대규모 인프라 공격에 대한 방어 기술의 발전 동향

아주대학교 정유석 · 홍만표*

1. 서 론

최근 정보통신 기술의 비약적인 발전과 제반 환경의 보급은 인터넷 기반의 새로운 시장과 문화를 창출할 뿐 아니라 기존 산업사회 전반을 정보사회로 변화시키고 있는 등 인간의 삶을 더욱 풍요롭게 하는데 일조를 하고 있다. 그러나 이와 같은 긍정적인 측면의 증가와 함께 개인 정보의 유출, 시스템의 오·남용, 인터넷을 통한 전산망 크랙킹 등 매우 위험하고 파괴적인 역기능의 문제 또한 발생하고 있는데, 이는 정보화가 진전될수록 더욱 확대되는 양상을 보이고 있으며, 그 피해 정도 또한 갈수록 심각해지고 있다.

호스트나 네트워크 자원에 대한 최초의 공격 형태는 특정 시스템의 버그를 공격하거나 시스템의 취약점을 찾는 스캐닝(scanning) 등의 단순한 형태였으며, 이후 방화벽 및 기타 보안 시스템을 우회할 수 있는 좀 더 진보된 형태의 공격 방법들이 등장했다. 이후 백오리피스로 대표되는 트로이 목마(trojan horse), 인터넷 웜(worm), 그리고 백도어 등 독립적인 코드로 활동할 수 있는 새로운 형태의 공격 도구가 등장했으며, 1990년대 말에는 이러한 독립적인 도구들의 협력 작업을 통한 공격 형태까지 등장했다.

2000년 초 야후(yahoo), 씨엔엔(CNN) 등의 대형 웹 페이지에 대한 공격 사건으로 널리 알려진 분산 서비스 거부 공격(distributed denial of service : DDoS)은 독립적인 도구들의 협력 작업을 통한 공격 형태의 대표적인 것으로, 인터넷상에 존재하는 불특정 다수의 호스트에 공격도구가 설치된 후, 공격자가 원하는 시점에 목표 서버나 네트워크를 동시에 공격하여 수행된다. 이는 과거 공격들의 특징인 은닉화(stealth), 분산화(distributed), 에이전트화(agent) 그리고 자동화(automation)를 모두 포함하고 있다. 이와 같이 분산 협력 작업을 통해 시스템을 공격하려는 방식들은 계속 진화하여, 현재에는 특정 서비스에 대한 공격 뿐 아니라, 그 서비스와 관련된 인프라 자체에 치명적인 문제를 일으킬 만한 수준으로 발전해 왔다. 결국 2002년에 발생한 SQL 슬래머(slammer)에 의한 인터넷 대란이 극명하게 보여주었듯이, 최종적 공격 형태는 인터넷 인프라에 치명적인 타격을 가하는 지능적 코드의 대규모 속도전으로 귀결되었으며, 특히 놀랄만한 것은 자동화된 악성 코드 기반의 공격 속도가 SQL Slammer를 기점으로 네트워크 운용자 중심의 대응 속도를 훨씬 능가하는 영역에 진입했다는 것이다.

안타깝게도 현재의 보안 솔루션들은 이에 대한 해답이 못되는 상황이며, 이를 해결하기 위해 국내·외에서 많은 연구들이 진행되고 있으나 아직까지는 특기할 만한 해결책을 제시하지 못하고 있다. 이에 대한 주된 이유 중 한 가지로 관련된 연구들의 시작 시점이 얼마 되지 않았기 때문에 체계적 연구의 체제가 갖추어지지 않았다는 것을 들 수 있으며, 따라서 본 논문에서는 현재까지 연구된 인프라 공격과 관련된 연구들을 분류한 후 이를 바탕으로 연구 동향을 분석함으로써 인프라 공격에 대한 해결 방법을 모색하는 학자들에게 필요한 정보를 제공하고, 이를 통해 관련 분야의 체계적인 연구 진행을 돕고자 한다. 이를 위해 2장에서는 기존 연구들을 다양한 기준에 따라 분류·분석하며, 3장에서는 분석된 정보를 바탕으로 기존 연구들의 문제점들을 살펴보고자 한다. 마지막으로 4장에서는 기존 연구들이 안고 있는 문제점들의 해결 방향과 함께 향후 관련 연구의 진행 방향성에 대해 논한다.

* 종신회원

2. 대규모 인프라 공격에 대한 방어 기술 동향

대규모 인프라 공격에 대한 기술 연구는 최근 3년간에 집중적으로 이루어졌는데, 공격 방법에 대한 원천적인 연구보다는 실제의 공격 경험을 토대로 한 탐지 및 대응 방법의 연구가 주류였다. 탐지 및 대응 방법에 관련된 대부분의 연구들에서는 공격 탐지와 대응 시점이 공격이 진행된 이후에 이루어지고, 이를 위해 단시간에 수집된 소량의 패킷 정보를 이용하고 있다. 또한 네트워크 전체적인 관점에서보다는 특정 위치에 국한된 탐지와 대응 방법들이 연구되어 왔다. 이와 같은 기존 연구들의 경향을 고려해 본 논문에서는 현재까지 진행된 연구 흐름들의 개괄적 분석을 위한 대규모 인프라 공격 연구 영역 전반에 걸친 기본 연구 분류와 함께, 현재 가장 많은 연구의 대상이 되고 있는 탐지 및 대응 관점에서의 연구 동향 및 에이전트 기반 방어 시스템 연구 동향을 분석한다.

2.1 기본 연구 분류

지금까지 진행된 대규모 인프라 공격 관련 연구들은 대체로 다음의 세 가지 방향성을 지니고 있다.

그 첫 번째는 인프라 공격 자체에 대한 분석이다. 대규모 인프라 공격이 관심을 끌게 된 시기는 1999년 이후이며, 2000년 대형 사이트들을 대상으로 한 인프라 공격이 발생한 후에야 이와 관련된 본격적인 연구들이 시작되었다. 그런데, 대규모 인프라 공격을 연구의 대상으로 한 시점이 그리 오래 되지 않았기 때문에 인프라 공격의 방어를 위해서 필수적인 정보인 인프라 공격 자체에 대한 지식이 많이 부족했으며, 결과적으로 인프라 공격의 특성을 조사하고 현재 네트워크 기반에서의 영향 등을 분석하려는 연구로 이어졌다. 그러나 현재까지도 인프라 공격에 대한 원론적인 분석조차 종료되지는 못했으며, 이와 더불어 인프라 공격 방법의 진화와 인프라 공격의 대상이 되는 네트워크 요소들의 질적·양적인 팽창으로 인해, 현재까지도 인프라 공격에 대한 분석을 목표로 하는 연구들이 인프라 공격과 관련된 연구 분야의 한 축을 이루고 있다.

인프라 공격과 관련된 두 번째 연구 방향은 인프라의 개선이다. 인프라 공격은 공격의 근원과 경로 그리고 그 대상이 다수가 될 수 있다. 이를 가능하도록 하기 위해서는 인프라 공격을 위한 공격 도구들이 공격 이전 혹은 공격 도중에 네트워크 인프라를 통해 확산되어야 하며, 실제 공격의 방법 또한 네트워크 인프라를 이용하거나 대상으로 하게 되기 때문에, 인프라 공격의 성공여부는 공격의 과정 및 대상이 되는 네트워크 인프라의 기반기술과 밀접한 관계가 있다고 할 수 있다. 특히 분산되어 공격하는 인프라 공격의 특성상 방어를 위한 방법 또한 네트워크 상에서의 분산·협력하는 방향으로 초점을 맞추어질 가능성이 크기 때문에, 방어 방법의 효율 극대화를 위한 기반기술 개선은 커다란 쟁점이 될 수 있다. 결국, 기반기술의 개선은 인프라 공격에 대한 효과적인 방어를 위해 필수적인 사안이 되고 있으며, 이와 관련된 많은 연구들이 수행되고 있다.

