능동 네트워크 기반의 DDoS 공격 대응 기술 동향

성균관대학교 한영주 · 양진석
김희승 · 정태명

1. 서 론

최근 컴퓨터 시스템의 공격 경향은 자동화, 분산화 되고 있다. 이러한 공격 경향은 큰 피해를 불러 일으키며 특히, 분산 서비스 거부(DDoS : Distri-buted Denial of Service) 공격은 인터넷상에서 가장 치명적인 위협 중에 하나이다. 예를 들어, 2001년 1월에 마이크로 소프트의 웹사이트 호스팅 서비스인 Hotmail, MSN, Expedia, 그리고 그 외의 다른 중요 서비스들이 DDoS 공격으로 인하여 22시간 동안 서비스가 불가능했던 사건이 있었다[14]. 이러한 DDoS 공격은 대량의 패킷을 네트워크로 보내서 자원을 고갈시키고 이로 인해 정상적인 트래픽에 대한 서비스마저 제공하지 못하게 하는 공격이다. 최근의 공격 경향으로 볼 때, 이에 대한 적극적인 대응이 어려운 상태이다. DDoS 공격은 짧은 시간에 많은 피해를 주며 대응 자체를 어렵게 한다. 이렇게 큰 피해가 생기는 이유는 공격 경향의 변화도 있지만 기존의 네트워크 기반 구조가 정적이며 유연하지 못하기 때문이다[17].

최근 공격들의 대응은 바이러스나 악의적인 코드가 감염된 이후 해결할 수밖에 없는 구조를 갖는다. 따라서 공격에 대한 백신 프로그램이 개발되었다 할지라도 이미 큰 피해를 입은 상태가 된다. 이러한 면에서 기존의 대응 체제는 사후약방문(死後藥方文)식의 효과를 가질 수밖에 없다. 네트워크 기반 구조의 비유연성은 또 다른 새로운 필요성을 가져왔으며 이러한 요구 사항은 능동 네트워크로 발전하였다.

본 논문에서는 DDoS 공격에 대한 보다 적극적이고 효율적인 대응 방법으로써, 차세대 네트워크 패러다임으로 제시되고 있는 능동 네트워크를 기반으로 하고 있는 DDoS 공격과 관련된 보안 프로젝트에 대하여 소개하고 이를 토대로 능동 네트워크 기반의 DDoS 공격 대응 동향 및 전망에 대하여 논하고자 한다.

2. DDoS 공격의 이해 및 분석

DDoS 공격은 서비스 거부 공격의 분산된 형태로써 공격자는 목적지 노드나 네트워크에 악의적인 대량의 패킷을 보내는 불법적인 행위로 자원을 고갈시켜 다른 합법적인 사용자의 이용을 방해한다.

DDoS는 매우 단순한 공격 기법이지만 방어하기 어려운 공격이다[7].

본 장에서는 DDoS 공격 방법을 살펴보고, 현재 널리 사용되고 있는 DDoS 공격 대응 기술을 분석 및 문제점을 고찰하고자 한다.

2.1 DDoS 공격 방법 분석

잘 알려진 DDoS 공격 유형으로는 SYN Flooding, Smurf, Fraggle, ICMP Flooding, UDP Flooding 등이 있다[20].

SYN Flooding은 3-way Handshake의 취약점을 이용한 것으로 SYN 패킷을 받은 서버는 자원을 할당한 후 SYN-ACK 패킷을 보내고 대기 상태에 놓여 있다. 공격자는 마지막 ACK를 발송하지 않고 계속 새로운 연결 요청을 하게 되어 서버는 자원 할당을 해지하지 않고 자원만 소비하게 된다[10].

Smurf는 IP 헤더의 송신지(source) IP 주소를 공격하고자 하는 목적지 IP로 변경한 다음, IP 헤더 뒤에 ICMP 메시지를 붙여서 ICMP Echo 요청을 브로드캐스트 주소로 전송한다. ICMP Echo 요청을 받은 모든 호스트들은 ICMP Echo 응답을 타겟으로 되돌려 보내게 된다.

Fraggle은 ICMP Echo 대신 UDP 패킷을 이용한 공격 툴이다.

ICMP Flooding나 UDP Flooding는 브로드케스트하지 않고 직접 대량의 ICMP Echo, UDP 패킷을 보

내는 것이다.

DDoS 공격 도구로는 TFN(Tribe Flood Network), Trin00, TFN2K, Stacheldraht과 같은 것들이 있고, 대부분의 DDoS 공격 도구는 SYN Flooding 유형을 이용하고 있다[19].

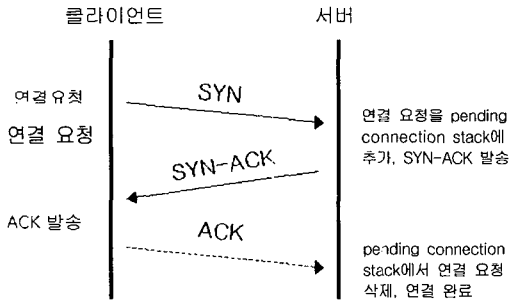

그림 1 TCP 3-way Handshake

SYN Flooding은 그림 1에서 보는 바와 같이 서버는 클라이언트의 연결 요청을 받고 SYN-ACK 패킷을 전송하면서 아직 완성되지 않은 대기 연결(pending connection)을 스택에 일정시간 보관하고 반 연결(half connection)을 유지하게 된다. 일반적으로 클라이언트는 ACK 패킷으로 응답하여 서버에 대기 연결을 스택에서 제거하고 연결을 완료하게 되지만 SYN Flooding는 마지막 ACK를 보내지 않고 계속 SYN 패킷으로 연결 요청을 하게 된다. 따라서 서버는 스택에 계속 대기 연결이 쌓여가게 되어 자원을 낭비하고 결국 더 이상 연결 요청을 받을 수 없게 된다. 스택에 대기 연결은 일정시간 동안만 보관되기는 하지만 SYN 연결 요청은 이보다 더 빠르게 이루어질 수 있고, 스택의 크기도 그다지 크지 않기 때문에 쉽고 빠르게 SYN Flooding에 의한 DDoS 공격이 성공될 수 있다[17].

