한국시뮬레이션학회 논문지
Vol. 18, No. 4, pp. 39-47 (2009. 12)

DDoS 공격 피해 규모 및 대응기법 비용분석을 위한 모델링 및 시뮬레이션 기술연구

김지연[2] · 이주리[1] · 박은지[1] · 장은영[2] · 김형종[1†]

A study of Modeling and Simulation for Analyzing DDoS Attack Damage Scale and Defence Mechanism Expense

Ji-Yeon Kim · Ju-Li Lee · Eun-Ji Park · Eun-Young Jang · Hyung-jong Kim

ABSTRACT

Recently, the threat of DDoS attacks is increasing and many companies are planned to deploy the DDoS defense solutions in their networks. The DDoS attack usually transmits heavy traffic data to networks or servers and they cannot handle the normal service requests because of running out of resources. Since it is very hard to prevent the DDoS attack beforehand, the strategic plan is very important. In this work, we have conducted modeling and simulation of the DDoS attack by changing the number of servers and estimated the duration that services are available. In this work, the modeling and simulation is conducted using OPNET Modeler. The simulation result can be used as a parameter of trade-off analysis of DDoS defense cost and the service's value. In addition, we have presented a way of estimating the cost effectiveness in deployment of the DDoS defense system.

Key words : Distributed Denial of Service(DDoS), Modeling and Simulation, OPNET, Damage Analysis

요 약

최근 특정 기업 또는 웹사이트에 대한 분산 서비스 거부 공격(DDoS:Distributed Denial of Service) 위협이 증가함에 따라 많은 기업들이 DDoS 공격 방어를 위한 보안 솔루션을 도입하고 있다. DDoS 공격은 대량의 트래픽을 네트워크에 전송함으로써 자원을 고갈시키고 정상적인 서비스 제공을 불가능하게 한다. DDoS 공격은 사전 탐지가 힘들고 효율적인 방어가 매우 어렵다. 본 연구에서는 이러한 상황을 고려하여 모델링 시뮬레이션을 통한 DDoS 공격에 대한 유연한 대응 방법을 연구하고자 한다. 특히, 서버의 개수를 변경할 경우 나타나는 DDoS 공격에 대한 동적 특성을 분석하고, DDoS 공격으로 인한 피해 규모의 객관적 산정을 위해 DDoS 탐지 시스템 운영 여부에 따른 손실 비용을 산정하는 방법을 제시한다. DDoS 공격 시뮬레이션은 OPNET Modeler를 이용하여 모델링하고, 시뮬레이션 결과를 통해 DDoS 공격으로 인한 서비스 가능 시간을 도출하여 네트워크 구조에 따른 서비스 가능여부를 확인 할 수 있다. 본 논문에서 수행하는 DDoS 공격 시뮬레이션은 현재의 네트워크 구성을 평가하고 신규 장비의 설치 또는 네트워크 구조 변경 시 발생 가능한 문제점을 예측하는 데에 활용가능하다.

주요어 : 분산 서비스 거부 공격(DDoS), 모델링 및 시뮬레이션, ,OPNET, 피해규모 산정

1. 서 론

현재 분산 서비스 공격(DDoS : Distributed Denial of Service)으로 인한 피해 사례가 증가하면서 많은 기업들이 DDoS 탐지 시스템을 도입하고 있는 추세이다. 그러나 기업의 입장에서는 DDoS 탐지 시스템의 설치 및 운영비용 대비 효과를 예측하기 어렵기 때문에 DDoS 공격을 고려한 효과적인 대응시스템 구축이 어렵다. 따라서 사전에

* 본 논문은 2009학년도 서울여자대학교 교내학술특별연구비의 지원을 받았음.
2009년 6월 30일 접수, 2009년 9월 8일 채택
[1] 서울여자대학교 정보보호학과
[2] 서울여자대학교 대학원 컴퓨터학과
주 저 자 : 김지연
교신저자 : 김형종
E-mail; hkim@swu.ac.kr

DDoS 공격에 대한 피해를 예측하고 대응 기법을 분석할 수 있는 모델이 필요하며, 이 모델을 기반으로 효과적인 DDoS 탐지 시스템을 구축할 수 있어야 한다. 본 논문에서는 DDoS 공격 시나리오를 구성하여 시뮬레이션을 수행하고, 대응 기법의 비용 및 효과를 고려하여 객관적인 피해 규모를 산정할 수 있는 시뮬레이션 환경을 모델링하고자 한다. 피해 규모는 시뮬레이션 결과를 반영하여 DDoS 탐지 시스템 운영 여부에 따른 손실 비용을 예측하여 산정할 수 있다. 본 논문에서는 DDoS 공격 시뮬레이션을 위해 네트워크 시뮬레이션 도구인 OPNET을 사용하였다. OPNET은 다양한 장비의 속성정보를 설정할 수 있기 때문에 실제 환경과 유사한 시뮬레이션이 가능할 뿐 아니라, 네트워크 구성 장비들의 처리 능력으로 인해 발생하는 문제점을 예측하고, 서버와 같은 장비의 성능 지표 도출을 통해 신규 장비의 설치 또는 네트워크 구조 변경 시 발생 가능한 문제점을 객관적으로 제시할 수 있다. 논문의 구성은 2장에서 관련연구를 설명하고 3장에서 DDoS 공격을 위한 시뮬레이션 네트워크를 모델링한다. 4장에서는 3장의 모델링을 기반으로 OPNET을 이용한 DDoS 공격 시뮬레이션을 수행하고, 5장에서 DDoS 탐지 시스템 운영 여부에 따른 손실 비용 산정 방법을 제시한 후 6장에서 결론을 맺는다.