인프라 공격과 관련한 세 번째 연구 방향은 공격에 대한 실제적인 방어 방법에 관한 것으로, 이 방향이야말로 인프라 공격을 방어하기 위한 적극적인 방법의 모색이다. 그런데, 원칙적으로는 앞서 기술한 두 연구 방향의 기초 하에 실제적인 방어 방법이 연구되어야 보다 완벽한 방어 방법으로의 접근이 될 수 있다. 그러나 현재 발발하고 있는 인프라 공격의 심각성으로 인해 방어 방법의 정확성 및 완벽성의 추구뿐만 아니라 빠른 시간 내의 해결 방법 제시가 현실적으로 매우 중요한 요소가 되며, 따라서 앞서 두 방향의 연구가 완벽하지 않은 현재의 상황에서도 근원적인 특성은 아니지만 경험상으로 체득한 인프라 공격의 특성에 맞춘 휴리스틱에 가까운 해결 방법들이 많이 등장하고 있다.

위와 같은 상황을 고려해 본 연구에서는 대규모 인프라 공격 연구 영역 전반에 걸친 분류를 그림 1과 같이 인프라 공격 방어 연구를 위한 정보 수집 및 수집된 정보들의 분석을 위한 기초 연구 분야와 인프라 공격에 취약성을 갖고 있는 현재의 네트워크 인프라를 개선해서 내구성 있는 인프라를 구축하는 방법을 연구하는 기반기술 분야, 그리고 인프라 공격에 대한 적극적인 탐지 및 대처에 초점을 맞춘 방어 방법 연구 분야로 나눈다.

2.1.1 기초 연구

대규모 인프라 공격에 대한 기초 연구에서는 우선 인프라 공격 자체에 대해 원론적으로 분석하거나 실험을 통해 현재의 네트워크 인프라에서 발생할 수 있는 인프라 공격의 영향을 조사한 인프라 공격 분석

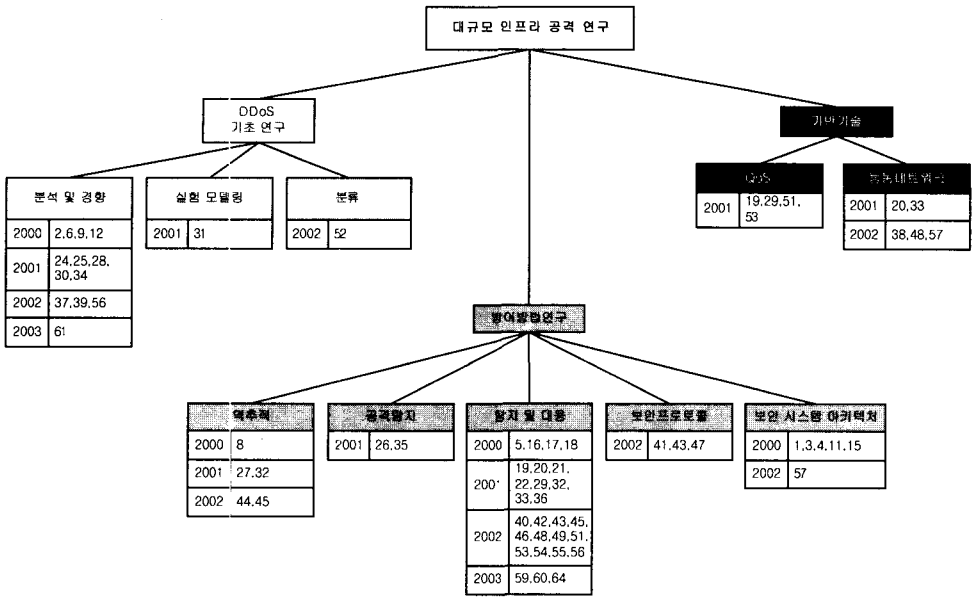


그림 1 대규모 인프라 공격 관련 연구들의 기본 분류

및 경향에 대한 연구가 주류를 이루며, 그 외에 인프라 공격에 대한 대응 방법의 효과 검증을 위한 실험적 방법론을 제시하는 실험 모델링 관련 연구와 기존에 공개된 인프라 공격 및 방어 방법들을 비교 분석하는 연구들이 있다.

인프라 공격은 처음 발생된 시점이 지금으로부터 그리 오래되지 않았기 때문에 관련된 연구가 충분히 이루어지지 못했으며, 결과적으로 현재까지도 근원적이면서도 현실성 있는 방어 방법은 없는 상황이다. 이에 대한 원인 중 한 가지는 인프라 공격에 대한 충분한 분석이 이루어지지 못했었기 때문이며, 이를 극복하기 위해 인프라 공격 자체에 대해 분석하거나 분석 결과에 따른 전반적인 대처 방향을 제시하는 연구들이 다른 기초 분야들의 연구보다 활발히 이루어졌다. 한편 인프라 공격과 관련된 실험 모델링 분야는 인프라 공격의 특성상 기존에 다른 분야에서 사용되던 실험 및 시뮬레이션 방법론을 인프라 공격 대응의 실험에 그대로 적용하기가 힘들다는 관점에서 매우 중요하다. 기존 분야에서 사용하던 방법들, 특히 네트워크 관련 실험 및 시뮬레이션들은 대개 국지적으로 한정된 상황이나 이상적인 환경 하에서의 방법들이기 때문에 네트워크 인프라 전반의 영향을 고려해야 하는 인프라 공격 관련 실험에서는 부분적인 적용만이 가능하다. 그런데 인프라 공격은 인프라 전반에 걸쳐 영향을 주고 피해를 입히기 때문에 이에 대한 대응 방법의 실험상 척도 또한 인프라 전반에 걸친 것을 반드시 포함해야 한다. 현재까지는 이와 관련된 연구가 충분히 이루어지고 있지 않으며, 대부분의 실험은 국지적 상황에서의 것으로 대체하고 있는 형편이다. 그 외에 인프라 공격 및 방어 방법의 분류 분야의 연구에서는 기존에 등장했던 인프라 공격들이나 이에 대한 방어 방법들에 대한 분류가 이루어지고 있는데, 이는 인프라 공격 관련 연구들의 질적·양적인 팽창과 더불어 실제 공격 경험을 토대로 한 지엽적 대처 방안 연구에서 벗어나 인프라 공격에 대한 체계적 접근이 시작되었다고 해석할 수 있다. 그러나 현재까지는 대응 방법보다는 인프라 공격 자체의 분류에 초점을 맞추고 있다.

분석 및 경향과 관련된 연구에서는 인프라 공격 전반에 대한 소개[12] 및 대처 방향 전반에 대한 연구[2,6,30]와 특정 공격 방법에 초점을 맞추어 분석한 연구[24,34,37] 그리고 현존하는 네트워크 인프라와 인프라 공격과의 상관관계에 대한 연구[9,25,34] 및 현존하는 방어책들을 비교한 연구[56]들이 있다. 실험 모델링과 관련된 연구에는 기존에 실시된 인프라 공격과 관련된 실험 방법의 타당성을 검증하는 연구[31]가 있으며, 분류와 관련된 연구에는 대규모 인프라 공격 자체에 대한 분류와 이에 대한 대응 방법들

에 대해 분류한 연구들이 있다[52,62].

