 있다. DEVS 모델링을 통해 DDoS의 기본적인 공격 구조를 파악할 수 있으며, 기존의 공격 시나리오와 공격 유형 그리고 악성코드 감염 방법을 분석하여 새로운 공격 시나리오를 만들고 이를 시뮬레이터에 적용시켜 피해정도를 산출시킬 수 있는 시뮬레이터를 구현하였다. 이 시뮬레이터에서는 악성코드에 감염시킬 클라이언트의 수와 각 클라이언트가 보내는 트래픽을 설정할 수 있으며, 공격 지속 시간 등을 설정할 수 있다. 이를 통해 시간별로 트래픽의 증가량을 볼 수 있는 그래프를 제공하고 인터넷 공격 성공률과 총 트래픽 양을 알아볼 수 있으며, DEVS 모델링을 통해 DDoS의 기본적인 구조를 알 수 있는 점과 접목시켜 정보보호 교육용 교재로 사용 할 수 있다.

Education Simulator Implementation for DDoS using DEVS Modeling

Hee-Suk Seo*, Ki-Kyung Lim*, Seung-Jae Lee**

ABSTRACT

In this paper, our goal is educational simulator implementation for DDoS using DEVS Modeling. With DEVS modeling we can understand basic structure of DDoS attack and we analyze existing attack scenarios and using infection method of malicious code to make a new attack scenario for make simulator which can calculate damage. This simulator can configure clients and traffic sending by clients.

Key Words : Information Security, DDoS, DEVS, Simulation, Attack Scenario

* 한국기술교육대학교 컴퓨터공학부
** 한국기술교육대학교 건축공학부
· 제1저자(First Author) : 서희석 · 교신저자(Correspondent Author) : 이승재
· 접수일(2010년 4월 30일), 수정일(1차 : 2010년 5월 28일), 게재확정일(2010년 6월 3일)

Ⅰ. 서 론

DDoS 공격이 성공했을 때 기업에 미치는 유·무형적 피해는 실로 엄청나다. 네트워크가 완전히 다운되는 경우는 논외로 친다고 할지라도, 단지 네트워크 속도가 급감하고 서비스가 불안정하게 되는 경우만 생각해보더라도 심각한 결과를 초래하게 될 것이다. 서비스를 24시간 이용하고 있는 수많은 고객들이 짜증과 불만족을 느끼며, 급격하게 경쟁사로 이탈하게 될 수도 있고, SLA(서비스수준협약, Service Level Agreement)에 위배되어 막대한 규모의 금전적인 피해보상을 하는 경우도 있을 수 있다. 또한 대규모의 집단소송에 휘말릴 가능성도 배제할 수 없을 것이며, 이로 인한 기업 이미지 실추, 주가하락, 매출감소 등 파장은 실로 엄청날 것이다.

초기에 DDoS 공격은 자기 능력과시를 위한 공격이었다면, 최근에는 뚜렷한 목적 및 대상을 상대로 DDoS 공격의 성격 및 범위를 확대해 가고 있다. 금전적인 이익을 목적으로 하는 DDoS 공격에서부터 게임물 등급위원회 홈페이지 사태 그리고 지난 2009년 7월 7일 DDoS 대란까지 개인적인 불만으로 인한 보복성 공격, 돈을 받고 경쟁사를 공격하는 청부공격 등이 등장해 DDoS 공격이 보다 조직적이고 위험한 사이버 범죄로 진화하고 있음을 알 수 있다.