2. 관련연구

2.1 DDoS 공격 및 대책방안

2009년 7월 7일 발생한 '7.7 인터넷 대란'은 청와대, 국방부, 외교통상부 등 국내 특정 사이트와 미국 주요 기관 홈페이지를 공격한 대표적인 DDoS 공격 사례이다. 3일 동안 세 차례에 걸쳐 계속된 공격은 보안 관련 기관과 이용자가 많은 우리나라의 주요 사이트들을 마비시켰고, PC 파괴 등 경제적인 손실을 유발하였다.

그림 1은 '7.7 인터넷 대란'의 공격과정을 보여준다. 개

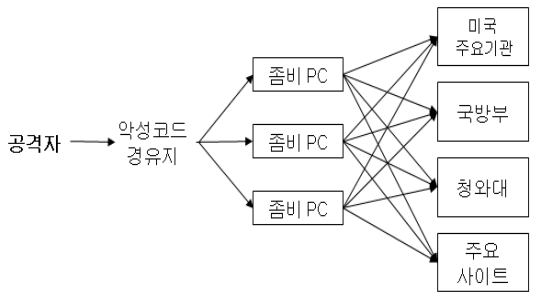

그림 1. '7·7 인터넷 대란' 공격 과정

인용 컴퓨터 하나하나가 좀비 PC가 되어 공격에 이용되는 DDoS 공격은 수많은 좀비 시스템들이 짧은 시간에 대상을 공격하기 때문에 시스템 단위의 해결방식으로는 총체적인 문제점을 해결하기 어렵다.

2.2 웹 트래픽의 특성과 웹 트래픽 발생을 위한 모델링

실제 DDoS 공격을 모델링하기 위해서는 정상적인 네트워크 환경의 트래픽과 공격 네트워크 환경의 트래픽 특성을 모두 고려하고, 두 환경에 대한 비교 분석을 수행해야한다. 웹 트래픽은 기존의 자기유사성(Self-Similar)을 띈 트래픽과 포아송(Poisson) 분포특성을 따르는 트래픽으로 구분하여 설명할 수 있다[1][2]. 이때 자기 유사한 트래픽을 처리할 경우에는 최번시(busy hour)의 트래픽양보다 훨씬 많은 트래픽을 처리할 수 있는 장비를 배치해야하고, 포아송 분포특성을 따른다면 최번시의 트래픽양보다 처리능력이 우수한 장비를 배치해야 한다. 모델링 시에는 혼잡 제어의 영향을 받는 트래픽에 대해 모델링을 수행하는 것이 바람직하다[2].

2.3 기존 피해규모 산정 모델

DDoS 공격으로 인한 피해는 다양한 기업과 개인에게서 발생할 수 있기 때문에 모두 같은 기준을 적용하여 피해를 산정하는 것이 어렵다. 기존에 제시된 피해규모 산정 모델 중 Backbone and Internet Service Providers, Large Corporate Customers, Web Service Provider, Insurance Companies, Telcos 등의 예제 시나리오는 공격 발생 시점과 중단 시점, 이후의 추가적인 손실에 대해서 피해규모를 제시하고 있고, 이 개념은 본 논문의 DDoS 공격 피해 규모 산정 시 활용이 가능하다. 예제 시나리오에서는 서비스 불가로 인한 생산적 손실(Downtime Loss), 침해 사고 복구로 인한 손실(Disaster Recovery), 서비스 제공 규약에 따른 사용자에 대한 손해배상(Liability), 사용자 감소로 인한 손실(Customer Loss) 등으로 손실의 종류를 구분하여 피해를 산정한다.

그림 2는 온라인쇼핑몰을 예로 고객과 온라인 쇼핑몰 간의 손실을 비교한 손실발생 사례이다. 그래프를 살펴보면 공격이 시작되는 t_0부터 공격이 중지되는 t_1의 기간에는 서비스 불가로 인한 생산적 손실과 침해 사고 복구로 인한 손실이 발생하며 t_1 이후에는 온라인쇼핑몰에서만 추가적으로 서비스 제공 규약에 따른 사용자에 대한 손해배상과 사용자 감소로 인한 손실이 발생하고 있다.