2.1.2 기반기술

대규모 인프라 공격을 방어하기 위한 기반기술의 연구는 다른 측면에서의 방어 연구들에 비해 그리 많이 진행되지는 못했었다. 이는 세계 도처에 수없이 설치되어 있는 기존 시스템을 새로운 기반 기술을 채용한 시스템으로 교체하는 것이 현실적으로 불가능하거나 가까운 시일 내에는 힘들다고 여겨지기 때문이다. 따라서 주로 연구되어 온 기반기술 대체 연구는 이미 포스트 네트워크로 많은 연구가 진행되었던 능동 네트워크(active network)를 채용하는 방법들이다[20,33,38,48,57]. 그러나 최근에는 기반기술 교체의 어려움과 인프라 공격의 심각성 및 시간적 측면의 급박함으로 인해 기반기술 개선을 통한 인프라 공격의 방어보다는 현재의 인프라를 변경시키지 않고 문제를 해결하려는 시도가 많아지고 있다.

능동 네트워크를 기반으로 한 연구들은 인프라 구축 자체와 방어 시스템 아키텍처에 초점을 맞추고 있으며, 세부적인 탐지 및 대응 방법 자체에 대해서는 고려하고 있지 않다. 이는 능동 네트워크를 채택한 인프라스트럭처가 되더라도 탐지 및 대응을 위한 세부 기법은 기존 인프라스트럭처에서와 동일한 것을 사용할 수 있기 때문이다. 현재까지의 연구들에서는 능동 네트워크의 장점인 라우터의 동적역할생성(programmable)이 방어 시스템의 외적인 능력인 방어 에이전트의 기능 확장 및 이동성 등을 가능하게 했을 뿐, 그로 인한 새로운 패러다임의 탐지 및 대응 방법을 제안하고 있지는 못했다.

능동 네트워크를 채용하는 방법 이외에 라우터들에 QoS(quality of service) 기능을 부여하여 의심스러운 정도에 따라 차별화된 라우터 자원을 사용하게 하는 방법들도 연구되고 있다[19,29,51,53]. 이런 방법들은 탐지가 아닌 대응에 적용되는 방법으로, 어느 정도 불명확한 탐지의 경우에도 적용 가능하다는 특성을 지니고 있으며, 따라서 완벽한 공격 패킷의 구분 방법이 알려져 있는 않은 대규모 인프라 공격에의 대응에 있어 좋은 대응 방법으로 판단된다.

2.1.3 방어 방법 연구

대규모 인프라 공격과 관련된 대부분의 연구는 방어 방법 자체에 관한 것으로 연구 초기 시절의 방어 시스템 아키텍처에 대한 것으로부터 현재에는 실제 공격에 대한 구체적 대처에 관한 것까지이다. 세부적으로는 공격에 대한 방어를 패킷의 경로 분별을 통해 수행하려는 역추적에 대한 연구와 공격 발생의 탐지 자체에 초점을 맞춘 연구 및 공격의 발생 탐지 방법과 이와 연관된 대응 방법을 제시한 연구 그리고 프로토콜의 개선을 통해 인프라 공격을 막고자 했던 연구[41,47]와 방어를 위한 보안 시스템 아키텍처에 관한 연구가 있다.

초기에는 주로 보안 시스템 아키텍처[1,3,4,11,15]에 관한 연구와 공격이 발생됐는지 여부를 탐지하는 데 초점을 맞춘 연구들이 이루어졌으나, 최근에는 공격 발생 탐지 자체보다는 공격 플로우 혹은 공격 패킷들을 정상 패킷과 구분하려는 관점에서의 탐지와 이에 연계되어 사용될 수 있는 대응 방법에 대한 연구가 주류를 이루고 있다.

역추적에 관한 연구들은 근본적으로 패킷 주소에 대한 위조가 가능한 현재의 네트워크 인프라의 취약성을 극복하기 위해, 특정 네트워크 노드를 지나가는 패킷에 표시를 하고, 그 표시를 분석함으로써 패킷의 경로를 찾아 필터링하거나 공격 근원을 역추적 하는 것에 초점이 맞추어져 있다[8,27,32,44,45]. 공격 탐지에 관한 연구[26,35]들은 탐지 노드로 유입되는 패킷의 양을 계산해서 공격 여부를 판단했으며, 보안 프로토콜과 관련된 연구[41,43,47]들은 공격자가 근원 주소(source address)를 속일 수 있는 현재의 프로토콜을 개선해 근본적으로 거짓 주소의 사용을 막는데 초점이 맞추어져 있다. 또한 보안 시스템 아키텍처와 관련된 연구들은 분산 보안 시스템의 구성에 대한 연구[15,57]와 네트워크 인프라스트럭처에 관한 연구[1,3,11]가 주를 이루어왔다.

현 시점에서 인프라 공격에 대한 방어와 관련된 대부분의 연구는 탐지 및 대응에 관한 연구이며, 이에 대한 자세한 설명은 다음 장에 기술한다.

2.2 탐지 및 대응 방식 기반 분류

최근까지 인프라 공격 방어와 관련된 연구들의 가장 큰 연구 대상이 된 분야는 인프라 공격의 탐지에 대한 것으로, 과거에는 공격 발생 여부의 탐지에 초점을 맞추었으나, 현재에는 이를 확장해 공격 플로우나 공격 패킷의 탐지에 초점을 맞추고 있다. 이와 같은 인프라 공격에 대한 탐지 방법들은 다양한 기준을 통해 분류할 수 있으나, 현재의 연구 수준에서는 그림 2에서 표현한 세 가지 기준으로 분류하는 것이 의