2008년 3 월 국내 대형 증권사 홈페이지가 악의적인 공격자에 의해서 DoS 공격을 당하는 사건이 발생하였다. 다행히 온라인 주식거래관련 시스템이 아니어서 홈페이지 접속이 어려운 것 외에는 큰 피해가 발생하지는 않았지만, 만약 홈트레이딩 시스템을 대상으로 하는 공격이었다면 엄청난 경제적, 사회적인 문제가 발생할 수 있었던 상황이었다. 지난해 발생한 게임아이템 거래 사이트들에 대한 분산 서비스 거부 공격(Distributed Denial of Service: DDoS)으로 인한 서비스 장애가 발생하여 막대한 손실을 보았다고 한다. 이러한 DDoS 공격은 수백 Mbps 의 공격에서부터 최근에는 최대 20~30Gbps 의 트래픽을 유발하는 대형 공격까지 다양한 형태로 발생하고 있는 현실이다. 이 같은 DDoS 공격에 속수무책으로 당하는 기업들이 연일 보도되면서 인터넷서비스 업체에서 기존의 경계보안이 가진 문제점이 대두되고 있다. 그 동안 방화벽 및 IPS(Intrusion Prevention System · 침입방지시스템), 바이러스 월 등이 경계보안의 역할을 해왔지만 제 몫을 다하지 못하면서 피해가 속출한 것이다. 그리고 현재 많은 기업들이 가장 우려하는 보안 위협으로 DDoS 공격을 꼽고 있어 이에 따른 대책 마련이 시급한 실정이다[1, 2].

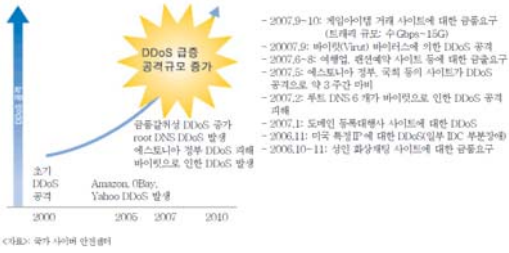

그림 1. DDoS 공격의 동향
Fig. 1. DDoS Attack Trends

DDoS 공격을 방어하기 힘든 이유는 이와 같다. 공격자인 좀비 PC들은 동일한 프로토콜의 절차 및 규칙을 사용해 DDoS 공격을 시도하기 때문에 보편적인 보안장비인 방화벽이나 침입방지시스템이나 고성능 통합위협관리 솔루션 등에서 원천 차단이 불가능하다. 즉 DDoS 공격은 고정 시그니처로 차단할 수 있는 취약점 공격이 아닌 일반적인 통신 환경 상에서 사용할 수 있는 극히 정상적인 변수 값을 이용하는 비취약점 공격이기 때문이다. 또한 공격자들의 공격 유형이 보다 체계적이고 다양한 접근 방법으로 변형되고 순환되고 있기에 기존의 보안장비로는 DDoS 공격 차단이 쉽지 않다[2, 3].

본 논문에서는 DEVS 모델링을 통해 DDoS의 기본적인 공격 구조를 파악할 수 있으며, 기존의 공격 시나리오와 공격 유형 그리고 Drive-by Download 라는 악성코드 감염 방법을 분석하여, 새로운 공격 시나리오를 만들고, 이를 시뮬레이터에 적용시켜 피해정도를 산출시킬 수 있는 시뮬레이터를 구현하였다. 또한 DEVS 모델링을 통해, DDoS공격의 기본적인 구조를 알 수 있다는 점과 접목시켜, 정보보호 교육용 교재로 사용하는데 목적이 있다.

II. 관련연구

2.1 Drive-by Download

Drive-by download는 사용자의 동의 없이 임의의 코드가 다운로드 되는 것을 의미한다. 특히 스파이웨어나, 컴퓨터 바이러스 또는 악성 프로그램에 의해 주로 사용되는 방식이다.

사용자가 임의의 웹사이트를 방문시, 해당 웹사이트는 HTML 코드를 사용자의 컴퓨터에 전송한다. 전송된 코드는 사용자의 웹 브라우저가 해당 사이트를 접속하기 위한 특별한 소프트웨어의 설치를 요구한다. 사용자는 대부분의 웹 브라우저가 특정 기능을 수행하기 위해 필요로 하는 적법한 플러그인 설치로 오인하여 의심 없이 설치하게 된다[4].

강제적인 사용자의 동의를 얻어 설치되는 경우 이외에도 해당 컴퓨터 사용자의 보안 설정에 따라 다이얼로그박스 없이 소프트웨어가 설치되기도 한다. 이러한 경우 사용자의 요구가 없어도 설치가 진행된다. [그림 2]는 Drive-by download 방법을 이용한 스파이웨어인 Gator의 설치 예이다. 본 논문에서는 해당 공격방법을 이용해 DDoS가 이루어진다고 가정하여 시뮬레이션을 진행하였다.

