사용자 인증을 통한 클라이언트 기반 DDoS 공격 대응 매커니즘

정종갑*, 이희조**
*고려대학교 컴퓨터정보통신대학원
**고려대학교 컴퓨터 · 통신공학부
e-mail : kbroad@korea.ac.kr*, heejo@korea.ac.kr**

A Client-based DDoS Attack Defense Mechanism through User Authentication

Jongkap Jeong*, Heejo Lee**
*Graduate School of Computer and Information Technology, Korea University
**Division of Computer and Communication Engineering, Korea University

요 약

최근의 분산 서비스 거부(DDoS) 공격 방법은 점점 더 자동화, 다양화되고 있으며, 단순한 개별 기업에 대한 공격에서부터 국가간의 사이버전쟁으로까지 그 영역이 확대되고 있다. DDoS 공격은 이미 2000 년도 이전부터 발생해온 오래된 공격이고, 이를 방어하기 위한 다양한 DDoS 공격 방어 시스템을 구축하고 있음에도 불구하고 아직까지 이를 효과적으로 차단하지 못하고 있다. 이는 그간 DDoS 공격 방어 시스템이 공격이 시작되었을 때 개개의 공격 패턴을 탐지하고 차단하는 방법으로 발전해 왔기 때문이다. 따라서 좀 더 효과적인 DDoS 공격 대응을 위해 공격 트래픽이 발송되기 전에 클라이언트에서부터 공격에 대응하는 방안이 필요하다. 이에 본 논문에서는 사용자 인증을 통하여 등록된 사용자임을 검증하고, 클라이언트와 인증장비간의 인증을 통해 인증된 사용자의 트래픽만 허용하는 매커니즘을 제안한다.

1. 서론

분산 서비스 거부(DDoS) 공격은 1990 년대 말부터 유행하기 시작하여 2000 년 2 월 9 일에 Yahoo, eBay, Amazon.com, E*Trade, ZDNet, Buy.com, FBI 등 유명 웹 사이트에 대한 대대적인 공격으로 큰 피해를 주면서 알려지게 되었으며[1], 최근 국내에서는 2009 년 7 월 7 일과 2011 년 3 월 3 일에 대규모 DDoS 공격이 있었다[2].

DDoS 공격은 과거에는 자기과시나 영웅심리에 의해 특정 대형 웹사이트를 공격했으나 최근에는 중소형 사이트를 포함, 금전을 갈취하는 협박형 공격으로 바뀌고 있다. 이러한 협박형 DDoS 공격 이외에도 국가간의, 혹은 다수 집단간의 정치적 목적으로도 DDoS 공격이 사용되고 있다[3].

이러한 위협적인 공격을 가하는 DDoS 공격에 대응하기 위해 보안 업체에서는 DDoS 전용 장비를 개발하여 출시하고 있지만, DDoS 전용 장비를 통한 방어에는 한계가 있다. 일반적으로 DDoS 공격을 탐지하는 원리는 특정 시간에 유입되는 트래픽을 감지하여 공격 발생여부를 판단하여, 정책에 따라 공격성 트래픽을 탐지하는 원리를 가지고 있다. 그러나 다수의 좀비 PC 를 통하여 미량의 패킷을 동시 다발적으로 발생시킬 경우 DDoS 전용 장비에서 공격성 트래픽인지 탐지해내기가 어렵다. 또한 공격 받고 있는 것을 감지할 수 있다 하더라도 대용량 트래픽이 유입되었다고 무조건 패킷을 차단한다면 서비스의 가용성을 침해하는 문제가 발생한다[4].

본 논문에서는 DDoS 전용 장비에서 인증 받지 않은 모든 패킷을 우회시키거나 폐기하고, 클라이언트에서 인증 장비와 상호 인증을 통하여 보호하고자 하는 서버에 등록된 사용자의 패킷만 해당 서버로 보내도록 하여 서비스의 가용성을 보장하는 DDoS 공격 대응 매커니즘을 제안한다.

2. DDoS 기술 동향

2.1 DDoS 공격 기술

DDoS 공격 기술은 표 1 과 같이 공격 대상에 따라 5 가지로 구분할 수 있다[5][6].