TFN, Trin00, TFN2K, Stacheldraht는 그림 2와 같은 형태로 이루어진다. 공격자는 마스터와 에이전트로 사용할 호스트를 선택하고 DDoS 공격 툴을 설치한다. 마스터와 에이전트들의 서로간의 종속관계가 설정되고 공격자의 명령에 따라 마스터가 에이전트들을 제어하여 일시에 공격 목적지 호스트에 패킷을 보내게 되는데 이때 각각의 에이전트는 마스터의 제어 정보에 따라서 SYN Flooding, ICMP Flooding, UDP Flooding 등을 이용하여 목적지 호스트로 대량의 패킷을 보낸다. 목적지 호스트는 일시에 대량의 패킷을 받게 되고 이것을 처리하기 위해 많은 자원을 소모하게 된다[19].

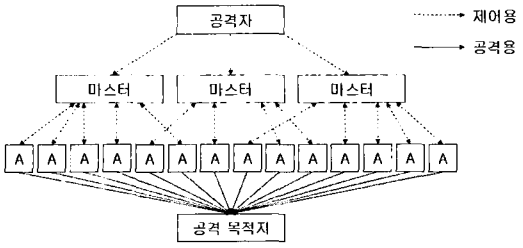

그림 2 DDoS 공격 도구의 공격 형태

2.2 현존하는 DDoS 공격 대응 기술

현존하는 DDoS 공격에 대한 대책은 다섯 가지의 단계 - 예방(prevention), 탐지(detection), 1차 대응(first response), 역추적(traceback), 2차 대응(second response)으로 구성된다[9].

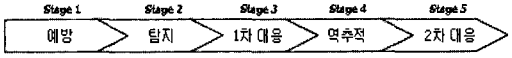

그림 3 현존 DDoS 공격 대응 단계

예방 단계에서는 자신의 호스트에 DDoS 에이전트가 설치되는 것을 막는 것이다. 이것은 두 가지 방법으로 달성할 수 있다. 첫 번째는 인터넷의 모든 사용자가 자신의 호스트에 DDoS 데몬이 존재하는지 검사하는 툴을 가지는 것이다. 이 방법은 DDoS 공격자로부터 자신의 호스트가 불법적인 목적으로 악용되는 것을 막아주지만, 그런 대대적인 협력을 얻는 것은 거의 불가능하다. 다른 예방 방법은 Cisco 라우터의 Ingress Filter를 사용하는 것이다. Cisco의 Ingress Filter는 모든 에지(edge) 라우터에서 외부로 나가는 패킷의 송신지 주소가 합법적인 것인지 검사하는 기능을 가진다. 에지 라우터의 네트워크에 일치되지 않는 IP 프리픽스(prefix)를 가지는 패킷은 외부로 전달되지 않는다. 이 기술은 DDoS 공격자가 스푸핑된 송신지 주소를 사용하는 것을 막아준다. 그러나 Ingress Filter는 두 가지 주요한 약점이 있다. 첫 번째는 현재 모든 에지 라우터에 이 기능이 설정되어 있지 않다. 만약 공격자의 에지 라우터에 Ingress Filter가 가능하게 되어 있지 않아서 스푸핑된 송신지 주소를 가지는 패킷이 외부로 나가게 되면 그것을

다시 잡는 방법은 거의 불가능하다. 두 번째 약점은 송신지 주소가 스푸핑 되지 않은 패킷에 대해서는 아무런 기능을 하지 못하는 것이다. 서버 자원을 소비하기 위한 목적의 공격들과 달리, 대역폭을 소비해 버리려는 공격들은 굳이 송신지 주소를 스푸핑 하지 않더라도 충분히 파괴적이다[3].

탐지 단계에서는 정상적인 패킷과 DDoS 공격 패킷에 대한 구별이 필요하다. 이것은 평소와는 다르게 갑작스럽게 패킷 양이 증가하는 비정상적인 상태를 확인하거나 ICMP, UDP 패킷이 일반적인 것들에 비해 큰 크기를 가지는지 확인하는 방법 등으로 이루어질 수 있다. 이미 많은 NIDS(Network based Intrusion Detection System)에서 비정상적인 트래픽을 모니터링 하는 기술이 개발되었다. 그러나 이 방법의 주요한 문제점은 NIDS는 정상적인 패킷을 악의적인 패킷으로 잘못 구별할 수 있다.

다음 과정은 1차 대응 단계로 악의적인 트래픽에 의해 대역폭이 막히기 전에 ISP(Internet Service Provider)에게 요청하여 Rate Limit를 수행하는 것이다. 이것은 라우터의 큐에 패킷 Rate Limit 기준을 미리 정해놓고 이 이상으로 들어오는 패킷을 폐기하게 된다. 하지만 이 방법은 우선 ISP로부터 이러한 도움을 받기까지 오랜 시간이 걸리고, 이 시간 동안에도 DDoS 공격은 계속되어 진다. 또한 네트워크는 패킷의 양 뿐 아니라 커다란 크기의 패킷들에 의해서도 공격받을 수 있기 때문에 한계를 가진다[3].

역추적 단계에서는 공격자의 근원지를 찾는 단계이다. 만약 공격 트래픽의 송신지 주소가 스푸핑된 것이라면, 각각의 라우터의 hop-by-hop 로그를 분석하여 실제 근원지를 추적할 수 있다. 하지만 이 방법의 약점은 상당히 느린 수동의 작업이고, 어떠한 라우터의 경우에는 송신지 주소를 구별하는 기능을 가지고 있지 않는 경우도 있다.

마지막 2차 대응에 대한 기술은 아직 미비하다. Flooding을 발생시키는 호스트가 공격자 자신의 호스트가 아니고 해킹되어 악용되고 있는 호스트일 수 있으므로, 공격에 참여하고 있는 호스트의 IP 주소를 얻더라도 할 수 있는 일이 다음과 같이 단 두 가지 밖에 없다. 첫째, 직접 각각의 호스트 사용자에게 연락하여 그들의 호스트가 해킹되어 DDoS 공격에 참여하고 있다고 알려주고 둘째, 그 호스트들의 ISP에게 연락하여 그들의 트래픽을 제한하도록 요청하는 것이다. 그러나 DDoS 공격은 수백, 수천의 호스트가 참여하기 때문에, 이 두 가지 방법은 실용적이지 못하다[9].