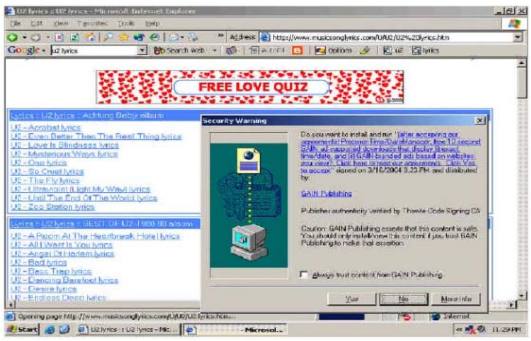

그림 2. Drive-by download 방법을 이용한 Gator의 설치
Fig. 2. Gator installation using Drive-by Download method

2.2 공격 유형

DDoS 공격은 여러 가지 형태로 구분되나 여기서는 설명의 편리를 위하여 대량의 트래픽을 유발하는 플러딩(Flooding)성 공격, 과도한 세션을 요구하는 커넥션(Connection) 공격,으로 구분하여 설명한다.

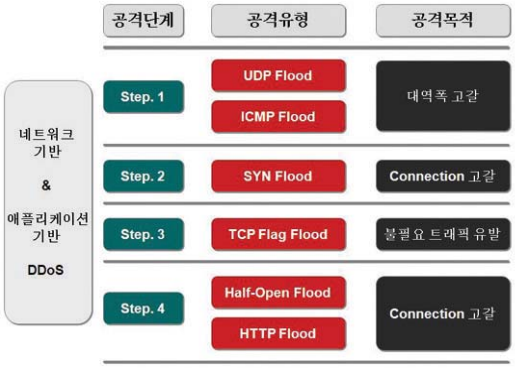

그림 3. 공격 단계별 공격 유형 및 목적
Fig. 3. Type and purpose of attack

(1) Flooding 공격

일반적으로 플러딩 공격은 정상 패킷과 동일한 패킷을 무작위로 전송하여 타깃시스템의 CPU, 메모리

등을 고갈시키고 네트워크의 병목을 야기해 정상적인 서비스 제공을 방해하는 형태의 공격방법이다. 이러한 플러딩 형태의 공격은 예전에는 소스를 스푸핑(Spoofing) 해서 공격하여 공격자를 숨기거나 운영자가 대응하는 것을 어렵게 했으나 최근에는 Zombie PC 를 조정하는 Botnet 의 확산으로 스푸핑을 하지 않고 real IP 로 공격하는 형태가 많은 상황이다.

SYN 플러딩 공격은 공격자가 TCP SYN 패킷을 무작위로 전송하여 착신 측의 TCP 세션으로 받는 Listen Queue 공간을 고갈시켜 정상적인 세션의 연결이 불가능하고, 시스템은 무차별적으로 들어오는 TCP 세션으로 인해 시스템이 마비되는 공격으로, 플러딩 공격의 대표적인 공격 중의 하나라고 할 수 있다. RST 플러딩 공격은 공격자가 TCP RST 패킷(TCP 패킷을 강제 종료 시 보내는 패킷)을 무작위로 전송하여 실제 액티브 세션을 단절시키는 공격이다. ACK Flooding 공격은 공격자가 TCP 세션이 없는 상태에서 TCP ACK 패킷을 무작위로 보내면 착신 측에서 변조된 발신 IP 로 RST 패킷을 무작위로 보내게 되고, 동시에 ICMP host unreachable 패킷을 보내면서 착신측 시스템의 과부하를 초래하는 공격이다.

UDP/ICMP 플러딩 공격은 각각 UDP/ICMP 패킷을 다량으로 유발시켜서 네트워크의 병목 및 시스템의 과부하를 유발시키는 공격방법이다. TCP Null 공격은 공격자가 TCP flag 를 설정하지 않은 비정상적인 패킷을 무작위로 전송하여 착신측을 마비시키는 공격이다. IP Null 공격은 공격자가 IP 헤더의 프로토콜 필드가 제로(0)인 패킷을 무작위로 전송하여 착신측을 마비시키는 공격이다.

