情 報 保 護 學 會 誌
第19卷 第3號, 2009. 6

DDoS 공격의 경제 손실 모델 사례 연구

전 용 희*

요 약

분산 서비스 거부(DDoS: Distributed Denial of Service) 공격은 다수의 소스에서 특정 목적지에 대하여 동시에 비정상적으로 대량의 패킷을 전송함으로써 목적지의 대역폭이나 처리력을 점유하게 된다. 최근의 DDoS 공격 통계에 의하면 초당 최대 오백만 패킷에 이르는 공격과 함께, 초당 백만 패킷 이상의 여러 공격들이 발생하고 있음을 보여준다. 이와 같이 DDoS 공격은 그 규모가 커지고 있고, 회수도 빈번하여 지고 있다. 본 논문에서는 DDoS 공격 대비를 위한 비용과 공격 발생시 서비스 중단으로 인한 경제 손실 모델 사례연구에 대하여 기술하고자 한다. 이를 통하여 비용 효율적인 DDoS 공격 대응 및 완화 기법의 설계를 위한 기초 자료로 활용하고자 한다.

Ⅰ. 서 론

DDoS 공격으로 인한 서비스의 중단은 어떤 조직에 대하여 심각한 결과를 초래할 수 있다. 일례로 한 대형 전자금융 회사에서 만약 한 시간 동안의 서비스가 중단된다면 천구백만 달러(한화로 247억 원 정도)의 손실을 볼 것으로 조사되었다[1]. 높은 가용성 요구사항을 가진 회사일수록 DDoS 공격이나 다른 이유로 인한 온라인 서비스의 중단이 심각한 기업적 손실을 야기 시킬 수 있다. 이 조사에서는 대부분의 회사들이 DDoS 공격에 대하여 적절한 보호 대책을 가지고 있지 않은 것으로 밝혀졌다. 대부분 DDoS를 포함하여 예기치 않는 트래픽에 대비하기 위하여 대역폭을 초과 비축(over-provisioning)하는 것으로 나타났다. 결과적으로 많은 회사들에서는 여분의 대역폭으로 75%를 보유하고 있음을 보여준다.

대역폭 초과 비축은 최악의 경우를 위한 접근이며, 경제적이지도 못하고 효과적인 해결책을 제공하는 것이 아님을 지적한다. 최근의 DDoS 공격 통계를 보면, 초당 최대 5백만 패킷(MPPS: Million Packets Per Second)에 이르는 공격과 함께, 백만 패킷이상을 운반하는 여러 공격들이 있음을 보여준다. 5 MPPS는 대략 40Gbps의 대역폭을 소모한다.

[표 1]은 년도 별 공격 크기 증가 추세를 보여준다.

〔표 1〕 년도 별 공격 크기의 변화

년도	Gbps	전년도 대비 크기 비율
2001	0.4	-
2002	1.2	300%
2003	2.5	208%
2004	10	400%
2005	17	170%
2006	24	141%
2007	40	167%

(자료: Arbor Networks)

현재의 증가율을 보면 곧 100Gbps 공격이 나타날 것으로 예측하고 있다.

Ⅱ. 악성코드 공격의 경제적 충격

웜과 모든 형태의 바이러스를 포함하는 악성 코드 공격의 수가 증가하고 있고, 그 결과로 회사, 정부 조직 및 개인에게 끼치는 비용도 증가하고 있다[2,3]. [표 2]는 대표적인 악성 코드 공격으로 인한 세계적 경제 충격에 대한 컴퓨터 경제학 분석을 보여준다[4].

경제적 충격은 바이러스 제거와 시스템 복구비용, 수입 손실 및 생산성 손실 비용을 포함한다. 2000년 이후의 경제적 손실이 감소된 것은 피해 복구 과정이 고도

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

로 자동화되었기 때문이다.

〔표 2〕 사고별 코드 공격 분석

연도	코드 이름	세계적 경제 충격 (원)
1999	ExploreZip	1조 3,260억
1999	Melissa	1조 4,300억
2000	Love Bug	11조 3,750억
2001	SirCam	1조 4950억
2001	Code Red	3조 4,060억
2001	Nimda	8,255억

(1달러 =1,300원)

보다 최근인 2008년 10월에 VeriSign은 기업에서의 DDoS 보호에 대한 상태와 필요성을 이해하기 위한 연구를 수행하기 위하여 Forrester Consulting에 의뢰를 하였다[1]. 19개의 IT 및 보안 전문가와의 심층적인 정성적 인터뷰를 통하여 DDoS 공격으로 인한 서비스의 중지가 기업에 어떤 경제적 손실을 가져오는지 조사하였다. 대상 기업은 십 억불 이상의 연 수입을 올리는 전자뱅킹, 온라인 전자상거래 및 ISP 서비스에 걸친 인터넷 서비스를 제공하는, 서비스 가용성에서 99.9% 이상이 요구되는 업체들이다. 조사된 19개의 회사 중에서, 적어도 99.9% 가용성 요구사항을 가지고 있으며, 그 중에서 6개의 회사는 99.99%의 가용성을, 5개의 회사는 99.999%의 가용성을 보고하였다. 99.999%의 가용성은 1년(365일×24시간×60분 = 525,600분) 중 5.25분 이하, 99.99%는 년 간 53분 이하, 99.9%는 8.76 시간 이하의 정지 시간을 요구함을 의미한다. [표 3]은 99.999% 가용성 요구사항을 가지는 기관에 대한 조사된 수입 손실을 보여준다.

〔표 3〕 서비스 손실로 인한 수입 손실(1달러=1,300원 기준)

구분	회사 A	회사 B	회사 C	회사 D
시간당 수입 손실	247억	3억 1,200만원	8억 4,500만원	2억 4,700만원
비즈니스 계열	E-뱅킹	E-뱅킹	전자상거래	전자상거래

위의 수치는 수입 손실만 고려한 것이고, 서비스 복구비용이나 사고 대응 비용을 포함하지 않는 것이다. Arbor Networks사에 의하면, 대표적인 DDoS 공격은 2시간에서 6시간 사이에 지속될 수 있다[5]. 이 경우, [표 3]의 회사 A는 평균적으로 988억이라는 엄청난 손실을 당할 수 있다. 24시간 내내 온라인 접근을 제공해야 하는 회사에 대하여, 성공적인 DDoS 공격이 엄청난 결과를 가져올 것이라는 것은 너무나 자명하게 보인다.