그림 3은 WSP(Web Service Provider)와 BSP(Business Service Provider), ISP(Internet Service Provider)간의 손

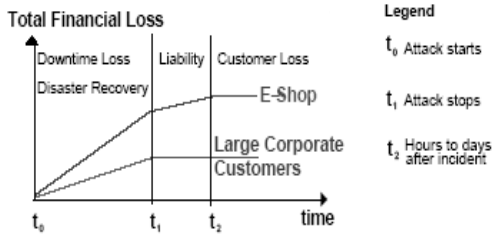

그림 2. Large Corporate Customers 와 온라인 쇼핑몰 간의 손실 비교[3]

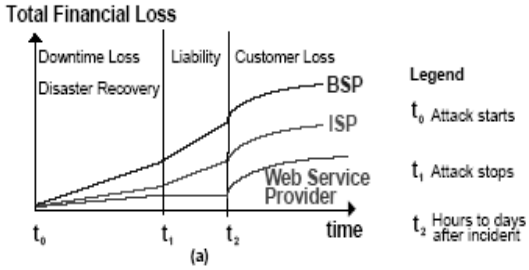

그림 3. Web Service Provider와 BSP, ISP 간 손실 비교[3]

실 비교를 보여주는 그래프이다. 공격도중에는 손실의 크기는 다르지만 WSP, BSP, ISP 모두 서비스 불가로 인한 생산적 손실과 침해 사고 복구로 인한 손실이 존재한다. 하지만 공격이 중단된 후의 WSP는 서비스 제공 규약에 따른 사용자 손해배상이 발생하지 않는다.

그림 4는 보험회사를 예시로 만든 손실발생 사례로 공격이 끝난 이후에 서비스 제공 규약에 따른 사용자에 대한

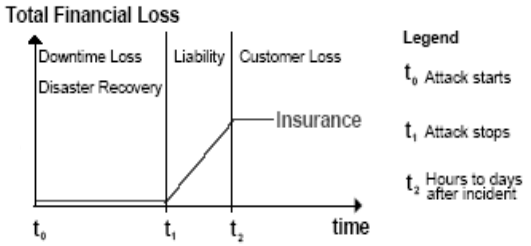

그림 4. Insurance Company의 각 유형별 손실[3]

손해배상에 의한 손실이 나타난다. 이는 보험회사의 특징을 고려하여 만들어진 손실 그래프이다.

3. DDoS 공격 네트워크 모델링

DDoS 공격 시뮬레이션을 위한 네트워크 구조는 그림 5와 같이 공격 모델링, 탐지 모델링, 성능 분석 모델링 단계로 구분할 수 있다. 그림 5는 DDoS 공격 트래픽이 IDC의 서버로 유입되는 과정을 보여준다.

공격 모델링 단계는 공격 형태를 결정하는 단계로서 공격자의 수와 전송 패킷 등을 모델링하여 공격 시나리오를 구성한다. 탐지 모델링 단계는 DDoS 공격에 대응하기 위한 대응 기법으로 공격 규모 및 서버의 성능에 따라 그 속성이 결정될 수 있다. 즉, 하나의 공격 시나리오에 대하여 DDoS 탐지 시스템의 속성을 변경함으로써 DDoS 탐지 시스템의 성능 분석을 수행할 수 있고, 반대로 DDoS 탐지 시스템 속성을 고정시킨다면 DDoS 공격 시나리오를 변경하여 DDoS 공격에 따른 서버의 성능 분석이 가능하다. 성

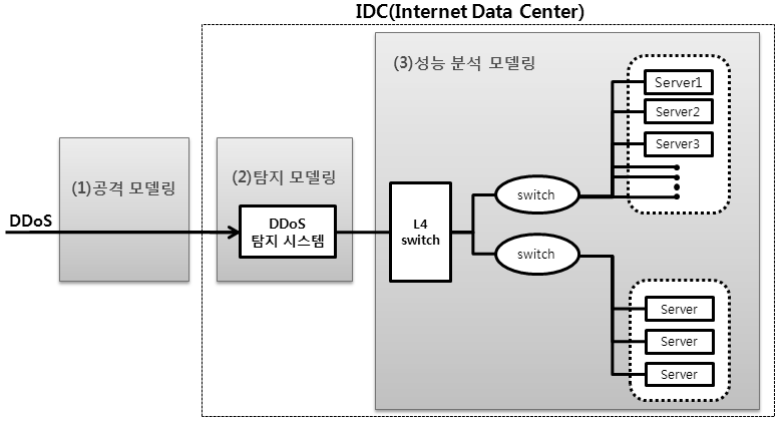

그림 5. DDoS 공격 시뮬레이션 환경 모델링

능 분석 모델링 단계는 서버가 DDoS 탐지 시스템으로부터 필터링 되지 않은 트래픽을 수신하는 단계로서 서버의 물리적 속성과 수신 트래픽 양에 따라 서버의 성능 즉, 서비스의 효율이 결정된다. 이 단계에서는 성능 분석 지표를 다양하게 도출함으로써 효율적인 대응 기법을 마련할 수 있다.