(2) 커넥션 기반 공격

커넥션 형태의 공격은 HTTP 공격의 경우에서 아파치 서버의 경우 일반적으로 한 개의 데몬이 1,024 개의 연결만 지원하므로 공격자가 임의로 특정 PC 에서 수십 개의 연결을 설정하여 여러 대의 PC 에게 동일하게 접속을 요청하여 서버의 HTTP 처리 커넥션 용량을 초과시켜서 정상적인 HTTP 연결을 방해하는 형태의 공격으로 이런 경우 트래픽의 유발은 극소로 유지하면서 실제 서비스는 마비시킬 수 있는 공격이라고 할 수 있다. 마찬가지로 과다 TCP 커넥션 형태의 공격도 정상적인 TCP 연결 가능수치를 초과하는 공격을 유발시켜서 서버의 정상적인 연결 시도를 방해하는 형태의 공격이라고 할 수 있다.

(3) 애플리케이션 기반 공격

애플리케이션 형태의 공격은 VoIP 의 경우 SIP 단말의 등록을 위한 REGISTER 패킷을 과도하게 요청하는 REGISTER storm 공격, 통화 시도를 과도하게 요청하는 INVITE 공격, BYE 공격 등이 있으며, 기타 FTP 공격, email 스팸, DNS 공격, DHCP 리퀘스트 공격, SQL 공격, Netbios 공격, RPC 공격 등의 각종 프로토콜의 취약점을 활용한 다양한 형태의 애플리케이션 공격이 존재한다. Cache Control 공격은 보통 웹서버는 메모리에 있는 데이터를 이용해서 서비스하나, 캐시를 이용하지 말고 직접 달라는 리퀘스트가 오면 DB 를 다시 쿼리하여 해당 데이터를 직접 읽게 된다. 이로 인해 CPU 의 부하가 높아지게 하는 형태의 공격방법으로서 HTTP1.0 에는 없고 HTTP1.1 부터 추가된 기능이다.

III. DDoS 공격 모델링

3.1 DDoS 공격을 위한 전체 구조도

해당 DDoS 공격은 악성코드를 이용하여 DDoS 스크립트를 감염 좀비PC를 생성하여 특정 서버에 DDoS 공격을 하도록 하였다. 따라서 특정 명령에 반응하여야 하며, 명령자의 명령에 따라 공격을 시도하게 된다[7]

DA(DDoS Attack)모듈은 Client module과 Control System 모듈로 구성된다. Client module 은 악성코드 즉 DDoS Script 에 감염되어 실제로 공격을 수행하는 컴퓨터로 흔히 좀비PC라고 한다. 해당 모듈은 하위에 Order Exectuer 모듈과 Response Sender 모듈을 가지고 있는데 Order Executer는 Control System 으로부터 받은 명령을 직접 수행하는 모듈로써, Client 내부에서 공격을 담당한다. Control Sytem 은 해당 모듈로 공격 목표와 공격 목표로 보낼 트래픽 사이즈를 보내며, Order Executer 는 해당 정보를 수신 받아 공격을 하고, 공격 성공 쿼리와 목표의 상태 등을 Control System 모듈로 전송하게 된다. Response Sender 모듈은 하위 모듈로 Query Sender 모듈과 Data Sender 모듈을 가지고 있으며, Client Module과 Control System 모듈간의 정보 송수신을 담당하고 있다. Query Sender 는 DDoS Script가 PC에 감염이 성공하였을 때 성공 메시지를 보내는 역할을 하며, Data Sender 는 Client module의 ip 주소와 같은 정보를 Control System 으로 전송하는 역할을 한다.

Control SYstem은 Client module 즉 좀비 PC를 관리하는 호스트로써 DBMS 모듈과 Monitoring System 그리고 Infection System으로 구성되어 있다. DBMS는 공격자가 수집한 Client 들의 정보를 수집하는 모듈이며, Monitoring System 모듈은 Client 들을 실시간으로 관리하는 모듈이다. Infection System 모듈은 DDoS Script 감염을 담당하는 모듈이다.