이렇게 DDoS 공격에 대한 대응 방법으로 제시되고 있는 Ingress Filtering, Rate Limit와 같은 대응 방법은 다음과 같은 문제점을 근본적으로 가지고 있다. 이는 DDoS 공격 대응에 관한 절차가 모두 관리자에 의한 "Expert-labor-intensive-manual" 절차에 의존한다는 것이다. 즉, 관리자는 항상 DDoS 공격 목적지에 가까이 있어야 하며, 로컬 라우터 인터페이스가 DDoS Flooding의 중간 노드로 사용되는지를 감시하고 이 인터페이스에 Packet Filtering이나 Rate Limit 룰을 적용하고 상위 조직과 접촉하여 DDoS 공격을 차단하여야만 한다. 하지만 동시 다발적으로 일어나는 DDoS 공격에 높은 기술을 가진 네트워크 관리자가 항상 적절히 대응할 수 없을 것이다.

3. 능동 네트워크

네트워크 기술이 발전함에 따라 네트워크를 기반으로 하는 다양한 응용 프로그램과 서비스들이 증가하고 있다. 그러나 현재 네트워크의 기반 구조는 고정된 프로토콜 스택이나 표준 제정의 시간 지연 등으로 인하여 다양한 형태의 네트워크 서비스들을 신속하게 수용하기에 한계를 가지고 있다[4,5,6]. 이러한 문제를 해결하기 위해 1994년과 1995년의 D-ARPA 회의에서 능동 네트워크의 개념이 도입되었으며, 현재 능동 네트워크에 대한 다양한 연구가 진행 중이다[6].

능동 네트워크는 중간 노드에서 응용 계층까지 조작할 수 있는 네트워크를 말한다[4]. 즉, 중간 노드를 실행 가능하게 만들어 기존 중간 노드들의 "저장-전달" 기능이 아닌 "저장-처리-전달"의 기능을 갖게 하여 서비스 및 새로운 프로토콜 전개에 유연하고 동적인 네트워크 구조를 제공한다[4]. 이러한 기능을 가지는 중간 노드를 "액티브 노드"라고 하며, 프로그램을 실어 전송하는 패킷을 "액티브 패킷"이라고 한다.

그림 4는 능동 네트워크의 개념을 나타낸다. 액티브 노드는 노드 운영체제, 실행 환경, 그리고 액티브 어플리케이션으로 구성된다. 각각을 살펴보면 다음과 같다[11].

3.1 노드 운영체제(NodOS:Node Operation System)

노드 운영체제는 패킷 스케쥴링, 자원 관리, 패킷

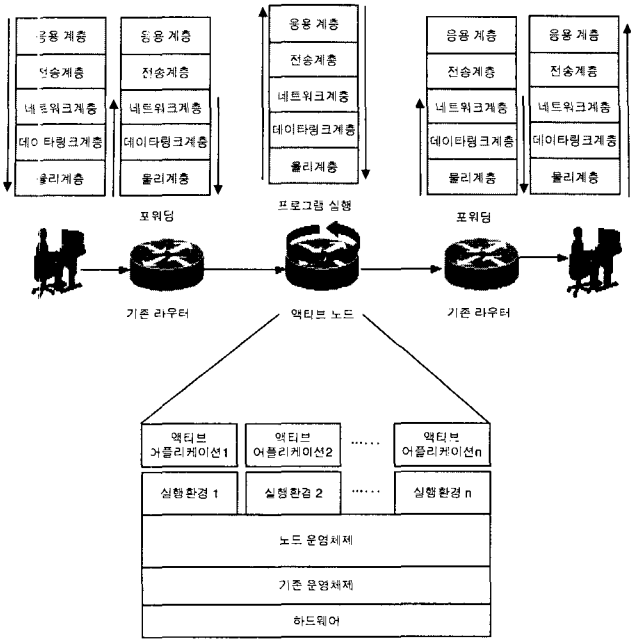

그림 4 능동 네트워크의 개념

구분과 같은 서비스를 제공한다. 또한 노드 운영체제 위에서 동작하는 실행 환경들에 대한 물리적인 자원 접근 및 할당에 관한 서비스를 제공한다[11].

3.2 실행 환경(EE:Execution Environment)

실행 환경은 유닉스의 쉘처럼 작동한다. 실행 환경은 액티브 패킷에 실행 프리미티브(primitive) 혹은 서비스를 제공한다. 현재 능동 네트워크 백본망인 ABone(Active Network Backbone)에서 운영 및 연구 중 실행 환경은 ANTS(Active Node Trans-fer System), PLAN(Packet Language for Active Network), ASP(Active Signaling Protocol) 그리고 CANES(Composable Active Network Elements) 등이 있다[1,8,13,15].

3.3 액티브 어플리케이션(AA:Active Application)

액티브 어플리케이션은 특정 실행 환경에서 실행될 수 있는 프로그램으로써 종단 간(end-to-end) 서비스를 제공한다. 즉, 액티브 어플리케이션은 실행 환경에서 제공하는 API (Application Program Interface)를 사용하여 개발되기 때문에, 최적화된 서비스를 구현할 수 있다. 액티브 어플리케이션은 능동 네트워크의 구현 방법에 따라 다양한 형태로 구체화된다. 대표적인 액티브 어플리케이션으로는 네트워크 보안, 망 관리, 혼잡 제어, 능동적인 신뢰성 보장 멀티캐스트 등이 있다[2,12,16].