<표 1> 대상별 DDoS 공격 기술

구분	특징
Application	특정 호스트내의 Application 공격 (L7) 정당한 사용자의 서비스 제한
	HTTP Get Flooding, 공격, Cache Control 공격, VoIP/SQL/RPC 공격 등

Host	특정 호스트의 모든 네트워킹 서비스 혹은 시스템 자체 마비시키는 공격(L3/L4)
	TCP SYN, SYN ACK, RESET Flooding, UDP Flooding 공격, IP Flooding, ARP, RARP 스푸핑, ICMP 플러딩 공격 등
Resource Attacks	공격 대상 네트워크 내의 중요 자원에 대한 공격
	DNS Lookup 플러딩, SYN 플러딩 등을 이용한 네트워크 장비의 세션 관리 기능 마비
Network Attacks	한정된 대역폭을 가지는 네트워크 회선 상에 막대한 공격 트래픽을 전송함으로써 네트워크를 마비시키는 공격
	UDP 혹은 ICMP 이용하여 대량 트래픽 전송
Infrastructure	전체 인터넷 망 자체를 마비시키기 위한 공격
	Root DNS 서버 공격, 대형 백본 라우터 및 라우팅 프로토콜 공격, 인증서 서버에 대한 공격 등

2.2 DDoS 공격 대응 기술

DDoS 공격에 대한 대응은 탐지와 차단으로 나눌 수 있다. 탐지 기술로는 IDS/IPS, 방화벽 등을 활용하는 방법이나 DDoS 전용 대응시스템이나 망 차원의 Netflow, ACL, MRTG(Multi Router Traffic Grapher)정보를 활용하는 방법 등이 있다. 차단 기술로는 URL 차단, IP 차단, Port/Protocol 차단 방법 등이 있다[6][7].

DDoS 방어 기법 또한 다양하게 연구되고 있다[5][8]. 그 중에서 네트워크상에 유효한 트래픽임을 검증하거나 패킷 패스포트를 발급하여 사용자 IP 를 인증하는 등 네트워크 아키텍처를 제한해서 DDoS 를 방어하는 기법이 있다[9][10].

2.3 DDoS 공격의 발전

DDoS 기술은 표 2 에서 보는 바와 같이 시간이 갈수록 점차 발전되는 양상을 보이고 있다[11].

<표 2> DDoS 공격의 발전

구분	시기	특징
1 세대	2000 년대 초반	많은 양의 공격 트래픽 생성 2000 년 아마존, 야후 등 공격
2 세대	2000 년대 초/중반	자동 전파 기능의 인터넷 웜 2003 년 1 월 25 일 (1.25 대란)
3 세대	2000 년대 중반	봇넷 (C&C 서버가 단일) 공격시에 C&C 서버와 반드시 통신
4 세대	2000 년대 후반	봇넷 (C&C 서버가 다수 혹은 변화함) 2009 년 7 월 7 일 (7.7 DDoS)

2.4 현재 DDoS 방어 시스템의 한계

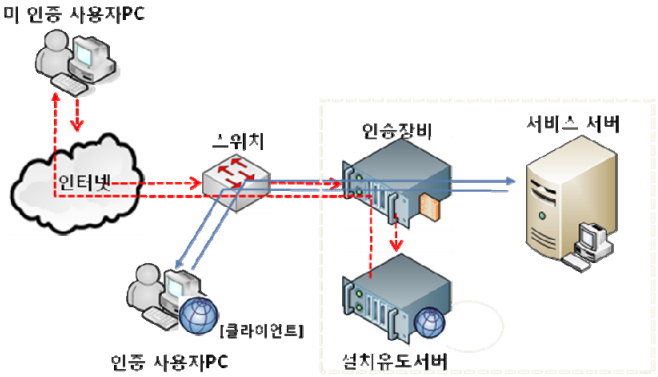
처음 발생한지 10 년이 지난 공격이 아직도 시도되고 있고 그로 인한 피해가 지속적으로 발생되고 있는 것은 DDoS 공격에 대한 전반적인 고찰 없이 시도되는 공격 형태만을 분석하여, 특정 형태의 공격을 탐지하고 차단 할 수 있는 방법을 개발해 왔기 때문이다. 이러한 형태의 대응 기술은 그에 대한 동작 방식이 공개되면 공격자들은 얼마든지 해당 기술을 우회할 수 있는 새로운 공격을 개발할 수 있다[11].

이로 인한 문제점은 4 세대 공격인 지난 2009 년 7 월 7 일의 DDoS 공격 대응에서 찾아볼 수 있다. 7/7 DDoS 의 경우 매우 지능화된 공격방법을 사용하고 있다. 대규모 좀비 PC 에서 소규모 공격이 이루어져 개개의 공격은 정상 트래픽과 구분이 불가능하여 기존의 보안장비를 우회하는 방식이 사용되었고, C&C 서버가 없어, DDoS 공격 명령을 차단할 방법이 없었다. 또한 정교한 TCP 공격으로 인해 해당 서버가 마비되거나 이를 방어하려고 할 때 서버, 방화벽, 스위치 등이 장애가 발생하는 구조였다[12].