3.2 Order Executer 의 모델링

[그림 4]는 Order Executer 의 구조이다. Order Executer 는 하부 모듈로 Target, Traffic Size, Self Destruct, Response Sender 모듈을 가지고 있다.

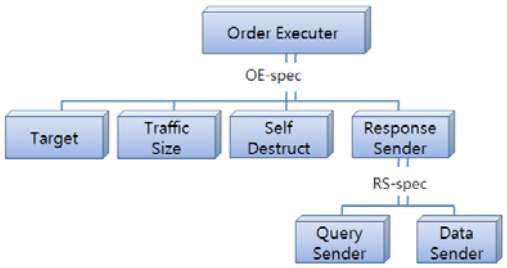

그림 4. Order Executer 의 구조
Fig. 4. Structure of Order Executer

Target 모듈은 공격 목표를 전송 받는 모듈이며, Self Destruct 모듈은 공격이 성공한 뒤 Control System에서 명령을 하달하면 Client 의 시스템을 손상시켜 피해를 증가시키는 기능을 한다. Traffic Size 모듈 은 공격 목표에게 보낼 트래픽 양을 결정하는 모듈이며, Response Sender 모듈은 하부 모듈로 목표에 쿼리를 보내 공격 성공 여부를 판별하는 Query Sender와 공격이 성공하면 목표에 대한 정보를 Control System 으로 보내는 Data Sender를 가지고 있다.

3.3Control System 의 모델링

[그림 5]는 Control System 의 구조이다. Control System은 DDoS Script에 감염된 좀비 PC들의 정보를 저장·관리하는 DBMS 모듈과 좀비 PC들을 실시간으로 관리하는 Monitoring System 그리고 DDoS Script 유포 와 감염자 증식을 위한 Infection System 으로 구성되어 있다. DBMS 는 Client Module의 하위 모듈인 Response Sender 모듈로부터 받은 좀비 PC의 정보를 저장 관리하여 공격 명령을 내릴 때 일괄적으로 처리할 수 있게 하는 역할을 한다.

Monitoring System은 하부 모듈로 Self Destruct 모듈과 Response Sender 모듈을 가지고 있는데, Self Destruct 모듈은 지난 2009년 7월 7일 DDoS 공격에

서도 있었듯이 각 좀비 PC에 있는 Order Executer 모듈 하부에 있는 Self Destruct 모듈에 명령을 내려, MBR 또는 중요한 시스템 파일을 손상시켜 특정 목표에 대한 공격 완료후 피해증가 및 역탐지 과정을 어렵게 만드는 역할을 한다. Infection System은 DDoS Script의 유포와 감염을 총괄하는 모듈로 하부에 Infector 와 Script Executor 가 있는데 Infector 는 웹페이지 또는 클라이언트의 취약점을 찾아 감염 경로를 확보하는 역할을 하고, Script Executor는 스크립트를 해당 경로에서 실행시켜 DDoS Script에 감염시키는 역할을 한다.

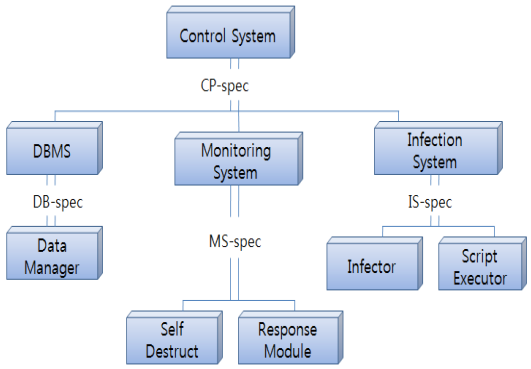

그림 5. Control System 구조 모델링

Fig. 5. Control System structure modeling

3.4 Monitoring System의 모델링

[그림 6]은 Monitoring System의 구조도 이다. 하부 모듈로는 Self Destruct 모듈과 Response Module 이 있다. Self Destruct 모듈은 Control System 이 관리하고 있는 좀비 PC가 공격에 성공한 뒤 좀비 PC의 시스템에 손상을 가해 피해를 증가시킴과 동시에 역탐지 과정에 어려움을 가져오는 기능을 하는 모듈이다. 하부 모듈로 자멸시킬 클라이언트를 설정하는 Target 모듈과 모듈 발동시간을 설정하는 Time Setter 모듈을 가지고 있다.