4. OPNET 시뮬레이션

4.1 공격자 비율에 따른 시뮬레이션

본 논문에서는 DDoS 공격 시뮬레이션을 위해 네트워크 시뮬레이션 도구인 OPNET을 이용하여 그림 6과 같은 공격 네트워크를 모델링하였다.

네트워크에는 공격자(Attacker)와 일반 사용자(Normal Client) 그룹이 존재하고, 두 그룹은 웹서버(Web Server)로 서비스 요청 패킷을 전송한다.

시뮬레이션을 위한 웹서버 및 공격 트래픽, 공격자와 일반 사용자의 시뮬레이션 속성 값은 각각 표 1, 2와 같다. 일반 사용자는 동시 접속자수를 가정하여 4000명으로 고정하고, 시나리오별로 공격자를 1명, 10명, 100명으로 하여 공격자에 대한 일반 사용자 비율을 각각 1/4000, 1/400, 1/40로 결정하였다.

시뮬레이션 시간은 1시간으로 일반 사용자는 시뮬레이션 시간 동안 패킷을 지속적으로 발생시키는 데에 비해, 공격자는 시뮬레이션 시작 30분 시점에 0.1초 간격으로 10분간 패킷을 전송한다. 공격자가 1명, 10명인 시나리오 1, 2에 대한 시뮬레이션 결과, 그림 7과 같이 공격이 발생하는 1800초 시점에 DDoS 공격에 의한 패킷량이 증가하는 것을 볼 수 있다.

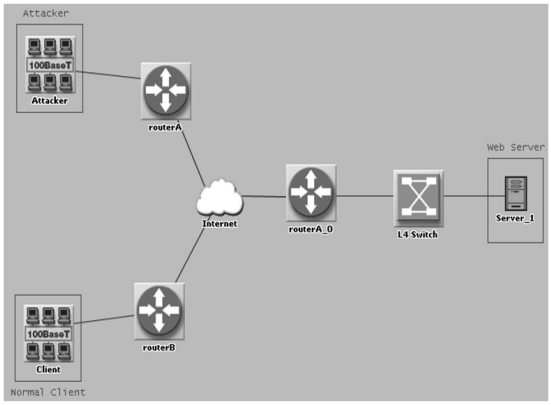

그림 6. DDoS 공격 시뮬레이션 모델링

표 1. 시뮬레이션 환경 설정

Attributes	Scenario 1	Scenario 2	Scenario 3
Attacker ratio (Attacker/ Normal Client)	1/4000	1/400	1/40
Web Server	Sun Blade 1000 Model 2900		
	2 CPU, 1Core(s) per CPU, 900MHz, Solaris, System		
Web Traffic	Http 1.1		
Transport Protocol	TCP		

Normal Client는 일반 사용자만 존재하는 환경으로서 공격자가 존재하는 시나리오 1, 2의 시뮬레이션 결과와 비교하기 위한 시뮬레이션 결과이다. 두 가지 공격 시나리오

표 1. 시뮬레이션 환경 설정

Profile configuration				Attacker	Normal Client
Application	Web traffic	Start time offset(sec)		uniform(5,10)	uniform(5,10)
		Duration(sec)		End of Profile	End of Profile
		Repeatability	Inter-repetition Time(sec)	Constant(0.1)	Exponential(300)
			Number of Repetitions	Unlimited	Unlimited
			Repetition pattern	Concurrent	Serial
Operation mode				Serial(ordered)	Serial(ordered)
Start time(sec)				Constant(1800)	Uniform(100,110)
Duration(sec)				Constant(600)	End of Simulation
Repeatability	Inter-repetition Time(sec)			Constant(60)	Constant(60)
	Number of repetitions			None	Constant(300)
	Repetition Pattern			Serial	Serial

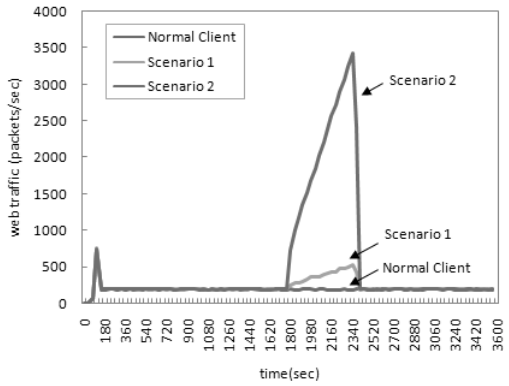

그림 7. 웹서버 송수신 패킷(Scenario 1, 2)

의 경우는 공격이 진행되는 동안 웹서버에 과부하가 발생하지만 시뮬레이션 종료 시까지 일반 사용자에 대한 정상적인 웹서비스 제공이 가능하다. 그러나 공격자의 수가 100명인 시나리오 3의 경우는 공격 발생 3분 53초 시점에 웹서버의 다운이 발생한다. 이것은 서버 모델 역시 소프트웨어이기 때문에 발생하는 현상이며 모델의 버퍼 관리에 대한 일부 코드 변경을 통해 적절한 형태의 서버 모델을 개발할 수 있다.