Ⅲ. 사례연구 1

사례연구 1에서는 [1]에서 제시된 DDoS 비용 모델에 대하여 기술한다.

3.1 개요

본 연구는 현재 공격 완화 메커니즘의 비용을 평가하고 그것의 효율성 및 유효성을 확인하기 위하여 실시되었다. DDoS에 대응하기 위하여 가장 많이 사용하는 방법은 대역폭 초과비축으로 조사되었다. 그 다음으로 DDoS-인지 침입탐지시스템(IDS) 및 방화벽을 포함하는 에지-기반, 구내망 DDoS 완화 기법을 사용하고, 마지막으로 단지 두 개의 기업만이 통합 DDoS 완화 서비스를 제공하는 것으로 조사되었다.

대역폭 초과비축은 소규모의 DDoS 공격에 대하여는 보호를 할 수 있지만, 대역폭 허용한도 이상의 공격에 대하여는 무용지물이 된다. 조사된 회사 중에서, 가장 높은 대역폭을 가진 회사는 7.5 Gbps overpeak 대역폭 할당을 보유하고 있어, 만약 40 Gbps 공격이 발생한다면 이 공격에 대응하기 위하여 추가적으로 32.5Gbps의 대역폭이 필요하게 된다. 설사 네트워크가 공격 트래픽을 수용할 수 있게 되더라도, 에지 방화벽이나 애플리케이션 서버가 다운될 것이다. 요즘은 경제적 이득을 목적으로 DDoS 공격[1]을 개시하기 위하여 대량의 봇넷 자원들이 거래되고 있어, 빅팀(victim)의 대역폭 비축을 무력화 시킬 수 있는 공격을 쉽게 생성할 수 있다.

3.2 비용 모델

이 모델에서는 자본 비용, 운용 경비 및 잠재적 서비스 붕괴를 포함하여 DDoS 완화(mitigation)의 전반적인 경제적 충격을 평가하기 위한 비용 모델을 제시한다. 이 모델은 아래 (1)식처럼 표현된다.

1) 이를 Ransom 형 DDoS 공격이라 한다.

총 DDoS 완화 비용= 초과 비축 경비 +
(DDoS 공격의 성공 확률 × 서비스 붕괴 비용) (1)

(1) 식에서의 비용 요소는 아래와 같이 기술된다.

- 초과 비축 비용: 대역폭 제공을 위하여 ISP에 지불하는 자본 경비와 운용 경비를 포함한다. 운용 경비는 대역폭 관리 비용을 포함한다.
- 서비스 붕괴 비용: 이 비용은 수입 손실, 수리 및 서비스 중단으로 인한 포렌식 경비 등의 결합된 비용이다.
- DDoS 공격의 성공 확률: 이것은 어떤 조직에서 보유 대역폭이 흡수할 수 없는 DDoS 공격을 경험할 확률이다.

3.2.1 초과 비축 비용 평가

초과 비축 비용은 대역폭 비용, 서버 다중화 비용 및 관리 비용으로 구성되며, 아래와 같다.

- 대역폭 비용: DDoS 대응을 위하여 사용되는 여분의 대역폭 비용이다. 여기서는 첨두(peak) 트래픽 이상으로 고려된 대역폭 양 만을 고려한다.
- 서버 다중화 비용: DDoS 트래픽을 다루기 위하여 사용되는 여분의 서버들을 위한 비용이다. 이것이 대표적인 자본 경비 비용이다.
- 관리 비용: DDoS 공격을 다루는데 소요된 인건비와 다른 비자본적 운용 비용을 포함한다.

가. 대역폭 비용

초과 비축 정도를 보기 위하여 초과비축지수(OPI: Over-Provisioning Index)를 도입한다. OPI는 첨두 대역폭의 백분율로 표시되며, overpeak 대역폭을 의미한다. 예를 들어, 어떤 조직의 첨두 트래픽이 100Mbps이고 200Mbps 가치의 대역폭을 보유하고 있다면, 이 조직은 100% 초과 비축을 하고 있고, OPI는 100%가 된다. [표 4]는 가용성 요구사항 및 회사 별 OPI를 보여준다.

〔표 4〕 가용성 요구사항 및 조직 별 OPI

가용성 요구사항	99.999%	99.99%	99.9%
1	43%	43%	40%
2	100%	50%	35%
3	100%	100%	50%
4	33%	18%	100%
5	100%	100%	50%
6		비공개	
평균	75%	62%	55%

나. 서버 다중화 및 관리 비용

이 비용은 트래픽 부하를 처리하기 위한 추가적인 서버 용량 비용과 서버 관리 비용이다. 높은 가용성을 요구하는 애플리케이션을 위하여, 대표적으로 복수의 서버들이 부하 공유나 대기 모드로 사용된다. DDoS 공격이 발생하는 경우를 대비하여 서버도 초과 트래픽을 처리하기 위한 여분의 용량을 보유해야 한다. 조사된 기관에서 대부분 2개에서 5개의 서버 상에 애플리케이션을 다중화하는 것으로 밝혀졌다. 그러나 첨두 트래픽 발생 시 서버들이 어떤 수준의 용량 레벨에서 수행되는지 알 수 없고, DDoS 대응이 아닌 다른 이유로 서버 다중화가 또한 필요하기 때문에, 서버 다중화 및 관리 비용 산정이 어려운 것으로 분석되었다.

3.2.2 서비스 중단 비용 평가

이 비용은 비즈니스 수입 손실 및 복구/포렌식 비용을 포함한다. 수입 손실은 비즈니스 계열, 회사 크기 및 서비스 용도에 따라서 회사마다 크게 다르다. 주식 거래와 같은 실시간 서비스를 제공하는 회사 같은 경우에는 서비스가 중단되면 즉각적이고 엄청난 수입 손실을 초래하는 반면에, 비 실시간 서비스를 운영하는 업체는 그 정도가 다소 완화된다. [표 5]는 조사된 19개 중에서 응답한 17개 회사에 대한 서비스 중단 비용 분포를 보여준다.