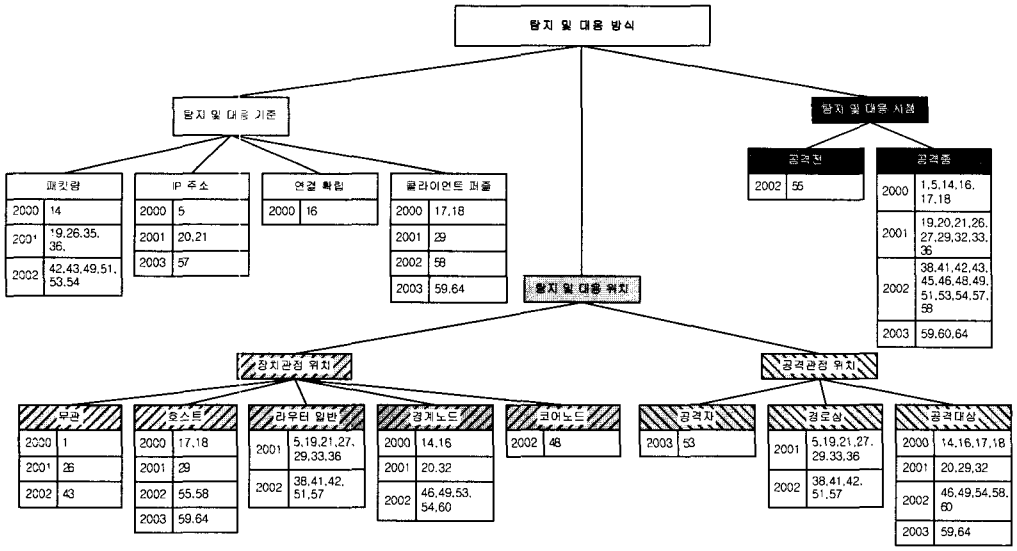


그림 2 탐지 및 대응 방식 기반 대규모 인프라 공격 관련 연구의 분류

미가 있다. 그 첫 번째는 탐지 기준에 따른 분류인데, 그 이유는 대부분의 탐지 방법들이 탐지 기준에 따라 특성이 결정되기 때문이다. 두 번째 분류 기준은 탐지 및 대응 시점으로, 현재 대부분의 연구들은 공격이 발생된 시점 이후에 가동되나, 많은 경우의 인프라 공격이 선 공격 도구 설치-후 공격의 형태로 이루어지기 때문에 실제 공격이 발생하기 이전의 대처가 필요하다. 또한, 공격이 종료된 시점 이후에도 동일한 공격 도구들로부터의 재공격이 가능하기 때문에 이와 관련된 대처는 매우 중요하다. 세 번째 분류 기준은 탐지 및 대응 위치로, 이는 탐지 및 대응의 기준이 되는 정보들과 연계되어 방어 기법의 특성을 결정짓는 중요한 요소이다. 인프라 공격의 특성상, 공격자에 가까운 위치에서의 공격 특성과 공격 대상에 가까운 위치에서의 공격 특성은 달라질 수밖에 없고, 또한 코어 라우터에서의 특성과 에지 라우터에서의 특성까지도 달라질 수 있기 때문에 방어의 목적과 대상에 따라 탐지 및 대응 위치가 달라져야 한다.

2.2.1 탐지 및 대응 기준

대규모 인프라 공격과 관련된 연구들의 탐지 및 대응 기준상 분류는 탐지 위치로 들어오거나 나가는 패킷량을 기준으로 공격을 탐지하는 연구와 패킷의 주소를 기준으로 공격 패킷과 정상 패킷을 구분하는 연구, 서버와 클라이언트 간 연결이 완전히 이루어졌는가를 통해 공격 관련 연결과 정상 연결을 구분하는 연구 그리고 서버가 제시하는 퍼즐을 풀었는가 여부로 정상적인 통신과 비정상적인 통신을 구분하는 클라이언트 퍼즐 관련 연구로 나뉜다.

패킷량을 통해 공격을 탐지하는 연구들은 정상의 패킷량을 프로파일로 갖고 있다가 임계치 이상으로 패킷량이 늘어날 경우 공격으로 판단하며, 최근의 논문들일수록 탐지 방법 자체보다는 탐지 이후 대응하는 방법에 초점이 맞추어져 있다. 인프라 공격의 특성상 개별 패킷의 대한 분석이 비현실적일 것이라는 판단으로 패킷별 탐지 및 대응보다는 플로우별 탐지 및 대응을 취한다. 패킷의 주소를 통해 공격을 탐지하는 연구들은 패킷의 근원과 목적지 정보를 통해 위조 여부를 알아내고 이를 통해 공격 패킷을 구분하는 연구들과[5,21], 패킷 주소의 위조를 근본적으로 차단하여 패킷별 정당성 여부를 판단할 수 있도록 한 연구[20] 그리고 이전에 접속한 호스트의 주소 리스트를 유지하여 이를 통해 공격 패킷을 차단시킨 연구[60]들이 있다. 연결 확립을 통해 공격을 탐지하는 연구들은 패킷의 순서 등을 이용해 공격 관련성을 탐지하는데, 예를 들어 TCP의 연결 과정 중 정상적인 연결 설정(3-way handshaking)이 수립되는 주소를 확인하고 이들로부터 발생되는 패킷만을 정상적인 패킷으로 판단할 수도 있다[16].

클라이언트 퍼즐은 지금까지 언급한 방법과는 다

르게, 보편적인 통신 패킷을 분석해서 침입 관련 통신을 탐지하는 것이 아니라 서버가 제공하는 문제를 클라이언트가 풀었을 경우에만 서비스를 제공하는 방식으로 인프라 공격으로부터 서버를 방어한다. 이 방법은 적법한 사용자들은 쉽게 풀 수 있지만 자동화된 공격 도구는 풀기 힘든 문제의 제시가 핵심이 되며, 따라서 클라이언트가 퍼즐을 풀기 위한 특별한 모듈을 지닌 적법한 에이전트나, 실제 사람인 경우에 유용할 수 있다. 클라이언트 퍼즐을 제공하는 보안 시스템은 퍼즐에 의한 적법성 구분 이후, 그 결과에 따라 서비스를 제공하거나 혹은 서비스를 제공받을 수 있는 새로운 서버로의 연결을 확립시킨다. 이러한 특성으로 인해 웹 서버와 같이 직접적으로 사람들이 접속하는 시스템의 경우가 주된 적용 분야가 된다[29,59].

2.2.2 탐지 및 대응 시점

대규모 인프라 공격과 관련된 연구들의 방어 시점 상 분류는 공격이 발생되기 이전에 공격 관련 정보를 탐지할 수 있는 공격전 탐지 방법[55]과 공격 과정 중 공격을 탐지하고 대응하는 공격중 탐지 방법으로 나뉜다. 그러나 공격 이전의 방어를 제안한 연구도 공격을 위해 분산 설치되는 도구들의 위치를 미리 파악하여 차단하는 수준이 아니라 단순히 허니(honey-pot) 설치를 통한 정보 수집에 불과하며, 대부분의 연구들은 공격이 발생한 시점 이후에 탐지와 대응을 시작한다. 많은 종류의 인프라 공격이 실제 공격이 발생하기 훨씬 이전에 공격을 위한 도구들이 설치되는 경우가 많음에도 불구하고 실제 공격이 발생 된 후에야 탐지 및 대응을 시작하는 이유는 공격 도구의 설치 과정을 정상적인 통신 흐름과 구분하는 효과적인 방법이 아직 발견되지 못했기 때문이며, 이것은 공격 도구의 확산이 바로 인프라에 대한 공격이 되는 슬래머와 같은 최근의 인프라 공격에 대한 효과적인 방어 방법 또한 현재로써는 없다는 것을 의미한다.

2.2.3 탐지 및 대응 위치

대규모 인프라 공격과 관련된 연구들의 탐지 및 대응 위치상 분류는 다시 방어 장치의 네트워크 위상 내 위치상 분류와 공격 도구의 위치 대비 공격 탐지 위치에 따른 분류로 나뉜다.

가. 장치관점 위치

장치관점 위치를 기준으로는 방어 도구들의 설치 위치에 제한이 없는 방법을 제안한 연구와 호스트에 방어 도구가 직접 설치되어야 하는 방식을 제안한 연구 그리고 네트워크의 경계 노드, 코어 노드 혹은 임의의 네트워크 노드에 설치되어야 하는 방식을 취하는 연구로 나눌 수 있다. 방어 위치상 제한이 없는 방법들을 제안한 연구들로는 분산된 에이전트가 임의의 호스트나 네트워크 노드에 설치되어 인프라 공격에 대응하는 프레임을 구성한 연구와[1,43] 패킷의 목적 주소와 분량을 통해 공격을 탐지하고 대응하려는 연구[26] 있으며, 호스트에 방어 시스템을 직접 설치하려는 연구에는 허니팟을 통해 공격 정보를 수집하려는 연구나[55] 클라이언트 퍼즐을 사용하는 연구들이 있다. 그러나 현재 대부분의 연구에서는 방어 장치를 라우터 등의 네트워크 노드에 위치하는데 초점을 맞추고 있으며, 그 중에서도 방어 장치가 설치되는 라우터의 네트워크상 위치에 관계없이 인프라 공격에 대응하려는 연구들이나 공격 패킷이 취합되어 탐지가 용이한 네트워크 경계 노드에 방어 장치를 설치하려는 연구들이 주류를 이룬다. 그 외에 인터넷 서비스 제공자(internet service provider)의 코어 노드에서의 방어를 초점으로 하는 연구도 있다[48].