4.2 시뮬레이션 확장

4.1에서 수행한 기본적인 DDoS 공격 시뮬레이션을 기반으로 공격자 서브넷 및 서브넷의 좀비 프로세스 수, 공격 대상인 서버 수에 변화를 주어 서버가 받는 공격 피해 및 유실데이터의 존재 여부를 분석하기 위한 추가 시뮬레이션을 수행하였다.

4.2.1 공격 및 서버 모델 변경 시나리오

공격 변경 모델에서는 공격 서브넷과 서버의 성능 및 공격 트래픽에 대하여 표 3과 같이 설정하였고, 서브넷은 1개, 3개, 5개, 공격 서브넷의 좀비 프로세스는 각각 1개, 3개, 6개로 변화시켜 1번부터 9번까지 총 9개의 시나리오에 대하여 시뮬레이션을 수행하였다. 확장된 시나리오에 대한 시뮬레이션 구성은 그림 8과 같다.

서버 모델 변경 시나리오에서는 좀비 프로세스의 수를 20으로 일정하게 유지하고 서버의 수를 1개, 3개, 5개로 변화시켜 시나리오 10부터 12까지 총 3개의 시나리오를 통해 서버가 받는 영향을 분석한다. 서버의 성능 및 공격 트래픽은 공격 모델 변경 시나리오와 동일하게 표 3과 같이 설정하였다. 서버 변경에 의한 시뮬레이션 모델은 그림 9와 같다.

4.2.2 시뮬레이션 결과

그림 10과 그림 11은 좀비 프로세스가 6개 존재하는 시나리오 3과 좀비 프로세스가 6개인 서브넷이 3개 존재하는 시나리오 6의 시뮬레이션 결과로서 좀비가 보낸 트래픽 양과 서버가 받은 트래픽양의 그래프를 보여준다.

그래프 상에서 보면 모든 서브넷에서 보내는 트래픽의 총 합과 서버가 받는 트래픽의 양이 동일한 것을 볼 수 있는데 이것은 패킷의 전송과정에서 손실된 패킷이 없음을

표 3. 시뮬레이션 확장 시나리오

구분	Scenario	Attacker subnet 수	Attacker 수	Server 수	Web Server	web Traffic	Transport Protocol
공격변경 시나리오	Scenario 1	1	1	1	Sun Blade 1000 Model 2900,2CPU·1Core(s) per CPU, 900MHz, Solaris, System	Http 1.1	TCP
	Scenario 2		3				
	Scenario 3		6				
	Scenario 4	3	1				
	Scenario 5		3				
	Scenario 6		6				
	Scenario 7	5	1				
	Scenario 8		3				
	Scenario 9		6				
서버변경 시나리오	Scenario 10	1	20	1			
	Scenario 11			3			
	Scenario 12			5			