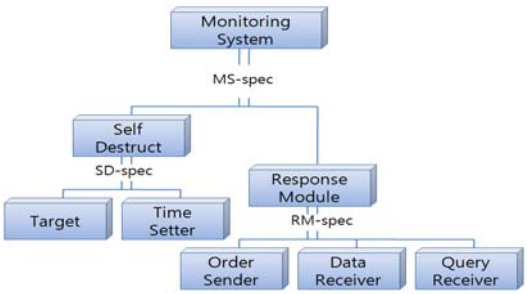

그림 6. Monitoring System 의 구조도

Fig. 6. Structure of Monitoring System

Response 모듈은 클라이언트와 데이터를 송수신하는 모듈로 주로 명령 전달, 데이터 수신 또는 감염·공격 성공 쿼리를 수신하는 모듈로 하부 모듈로는 Order Executer 모듈로 명령을 전송하고 클라이언트에게 감염 성공 질의 쿼리를 보내는 Order Sender 모듈과, 좀비 PC 또는 공격 목표에 대한 데이터를 전송받는 Data Receiver 모듈 그리고 공격 성공 또는 감염 성공시 클라이언트가 보내는 쿼리를 수신 받는 Query Receiver 모듈이 존재한다.

3.5 Infection System의 모델링

Infection System 은 Control System 하부 모듈로써 DDoS script 유포와 감염을 총괄하는 모듈이다.

[그림 7]을 보면 Infection System 하부 모듈로 Infector 와 Script Executor 가 존재한다. 웹페이지 또는 클라이언트의 취약점을 찾고 악성코드를 삽입하는 역할을 하는 Infector에는 하위 모듈로 웹페이지 또는 클라이언트의 취약점을 찾는 Vulnerability Finder 모듈과 실행파일 또는 웹페이지에 코드를 삽입해 숨겨두는 Packer 모듈 그리고 Packer 로 숨긴 악성코드를 실질적으로 클라이언트 또는 웹페이지에 삽입시키는 Injector 모듈이 있다.

Script Executor 모듈은 Infector 가 감염시킨 클라

이언트 또는 웹페이지 내의 DDoS Script의 실행을 관리하는 모듈이다.

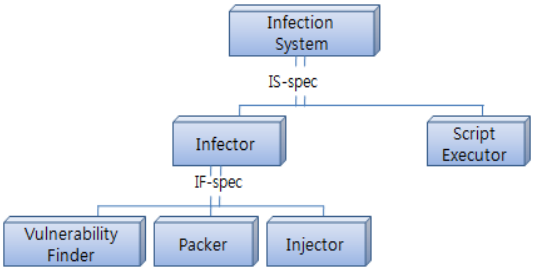

그림 7. Infection System의 구조도
Fig. 7. Structure of Infection System

3.6 모델링 시뮬레이션 결과

DEVS 모델링을 기반으로 구현한 시뮬레이션을 수행한 결과이다. 우선 시뮬레이터는 ISP 업체의 수와 최대 인터넷 수용 트래픽 그리고 평소 인터넷 트래픽 대여 폭을 설정할 수 있으며, 인터넷 공격자 수와 공격 성공 비율 그리고 Client 한 대당 공격 목표에 보낼 트래픽 대역폭을 입력받는다. 이에 따른 출력 결과로는 일별 인터넷 트래픽과, 그에 따른 상태 그리고 그래프를 출력해준다. 위의 결과 값은 인터넷 공격자가 1600명이고 공격 성공률이 40%일 경우 결과 값이다. 각 IX 망 별로 트래픽이 얼마만큼 있는지 알 수 있다. 초록색은 정상, 노란색은 경계 빨간색은 위험 수준의 결과이고, 그래프는 평소 트래픽을 보여준 다음 공격일로부터 트래픽이 대폭 증가하게 되었다.