나. 공격관점 위치

공격관점 위치상 분류는 공격을 실제 수행하는 호스트 부근에서 대응하는 방식을 제안한 연구와 공격 대상 부근에서 대응하는 방식을 제안한 연구 그리고 공격자와 공격 대상의 경로 상에서 대응하는 방식을 취하는 연구들로 나뉜다.

공격 호스트 부근에서 대응을 취하려는 연구들에서는 호스트에서 나가는 패킷량에 제한을 두어 공격을 차단하는 방법을 사용하는데, 공격의 발생 탐지 자체는 상대적으로 어려우나, 긍정적 오류가 적은 차단을 할 수 있다는 장점이 있다[53]. 공격 대상 부근에서 대응하려는 연구들은 앞장에서 기술한 장치관점 설치 위치상 경계 노드에 설치되는 방법들을 제안한 연구들과 동일하며, 공격 호스트와 공격 대상의 경로 상에서 대응하는 연구들은 설치되는 라우터의 위치에 관계없이 대응하는 연구들과 동일하다.

2.3 에이전트의 특성 기반 분류

대규모 인프라 공격과 관련된 연구들에서는 많은 경우에 있어서 에이전트를 기반으로 하여 대응하는 방법을 취하고 있다. 그 이유는 인프라 공격은 단일

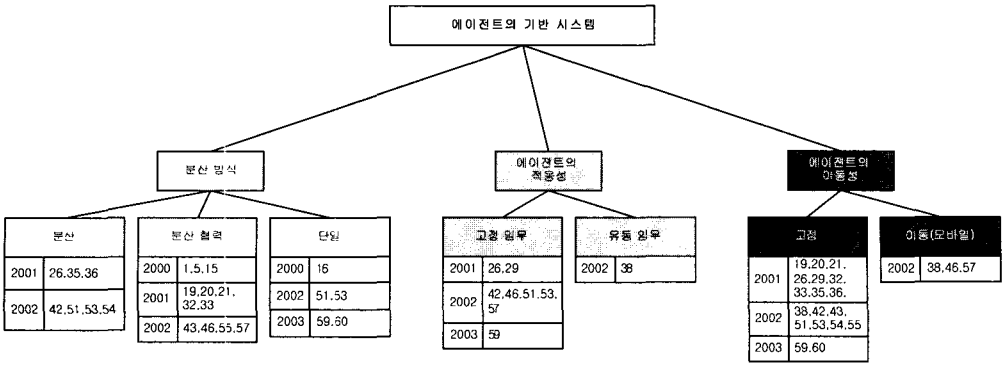


그림 3 에이전트의 특성을 기반으로 한 대규모 인프라 공격 관련 연구들의 분류

의 공격이라도 국지적이 아닌 대규모의 네트워크 전체에 걸쳐 발생하기 때문에 이에 대한 대응 또한 여러 위치에서 동시적으로 수행되어야 한다는 것과, 방어 시스템이 독자적으로 운영되기 보다는 이미 존재하는 인프라인 라우터 등에서 이루어지는 것이 유리하기 때문에 에이전트의 형태로 존재하는 것이 현실적이라는 것 때문이다. 결과적으로 에이전트의 채용이라는 것은 인프라 공격에 대한 탐지 및 대응을 효율성을 극대화하기 위한 것이며, 따라서 방어 시스템을 이루는 에이전트 전체의 총합적 지능을 결정짓는 요소에 따라 분류가 가능할 것이다. 그러한 요소들 중 현재까지 진행된 에이전트 관련 연구들에서 고려한 것들은 에이전트의 분산화 정도와 임무의 유동성 그리고 에이전트의 이동성 등이며, 따라서 본 논문에서는 이들을 기준으로 그림 3과 같이 관련 연구들을 분류한다.

2.3.1 분산 방식

에이전트를 기반으로 하는 대응 시스템 중 분산 방식에 관한 연구들을 대응 시스템이 어느 정도 분산화 되어 있는지에 따라 세 가지로 나누어서 살펴볼 수 있다. 대응 시스템이 완전 분산되어 독립적인 역할을 수행함으로서 공격에 대응할 수 있는 방법과 대응 시스템이 분산화 되어 있긴 하지만 서로 협력하는 방법 그리고 전혀 분산되어 있지 않고 단일 시스템으로 대응을 하는 방법이 있다.

완전 분산화된 대응 방식에 관한 연구들의 대부분은 패킷량의 추이에 따라 필터링 여부를 결정하는 것들이며, 분산 협력을 통한 정보 수집의 용이성 보다는 독립 운용을 통한 수행성 증가에 초점을 맞추고 있다. 에이전트를 기반으로 한 인프라 공격 방어를 추구하는 대부분의 연구들은 에이전트의 분산 협력과 관련된 것으로, 침입 탐지 및 대응 시스템들이 네트워크의 곳곳에 설치되어 있어 서로 간의 정보 교환을 통해 공격의 탐지와 대응 효과를 높이고 있다. 이러한 방식의 시스템들은 에이전트 간 의존성으로 인해 탐지 및 대응 방법 자체 뿐 아니라, 에이전트 간 통신 방법이나 과다한 정보 수집에 대한 처리 등의 문제도 해결해야 한다. 그 외에 단일 시스템을 통해 대응을 하는 방식들은 보통 보호하고자 하는 호스트나 서브 네트워크의 통신 특성을 방어 시스템이 지니고 있어서 이를 기반으로 인프라 공격을 탐지하고 차단한다. 대표적인 연구로는 웹 서버 보호를 위해 기존에 접속빈도가 높았던 주소를 저장해 두었다가 공격이 발생하는 저장한 주소로부터 오는 패킷에 대해서만 서비스를 제공하는 방법이 있다[60]. 또 다른 연구로는 외부로 나가는 트래픽에 대해 사전에 정의된 정상 트래픽의 조건에 위배될 경우 전송을 제한하거나 차단시켜 공격 트래픽이 공격 대상 네트워크에 유입되는 것을 막는 방법이 있다[53].

2.3.2 에이전트의 적응성

에이전트를 통한 대규모의 인프라 공격에의 방어 방법은 에이전트의 적응성에 따라 고정임무 방식과 유동임무 방식으로 나눌 수 있다.

고정임무 방식은 에이전트가 최초 생성될 때 주어진 고정된 임무만을 수행하는 것을 가리키며 에이전트 관련 연구들의 대부분에서는 고정임무의 에이전트를 채택했다. 유동임무는 에이전트가 고정된 일을 수행하는 것이 아니라 상황에 따라 유동적인 임무를

수행하는 것이나, 현재까지 구체적인 방법이 제안되지는 못했었고, 단지 유동임무가 가능한 에이전트 기능이 필요하다는 언급에 그치고 있다[38].

2.3.3 에이전트의 이동성

에이전트 기반 인프라 공격 방어 연구들은 에이전트들의 이동성에 따라 고정 에이전트와 이동 에이전트로 나눌 수 있다. 고정 에이전트들은 처음에 설치한 곳에 고정되어서 공격에 대응하는 것에 반해 이동 에이전트들은 중앙의 제어 시스템에 의해서나 혹은 스스로의 판단에 따라 복제, 수정, 삭제할 수 있는 기능을 가지고 네트워크 상의 여러 곳을 이동해 위치함으로서 공격에 대응한다. 현 네트워크 인프라에서는 이동 에이전트가 네트워크 노드 상에서 이동할 수 없으므로 대부분의 연구들은 능동 네트워크 상에서의 방어 시스템에 초점을 맞추고 있다. 그러나 구체적인 이동 방법 등은 제시하지 못하고 있으며, 에이전트의 유동임무 기능과 마찬가지로 에이전트의 이동 기능이 필요하다는 의견 제시에 그치고 있다[38,46,57].