3. 제안 메커니즘을 이용한 DDoS 공격 대응

3.1 제안 메커니즘 구성

본 논문에서 제안하는 메커니즘의 구성은 그림 1 과 같이 공격이 시작되는 사용자 PC 에 클라이언트 S/W 와 방어하고자 하는 대상이 있는 곳에 인증된 사용자 패킷임을 검증하는 H/W 장비(인증장비, 설치유도서버)로 이루어져있다.



(그림 1) 제안 메커니즘 구성

제안 메커니즘의 구성 요소는 클라이언트, 인증장비, 설치유도서버로 구분된다. 각 구성 요소들의 역할은 표 3 과 같다.

<표 3> 구성 요소 별 역할

구분	역할
클라이언트	사용자 인증을 통해 인증 받은 사용자의 패킷은 패킷에 인증데이터를 삽입해서 보내고 미 인증 사용자의 패킷은 정책에 따라 우회 시키거나 폐기된다.
인증장비	TCP 패킷을 검사하여 인증 받은 사용자에게서 온 패킷(패킷내 인증데이터 검증)이면 서비스 서버로 전송하고 그렇지 않으면 설치유도서버로 보낸다.
설치유도서버	사용자에게 클라이언트 설치유도 페이지를 생성해서 전달한다.

본 논문에서 제안하는 매커니즘에서 핵심요소라고 볼 수 있는 것은 클라이언트이다.

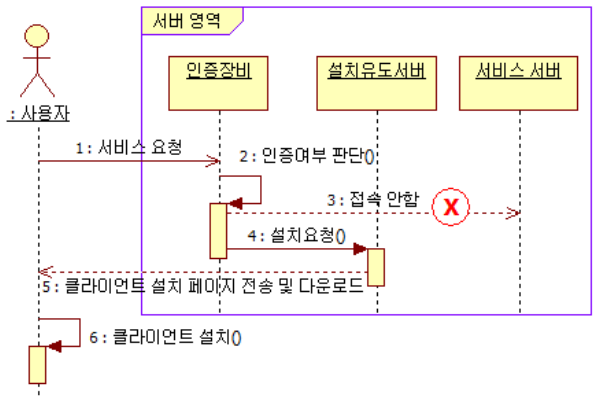
클라이언트가 설치되지 않았다면 사용자의 패킷은 서비스 서버로 전달되지 않고 설치유도서버로 전달되어 클라이언트를 설치할 수 있도록 해준다.

클라이언트가 설치되었다면, 사용자 인증을 하지 않은 사용자의 패킷은 클라이언트에서 우회시키거나 폐기한다. 사용자 인증을 받은 사용자의 패킷은 패킷 내에 특정 인증데이터를 삽입한 후 전송하여 인증장비에서 해당 인증데이터를 검증한 후 검증이 확인되면 서비스 서버로 패킷을 전송한다.

요약하자면, 서비스 서버에 접속이 가능 하려면 첫째로 클라이언트가 설치되어 있어야 하고, 둘째로 사용자 인증을 받아야 하며, 셋째로 패킷 내에 인증데이터가 있어야 한다. 이러한 3 중 작업으로 인해 인증된 사용자의 신뢰성과 서비스의 가용성을 보장하면서 서비스 서버를 DDoS 공격으로부터 좀 더 효율적인 방어를 할 수 있도록 해준다.

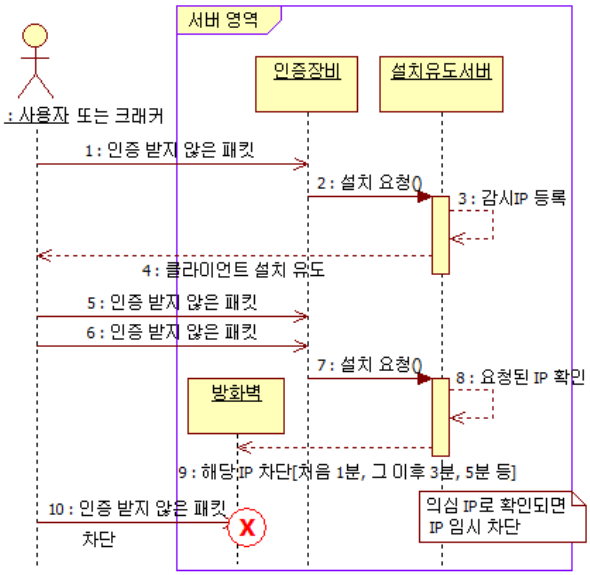
3.2 클라이언트 미 설치 시 DDoS 공격 대응

클라이언트가 설치 되지 않는 사용자(정상 이용자 또는 크래커)로부터의 서비스 요청이 오면 그림 2 와 같이 설치유도서버로 내용이 전달되어 설치유도페이지를 생성하여 사용자에게 전송한다. 클라이언트가 설치되어 있지 않다면, 서비스 서버에는 접속 자체가 되지 않으므로 DDoS 공격이 시작되었다 하더라도 서비스 서버는 공격에 대한 영향을 받지 않게 된다.