액티브 노드에서의 액티브 패킷의 실행은 네트워크에 유연성 및 확장 적응성을 제공하는 장점을 가진다. 능동 네트워크는 네트워크 상에 액티브 노드들을 배치하여 이를 통과하는 액티브 패킷들이 노드가 제공하는 서비스를 실행시키거나 액티브 패킷 자신이 운반하는 실행 코드를 이용하여 노드 상에서 처리가 가능하도록 한 환경이다. 사용자는 이러한 기반 구조를 이용하여 최적화된 새로운 네트워크 서비스 및 프로토콜을 좀 더 빠르고 유연하게 배포할 수 있다. 따라서 DDoS 공격에 대한 대응과 같이 빠르고 자동화된 대응이 절실한 공격에 대하여 능동 네트워크는 최적의 기반 구조를 제공할 수 있다. 능동 네트워크는 다음과 같은 장점을 제공한다[4,7].

- 새로운 서비스의 빠른 배포
- 새로운 서비스의 자동화된 배포
- 제 3자(third party)에 의한 배포
- 중단 없는 실행(non-disruptive)

- 확장성(scalability)
- 적응성(adaptiveness)

4. 능동 네트워크 기반의 DDoS 공격 대응 기술 동향

본 장에서는 능동 네트워크를 기반으로 하는 DDoS 대응 기법에 대한 시대별 연구 동향을 기술한다.

4.1 동적 필터링(Dynamic Filtering)

능동 네트워크를 이용한 주소 스푸핑(Address Spoofing) 대응 기법인 Dynamic Filtering은 1997년에 Massa-chusette 대학의 Van에 의해 제안되었다[17]. 이 프로젝트는 ANTS 기반의 능동 네트워크 기술을 이용하여 SYN Flooding을 이용하는 DDoS 공격을 방어하는 기술로써, 기존의 Ingress Filtering의 단점을 보완한 시스템이다. SYN Flooding과 같은 주소 스푸핑을 이용한 DDoS 공격을 막기 위해서는 관리하고자 하는 도메인 내에 어느 위치에서도 적용이 되어야 하는데 기존의 Ingress Filtering은 효과적인 필터링을 적용하기 위해서는 ISP간의 협약이 필요하며, 라우터들의 갱신, 환경 재설정 등이 필요하다. 이처럼 더딘 대응 방법은 짧은 시간안에 급속히 증가하는 DDoS 공격에 효과적으로 대응하기에는 부적합하다.

이 프로젝트의 목적은 이러한 Ingress Filtering 소프트웨어를 능동 네트워크를 이용하여 공격이 발견되었을 경우 동적으로 빠르게 배포하여 각 라우터에서 효과적으로 필터링을 수행할 수 있도록 하는 것이다. Dynamic Filtering System의 구성 요소는 다음과 같다.

4.1.1 TCPApplication과 TCPCapsule

SYN Flooding 공격을 감지하고 네트워크 내에 대응 메카니즘을 동적으로 배포하기 위하여 TCPApplication이라는 액티브 어플리케이션이 액티브 노드에 존재한다. 이는 기본 TCP 메커니즘과 공격을 탐지하는 대응 메커니즘을 가지고 있으며, TCP 메커니즘은 TCPCapsule이라는 단일 캡슐(Capsule)을 이용하여 동작한다. 이는 클라이언트와 서버간의 통신에 사용되며, 기존의 TCP 헤더를 그대로 상속하고 있다. 기존의 TCP 헤더와 크게 다른 점은 이전 노드 정보를 가지고 있어 필터링 메커니즘을 적용할 때 사용된다. DefendCap을 사용하는 DefendObj라는 필터를 동적으로 배포할 수 있다. 이러한 동적 배포를 통하여 DefendObj라는 필터는 공격 근원지에 점차 가까워진다.

4.1.2 DefendObj와 DefendCap

DefendObj는 액티브 노드의 캐쉬(cache)에 저장되는 필터로서, 네트워크 내 액티브 노드마다 존재하므로 호스트에 공격이 발생되었을 때만 배포된다. 즉, 공격 발생이 탐지되면, TCPApplciation은 DefendCap이라는 캡슐을 전송하여 이를 통해 DefendObj를 생성한다. 한번 생성된 DefendObj는 스푸핑된 캡슐을 필터링하고 공격 근원지에 가능한 한 가까이에서 필터링을 할 수 있도록 Push-back을 수행한다.

4.1.3 Push-back

Push-back의 기능은 필터링을 가능한 한 공격 근원지 가까이에서 수행할 수 있도록 필터를 옮기는 기능이다. 즉, DefendCap이 수행될 때마다 캡슐의 이전 노드를 검사하여 이전에 이 노드에 DefendCap이 전송되었는지를 검사하고 전송되지 않았을 경우, 이전 노드로 DefendCap을 전송한다. 그림 5는 Dynamic Filtering 시스템의 적용의 예를 나타낸다.

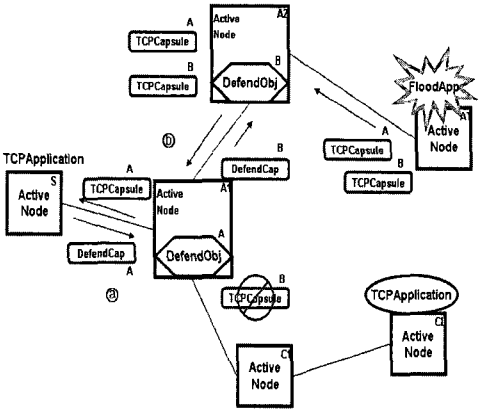

그림 5 Dynamic Filtering System

액티브 노드 AT에서 현재 액티브 노드 S를 향한 SYN-Flooding을 이용한 공격을 수행하고 있다. ⓐ의 과정은 공격이 발생하는 동안 노드 S에 TCP Capsule이 도착하면, TCPApplication은 이전 노드에 DefendCap을 전송함을 나타내며, ⓑ의 과정은 이를 수신한 노드 A1은 DefendObj를 생성한 후 스푸핑된 TCPCapsule이 도착하면 이를 필터링한 후Push-

back을 위하여 이전 노드 B에 DefendCap을 전송하는 과정을 나타낸다.