3. 기존 방법들의 문제점

앞서 살펴본 인프라 공격과 관련된 많은 연구들은 여러 분야에서 다양한 방법을 통해 문제를 해결하고자 시도했으나 짧은 연구의 역사로 인해 아직까지도 해결해야 할 많은 문제들이 남아있다. 그 중에서도 다음 몇 가지 사항들은 인프라 공격 방어를 위해 해결이 필요한 중요한 문제점들이다.

- ○ 공격 코드들의 진화 특성에 대한 기초 연구가 미비 : 지금까지의 연구들은 과거에 등장한 인프라 공격에 대한 경험적인 지식을 바탕으로 해결책을 모색했다. 그러나 이러한 방식으로는 계속적으로 진화하는 인프라 공격에 대한 적시의 대응이 어렵다. 따라서 원천적인 방어를 위해 공격 코드들의 진화 특성에 대해 연구할 필요가 있다.
- ○ 지역적인 탐지 결과에 따른 수동적 대응 : 기존 연구의 대부분에서는 인프라 공격에 대한 대응이 공격이 발생한 시점 이후에 공격이 집중되는 지역에서의 탐지 결과에 의존한다. 그런데 공격을 탐지할 수 있는 지역이라는 것은 이미 상당량의 공격이 집중된 위치를 의미하며, 이 위치에서는 공격 발생 여부를 탐지하기 용이하지만, 탐지가 된 시점에서는 이미 대처하기에 늦은 상황일 가능성이 높다. 결국 공격이 집중된 위치의 국지적 정보 이외에 인프라 공격에 대해 대처에 사용할 수 있는 범용적인 탐지 방법이 필요하다.
- ○ 네트워크의 대응 정보와 응용 서비스 및 시스템에서의 대응 정보 간의 연계 부족 : 인프라 공격의 대상은 호스트 즉, 응용 서비스와 시스템이 될 수 있지만 그 경로로 사용되는 것은 네트워크의 요소들이 된다. 따라서 이 두 요소간의 유기적인 협력은 인프라 공격에 대한 효과적인 방어를 가능하게 할 수 있다. 그러나 현재까지의 연구들은 각 요소에서의 대응에만 초점을 맞추고 있다.
- ○ 중앙집중 방식의 탐지 및 대응 전략 : 대규모 인프라 공격은 네트워크 전반에 걸쳐 발생할 수 있기 때문에 해당 네트워크를 사용하는 방어 요소들까지도 마비시킬 수 있다. 따라서 인프라 공격에 대한 대응 결정을 중앙집중된 단일 요소에서 내린다는 것은 상당히 위험할 수 있다. 결국, 인프라 공격에 대한 대응 결정은 방어 요소들의 생존성을 고려해 다양한 위치에서 가능해져야 한다.
- ○ 공격 생명주기 전반에 걸친 탐지 및 대응 능력 부재 : 대부분의 인프라 공격에 사용되는 도구들은 특정 생명주기를 갖고 활동하며, 특히 공격 도구가 설치되기까지의 과정이 공격 과정에 비해 상대적으로 오랜 시간이 걸린다. 그러나 현재의 연구들은 공격 도구들의 설치가 끝난 시점 이후의 대처가 대부분임으로 그 이전 단계에서의 탐지를 위해 연구의 초점을 넓힐 필요가 있다.
- ○ 트래픽의 지엽적 혹은 단기간 정보에 의존한 탐지에 따른 높은 오류율 : 현재까지 연구된 인프라 공격에 대응하는 방법들 대부분은 지엽적이면서 단기간에 수집된 정보를 기반으로 인프라 공격을 탐지하고 대응한다. 이는 결국 정상적인 통신을 비정상적인 것으로 오인하거나 비정상적인 통신에 대해 미처 대응하지 못하는 경우를 발생시킬 수 있다.
- ○ 실제 상황을 반영하는 실험 환경의 부재 : 대규모 인프라 공격은 넓은 범위의 네트워크 노드 상에서 발생·전파되며, 이는 현재까지 다루던 지엽적이면서 이상적인 네트워크 실험 상황과는 많이 다르다. 따라서 새롭게 제안되는 대응 방법들을 검증하기 위한 실험 환경의 구성이 필요하다.

4. 결 론

인터넷으로 대표되는 네트워크 관련 산업의 질

적·양적인 팽창과 이를 토대로 한 산업 전반에 걸친 변화는 우리 삶의 질을 향상시키는 동시에 결과적으로 이들의 근간이 되는 인프라에 대한 공격 위험성을 증가시키고 있다. 특히 인프라 공격이 현대 산업 전반에 미치는 엄청난 영향 때문에, 정확하고 효과적인 대응 방법의 모색뿐 아니라 그 적용 가능 시점을 최대한 앞당기는 것이 매우 중요하다. 그런데 문제는 현재의 기술 수준으로는 인프라 공격에 대한 근본적인 해결을 위한 연구 방향조차 확정되지 않았다는 것이다. 이와 같은 상황을 고려해 본 논문에서는 인프라 공격 관련 연구 과정의 시간적·공간적 노력을 절약하기 위해 관련 연구에 매진하는 학자들에게 필요로 한 정보인 기존 인프라 공격 관련 연구들을 분석하고 분류한 결과를 서술했다.

그 첫 번째로 우선 전반적인 관점에서 인프라 공격 관련 연구들을 기초 연구와 기반 연구 그리고 방어 방법 연구 분류하여 각각에 대해 기술했으며, 이후 관련 연구들 중 최대의 관심사인 대규모 인프라 공격에 대한 탐지 및 대응 관점을 주제로 하는 연구들을 각각 탐지 및 대응 기준, 시점, 위치로 구분했다. 또한 현재까지 많은 연구들에서 채용한 에이전트 기반의 방식들에 대해 분산 방식, 적응성, 이동성을 기준으로 분류했다. 기존 연구들에 대한 분석 결과 다양한 문제점들이 드러났으며 이는 공격 코드에 대한 진화 특성 연구, 범 계층적인 글로벌 탐지 및 대응 체계의 필요, 거시적 탐지 및 대응으로 지역적·시간적 제약의 극복, 사전 공격 징후 탐지를 통한 예방 방법론 개발, 공격 원인 사전 제거 방안 고안 등의 통해 극복될 수 있을 것이다.