(그림 2) 클라이언트 미 설치 시 동작 흐름

하지만, 이러한 경우 서비스 서버는 피해를 받지 않겠지만, 인증장비나 설치유도서버의 경우 요청에 대한 처리에 많은 부하를 받게 되어 자칫 가용성에 문제가 발생할 수 있다. 본 논문에서 제안하는 매커니즘은 클라이언트를 기반으로 동작하므로 인증데이터가 있는 인증된 패킷이 아닌 일반 패킷이 지속적으로 들어온다면, 클라이언트가 설치되지 않는 상태에서 잘못된 사용으로 인한 것이거나 DDoS 공격에 의한 것이라 볼 수 있으므로 이 경우 그림 3 과 같이 해당 IP 를 차단해서 시스템을 보호하도록 한다. IP 를 차단할 경우 정상 사용자의 피해를 막기 위해 특정 시간 동안만 차단하여 다시 시도할 수 있도록 한다. 처음 여러 번 요청이오면 1 분 동안 IP 를 차단한 후 해제하고, 그 이후 여러 번 요청이 오면 3 분 동안 차단하고, 그 이후엔 5 분, 10 분 등으로 차단 시간을 늘려 DDoS 의심 공격으로부터 대응하면서 동시에 가용성을 확보한다. 이렇게 의심되는 IP 는 따로 관리하여 좀비 PC 라 판단되면 해당 IP 를 영구적으로 차단하도록 한다.

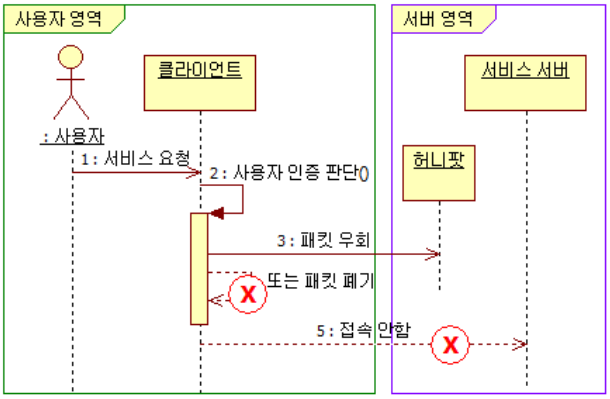


(그림 3) 의심 IP 차단 동작 흐름

3.3 클라이언트 설치 시 DDoS 공격 대응

클라이언트가 설치되었을 경우에는 사용자 인증을 받은 경우와 그렇지 않은 경우로 대응 동작이 나뉘게 된다.

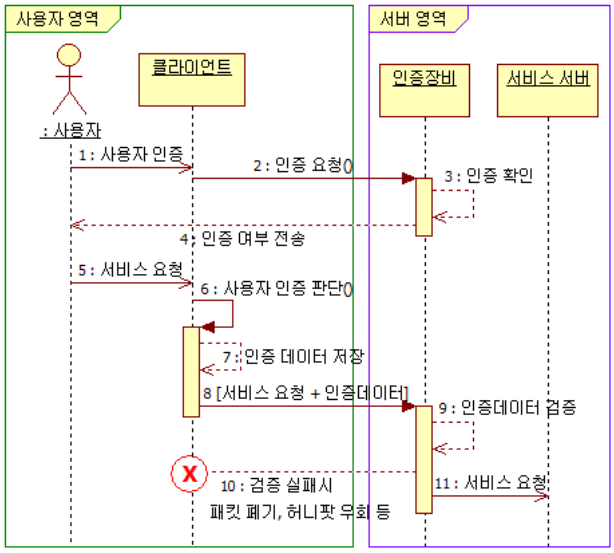
사용자 인증을 받지 않은 경우는 그림 4 과 같이 서비스 서버로 서비스를 요청하는 패킷을 정책에 따라 우회시키거나 폐기하도록 하여 아예 서비스 서버로의 접속을 차단하여 대응한다.