〔표 5〕 시간 당 수입 손실 분포

시간당 손실 비용	6,500만원~ 2억 6천만원	2억 6천만원~ 6억 5천만원	6억 5천만원~ 9억 7천5백만원	13억원~ 26억원	130억원 이상
해당 회사 수	8	5	1	2	1

[표 5]에 의하면, 회사가 제공하는 온라인 서비스 형태에 따라서 수입 손실 범위가 넓게 나타난다. 가장 큰 시간당 손실 비용을 가진 회사는 고가의 실시간 온라인 금융 거래를 수행하는 금융 서비스 회사인 것으로 나타났다.

복구 및 포렌식 비용은 서비스 중단 이후, 서비스를 복구하고 포렌식 분석을 수행하기 위한 단계에서 소요되는 비용이다. [표 6]은 99.999%의 가용성 요구사항을 가지는 온라인 서비스를 복구하기 위하여 사고 대응 절차에 들어가는 대표적인 인건비 조사 내용을 보여준다.

〔표 6〕 복구 및 포렌식 비용

회사	사고 취급 man-hours	지역	비용
A	38	미국	193만원
B	200	미국	1,017만원
C	70	영국	430만원

위비용에서 미국의 경우 정규직 네트워크 기술자 연봉기준은 1억 170만원, 영국은 1억 2,285만원 기준으로 작성되었다. 회사마다 이 비용은 다르겠지만, 대표적인 복구 및 포렌식 비용은 수백만 원에 이른다. 이 비용은 수입 손실에 비하면 무시할 수 있기 때문에, 서비스 중단 비용은 서비스 중단으로 인한 비즈니스 수입 손실 비용만 포함시키도록 하였다. 따라서 식 (2)가 성립된다.

서비스 중단 비용 = 서비스 중단으로 인한 비즈니스 수입 손실 (2)

3.2.3 DDoS 성공 확률 평가

해마다 DDoS 공격의 규모와 빈도가 증가되고 있다. 2007년 9월의 E-Crime Watch Survey에 의하면 2006년과 2007년 사이 12 개월 기간 안에 DDoS 공격을 경험한 회사가 94%에 이르는 것으로 조사되었다. 특정한 회사가 DDoS 공격의 타깃이 된다는 것을 결정하는 것은 어렵지만, 장기간 관찰을 통하여 보면 일년 중 한번은 적어도 DDoS 공격을 경험할 가능성이 높다고 지적하고 있다. 공격 규모와 조직의 하부구조와 운영에 대한 충격 정도를 결정하기 위하여, Arbor Networks, Shadowserver 및 US-CERT를 포함하는 다양한 소스들로부터의 공격 데이터와 표본들을 수집하였다. Arbor Networks 사의 255-일 트래픽 연구는 140,000 건 이상의 DDoS 공격 통계치를 수집하였다. [표 7]에 일부 공격 크기를 보여준다.

이 통계치와 관련 통계치들을 이용하여 인터넷상의 일반적인 DDoS 공격 확률 밀도 함수(pdf: probability density function)를 유도하였다. 예를 들어, 1.2 Gbps의 초과 비축은 80만 PPS까지의 공격을 견딜 수 있다. 제시된 pdf에 의하면, 80만 PPS 보다 더 큰 공격이 발생할 확률은 대략 11% 정도이다. 따라서 1.2 Gbps overpeak 비축을 가지고도 DDoS 공격을 경험할 확률이 대략 11%가 된다. 이 확률 분포는 전체적인 인터넷 트래픽의 통계치로부터 유도된 일반적인 분포 함수이며, 기대되는 공격율에 따라서 특정 조직에 대한 확률은 달라질 수 있다. 그러나 이것은 보유 대역폭이 흡수할 수 없는 공격을 경험할 수 있는 기본 확률을 평가하는 모델로 사용될 수 있다.

〔표 7〕 DDoS 공격 통계치

대역폭	수
5 MPPS 이상	12
4~5 MPPS	21
3~3.99 MPPS	20
2~2.99 MPPS	38
1~1.99 MPPS	60
1 MPPS 이하	140,000

3.3 최종 비용 모델

위의 제시된 내용을 바탕으로 최종적인 전체 DDoS 완화 비용은 식 (3)과 같이 된다.

총 DDoS 완화 비용 = 초과 비축 대역폭 비용 + (DDoS 공격의 성공 확률 × 서비스 중단으로 인한 수입 손실) (3)

3.4 비용 산정 예

이 비용 모델은 기대 비용의 하한 경계를 평가하는 보수적인(conservative) 모델로 기술하고 있다. 이 절의 비용 산정 예는 일년에 성공적인 DDoS 공격이 한 번 발생할 경우의 비용을 보여준다. 다수의 공격이 발생한다면, 비용이 상승하게 된다.

3.4.1 대형 금융 회사의 예

첫 번째 비용 산정의 예는 대형 금융 회사로써 온라인으로 전자 뱅킹 및 다른 금융 거래를 운영하는 회사이다. 이 서비스는 99.999%의 매우 엄격한 가용성 요구사항을 가지고 있다. 이 은행의 첨두 대역폭 사용은

10Gbps이고 75% 정도의 OPI를 사용하고 있다. 서비스 중단 시간 당, 이 회사는 8억 4,500만원 정도의 사업 손실을 당한다. 75% OPI는 7.5Gbps까지의 공격을 허용할 수 있고, 대략 625,000 PPS에 해당한다. 이 규모 이상의 DDoS 공격 발생 확률 밀도 함수는 2.5%로 제시되어 있다. DDoS 공격 평균 길이가 4시간으로 가정하고, 1 Mbps 대역폭 비용이 매월 13,000 원으로 가정하여, 아래와 같은 비용을 산정하였다.

총 DDoS 완화 비용 = 초과 비축 비용 + (DDoS 공격의 성공 확률 × 서비스 중단 비용)
= (7,500 Mbps × 13,000원/Mbps × 12월) + ((0.025 × (4시간 × 8억 4,500만원/시간)) = 12억 5,450만원

따라서 이 회사는 매년 DDoS 위협으로 거의 13억을 소비해야 하는 것으로 나타났다.

3.4.2 중규모 전자상거래 회사의 예

이 회사는 99.9%의 가용성 요구사항을 가지고 있는 전자상거래 서버를 운용하고 있다. 이 회사의 정상 대역폭 소비는 10Mbps이고 첨두 대역폭은 때때로 25Mbps에 이른다. 이 회사는 ISP로부터 50Mbps 링크를 사용한다. 매 서비스 중단 시간 당, 2억 8,600만원의 수입 손실을 당한다. 대형 금융회사에 비하여 규모와 수입 정도가 중간 정도 되는 셈이다.