이처럼 ANTS의 서비스 배포 메커니즘을 이용한 Dynamic Filtering 기법은 공격의 빠른 대응, 사용자 투명성, 쉽고 빠른 배포와 같은 장점을 나타낸다. 그러나 이는 대칭형 라우팅에 기반을 두기 때문에 좀더 일반적인 네트워크 환경에 적용하기에는 부적합한 단점이 있으며, 현재는 SYN-Flooding을 제외한 다른 주소 스푸핑 방법에는 적용할 수 없다는 단점을 가지고 있다.

4.2 AEGIS

AEGIS(An Active-Network-Powered Defense Mechanism against DDoS Attacks)는 2001년에 NTT의 정보 공유 플랫폼 연구소에서 제안되었으며, 능동 네트워크 기반의 DDoS 공격에 대한 방어 메커니즘을 제시하고 있다. 이 프로젝트에서는 존재하는 기존의 DDoS 대응 솔루션에 대한 약점들을 고찰하고 이를 극복하기 위해 능동 네트워크를 기반구조로 하고 있다[9].

기존의 DDoS에 대한 대응책은 예방 단계의 경우 스캐닝 범위의 한계와 Ingress Filtering의 단점을 보완한 보안 솔루션으로써 다음과 같은 요구 사항을 갖는다.

- 새로운 기능과 네트워크 서비스는 라우터에서 로딩되고 실행될 수 있는 표준화된 모듈의 형태로 구현된다. 여기서 표준화된 모듈은 액티브 코드를 말한다.
- 모든 액티브 코드는 인증을 받아야만 한다.
- 액티브 코드는 특정 IP 주소에서 들어오는 패킷을 트리거할 수 있다. 특정 IP에서 들어오는 패킷은 액티브 코드가 명시된 수정된 라우팅 테이블에 의해서 노드이 상주하는 액티브 코드를 실행시킨다.
- 어떤 액티브 노드는 자신의 이웃에 있는 모든 액티브 노드에 대한 정보가 있어야만 한다. 여기서 이웃 노드는 물리적인 다음 홉을 의미하는 것이 아니다.
- 각 액티브 노드는 나가는 패킷에 대해서 Class-Based Queuing(CBQ)를 지원한다.

AEGIS는 그림 6과 7에서 보는 바와 같이 DD-oS 공격에서 기존의 방화벽 시스템이 가지는 단점을 해결하는 메커니즘을 제공한다.

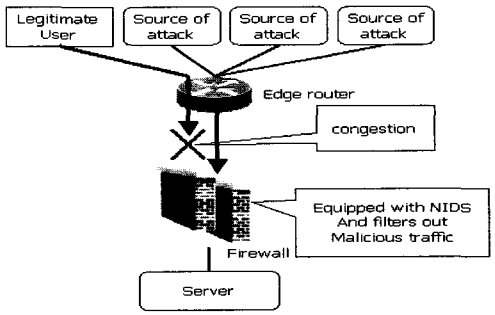

그림 6 기존의 방화벽

공격자가 네트워크 대역폭 소진을 목적을 가질 경우 그림 6에서 보는 바와 같이 ISP의 에지 라우터와 공격 목적지의 방화벽 사이에 혼잡이 발생한다. 그 결과로 정당한 사용자는 서버에 접근할 수 없다. 그러나 그림 7에서 보는 바와 같이 AEGIS는 공격자 네트워크의 에지 라우터에 코드를 분배하여 트래픽의 영향이 ISP의 에지 라우터까지 미치지 않는다.

이러한 동작을 위한 AEGIS의 구성 요소는 표 1과 같다.

AEGIS는 능동 네트워크 환경을 기반 구조로 하는 분산 방화벽 시스템이라고 할 수 있다. 이는 기존의 피해자 측 방화벽에서의 필터링을 공격자 측에서 필터링함으로써 공격으로 인한 대역폭 손실을 최소화하는 장점이 있다.

그러나 아직 특정 실행 환경을 고려하지 않고 있으며, 구현하여 테스트 해야 할 필요가 있다. 또한, AEGIS는 모든 공격의 경로는 고정되어 있음을 가정하고 있으며, 현재 DDoS 공격의 에이전트까지 가능한 역추적 메커니즘을 마스터까지 가능하도록 보완되어야 한다.

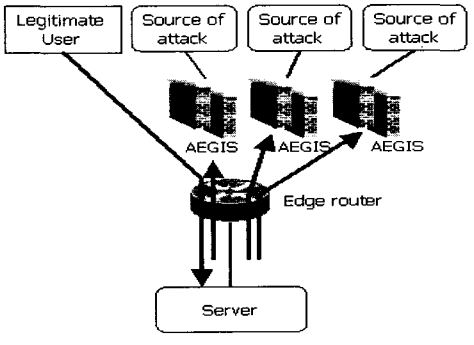

그림 7 AEGIS

표 1 AEGIS의 구성 요소 및 기능

구성요소	기 능
Shield	· 관련된 패킷을 모니터링 · 패킷을 의심 정도에 따라 3개의 레벨로 분류 · DDoS 공격이 결정되면 해당 패킷을 필터링
Commander	· AEGIS를 제어하는 중앙 제어 센터 · Shield 모듈을 설정 및 제어
Probe	· Flood가 발생한 근원지를 향해서 배포 · 근원지 측에서 패킷을 브로킹 · 공격의 증거를 수집

4.3 AN-IDR

AN-IDR(Active Networks Intrusion Detection and Response) 프로젝트는 2002년에 Network Associates Laboratories와 Boeing Phantom Works이 연합하여 DARPA에 의해 지원을 받아 뛰어난 적응성, 이동성, 효율성을 갖는 침입 탐지 및 대응(intrusion detection and response) 시스템 개발을 위한 프로젝트이다[7]. AN-IDR은 기존의 IDR 메커니즘이 갖는 새로운 공격 패턴에 대한 늦은 대응, 대응 소프트웨어 배포의 어려움 등의 단점을 극복한 새로운 메커니즘으로써, 자율적인 자기 복제와 위치와 다양한 토폴로지에 적응성이 뛰어난 침입 탐지, 추적, 응답 그리고 대응 메커니즘을 제공하는 능동 네트워크 기반의 프로토타입(prototype)이다[18].