(그림 4) 클라이언트 미 인증 시 동작 흐름

사용자 인증을 받은 경우는 그림 5 와 같이 서비스 서버로 접속하는 패킷에 인증데이터를 추가하여 보내고 인증장비에서 해당 패킷의 인증데이터를 검증한 후 서비스 서버로 패킷을 보내도록 한다. 이렇게 하여 안전하다고 판단되는 패킷만 서비스 서버를 요청

을 받게 됨으로써, DDoS 공격이 일어나는 상황에서도 가용성을 확보하면서 서비스를 할 수 있다.



(그림 5) 클라이언트 인증 시 동작 흐름

4. 결론

DDoS 공격은 시스템을 악의로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다. 이미 오래 전부터 시도 되고 있는 공격임에도 불구하고 그 공격의 파괴력을 오히려 강화시키면서 현재에도 계속 발생하고 있고 그에 대한 피해도 계속되고 있다. 이는 지금까지의 전용 DDoS 방어 장비들이 특정 공격 형태를 탐지하고 차단하도록 개발되어 왔기 때문이다. 하지만 DDoS 공격이 날로 지능화 되고 있어 정상적인 트래픽인지 명확히 구분하기 어려워지고 있으며, 장비에서 감당할 수 없는 트래픽이 발생되고 있어 DDoS 공격에 대한 방어 효과를 크게 기대하기 어렵다.

본 논문이 제안하는 메커니즘은 사용자 인증을 통해 서비스를 사용하는 사용자를 확실히 구분하여, 클라이언트가 설치된 인증된 사용자만 서비스 서버에 접근을 허락하는 구조로 되어 있어, 임의의 공격지로부터 공격을 방어하고 DDoS 공격 시 클라이언트로부터 해당 공격을 막아내도록 하여 보호하고자 하는 서버의 신뢰성과 서비스의 가용성을 보장 해 줄 수 있다.

기존 전용 DDoS 방어 장비의 대체 기술이 아니라 전용 DDoS 방어 장비를 포함한 여러 네트워크 보안 장비들과 연동하여 좀 더 효율적으로 DDoS 공격 대응 시스템을 구성할 수 있을 것으로 기대된다.

향후 연구로는 본 논문에서 제안한 메커니즘의 효율성을 향상시키기 위해 패킷 패스포트 등을 활용하여 인증 받은 사용자에게서 온 패킷임을 빠르고 효율적으로 검증하는 연구를 진행할 예정이다.

참고문헌

[1] T. Peng, C. Leckie and K. Ramamohanarao, "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Computer Serveys, Vol.39, No.1, Article 3, April 2007.

[2] “다시 터진 DDoS 공격 누가 왜?”, 연합뉴스, 2011.3.4, http://www.yonhapnews.co.kr/bulletin/2011/03/04/0200000000AKR20110304103900017.HTML

[3] 정구현, 서동원, 박현도, 이희조, “DDoS 를 통한 네트워크 마비 협박과 공격 대응”, 경영과컴퓨터, pp.152-155, 2008. 6.

[4] 안성호, 강창구, 최용락, “Agent 와 협력을 통한 DDoS 공격 대응 매커니즘”, 한국인터넷정보학회 학술발표대회 논문집, pp.333-336, 2009. 10.

[5] Jelena Mirkovic and Peter Reiher, “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms”, ACM SIGCOMM Computer Communication Review, Vol.34, No.2, Apr. 2004.

[6] 전용희, 장종수, 오진태 “DDoS 공격 및 대응 기법 분류”, 정보보호학회지 제 19 권, 제 3 호, pp.46-57, 2009. 6.

[7] 구자현, “서비스 거부 공격(Denial of Service)의 유형 및 대응”, 주간기술동향, 통권 1377 호, 2008. 12.

[8] Vamsi Kambhampati, Daniel Massey, Christos Papadopoulos, “A Taxonomy of Capabilities Based DDoS Defense Architectures”, ACM SIGCOMM, Aug. 2008.

[9] Xin Liu, Xiaowei Yang and Yanbin Lu, “To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-node Botnets”, ACM SIGCOMM Computer Communication Review, Vol. 38, No. 4, pp.195–206, Aug. 2008.

[10] Xin Liu, Ang Li, Xiaowei Yang and David Wetherall, “Passport: Secure and Adoptable Source Authentication”, In Proceedings of the 5th USENIX NSDI, pp.365-376, Apr. 2008.

[11] 최양서, 오진태, 장종수, 류재철, “분산서비스거부(DDoS) 공격 통합 대응체계 연구”, 정보보호학회지 제 19 권, 제 5 호, pp.11-20, 2009. 10.

[12] Cisco Systems Korea, “DDoS 공격 비상, 어떻게 대처할 것인가? – 7.7 DDoS 공격 유형 분석 및 대응 방안”, Cisco Webseminar, 2009. 7.