이 회사의 OPI는 추가적으로 25Mbps를 보유하고 있기 때문에, 100%가 나온다. 따라서 매년 대역폭 초과 비축 비용이 25 Mbps × 13,000원/Mbps × 12월 = 390만원이다. 초과 대역폭 25 Mbps는 대략 1,666 PPS에 해당하며, 공격 가능 확률은 90%로 제시되어 있다. 그러므로 아래와 같은 비용을 산정하였다.

총 DDoS 완화 비용 = 초과 비축 비용 + (DDoS 공격의 성공 확률 × 서비스 중단 비용)
= 390만원 + ((0.9 × (4시간 × 2억 8,600만원/시간))
= 10억 3,350만원

따라서 이 회사는 매년 DDoS 위협을 다루는데 적어도 10억을 소비해야 하는 것으로 나타났다.

Ⅳ. 사례연구 2

[6]에서는 DDoS 공격의 충격을 다루기 위하여 지진과 토네이도의 충격을 분류하기 위하여 사용되는 시스템과 유사한 네트워크 중심적 MIDAS(Measure of Impact of DDoS Attacks) 스케일을 제안하고 있다. 아래에 제시하는 MIDAS 스케일은 전역적으로 관련된 DDoS 공격 충격 스케일에 대한 처음 시도로 보여 진다.

4.1 개요

현재 대부분의 DDoS 공격을 특성화하는 방법은 PPS(Packet Per Second) 혹은 BPS(Bit Per Second)와 같은 측정을 사용하는데, 이와 같은 방법이 잘 못되었다는 것이다. 예를 들어, 같은 100Mbps 공격이라도 케이블 모뎀으로 연결된 종단 호스트에 비하여 데이터 센터에 있는 성능이 좋은 서버에게는 무시할 수 있는 충격이 될 수 있다.

지진에서 사용되는 리히터(Richter) 스케일과 토네이도에 사용되는 후지타 스케일은 두 개의 다른 방식을 보여준다. 리히터 스케일은 지진이 미치는 영향에 관계없이 지각 판(tectonic plate)의 운동으로부터 방출되는 에너지에 대한 평가를 통하여 지진의 크기를 측정한다. 반면에 후지타 스케일은 토네이도 발생 후 수행되는 조사를 기반으로 발생한 실제적 손해를 평가한다. 그러므로 토네이도의 크기가 아니라 충격을 평가하는 것이다.

본 사례에서는 후지타 스케일과 비슷한 방법을 이용하여, 네트워크 서비스 제공자의 관점에서 DDoS 공격 충격 규모를 파악할 수 있는, 소위 MIDAS 스케일을 개발하고자 한다.

4.2 DDoS 공격의 영향

DDoS 공격의 비용을 파악하기 위하여 MIDAS 스케일은 특정 네트워크의 상황(context) 차원에서 비용 초점을 맞추고 있다. 공격 비용에서 네트워크 갱신이나 DDoS 완화 장비 설치비용과 같은 장기 비용은 제외시킨다. 특정 네트워크 상황에서 네트워크 제공자에 대한 DDoS 공격의 잠재적 경제적 충격에 초점을 맞추는 방법을 사용한다. 구체적으로, 잠재적인 경제적 충격으로 SLA(Service Level Agreement) 위반 비용과 고객 손실 비용을 고려한다.

4.2.1 SLA 위반 비용

DDoS 공격 발생으로 네트워크 운용자가 고객에게

지불해야 할 네트워크에 특징적인 비용이다. SLA는 다음과 같은 특성을 기초로 하고 있다는 사실을 찾아서 이용하고 있다.

- 네트워크 성능: 네트워크 가용성 혹은 정지시간, 지연, 손실 율과 지터
- 신뢰성: 사이트 대 사이트 신뢰성, 백본 신뢰성
- 패킷 전달 보장: 백본 네트워크 내의 허브 라우터 사이, 패킷 전달 율 일정한 값 이상.
- 기타 사항: 정전 보고 보장 및 전력 가용성

위의 대부분은 네트워크 관련 특성이다. 이런 SLA들이 네트워크-레벨 특성 측정을 경제 비용으로 변환하는데 도움을 준다는 분석이다.

DDoS 공격 발생으로 네트워크에 결친 SLA 위반사항이 발생하면, 시간 간격 T 동안 이 SLA와 연관된 고객비용의 총계를 계산하여 개략적으로 구한다.

4.2.2 위험 비용(Risk Cost)

고객에 대한 서비스 중단으로 네트워크를 떠나는 DDoS 공격 위험을 포착한다. 네트워크 운용자의 미래 수입에 직접 영향을 미치는 요소이다. Risk(c)가 고객 c가 DDoS 공격으로 인하여 네트워크를 떠날 확률이고, $Rev_{future}(c)$가 고객 c로부터의 미래 수입이라면, 한 고객에 대한 위험 비용 $C_{risk}(c)$은 아래와 같다.

$$C_{risk}(c) = Rev_{future}(c) \times Risk(c)$$

모든 영향을 미치는 고객들에 대하여 계산하면 총 위험 비용이 계산된다. 정확한 측정이 불가능하므로 다음과 같이 근사화 방법을 시도한다.

가. 위험한 고객 수입: 대부분의 계약자가 최소 1년 기간이라 가정하고, 미래에서의 1년을 12개월로 시간 간격을 고정시킨다.

나. 고객 이탈 위험: 여러 가지 다른 이유로 인하여 고객 이탈이 발생할 수 있으나, 다음과 같이 분류한다.

(i) 공격 범주: 고객 트래픽의 영향 정도

(ii) 공격 기간: 고객 트래픽의 영향 기간

(iii) 공격 빈도: DDoS 공격에 의한 고객 영향 빈도

고객 행위에 대한 정확한 모델의 어려움과 모델을 위한 실제적인 데이터가 없기 때문에, 고객 이탈의 위험을 평가하기 위하여 다음과 같은 가정을 한다.