표 1. DDoS 공격 시뮬레이션 설정 값
Table 1. DDoS attack simulation setting value

값 입력 사항			
시작일	2009-10-01	Client	1600명
종료일	2009-11-30	인터넷 공격 성공률	40%

인터넷의 최대 수용 트래픽은 2456Gbps 이다. 평소 인터넷 트래픽은 600Gbps 이고 공격 후는 최대 1771.08Gbps 트래픽이다. 위의 그래프의 결과 값으로 봤을 때 40%의 공격 성공률만으로도 인터넷 최대 수용 트래픽의 약 72%를 소모하는 것으로 나타난다.

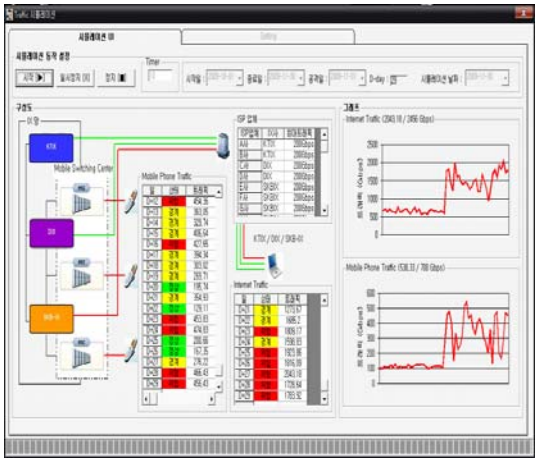

그림 8. DDoS 공격 시뮬레이션 결과2
Fig. 8. DDoS attack simulation results screen

표 2. DDoS 공격 시뮬레이션 설정 값
Table 2. DDoS attack simulation setting value

값 입력 사항			
시작일	2009-10-01	Client	1600명
종료일	2009-11-30	인터넷 공격 성공률	70%

위의 결과 값은 공격자가 1600명 이고 공격 성공률이 70%일 때의 시뮬레이션 결과 값이다. 40%의 성공률로 설정했을 때보다 위험수준의 결과가 많음을 알 수 있으며, 그래프는 평소 트래픽을 보여준 다음, 다음 공격일 부터 트래픽이 대폭 증가하였음을 알 수 있다. 인터넷 최대 수용 트래픽은 2456Gbps로 설정하였으고 평소 인터넷 트래픽은 600Gbps로 설정하였다. 공격 후 최대 2049.18Gbps 까지 트래픽 사용량이 올라감

을 알 수 있다. 위의 그래프의 결과값으로 봤을 때 70%의 공격 성공률로 테스트할시 최대 수용 트래픽까지 근접하여 공격에 효과가 나타남을 알 수 있다.

위의 결과 값은 인터넷 공격자가 5700명이고 공격 성공률이 95%일 경우 결과 값이다. 각 IX망 별로 트래픽이 얼마만큼 있는지 알 수 있다.

초록색은 정상, 노란색은 경계 빨간색은 위험 수준의 결과를 나타낸다.

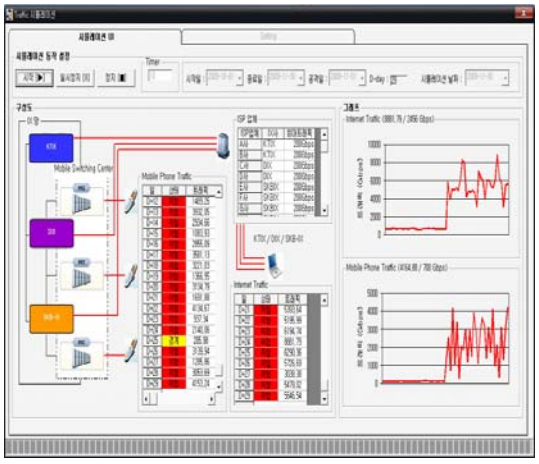

그림 9. DDoS 공격 시뮬레이션 결과 화면
Fig. 9. DDoS attack simulation results screen

표 3. DDoS 공격 시뮬레이션 설정 값
Table 3. DDoS attack simulation setting value

값 입력 사항			
시작일	2009-10-01	Client	5700명
종료일	2009-11-30	인터넷 공격 성공률	95%

그래프는 평소 트래픽을 보여준 다음 공격일로부터 트래픽이 대폭 증가하게 되었다. 인터넷의 최대 수용 트래픽은 2456Gbps 이다. 평소 인터넷 트래픽은 600Gbps 이고 공격 후는 최대 8881Gbps 트래픽이다. 위의 시나리오는 최악의 시나리오로 공격 성공률이 95% 이상일 때 우리나라의 네트워크가 전체적으로 마비 상태가 되어 네트워크를 활용 할 수 없게 된다.