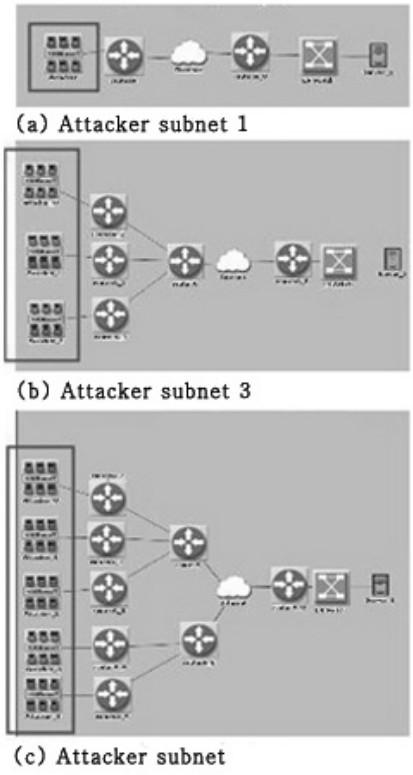

그림 8. 공격 모델 변경 시나리오

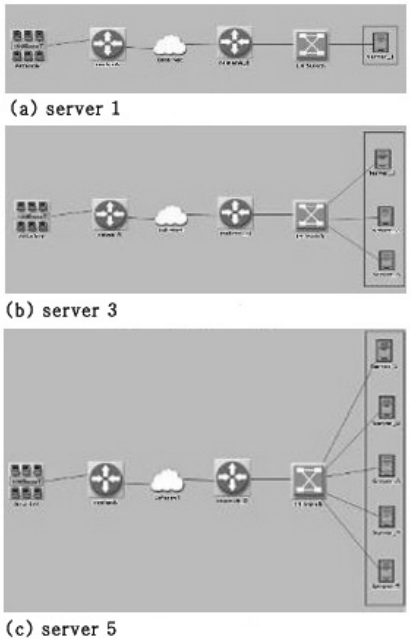

그림 9. 서버 변경 시나리오 모델링

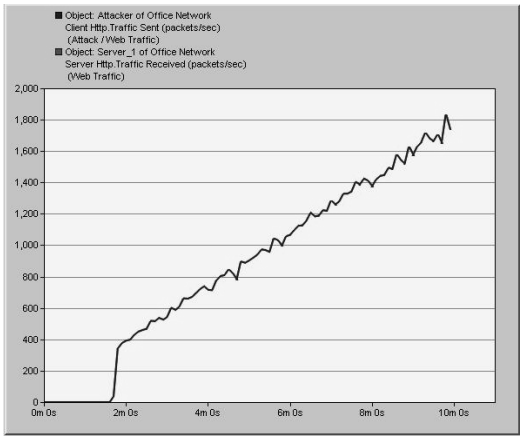

그림 10. 시뮬레이션 결과 -시나리오 3

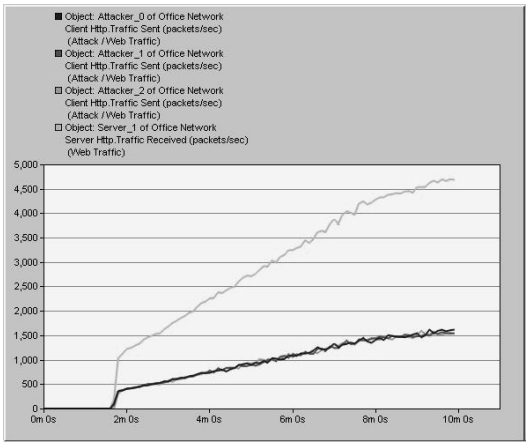

그림 11. 시뮬레이션 결과 -시나리오 6

의미한다. 서브넷이 5개인 경우 시나리오 7 ,8은 패킷 손실이 없이 모두 서버에게 전송되었지만 시나리오 9인 경우 즉, 좀비 프로세스가 30개인 경우에는 그림 12와 같이 시뮬레이션 종료 약 1분 30초 전 서버 과부하로 인해 시뮬레이션이 중단되었다. 그러나 각 서브넷에서 전송한 트래픽의 양과 서버가 수신한 트래픽의 양을 비교하였을 때에는 그 값이 동일하였고, 따라서 서브넷이 1개, 3개인 경우와 같이 패킷의 손실은 발생하지 않았음을 알 수 있다.

서버 변경 모델에서 서버가 1개인 경우의 서버 수신 트래픽은 그림 13과 같이 좀비 프로세스 20개가 송신한 트래픽의 양과 동일하다.

그림 14와 그림 15는 각각 서버가 3개, 5개인 경우의 송수신 트래픽 결과로서 하나의 서버가 수신하는 트래픽의 양이 각각 서버가 1개인 경우의 1/3, 1/5의 수준이다.