- 트래픽 총량의 1% 이상이 영향을 받으면, 고객에게 영향이 있다고 가정한다. 여기서 영향을 받는다는 것은, 최대 손실율과 지터와 같은 응용 특정 성능 요구사항이 만족되지 않음을 의미한다.
- 직관적으로 DDoS 관련 영향에 대한 고객의 불만족은 공격 기간의 비-선형 함수로서 커지는 것을 예측한다. 공격 기간이 더 오래 지속될수록, 고객 이탈 확률은 증가된다는 분석이다.
- 공격 빈도 영향도 지수적 증가로 모델한다.

4.3 MIDAS 스케일 평가

MIDAS 스케일 평가를 위하여 DDoS 공격을 아래와 같은 4개의 범주로 구분한다.

- 강하고 집중된 공격(Strong and Concentrated): S&C 공격은 대량의 트래픽 양을 가지고 몇 개의 소스로부터 시작되고, 소수의 목적지를 타깃으로 하는 공격을 지칭한다.
- 약하고 집중된 공격(Weak and Concentrated): W&C 공격은 S&C 공격에 비하여 훨씬 적은 공격 양을 가지고 있으나, 집중도 측면에서는 동일한 공격 양상을 지칭한다.
- 강하고 분산된 공격(Strong and Distributed): S&D 공격은 다수의 소스로부터 시작하며, 네트워크를 따라 통상적으로 확산된다. 따라서 네트워크 링크의 많은 부분에 과부하를 발생킨다.
- 약하고 분산된 공격(Weak and Distributed): W&D 공격은 S&C 공격의 반대 특성을 가지는 공격을 지칭한다.

그리하여, 예를 들어, S&D 공격은 더 많은 고객에게 영향을 주는 더 많은 링크를 과부하 시키기 때문에, 높은 MIDAS 스케일이 기대된다.

미국의 인구 밀도를 반영하는 가상적인 토폴로지를 사용하여 평가 결과를 보여준다. 강한 공격은 약한 공격의 거의 12배 대역폭을 차지하는 것으로 설계되었다. 분산 공격은 적어도 2개의 PoP(Point of Presence)로부터 선택된 적어도 5개의 소스로부터 시작되며, 적어도 2개의 PoP에 있는 5개 이상의 목적지를 공격하는 것을 가정하였다. 반면에 집중 공격은 동일한 PoP에 있는 2개 이하의 소스로부터 시작하여, 같은 PoP에 위치한 2개 이하의 타깃을 공격하는 것을 가정하고 있다.

본 연구에서는 이러한 가정을 바탕으로 여러 가지 공격 경우의 행위를 보여준다. S&D 공격은 소수의 코어

링크뿐만 아니라 액세스 링크의 집합을 과부하 시킨다. 따라서 충격 커브가 W&D 공격에 비하여 급하게 증가하는 것을 보여준다. 반면에 W&D 공격은 어떤 시간에서 더 작은 수의 링크에 통상적으로 영향을 주며, 결과적으로 더 많은 단계를 가지고 점차적인 증가를 보여준다. 유사한 행위가 집중 공격에 대하여도 관측되었으나, 최대 충격값을 가지는 기간은 훨씬 작게 나타났다.

V. 사례연구 3

[7]에서는 대규모 인터넷 공격에서의 경제 손실 모델에 대하여 SWITCH 인터넷 백본에서의 공격을 조사한 연구 프로젝트 DDoSVax[8]의 일부를 제시하고 있다.

5.1 개요

현재 인터넷 하부구조의 복잡성을 다루기 위하여 개념 레벨로 축약된 인터넷 시스템 모델을 제시한다. 이를 통하여 하부구조에 대한 공격에 의하여 유발되고 개별 요소들에 의하여 입게 되는 직간접의 재정적 손실을 평가하기 위하여 관련 있는 의존성에 대한 조사가 가능하다는 분석이다.

DDoS와 같은 형태의 공격으로 유발되는 재정 손실과 포함된 상호의존성을 분석하기 위하여 단계적 방법을 택한다. 이를 위하여, 정성적 방법으로 시간 별 손실을 보여주는 그래픽 플롯, 다른 형태의 손실에 대한 재정 손실을 계산하기 위하여 사용되는 수학 공식과 구체적인 설정에 대하여 재정 손실을 계산하는 방법을 보여주는 시나리오 예제를 사용한다.

5.1.1 손실 대 시간

재정 손실은 인터넷 성능의 심각한 저하로 기대되는 영향이다. 게다가 재정 손실은 시간에 따라서 변한다. 경제 손실은 기술적 문제와는 다르게 시간에 따라서 같은 특성을 지니지 않는 것이 보통이다. 기술적 문제가 해결되고 공격이 정지된 때에도 경제 손실은 여전히 증가될 수 있다. 첫 방법으로 시간 $t \to \infty$에 대하여 손실을 평가하는 것이 합리적이라고 기술한다. 공격 개시 시간을 $t = t_0$로, 공격이 완전히 멈춘 시간을 $t = t_1$으로 설정한다. 시간 간격 $[t_1, t_2]$는 공격 바로 이후의 기간을 나타내며, $t > t_2$는 사고 후의 기간을 나타내며, 수주에서 수개월일 수 있다.

5.1.2 손실 유형

인터넷 서비스 중단의 결과로 생기는 재정 손실을 다음과 같은 4가지 범주로 나눈다:

- 정지시간 손실: 이 비용은 다시 생산성 손실과 수입 손실로 나눌 수 있다. 생산성 손실은 비즈니스를 정상적으로 수행할 수 없고 덜 효율적인 방법을 사용하는 것으로 인한 비용이다. 수입 손실은 서비스 접근이 가능하지 않아 발생하거나 혹은 고객의 요구를 충족할 수 없어 발생하는 거래 손실로 인한 비용이다.
- 손실 복구: 사고 후 복구를 위하여 투입되는 인건비와 자재비, 재료비 등을 포함한다.
- 배상 책임: 서비스 품질이 SLA를 벗어나는 경우, 고객에 대한 보상비용이다. 배상책임은 일부 보험으로 충당되며, 사고 며칠 후에 발생한다.
- 고객 손실: 서비스 품질 저하로 인한 불만족 고객의 계약 종료에 따른 손실 비용이다. 신규 서비스 가입률도 심각하게 저하될 수 있다. 이런 기회비용은 사고 후 보통 수주에서 수개월 뒤에 발생한다.