과거에 연구되었던 인프라 공격에 대한 방어 방법들은 인프라 공격의 막강한 위력으로 인해 현실적인 대응 방법으로의 모색을 우선하기보다는 보다 효율적인 방어 기술의 연구에 초점을 맞추고 있다. 그러나 최근 연구되고 있는 인프라 공격에 대한 최신 방어 기법들은 지금까지 등장했던 방법들과는 조금 방향을 달리하고 있는데, 기존의 방식들이 인프라의 개선을 보편적인 인프라 공격에 방어하기 위해 해답으로 찾았다면, 최근 발표되는 연구들은 그보다는 현실적이고 구체적인 방식으로 문제에 접근하고 있다. 이들은 크게 두 가지 방향을 취하고 있는데, 그 첫번째로 범용적 인프라 공격에 대한 대응이 아닌 특정 인프라 공격에 대한 효과적인 차단을 목적으로 하고, 두번째로는 현재의 인프라를 유지하면서 기존의 틀을 해치지 않는 범위 내의 변화를 통해 인프라 공격에 대응하고자 한다. 왕의 논문에서는 익명의 접속자에 대해 퍼즐을 풀도록 하여 정상적 사용자와 공격을 위한 접속임을 구별했는데 이때 퍼즐과 답을 주고받는 과정이 현재의 TCP/IP에서의 패킷 전달 방식을 전혀 해치지 않는다[62]. 또한 버케리의 논문에서는 현재 사용하는 IP 패킷의 내역을 변경시키지 않고도 패킷의 경로를 구분하여 공격 패킷과 정상 패킷을 구분할 수 있게 하여 기존 주소 역추적(IP Traceback)의 단점을 극복했다[63]. 이와 같은 최근 연구들의 방향성은 대규모의 인프라 공격을 막기 위해 전 세계에 광범위하게 펼쳐진 네트워크 인프라스트럭처를 변경하는 것이 현실적이지 않다는 점과, 인프라 공격에 대한 대처가 시급하다는 점에서 당분간 지속될 것으로 예상된다.

결국에는 인프라 공격의 지속적이고도 강력한 위협으로 인해 이에 대한 방어를 위한 연구들이 근원적인 해결방법의 모색과 함께 현실적이면서 근 시일 내에 적용이 가능한 방법의 모색이라는 두 가지 방향으로 진행될 것이며, 결과적으로는 두 방향이 서로를 보완하여 궁극적인 해결점을 찾게 될 것이다.

참고문헌

[1] SCHNACKENBERG, D., DJAHANDARI,K., AND STERNE, D. "Infrastructure for intrusion detection and response," In Proc. First DARPA Information Survivability Conference and Exposition, Jan. 2000

[2] Jhon Elliott, "Distributed Denial of Service Attacks and the Zombie Ant Effect," IEEE IT Pro, 2000. 3.

[3] George Cybenko, Guofei Jian, "The Infrastructure Web : A System for distributed Monitoring And Management," Infrastructure Protection and Emergency Management Symposium, 2000

[4] Andrew Barkley, Steve Liu, Quoc Thong Le Gia, Matt Dingfield,Yashodhan Gokhale "A Testbed for Study of Distributed Denial of Service Attacks," 2000 IEEE, June 29, 2000

[5] K. Park and H. Lee, "A proactive approach to distributed DoS attack prevention using

route-based distributed filtering," Tech. Rep. CSD-00-017, Department of Computer Sciences, Purdue University, December, 2000

[6] Xianjun Geng, Andrew B. Whinston, "Defeating Distributed Denial of Service Attacks," IEEE IT Pro, July, 2000

[7] Yongguang Zhang, Wenke Lee, "Intrusion Detection in Wireless AdHoc Networks," Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom'2000), August, 611, 2000, Boston, Massachussetts

[8] Dawn Song and Adrian Perrig, "Advanced and authenticated marking schemes for IP traceback," Tech. Rep. UCB/CSD-00-1107, Computer Science Department, University of California, Berkeley, 2000

[9] Felix Lau, Ljiljana Trajkovic, "Distributed Denial of Service Attacks," IEEE, Simon Fraser University, Purdue University, 2000

[10] Haining Wang, Shin, K.G, "Layer-4 service differentiation and resource isolation," Real-Time and Embedded Technology and Applications Symposium, 2002

[11] J. Yan, S. Early, and R. Anderson, "The XenoService-A Distributed Defeat for Distributed Denial of Service," presented at Information Survivabiloity Workshop, 2000

[12] Lee Garber, "Denial-of-Servce Attacks Rip the Internet," Computer magazine, 2000

[13] Samuel Patton, William Yurcik, David Doss, "An Achilles' Heel in Signature-Based IDS_Squealing False Positives in SNORT," IEEE 2000

[14] Thomer M. Gil, "MULTOPS : a data structure for denial-of-service attack detection," 2000 IEEE

[15] Wenke Lee, Rahul A. Nimbalkar, Kam K. Yee, Sunil B. Patil, Pragneshkumar H. Desai, Thuan T. Tran, Salvatore J. Stolfo "A Data Mining and CIDF Based Approach for Detecting Novel and Distributed Intrusions," Recent Advances in Intrusion Detection 2000

[16] Xiaobing Zhang, S. Felix Wu, "Malicious Packet Dropping : How It Might Impact the TCP Performance and How We Can Detect It," IEEE, 2000

[17] V. Razmov, "Denial of Service Attacks and How to Defend Against Them," In Graduate Networking Course, Survey Project Paper, Dept. of Computer Science and Engineering, University of Washington, Seattle, WA, May 2000

[18] Tuomas Aura , Pekka Nikander , Jussipekka Leiwo, "DOS-Resistant Authentication with Client Puzzles," Revised Papers from the 8th International Workshop on Security Protocols, p.170-177, April 03-05, 2000

[19] Yong Xiong, Steve Liu, and Peter Sun, "On the Defense of the Distributed Denial of Service Attacks: An OnOff Feedback Control Approach," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS-PART A: SYSTEMS AND HUMANS, VOL. 31, NO. 4, JULY, 2001

[20] Kim, G., Bogovic, T., and Chee, D., "ACtive edge-Tagging(ACT) : An Intruder Identification & Isolation Scheme in Active Networks," Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium on , 3-5 July, 2001

[21] Kihong Park, Heejo Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," SIGCOMM, Aug. 2001

[22] D. Sterne et al., "Autonomic Response to Distributed Denial of Service Attacks," In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID), Davis, California 10-12 October, 2001

[23] K. G. Anagnostakis, S. Ioannidis, S. Miltchev, and J.M. Smith. "Practical network applications on a lightweight active management environment," In Proceedings of the 3rd IFIP

International Working Conference on Active Networks(IWAN), October, 2001

[24] C. C. Center. "Trencs in denial of service attack technology," World Wide Web, http://www.cert.org/archive/pdf/DoS_trends.pdf, Oct. 2001

[25] Y. Chen, A. Bargreil, R. Katz and J. Kubiatowicz, "Quantifying Network Denial of Service : A Location Service Case Stydy," ICICS, November, 2001

[26] A.B. Kulkarni, S.F.Bush, S.C.Evans, "Detecting Distributed Denial-of-Service Attacks Using Komogorov Complexity Metrics," IEEE 2001

[27] Allison Mankin, Dan Massey, Chien-Lung Wu, S. Felix Wu, Lixia Zhang, "On Design and Evaluation of Intention-Driven ICMP Traceback," 2001 IEEE

[28] D.W. Gresty, Q. Shi, M. Merabti, "Requirements for a General Framework for Response to DDoS," IEEE Computer Security Applications Conference, 2001

[29] Frank Karg, Joern Maier, Michael Weber, "Protecting Web Servers from Distributed Denial of Service Attacks," ACM, 2001.