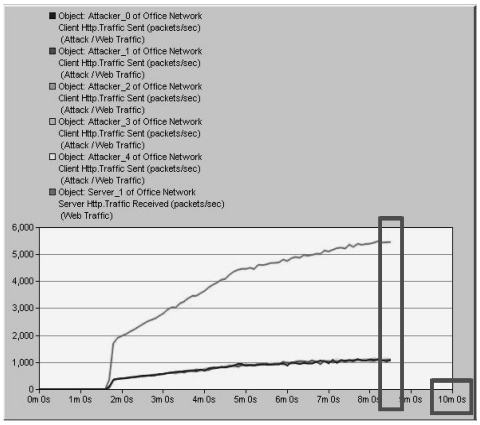

그림 12. 시뮬레이션 결과 -시나리오 9

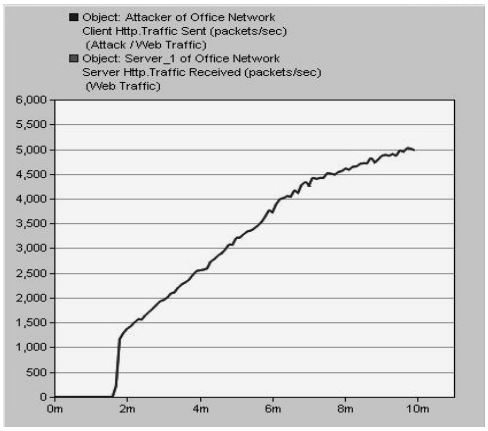

그림 13. 시뮬레이션 결과 - Server 1

이것은 동일한 수의 좀비 프로세스가 여러 서버에 분산시켜 패킷을 송신하기 때문이며 스위치에 연결되는 서버의 대수가 늘어날수록 하나의 서버로 집중되는 트래픽의 양이 분산되는 효과를 얻을 수 있음을 보여준다. 즉, 서버가 서버의 실질적인 트래픽 수신 한계량을 넘는 DDoS 공격을 받아도 서버가 여러 대 존재한다면 서버가 다운되는 피해를 줄일 수 있다는 것을 시뮬레이션을 통해 확인할 수 있다.

5. DDoS 공격 피해 규모 산정

5장에서는 DDoS 공격 시뮬레이션을 통해 도출할 수 있는 서버의 생존 시간을 이용하여 DDoS 공격으로 인한 피해 규모를 사전에 예측할 수 있는 피해규모 산정 방법을 제시한다. 피해 규모 산정 시에는 DDoS 공격으로 인한 직

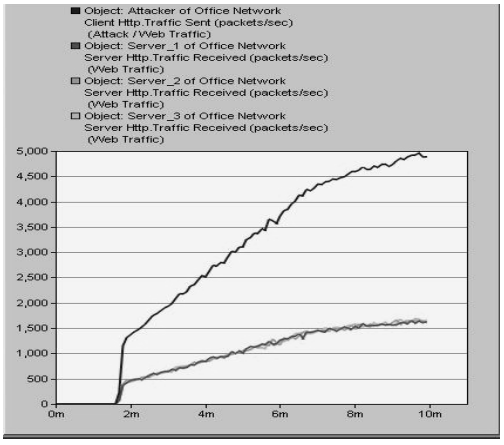

그림 14. 시뮬레이션 결과 - Server 3

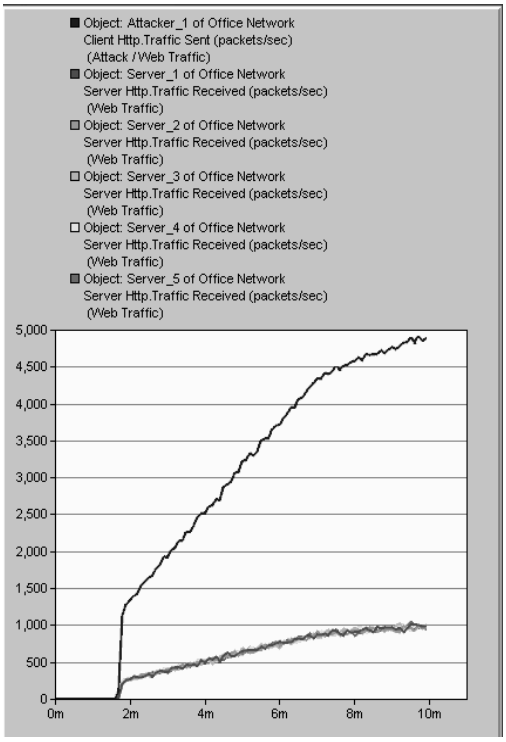

그림 15. 시뮬레이션 결과 - Server 5

접적인 피해 비용 뿐 아니라 탐지 및 복구에 소요되는 비용이 모두 고려되어야 하며 이는 기업의 효과적인 DDoS 탐지 시스템 도입 및 운영체계 수립을 가능하게 한다. 본 논문에서는 수식 (1), (2)와 같이 DDoS 탐지 시스템의 운영 여부에 따른 손실 비용을 계산하여 DDoS 공격으로 인한 피해 규모를 산정하고 있다.

DDoS 탐지 시스템 미운영시 :

$$L_{Cost} = T_{Service} \times C_{Utime} + C_{Recovery} \quad (1)$$

DDoS 탐지 시스템 운영시 :

$$L_{Cost} = T_{Service} \times C_{Utime} + C_{Recovery} + C_{System} \quad (2)$$

단,
- L_{Cost} : 손실비용
- $T_{Service}$: 서비스 중단시간
- C_{Utime} : 단위시간당 손실비용
- $C_{Recovery}$: 피해복구비용
- C_{System} : *DDoS* 대응시스템 운영비용

서비스 중단시간은 DDoS 공격 피해로 인해 기업이 정상적인 서비스를 제공 할 수 없는 시간을 의미하고, 여기에는 정상적인 서비스 제공을 위한 피해 복구 시간이 포함된다. 단위 시간당 손실비용은 기업이 정상적인 서비스를 제공하여 단위시간당 얻는 매출 이익을 의미하고, 피해복구 비용은 DDoS 공격 피해로부터 시스템을 복구하는 데에 소요되는 모든 비용을 의미한다. 또한 DDoS 대응시스템 운영비용에는 시스템의 도입 및 설치 비용 등 시스템 운영에 필요한 모든 비용이 포함된다.