5.2 재정 손실 계산

손실 계산에 사용된 공식 내의 인수들은 인터넷 종속적 기업과의 인터뷰 분석으로부터 만들어 졌다. 개선된 하부구조에 대한 투자비용과 필요한 신속한 복구비용을 평가하기 위한 기초로써 개략적인 계산을 제공한다.

- 정지시간 손실: 공격 발생으로 실제 정지 시간 $[t_0, t_1]$동안 유발되는 손실 유형이다.

$$L_D = \frac{E_{ca}}{d_a} \cdot d_o \cdot E_{no} \cdot E_{po} + \frac{R_a}{ds_a} \cdot ds_o \cdot R_0 \cdot S_o$$

여기서,

L_D = 정지 시간 손실,

E_{ca} = 종업원 평균 연봉,

d_a = 종업원 년 근무 시간,

d_o = 정지 시간과 중복되는 근무 시간,

E_{no} = 손실로 영향 받는 종업원 수,

E_{po} = 정지 동안 생산성 저하,

R_a = 총 연 수입,

ds_a = 연간 서비스 운영 시간,

ds_o = 정지로 인하여 영향 받는 서비스 운영 시간,

R_o = 완전 정지로 인하여 영향 받는 수입 부분,

S_o = 서비스 저하 정도.

· 손실 복구비용: $[t_0, t_1]$동안 시스템 복구를 위한 인건비와 자재비 등의 비용이다.

$L_r = E_r \cdot E_{ch} \cdot d_r + M_c$

여기서,

L_r = 손실 복구비용,

E_r = 복구 팀에 투입된 종업원 수,

E_{ch} = 복구 팀 구성원 시간당 비용,

d_r = 근무 시간외의 복구 작업 시간,

M_c = 필요 자재비

· 배상 책임: 이 손실은 $[t_1, \infty]$ 동안 유발되며, 다음과 같은 청구들의 합이다.

$L_c = \sum C_c + \sum C_l$

여기서,

L_c = 배상 책임 합계,

C_c = 계약 위약금 청구,

C_l = 다른 배상 책임 청구.

청구가 법정 논쟁으로 되면, 심각한 법적 비용이 추가될 수 있다. 이 비용은 실제적인 손실에 의하여 제 3자가 청구하는 비용으로 평가가 어렵다. ISP는 보통 서비스를 제공하지 못한 시간에 대하여 고객에게 배상한다.

· 고객 손실: 이 유형의 손실은 $[t_2, \infty]$ 동안 아주 긴 시간에 걸쳐 발생하며, 잠재 신규 고객의 손실도 포함한다.

$L_{CL} = [C_A(\Delta t) + C_p(\Delta t)] \cdot R_c(\Delta t)$

여기서,

L_{CL} = 고객 손실 비용 합계,

C_A = 실제 고객 손실 수,

Δt = 시간 간격,

C_P = 잠재 고객 손실 수,

R_C = 고객 당 평균 수입.

5.3 비용 계산 예제

4개의 시나리오에 대한 비용 계산 예를 보여준다. 본 논문에서는 스위스 프랑으로 표시되어 있으며, 논문 작성 시점 기준으로, 1CHF를 1,118원으로 환산하여 표시한다. 본 절의 표에서 BSP는 백본 서비스 제공자, WSP는 웹 서비스 제공자, 국가 1과 2는 스위스 연방 정부의 통계를 기반으로 한 시나리오를 보여준다.

5.3.1 정지시간 파라미터

[표 8]은 정지 시간에 대한 파라미터를 보여준다.

〔표 8〕 정지 시간(outage time) 파라미터

인수	BSP	WSP	국가 1	국가 2
정지시간	24시간	168시간	24시간	168시간
d_o	8시간	40시간	8시간	40시간
ds_o	24시간	168시간	24시간	168시간
S_o	100%	100%	100%	100%

5.3.2 정지 시간 손실 비용

[표 9]는 정지시간 손실 비용을 보여준다.

〔표 9〕 정지시간 손실 비용

인수	BSP	WSP	국가 1	국가 2
정지시간 손실				
1) 생산성 저하				
E_{ca}	109,647,870원	109,647,870원	109,647,870원	109,647,870원
d_a	1,880	1,880	1,880	1,880
E_{no}	3,500	4	1,038,228	1,038,228
E_{po}	20%	20%	20%	50%
소계	326,599,104원	1,865,942원	969억	2조 184억
2) 수입 손실				
R_a	3조 1,471억 7천만원	11억 1,800만원	53조 8,876억원	53조 8,876억원
ds_a	8,760	8,760	8,760	8,760
R_o	0%	0%	15%	40%
소계	0	0	2,215억	4조 1,338억
정지시간 손실	326,599,104원	1,865,942원	3,184억원	6조 1,522억

5.3.3 복구 비용

[표 10]은 사고 복구비용을 보여준다.

〔표 10〕 사고 복구 비용

인수	BSP	WSP	국가 1	국가 2
E_r	1,750 (50%)	0	10,382 (1%)	17,304 (1%)
E_{ch}	167,700원	167,700원	167,700원	167,700원
d_r	16시간	0시간	16시간	128시간
M_c	11억 1,800만원	0	0	0
복구비용 합계	58억	0	279억	3,715억

5.3.4 배상 책임

배상 책임 부분에 대하여는 BSP에 대한 고객 위약금으로 168억원을 평가하였다.

5.3.5 고객 손실

[표 11]은 고객 손실 비용을 보여준다.

〔표 11〕 고객 손실 비용

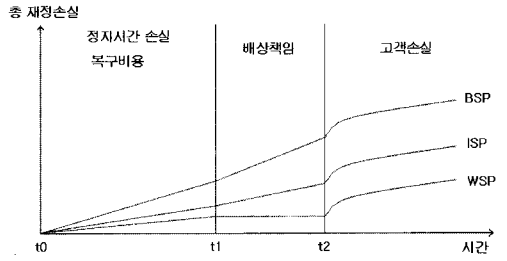
인수	BSP	WSP	국가 1	국가 2
Δt	1년	1년	0	0
C_A	20	100	0	0
C_P	5	30	0	0
R_C	5억 5,900만원	1,453,400원	0	0
고객손실 합계	140억	1억 9천만원	0	0

5.4 누적 재정 손실 특성

시나리오 예제에서 대규모 인터넷 공격으로 인한 기관별 총 경제 손실 평가 금액은 아래와 같다.