AN-IDR은 여러 개의 네트워크 경계를 넘나드는 침입에 대하여 해당 공격 근원지에 가능한 가깝도록 자동화된 추적 및 차단을 제공하기 위하여 침입 탐지 시스템, 방화벽, 라우터, 네트워크 관리 구성요소, 그리고 호스트 사이에 상호 협력을 제공하는 IDIP(Intruder Detection and Isolation Protocol)를 기반으로 하고 있다. 또한, DDoS 공격에 대한 자동 침입 탐지 및 응답(automated intrusion detection and response)의 대응 소프트웨어의 동적 배포를 능동 네트워크를 사용한다. 이는 새로운 방어 소프트웨어의 빠른 배포에 유용하며, 대응 소프트웨어를 네트워크 상에 효과적이고 능률적으로 작동할 수 있는 위치로 이동시킬 수 있는 장점을 가진다.

AN-IDR은 능동 네트워크 기반 구조에서 침입 탐지 및 대응을 위한 구조와 기능을 정의하고 있다. 침입과 대응은 표 2에서 보는 바와 같이 몇 개의 기능적 영역으로 구별하였으며, 이를 다시 프로그램 별로 구분하였다. 각 행은 IDR을 기능별로 나눈 것으로써, 스캐닝, 탐지, 추적, 대응, 보완 및 복구, 관리, 커뮤니티 기능을 나타낸다. 각 열은 IDR을 프로그램 별로 구분한 것이다. 다음은 AN-IDR의 기능 중 DDoS 공격 대응과 관련된 기능을 설명한 것이다.

4.3.1 탐지(Detection)

그림 2의 탐지 단계에 해당하는 것으로써 일정 시간 안에 peak-rate를 가지는 비정상 트래픽을 탐지하여 DDoS 공격 여부를 결정하는 기능으로 Stationary 프로그램으로 구현된다. 이는 각 노드에 동적으로 탑재되어 실행되며, 다른 액티브 패킷 프로그램에 비해 상대적으로 노드에 머무르는 시간이 길다는 특성을 갖는다.

표 2 AN-IDR의 문제 영역

프로그램 / 기 능	Stationary	Roving	Variable Destination	Escort
Scanning		○		
Detecting	○			
Tracing				○
Response		○	○	
Repair				
Management		○		
Communities		○		○

4.3.2 추적(Tracing)

추적은 DDoS 공격이 탐지된 후 비정상 트래픽의 incoming 인터페이스를 추적하여 공격 근원지를 찾아 가는 역추적 기능으로써 Escort 프로그램으로 구현된다. 이는 모니터링, 제어, 침입자의 고립화의 기능을 수행하며, 특정 목적지로 이동하는 패킷 뒤에 첨부되어 해당 패킷과 동일한 이동 경로로 이동하면서 경로 상의 노드에서 실행되는 프로그램이다.

4.3.3 대응(Response)

대응은 DDoS 공격이 탐지된 후 추적 프로그램이 공격 근원지 역추적의 경로를 따라 이동하면서 실질적인 DDoS 공격 대응을 수행한다. 즉, 이 기능에서 Rate Limit나 Ingress Filtering을 수행할 수 있다. 이는 Roving 프로그램으로 구현된다. Roving 프로그램은 특정 목적에 따라 네트워크 상의 여러 노드를 이동하는 액티브 패킷 프로그램으로 필요에 따라 복제(clone) 및 변환될 수 있는 특성을 갖는다.

AN-IDR에서의 DDoS 공격 대응 시나리오는 다음과 같다. 그림 8은 현재 HIC 도메인 내 스트리밍 서비스를 제공하는 비디오 서버에 대한 UDP Flooding을 이용한 DDoS 공격을 보여주고 있다. DDoS 공격 도구로는 Stacheldraht를 사용하고 있다. 공격 master는 Org A에 있으며 이에 대한 좀비 데몬들은 Org B,C,D에 배포되어 있다. 각 좀비 데몬들로부터의 UDP Flooding에 의하여 HIC 도메인의 백본 네트워크와 HIC 도메인과 MAP 도메인의 경계 영역, 그리고 비디오 서버에 트래픽이 몰려서 비디오 서버는 제대로 동작을 할 수 없는 상황이다.

이에 대한 능동 DDoS 대응을 살펴보면 그림 9와 같다.

UDP Flooding이 발생하는 동안 비디오 서버의 트래픽이 급속히 증가하는 것을 디텍터(detector)가 감지하게 되면, 디텍터는 자신의 첫 번째 이웃인 라우터 1과 관리 스테이션에게 역추적 및 대응을 요청한다. 관리 스테이션은 액티브 프로그램인 Mobile