Ⅳ. 결론

본 연구에서는 인터넷을 통해 급격히 확산되고 있는 DDoS 공격을 DEVS 모델링을 통해 체계적으로 정리함으로써 전체적인 공격 흐름과 구조에 대해 파악할 수 있게 되었다. 기존 DDoS 공격의 공격 방법과 경로 그리고 구조 등을 고찰하여 모델링을 하여 공격 탐지 및 구조파악시 어느정도의 기준이 될 만한 구조를 제시하였고 시뮬레이션 구현을 통해 DDoS 의 피해를 어느 정도 예측해 볼수 있었다. 이 시뮬레이션을 정보보호 교육에 접목시켜 교육용 교재로 사용한다면 DDoS 공격 과정과 구조에 대한 기초적인 지식을 얻는데 매우 도움을 줄 수 있을 것이다.

DDoS 공격 구조는 나날이 발전하고 있기 때문에 본 연구보다 더욱 자세한 연구가 필요하다. 또한 지난 2009년 7월 7일 공격뿐만 아니라 대부분의 DDoS 공격의 시발점이 Drive-by Download 공격 등을 통한 악성코드 감염이라는 점을 고려해본다면 악성코드 감염 기술에 대한 연구역시 필요하다.

또한 DDoS 공격을 위한 봇넷 구성과 패턴이 나날이 지능적으로 변하고 더욱더 복잡해짐에 따라 패턴 분석과 봇넷에 대한 연구가 되어야 할 것이다.

참고 문헌

[1] 구자현, *서비스거부공격의 유형 및 대응*, 정보통신연구진흥원, pp 5-8, 2008년 12월
[2] 서희석, 조대호, "IDS 성능 향상을 위한 DEVS 모델링," *한국시뮬레이션학회 추계학술대회*, pp. 125-130, 2000년 11월
[3] 시만텍, *Internet Security Threat Report Volume XII*, 2007년 11월

[4] 이형우, DDoS 공격에 대한 개선된 라우터 기반 ICMP Traceback 기법, 175 page, 2003
[5] 전용희 ,"*DDoS 공격의 경제 손실 모델 사례 연구*", 정보보호학회지 제19권 제3호, pp 58-69, 2009년 6월
[6] 한국정보보호진흥원, "*인터넷침해사고 동향 및 분석 월보*", 2008
[7] Forrester Consulting, "*DDoS: A Threat You Can't Afford To Ignore*", 2009년 1월
[8] *2009 정보보호백서*, 국가정보원, pp 297 2009.
[9] 조상엽, "경제 사회 시스템 보호를 위한 정보보안 정책 및 대응방안 수립", *한국지식정보기술학회 논문지*, 제4권 제1호, pp.11-19, 2009.
[10] 황문영 외, "클라우드 컴퓨팅 환경에 적합한 사용자 중심의 ID 관리기술", *한국지식정보기술학회 논문지*, 제5권 제1호, pp.51-58, 2010.

서희석(Hee-Suk Seo)
2000년 성균관대학교 공학사
2002년 성균관대학교 공학석사
2005년 성균관대학교 공학박사
2005년 한국시뮬레이션학회 편집위원
2005년~현재 한국기술교육대학교 교수
※ 관심분야 : 네트워크보안, 모델링 방법론

임기영(Ki-Young Lim)
2010년 한국기술교육대학교 재학
※ 관심분야 : 취약성분석

이승재(Seung-Jae Lee)
1995년 동경대학교 공학석사
1998년 동경대학교 공학박사
1998년 동경대학교 전임강사
2003년~현재 한국기술교육대학교 교수
※ 관심분야 : 건축구조해석