6. 결 론

본 논문에서는 다양한 DDoS 공격 시나리오를 기반으로 서버의 서비스 가능 시간을 도출하기 위한 DDoS 공격을 모델링하고, OPNET modeler를 이용한 시뮬레이션을 수행하였다. DDoS 공격 시뮬레이션은 공격 유형 및 성격을 결정하는 공격 모델링 단계와 DDoS 공격을 탐지하고 대응하기 위한 탐지 모델링 단계, DDoS 공격에 따른 시스템의 피해를 측정하기 위한 성능 분석 모델링 단계로 구분되고, 각 단계의 모델링 및 시뮬레이션을 통해 DDoS 공격으로 인한 서비스 지연 시간, DDoS 탐지 시스템의 성능, 서버의 성능에 따른 서비스 효율을 도출할 수 있다. DDoS 공격 시뮬레이션 결과는 DDoS 공격으로 인한 피해 규모의 객관적 산정에 활용할 수 있고, 본 논문에서는 DDoS 공격으로 인한 피해 규모를 사전에 예측하고 대응 기법의 비용 및 효과를 산정할 수 있는 DDoS 탐지 시스템의 운영 여부에 따른 손실 비용 산정방법을 제안하였다. 본 논문에서 제시하는 DDoS 공격 시뮬레이션 및 피해 규모 산정 방안은 효과적인 DDoS 대응 시스템의 운영방안을 수립하는 데에 활용할 수 있고, 이를 기반으로 DDoS 공격을 고려한 효율적인 네트워크 구조를 제안할 수 있을 것이다.

참 고 문 헌

1. 임석구 외, “인터넷에서의 데이터 트래픽 발생 모델링”, 한국통신학회 추계학술대회, 2003.
2. 전의수 외, “통계적 분석을 이용한 HTTP 트래픽 모델링 및 분석”, 한국인터넷정보학회, 제5권, 제4호, 2004.
3. T.Tidwell 외, “Modeling Internet Attacks”, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Acad-emy, 2001
4. 김명섭 외, “Flow 기반의 인터넷 응용 트래픽 분석”, Knom review, 제7권, 제1호, 2004.
5. 박진수 외, “Web Server 규모 산정에 관한 연구”, 정보통신연구진흥원, 2001.
6. 한경은, “OPNET을 이용한 자기유사성 트래픽 발생기 설계 및 성능 평가”, 한국통신학회 논문지 Vol. 31, No. 5A, 2006.
7. Gabriel Macia-Fernandez, Jesus E. Diaz-Verdejo, Pedro-Teodoro, “Evaluation of a low-rate Dos attack against application server”, COMPUTER & SECURITY Vol. 27, 2008.
8. Ming Li, “An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition”, Computer & security Vol. 23, 2004.
9. Shabana Razak 외, “Network Intrusion Simulation Using OPNET”, OPNETWork Proceedings 2002, 2002.
10. Thomas Dubendorfer 외 “An Economic Damage Model for Large-Scale Internet Attacks”
11. 유황빈 외, “서비스거부공격 위협 분석 및 대응체계 연구”, 한국정보보호진흥원, 2000.

김 지 연 (jykim07@swu.ac.kr)

2007 서울여자대학교 정보보호공학과 공학사
2007~현재 서울여자대학교 컴퓨터학과 석박사통합과정

관심분야 : 정보보호, VoIP 보안, 모델링&시뮬레이션

이 주 리 (love_in_action@cyworld.com)

2010 서울여자대학교 정보보호학과 학사 졸업예정

관심분야 : 모델링&시뮬레이션, 스케쥴링

박 은 지 (eunji579@hanmail.net)

2010 서울여자대학교 정보보호학과 학사 졸업예정

관심분야 : 모델링&시뮬레이션, 스케쥴링

장 은 영 (yadury@swu.ac.kr)

2008 서울여자대학교 멀티미디어통신공학과 공학사
2009~현재 서울여자대학교 컴퓨터학과 석박사통합과정

관심분야 : 개인정보보호, 네트워크 보안, 취약점 분석 및 모델링, 접근제어

김 형 종 (hkim@swu.ac.kr)

1996 성균관대학교 정보공학과 공학사
1998 성균관대학교 정보공학과 공학석사
2001 성균관대학교 전기전자 및 컴퓨터공학과 공학박사
2001~2007 한국정보보호진흥원 수석연구원
2004~2006 미국 카네기멜론대학 CyLab Visiting Scholar
2007~현재 서울여자대학교 컴퓨터학부 조교수

관심분야 : 인터넷전화 보안, 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론