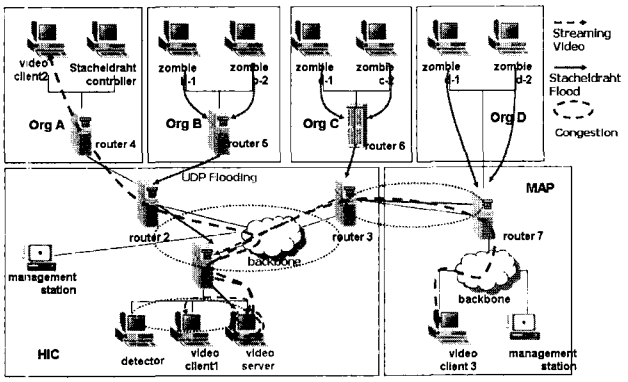

그림 8 테스트베드 토폴로지와 DDoS 공격

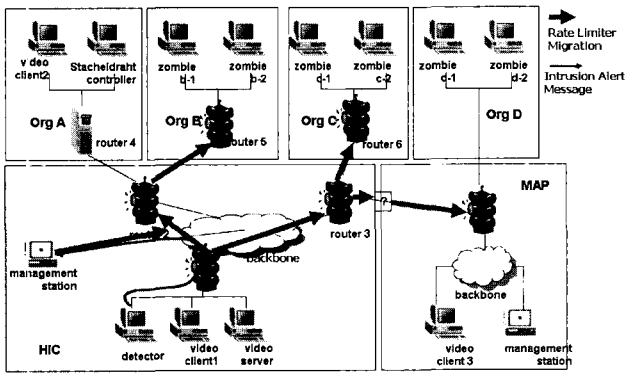

그림 9 DDoS 공격의 능동 대응

r-ate limiter 프로그램을 라우터 1에게 전송하고 라우터 1에서는 이를 실행하여 트래픽의 수를 줄인다. 그와 동시에 자신의 네트워크 인터페이스 중 Flooding 근원지와 가까운 것을 선택하여 해당 인터페이스를 통해 이웃하는 라우터에게 Mobile rate limiter의 복사본을 전송한다. 이와 같은 방법으로 Mobile rate limiter는 공격 근원지에 점차 가까워지게 되면서 네트워크 상의 트래픽의 양이 점차 줄어 비디오 서버는 정상 동작을 재개할 수 있다. 여기서 주의할 점은 HIC과 MAP는 다른 도메인이기 때문에 HIC의 라우터로부터 수신한 Mobile rate limiter에 대한 인증이 필요하며 이는 IDIP를 통하여 제공된다. 능동 DDoS 대응 프로토타입에 사용된 Mobile rate limiter는 AN-IDR의 기능 영역 중 Roving 프로그램으로 구현된 대응 기능에 해당된다.

5. 능동 네트워크 기반의 DDoS 공격 대응 기술의 비교 분석 및 고찰

본 절에서는 4장에서 구성 요소 및 시나리오를 중심으로 살펴본 능동 네트워크 기반의 프로젝트에 대한 장점 및 단점을 비교·분석할 것이며, 각 프로젝트를 주요 DDoS 공격 대응 단계를 기준으로 분석하여 공통점을 찾아 앞으로 능동 네트워크 기반의 DDoS 공격 대응 기술에서 개선되어야 할 요소를 추출하고자 한다.

표 3은 각각의 프로젝트별 장·단점을 나타낸다.

표 3에서 보는 바와 같이 능동 네트워크는 기반 구조가 제공하는 유연성으로 인해 기본적으로 빠르고 효율적인 서비스 배포가 가능하다는 장점을 가지고 있으며, 기존의 탐지 및 차단 기술과 능동 네트워크와 통합할 때 생기는 단점과 한계가 있다.

표 3 프로젝트별 장·단점

프로젝트	장 점	단점 및 한계
Dynamic Filtering	·Ingress Filtering의 보완 ·공격자에 가까운 곳에서 필터링 공격으로 인한 대역폭 손실을 최소화	·대칭형 라우팅 기반으로 일반적인 네트워크에 적용이 부적절 ·SYN-Flooding 이외의 주소 스푸핑은 적용 불가능
AEGIS	·Ingress Filtering의 보완 ·스캐닝 범위의 한계 극복 ·공격자에 가까운 곳에서 필터링함으로써 공격으로 인한 대역폭 손실을 최소화	·특정 실행 환경을 고려하지 않음 ·모든 공격의 경로는 고정되어 있음을 가정 ·마스터(master)까지의 추적이 불가능
AN-IDR	·공격자에 가까운 곳에서 필터링함으로써 공격으로 인한 대역폭 손실을 최소화 ·취약한 서비스의 트래픽만 검사	·AN-IDR 설계의 테스트 수준 ·관리자의 개입이 많음

표 4는 주요 DDoS 공격 대응 단계 별로 각각의 프로젝트를 분석한 것이다. 이를 살펴보면, 능동 네트워크 기반의 DDoS 공격 대응의 공통점으로 이동성

표 4 DDoS 공격 대응 단계별 프로젝트 분석

프로젝트	탐 지	역추적	대 응
Dynamic Filtering	·SYN-Flooding 탐지에만 한정	·ANTS 프로토콜의 특성을 이용하여 역추적 수행	·Ingress Filter- ing을 변형하여 공격 근원지에 접근하며 필터링 수행
AEGIS	·패킷 모니터링을 이용한 비정상 트래픽 탐지	·액티브 패킷 프로그램인 Probe를 이용한 공격 근원지 추적	·중앙에 Shield와 분산된 Probe를 이용한 분산 필터링 수행
AN-IDR	·peak rate을 이용한 비정상 트래픽 탐지	·액티브 패킷 프로그램인 tracing 프로그램을 이용하여 실시간으로 추적	·역추적과 함께 Rate Limiter 액티브 프로그램을 이용하여 필터링

을 갖는 액티브 패킷 프로그램을 이용한 역추적과 대응에서의 향상을 꾀하고 있다는 것을 볼 수 있다. 이는 기존의 DDoS 공격 대응 방법이 가지고 있던 역추적의 어려움과 동시 다발적으로 일어나는 공격에 적절히 대응할 수 없었던 단점을 효과적으로 개선한 것이다. 그러나 이러한 장점에도 불구하고 효과적으로 DDoS 공격 트래픽을 추출할 수 있는 탐지 기법의 부재라는 근본적인 한계를 가지고 있다. 즉, 이는 표 4의 탐지 단계에서 볼 수 있듯이 기존의 DDoS 공격 탐지 방법을 그대로 사용하고 있기 때문이다. 따라서 좀 더 효율적이고 효과적인 D-DoS 공격 트래픽 탐지 기법이 연구되어야 한다.

현재 실시간 트래픽 흐름 측정에 관한 연구가 IETF를 중심으로 진행 중이다. 실시간 트래픽 흐름 측정이란 실시간으로 트래픽 흐름(traffic flow)을 측정하는 것으로써, 네트워크 상의 트래픽을 실시간으로 수집하여 흐름 단위로 정보를 분석하는 것이다 [20]. 이는 네트워크 관리와 보안 관리에 적용되어 다양하게 적용될 수 있는데, DDoS 공격 트래픽 탐지 기법에도 적용될 수 있다. 즉, 기존의 IP 헤더의 정보에 의존한 패킷 수집에서 벗어나 각종 Flooding 공격에 대하여 흐름 별로 패킷을 수집하면 공격 패턴의 분석이 좀 더 효율적으로 예상된다.