- BSP: 369억원
- WSP: 1억 9천만원
- 국가 1: 3,463억
- 국가 2: 6조 5,237억

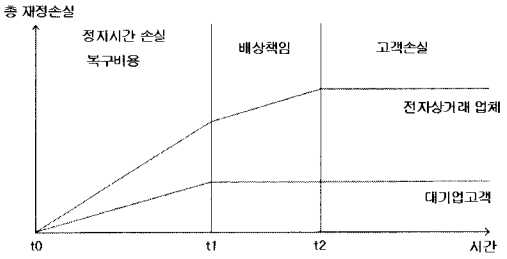
[그림 1]은 BSP, ISP, WSP의 총재정 손실 특성을 보여준다.



〔그림 1〕 BSP, ISP 및 WSP의 재정손실 특성

정지시간 $[t_0,t_1]$동안 정지시간 손실과 복구비용은 선형적으로 증가한다. BSP가 ISP보다 배상 책임 청구에 대하여 더 강하게 충격을 받는 것을 보여준다. ISP에서의 최선 노력(Best-effort) 서비스 보장이 이런 청구를 감소시키고 있다. 사고 후 몇 주 혹은 몇 개월 후에, 고객들의 계약 종료로 고객 손실이 갑자기 증가하는 것을 보여준다. WSP에 대한 정지시간 손실, 복구비용 및 배상 책임으로 인한 총 손실은 ISP의 특성과 유사한 모습을 보여준다. 고객 손실은 호스팅 컴퓨터와의 SLA 유형에 의존한다.

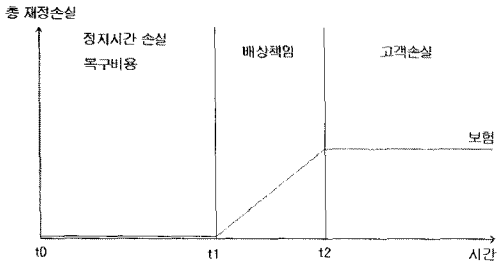
[그림 2]는 전자상거래 업체 및 대기업 고객의 총재정 손실 특성을 보여준다.



〔그림 2〕 전자상거래 업체 및 대기업 고객 재정손실 특성

전자상거래 업체는 사고가 발생하면, 고객들이 온라인 숍에 연결을 못하기 때문에, 심각한 수입손실이 발생한다. 반면에 대기업은 다양한 채널을 통하여 판매하기 때문에 인터넷 차단으로 덜 손실을 입게 된다. 정지시간 손실은 선형적으로 증가한다. 복구비용은 기술적인 문제가 ISP나 BSP에 의하여 보통 해결되기 때문에 작은 편이다. 배상 책임 요구는 장기간 중지를 제외하고 단기간의 사업 차단에 대하여는 드물게 발생한다.

[그림 3]은 보험 회사의 재정손실 특성을 보여준다.



〔그림 3〕 보험 회사의 재정손실 특성

대규모 인터넷 공격 사건으로 보험회사에 끼치는 손실은 보험정책으로부터의 배상 책임 청구이다. 물론 이러한 인터넷 연관 사이버 위험에 대하여 보험 보장을 받기 위하여 국내에서도 BSP와 ISP가 보험을 들어야 하겠다.

VI. 사례 연구 4

국내에서도 인터넷 침해사고 피해액 산출모형을 개발하고, 정량적인 피해액 산출을 위한 연구가 있었다[9]. 인터넷 침해사고의 피해 유형과 발생 요소에 대한 Gordon & Loeb[10]의 개념적인 정의 및 구분을 이용하여, 인터넷 침해사고 피해비용에서 직접 비용과 명시적 비용 부분을 상세화하고 있다.

각 손실은 다음과 같이 정의된다.

- 매출이익 손실 = 인터넷에 의한 시간당 이익 × 피해시간 × 침해사고 영향도

여기서 인터넷에 의한 시간당 이익은 아래와 같이 계산된다.

인터넷에 의한 시간당 이익=
{연간매출 × 매출영업이익률 ×인터넷의존도}/
연간 인터넷 영업시간

- 생산효율 저하로 인한 손실액 = 사고로 영향을 받은 직원 수 × 시간당 생산성 × 피해시간 × 생산효율 저하비율
- 시스템 복구비용 = S/W 복구비용 + H/W 대체비용 + 복구 가능한 데이터 복구비용
- 복구 불능 데이터의 가치 = 복구불능 데이터의 양 × 데이터별 평균 재생산 소요시간 × 재생산 인력의 시간당 인건비

위와 같은 측정 기준에 따라, 2003년 발생한 1.25 인터넷 침해 사고로 인한 국내 피해액규모를 다음과 같이 산출하고 있다.

- 확보 가능한 데이터 이용 산출 피해액: 1,055억원
- GDP 이용 추정 금액: 1,675억원

확보 가능한 피해액의 경우는 실제로 데이터를 확보할 수 있는 전자상거래, 인터넷 뱅킹, PC 방 매출 이익의 손실에 의존한 것이다. 개발된 모형을 이용하여 1.25 인터넷 침해사고에 대한 피해액을 해외 기관에서 추정한 값과 비교한 결과와 2005년도 국내 민간기업에서 발생한 연간 누적 인터넷 침해사고 피해액 산출 결과를 제시하고 있다.

VII. DDoS 대응 기법 개발 방향

DDoS 문제의 심각성과 증가된 빈도로 여러 가지의 대응 기법들이 제안되었다. 그러나 많은 솔루션들이 개발되었음에도 불구하고, 아직 문제는 제대로 다루어지지 않고 있으며, 해결되지 않은 상태이다. 이런 기존 기술들은 대부분 단일 지점에서의 공격을 차단하기 때문에 네트워크 전반에 걸친 근본적인 DDoS 공격 차단이 불가능하다. 따라서 정보통신 전반을 보호할 있는 통합적인 차원에서의 DDoS 대응 전략을 개발할 필요가 있다. 통합적 대응 전략은 다음과 같은 장점이 있다[1].