[30] Xiaobing Zhang, S. Felix Wu, "No Longer in Denial," IEEE SPECTRUM, 2001

[31] Sara Kaufman, Stephen Ying "DARPA Information Assurance Progra Experimental Confirmation DdoS," 2001 IEEE

[32] Schnackengerg, D. and Djahandari, K, "Cooperative Intrusion Traceback and Response Architecture (CITRA)," DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings, Vol.1, Iss., 2001

[33] Scott Shyne, Adam Hovak, and Joseph Riolo, "Using Active Networking to Thwart Distributed Denial of Service Attacks," Aerospace Conference, 2001, IEEE Proceeding

[34] Vern Paxson, "An Analysis of Using Reflectors in Distributed Denial-of-Service Attacks," ACM Computer Communications Review 2001

[35] Joao B. D. Cabreraa, Lundy Lewisb, Xinzhou Qinc, et al., "Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables-A Feasibility Study," Integrated Network Management Proceedings, 2001 IEEE/IFIP International Symposium

[36] Zhao Wen-Wang, Qin Shi-Yin, "The diagnosis of DDoS attack and a novel approach to optimizing control," Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing. 2001 International Conferences

[37] Andrian Piskozub, "Denial of service and distributed denial of service attacks," TCSET 2002, February 18~23, 20

[38] Dan Sterne, Kelly Djahandari, Ravindra Balupari, William La Cholter, Bill Babson, Brett Wilson, Priya Narasimhan, Andrew Purtell, Dan Schnackenberg, Scott Linden, "Active Network Based DDoS Defense," Proceedings, DANCE* 02', 2002 IEEE

[39] Stajano, F.; Isozaki, H.; "Security Issues for Internet Appliances," Applications and the Internet (SAINT) Workshops, 2002. Proceedings. 2002 Symposium on, 28 Jan.-1 Feb. 2002

[40] John Ioannidis, Steven M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks," Network and Distributed System Security Symposium, February, 2002.

[41] Jun Li; Mirkovic, J.; Mengqiu Wang; Reiher, P.; Lixia Zhang;, "SAVE: Source Address Validity Enforcement Protocol," INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, Volume: 3, 23-27, June, 2002

[42] Ratul Manajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. "Controlling high bandwidth aggregates in the network," ACM Computer Communication Review, 32(3), July, 2002

[43] Wan, K.K.K. Chang, R.K.C, "Engineering of a global defense infrastructure for DDoS attacks," 10th IEEE International Conference, Page(s): 419-427, Aug. 2002

[44] K.T. Law, John C.S. Lui, and David K.Y. Yau, "You Can Run, But You Can't Hide: An Effective Methodology to Traceback DDoS Attackers," Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002. MASCOTS 2002. Proceedings. 10th IEEE International Symposium on, 11-16 Oct. 2002

[45] Minho Sung and Jun Xu, "IP Traceback-based Intelligent Packet Filtering: A Novel Technique for Defending Against Internet DDoS Attacks," in 10th IEEE International Conference on Network Protocols(ICNP), Paris, France, Nov 2002

[46] Tieyan Li, Wai-Meng Chew, and Kwok-Yan Lam, "Defending against distributed denial of service attacks using resistant mobile agent architecture," Parallel and Distributed Processing Symposium., Proceedings International, IPDPS 2002

[47] Xiaobing Zhang, S. Felix Wu, "An Active Security Protocol against DoS attacks," IEEE SPECTRUM, 2002

[48] Dai kashiwa, Eric Y. Chen and Hitoshi Fuji "Active Shaping : A Countermeasure against DDoS attack," 2002 IEEE

[49] David K. Y. Yau, John C. S. Lui, and Feng Liang, "Defending Against Distributed Denial of Service Attacks with Max-Min Fair Server-centric Router Throttles," Quality of Service, 2002. Tenth IEEE International Workshop

[50] David Mankins, Rajesh Krishnan, Ceilyn Boyd, John Zaho, Michael Frentz, "Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing," Proceedings of Annual Computer Security Applications Conference (ACSAC), 2002.

[51] Garg, A., Narasimha Reddy, A.L., "Mitigation of DoS attacks through QoS regulation, Quality of Service," 2002. Tenth IEEE International Workshop on, 15-17 May, 2002 Page(s): 45 - 53

[52] Jelena Mirkovic, Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM 2002

[53] Jelena Mirkovic, Gregory Prier, Peter Reiher, "Attacking DDoS at the source," Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP'02), 2002 IEEE

[54] M. Kalantari, K. Gallicchio and M.A. Shayman, "Using Transient Behavior of TCP in Mitigation of Distributed Denial of Service Attacks," Decision and Control, 2002, Proceedings of the 41st IEEE Conference on, Volume: 2, 10-13 Dec. 2002 Page(s): 1422 1427

[55] NathalieWeiler, "Honeypots for Distributed Denial of Service Attacks," IEEE, 2002

[56] Rocky K.C. Chang r, "Defending against flooding-based distributed denial-of-service attacks," IEEE, 2002

[57] Stamatis Karnouskos, "Dealing with Denial-of-Service Attacks in Agent-enabled Active and Programmable Infrastructures," Proceedings of the 25th Annual International Computer Software and Applications Conference (COMPSAC.01) 2002 IEEE

[58] Simon Byers, Aviel D. Rubin, David Kormann, "Defending Against an Internet-based Attack on the Physical World," ACM Workshop on Privacy in the Electronic Society, November, 2002

[59] Jun Xu; Wooyong Lee, "Sustaining availability of web services under distributed denial of service attacks," Computers, IEEE Transactions on, Volume: 52 Issue: 2, Feb. 2003 Page(s): 195-208

[60] Tao Peng, Leckie, C., Ramamohanarao, K. "Protection from distributed denial of service attacks using history-based ip filtering," Communications, 2003. ICC '03. IEEE Inter-

national Conference on, Volume: 1 Page(s): 482-486, 2003

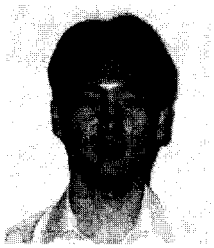
[61] W. J. Blackert, D. M. Gregg, A. K. Castner, E. M. Kyle, R. L. Hom, R M. Jokerst, "Analyzing interaction between distributed denial of service attacks and mitigation technologies," DARPA Information Survivability Conference and Exposition (DISCEX'03), IEEE 2003

[62] XiaoFeng Wang; Reiter, M.K."Defending against denial-of-service attacks with puzzle auctions," Security and Privacy, 2003. Proceedings. 2003 Symposium on, May 11-14, 2003, Page(s): 78 -92

[63] Yaar, A.; Perrig, A.; Song, D. "Pi: a path identification mechanism to defend against DDoS attacks," Security and Privacy, 2003. Proceedings. 2003 Symposium on, May, 11-14, 2003, Page(s): 93 -107

[64] B. Bencsath, L. Buttyan, I. Vajda, "A game based analysis of the client puzzle approach to defend against DoS attacks," Proceedings of SoftCOM 2003 11. International conference on software, telecommunications and computer networks, 2003, pp. 763-767

정 유 석



1999 아주대학교 정보통신공학과(학사)
2001 아주대학교 정보통신공학과(석사)
2002~현재 아주대학교 정보통신공학과 박사과정
관심분야: 정보보호, 인공지능, 알고리즘
E mail : j8508@ajou.ac.kr

홍 만 표

1981 서울대학교 계산통계학과(이학사)
1983 서울대학교 계산통계학과(이학석사)
1991 서울대학교 계산통계학과(이학박사)
1983~1985 울산공과대학 전자계산학과 전임강사
1985~현재 아주대학교 정보 및 컴퓨터 공학부 교수
1993~1994 미네소타대학 전자공학과 교환 교수
관심분야 : 병렬처리
E mail : mphong@ajou.ac.kr

The 9th International Conference on Database Systems for Advanced Applications

- 일 자 : 2004년 3월 17~19일
- 장 소 : 제주도
- 주 최 : 데이타베이스연구회
- 상세안내 : http://aitrc.kaist.ac.kr/~dasfaa04