현재 능동 네트워크 기반의 DDoS 공격 대응 기술에서 탐지 기법의 미비함은 트래픽 분석을 통해서 좀 더 나은 탐지가 가능할 것으로 보이며 트래픽 분석을 통한 탐지 후, 능동 네트워크의 장점을 이용한 빠른 배포 및 자동 대응을 적용한다면 좀 더 효율적인 DDoS 공격 대응이 가능할 것이다.

6. 결 론

컴퓨터 시스템의 보안은 지능화, 자동화, 통합화되고 있다. 이러한 과정은 점차 고도화되어 가고 있는 공격 방법과 맞물려 발전하고 있는 것이다. 이러한 공격 방법을 대표하는 것이 DDoS 공격이다. DDoS 공격은 스푸핑된 송신지 주소로 여러 호스트에서 분산 공격을 수행하기 때문에 공격 근원지 추적 및 대응이 어렵다. 현재 Rate Limit나 Ingress Filtering과 같은 다양한 대응 방법이 있으나 이러한 대응 방법은 근원 공격지에 대한 추적이 어려울 뿐만 아니라 전체 도메인에 대한 대응이 어렵다는 단점이 있다. 본 논문에서는 이러한 기존의 대응 방법의 단점을 극복한 대응 방법으로 능동 네트워크의 유연성 및 효율성의 장점을 살린 다양한 능동 네트워크 기반의 DDoS 공격 대응 프로젝트들을 살펴보았다. 프로젝트들의 공통된 특징을 살펴보면, 탐지 후 공격 근원지 가까이에서 Rate Limiter나 필터링을 수행하도록 대응 소프트웨어의 빠른 배포에 초점을 맞추고 있다. 이처럼 능동 네트워크를 기반으로 하는 대응 기법은 DDoS 뿐만이 아닌 실시간 대응이 필요로 하는 다양한 분야에 최적의 환경을 제공할 것이다. 그러나 DDoS 공격 트래픽 탐지 기법이 기존의 방식을 그대로 적용되고 있기 때문에 좀 더 효율적인 탐지 기법의 연구가 필요하다.

참고문헌

[1] B. Braden, et al., "The ASP EE: An Active Network Execution Environment," DARPA Active Networks Conference and Exposition (DANCE) 2002. San Francisco, CA., June, 2002.

[2] B. Schwartz, et al., "SmartPacket for Active Networks," BBN Technologies, Jan. 1998.

[3] Cisco Systems, Inc, "Using CAR During DOS Attacks"

[4] D. L. Tennenhouse, et al., "A Survey of Active Network Research," IEEE communications magazine, Jan. 1997.

[5] D. L. Tennenhouse, et al., "Towards an active network architecture," In Multimedia Computing and Networking '96, Jan. 1996.

[6] D. Raz, et al., "An Active Network Approach to Efficient Network Management," IWAN '99, 1999.

[7] D. Sterne, et al., "Active Network Based DDoS Defense," Proceedings of the DARPA Active Networks Conference and Exposition, May, 2002.

[8] D. Wetherall, et al., "ANTS: A Toolkit for Building and Dynamically Deploying Network Protocols," IEEE OPENARCH'98 Proc., Apr. 1998.

[9] Eric Y. Chen, "An Active-Network- Powered Defense Mechanism against DDoS Attacks," IWAN'01, Sept. 2001.

[10] Jonathan Lemon, "Resisting SYN flood DoS

attacks with SYN cache," Proceedings of BSDCon, 2002
[11] K. Calvert, et al., "Architectural Framework for Active Networks," AN Working Group, July, 1999.
[12] L. H. Lehman, et al., "Active Reliable Multicast," IEEE INFOCOM '98,1998.
[13] M. Hicks, "Planet: An Active Internetwork," IEEE INFOCOM '99, 1999.
[14] R. Lemos, "Glitch, attack hit Microsoft Web Sites," CNET News.com, Jan. 2001.
[15] S. Marugu, et al., "Bowman and CANEs: Implementation of an Active Network," 37th Annual Allerton Conference, Sep. 1999.
[16] T. Faber, "ACC: Active Congestion Control," IEEE Network, May/June, 1998.
[17] Van C. Van. A defense against address spoofing using active networks. Master's thesis, MIT, May, 1997.
[18] 이수형, 나중찬, 손승원, "액티브 네트워크 기반 네트워크 보안 기술동향", 2001년 5월.
[19] 이철호, "DDoS 공격도구 분석", Real-Time Packet Analysis Lab, 2002년 2월.
[20] 최연숙, 김재영, 홍원기, "웹기반의 실시간 인터넷 트래픽 흐름 측정 및 분석", KNOM Review, May, 2000.

한 영 주

1999 성균관대학교 정보공학과(학사)
2002~현재 성균관대학교 컴퓨터공학과 (석사과정)
관심분야 : 능동 네트워크, 네트워크 보안, 침입 탐지 시스템
E mail : yjhan@imtl.skku.ac.kr

양 진 석

2003 성균관대학교 정보공학과(학사)
2003~현재 성균관대학교 컴퓨터공학과 (석사과정)
관심분야 : 능동 네트워크, 침입감내 시스템, 네트워크 관리, 네트워크 보안, IPv6
E mail : jsyang@imtl.skku.ac.kr

김 희 승

2003 성균관대학교 정보통신공학부(학사)
2003~현재 성균관대학교 컴퓨터공학과 (석사과정)
관심분야 : 능동 네트워크, 시스템 보안, 네트워크 보안, 해킹
E-mail : hskim@imtl.skku.ac.kr

정 태 명

1984 일리노이주립대학 전자계산학과 (학사)
1987 일리노이주립대학 대학원 컴퓨터공학(공학석사)
1995 Purdue대학교 대학원 컴퓨터공학과(공학박사)
1995~1999 성균관대학교 전기전자 및 컴퓨터공학부 조교수
2000~현재 성균관대학교 전기전자 및 컴퓨터공학부 부교수
관심분야 : 능동 네트워크, 네트워크 관리, 네트워크 보안, 통합보안 관리
E-mail : tmchung@ece.skku.ac.kr