- 다수의 클라이언트와 네트워크 사이의 트래픽에 대한 광범위한 관점으로 트래픽 특성을 파악할 수 있고, 대응이 가능하다. 이를 통하여 DDoS 공격에 포함된 악성 소스들을 신속하게 인식하고 시의적절하고 효과적인 조치를 취할 수 있다.
- 대응 전략의 공유를 통하여, 단독적인 대응보다 비용이 절약되고 더 나은 서비스가 가능하다.
- 종단 사용자 측면에서 원하지 않는 트래픽을 대응하기 위한 투자 및 운용비용이 절감된다.
- 코어 망에 대한 연결성을 가지고 통합적 대응을 함으로써, 단독 대응보다 훨씬 더 큰 규모의 DDoS 공격 트래픽을 다룰 수 있다.

VIII. 맺음말

DDoS 공격이 인터넷의 안정성과 신뢰성에 심각한 위협을 제공하고 있다. 공격은 점점 더 정교화되고 조직화 되고 있으며, 규모도 대형화 되고 있다. 따라서 본

논문에서는 DDoS 공격 대비를 위한 비용과 공격 발생 시 서비스 중단으로 인한 경제 손실 모델에 대하여 기술하였다.

사례연구 1에서는 자본 비용, 운용 경비 및 잠재적 서비스 붕괴를 포함하여 DDoS 완화의 전반적인 경제적 영향을 평가하기 위한 모델을 제시하였다. 제시된 결과를 국내에 일반적으로 적용하는 것은 조심스럽게 보이나, 국내의 DDoS 공격에 대한 경제 손실 모델을 정립하기 위한 하나의 프레임워크로 사용될 수 있을 것으로 보인다.

사례연구 2에서는 DDoS 공격에 대한 네트워크 운영자 중심의 충격 스케일을 계산하기 위한 프레임워크를 제시하고 있다는 것이 가장 큰 의미로 보여진다. 이를 통하여 발생하는 DDoS 공격에 대하여 제시된 스케일에 따라 순위를 정할 수 있고, 자원과 인력의 우선적 사용을 결정하고, DDoS 완화 전략의 유효성을 비교하기 위하여 사용할 수 있을 것으로 보인다.

사례 연구 3에서는 스위스에서 수행되고 있는 DDoSVax 연구 프로젝트의 일부로 개발된 결과로써, 대규모 인터넷 공격으로 발생하는 인터넷 연결성의 부분적인 혹은 완전한 단절로 인하여 발생하는 가능한 재정 손실을 정성적이고 정량적으로 평가하기 위한 모델 및 방법론을 제시하고 있다. 표본 시나리오를 실제 경우에 대하여 융통성 있게 적용할 수 있을 것으로 보여 진다.

마지막으로 국내 사례 연구에서는 Gordon & Loeb[10]의 개념적 정의를 활용하여, 직접 비용과 명시적 비용을 상세화한 인터넷 침해사고 피해액 산출 모형에 대하여 간략하게 기술하였다. DDoS 공격으로 정보보호의 3대 원칙 중 가용성이 침해되므로, 본 연구의 결과가 가용성 상실로 인한 피해를 산출하는 한 방법으로 사용될 수 있을 것으로 판단된다. 논문에서 지적하고 있는 몇 가지 한계점을 극복한다면 훨씬 더 나은 비용모델이 될 것으로 보인다.

DDoS 공격으로 인한 경제 손실 비용을 보다 정확하게 분석하기 위하여, 다음과 같은 자료를 수집하고 분석해야 할 것으로 판단된다.

- DDoS 공격에 대한 통계 보고서 및 분석
- DDoS 공격의 경제적 측면에 대한 자료 수집
- DDoS 공격 완화, 대응 및 복구비용 벤치마킹
- 조직의 형태별 특성을 고려한 생산성 영향 벤치마킹
- 정지시간으로 인한 수입 손실 벤치마킹
- DDoS 공격 형태, 발생 및 빈도와 같은 보안 모니터링

참고문헌

[1] Forrester Consulting, DDoS: A Threat You Can't Afford To Ignore, Jan, 2009.

[2] Anita D. D'Amico, What Does a Computer Security Breach Really Cost?, Web Document, Secure Decision. Sep. 2000.

[3] D. A. Patterson, A simple way to estimate the cost of down-time, http://roc/cs.berkeley.edu/papers/Cost_Downtime_LISA.pdf, 2002.

[4] CISCO Systems, Economic Impact of Network Security Threats, http://www.cisco.com/warp/public/cc/so/sqso/roi1_wp.pdf.

[5] Arbor Networks, "Worldwide Infrastructure Security Report, Volume IV," Nov. 11, 2008.

[6] R. Vasudevan, Z. M. Mao, O. Spatscheck, and J. V. Merwe, "MIDAS: An Impact Scale for DDoS attacks", http://www.research.att.com/~kobus/docs/midas.lanman.2007.pdf.

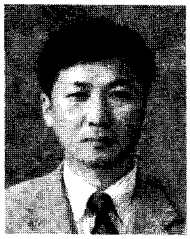
[7] Thomas Duebendorfer, Arno Wagner and Bernhard Plattner, "An Economic Damage Model for Large-Scale Internet Attacks", IEEE WET-ICE/ES, 2004.

[8] DDoS Vax, In Search of a Vaccine against DDoS Attacks, http://www.tik.ee.ethz.ch/~ddosvax.

[9] 유진호, 지상호, 송혜인, 정경호, 임종인, "인터넷 침해사고에 의한 피해손실 측정", 정보화정책, 제15권 제 1호, pp. 3-18, 2008년 봄.

[10] L. A. Gordon and M. P. Loeb, Managing Cybersecuriy Resources: A Cost-Benefit Analysis, 2006.

〈著者紹介〉



전 용 희 (Yong-Hee Jeon)
종신회원

1971년 3월~1978년 2월: 고려대학교 전기전자전파공학부, 학사
1985년 8월~1987년 8월: 미국 플로리다 공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월: 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월: 삼성중공업(주)
1978년 11월~1985년 7월: 한국전력기술(주)
1979년 6월~1980년 6월: 벨기에 벨가톰사 연수
1989년 1월~1989년 6월: 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월: 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월: 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재: 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년 3월~2003년 2월: 대구가톨릭대학교 공과대학장 역임
2004년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 초빙연구원
2007년 1월~2007년 12월: 한국정보보호학회 학회지 편집위원장
2008년 1월~현재: 한국정보보호학회 부회장
2009년 1월~현재: 한국정보과학회 정보보호연구회 위원장
<관심분야> 네트워크 보안, DDoS 탐지 및 대응 기술, DDoS 경제손실 분석, 통신망 성능분석