Software-Defined Networking 기반 DNS 증폭공격 탐지 방법에 대한 연구

조금환, 김형식, 정재훈*

성균관대학교 전자전기컴퓨터공학과, *성균관대학교 소프트웨어학과

A Study on defense mechanism against DNS amplification attacks based on Software-Defined Networking

Geumhwan Cho, Hyoungshick Kim, Jaehoon (Paul) Jeong*

Department of Computer Science and Engineering, Sungkyunkwan University

*Department of Software, Sungkyunkwan University

요 약

DDoS(Distributed Denial-of-Service) 공격 유형 중 하나인 DNS 증폭공격은 Open Recursive DNS 서버에서 대량의 DNS 응답 트래픽을 발생시키는 특징을 이용하는 공격 방법으로, 일반적인 DDoS 공격과 달리 탐지 및 방어하는데 어려움이 많다. 기존 연구에서는 사용자에 의해 발생된 쿼리 정보를 저장한 뒤, 응답 정보와 비교하는 방식으로 DNS 증폭공격을 탐지하였다. 하지만, 이와 같은 방법은 저장매체(예, 데이터베이스, 블룸필터 등)에 따라 성능차이가 크고, 실제 네트워크 환경에 적용하기에 한계가 존재한다. 따라서 본 논문에서는 SDN 컨트롤러에 모든 쿼리 정보를 저장하는 방법으로 높은 탐지 정확도를 달성할 수 있는 방법을 제안한다.

I. 서론

인터넷 서비스를 이용하기 위해서는 URL (Uniform Resource Locator)이라는 인터넷 주소를 입력하지만, 실제 네트워크에서는 인터넷 호스트를 식별하기 위해 IP주소가 사용된다. 도메인 네임 시스템(DNS, Domain Name System)은 사용자가 입력한 URL을 IP주소로 자동적으로 변환하는 시스템이다. 그 결과, 사용자는 기억하기 어려운 IP주소보다 상대적으로 기억하기 쉬운 URL를 통해 웹페이지에 접속할 수 있게 되었다. 그로인해, 오늘날의 인터넷에서는 엄청난 양의 DNS 쿼리(query)가 이용되고 있다[1].

DNS는 (1)인증이나 확인절차 없이 쿼리를 요청하고, 쿼리에 대한 응답(response)을 받는 단순한 구조로 설계되어 있고, (2)쿼리에 의해 발생되는 네트워크 트래픽보다 응답에 의해 발생되는 트래픽의 양이 훨씬 크다는 특징을 갖고 있다[2]. DNS 증폭공격은 DDoS 공격의 유형으로 이러한 특징을 이용한 대표적인 공격 방법이다.

전통적인 DDoS 공격에서는 공격자가 봇넷(botnet)을 이용해 대량의 트래픽을 발생시킴으로써 사용자의 정상적인 서비스 접근을 방해하는 공격을 시도했기 때문에, 봇넷의 IP주소를 차단하는 방법을 통해 방어가 가능하였다.

그러나 DNS 증폭공격의 경우, 공격자 **A**가 정상적인 사용자 **B**의 IP 주소를 스푸핑하고 Open Recursive DNS 서버에 쿼리를 요청한다. 서버는 정상적인 사용자 **B**에게 응답메시지를 전송한다. 전송된 응답메시지는 공격자 **A**가 보

본 연구는 미래창조과학부 및 정보통신기술진흥센터 의 정보통신·방송 연구개발사업[R0166-15-1041, 중앙 집중제어 기반 네트워크 보안기술 표준개발]과 대학ICT연구센터육성 지원사업(IITP-2015-H8501-15-1008)의 연구결과로 수행되었음. 또한, 2014년도 정보통신·방송(ICT)연구개발 사업[2014044072003, SDN 기술을 이용한 사이버 검역 시스템 개발] 및 한국연구재단의 신진연구지원사업(2014R1A1A1003707)에 의하여 연구되었음

낸 쿼리보다 더 많은 양의 트래픽을 발생시킨다. 또한 봇넷을 이용해 다수의 Open Recursive DNS 서버에 쿼리를 요청하면, 사용자 B는 DNS 증폭공격으로 인해 인터넷 서비스 이용이 불가능해진다.

이러한 DNS 증폭공격을 탐지하기 위해 기존연구[3,4]에서는 정상적인 사용자가 요청했던 쿼리 정보를 저장하고, 응답과 비교하여 증폭공격의 발생 유무를 판단하는 방법을 제안하였다. Kambourakis 등[3]은 데이터베이스에 쿼리 정보를 저장하는 방식을 사용하였고, Paola 등[4]은 쿼리 정보를 블룸필터에 저장하였다. 하지만, 데이터베이스를 사용한 방법은 추가적인 통신비용(communication cost)이 발생하고, 블룸필터를 사용하면 정확도(accuracy)가 감소할 수 있다. 따라서 본 논문에서는 SDN 컨트롤러에 모든 쿼리 정보를 저장하여 정확도를 높일 수 있는 DNS 증폭공격 탐지 방법을 제안한다.

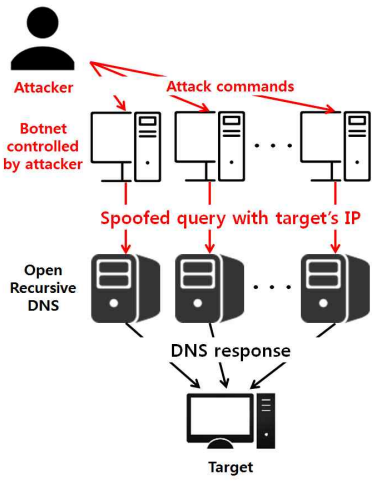
본 논문의 구성은 다음과 같다. Ⅱ장에서는 DNS 증폭공격을 탐지하기 위한 기존연구 및 배경지식에 대해 알아보고, 제안하는 SDN 기반 DNS 증폭공격 탐지 방법 및 시스템을 적용하기 위한 이슈사항들에 대해 Ⅲ장에서 설명하고, 마지막으로 Ⅳ장에서 결론을 도출할 것이다.

II. 배경지식 및 관련연구

2.1 DNS 증폭공격(DNS amplification attack)

전통적인 방식의 DDoS 공격은 (1)공격자가 많은 양의 트래픽을 발생시켜야 하고, (2) 공격 트래픽을 발생시키는 봇넷의 IP주소를 차단함으로써 방어가 가능하기 때문에 공격자가 갖는 혜택(benefit)이 적었다. 하지만, DNS 증폭공격에서는 공격자가 많은 양의 트래픽을 발생시킬 필요가 없고, 공격자의 위치를 찾기가 매우 어렵기 때문에 IP주소 차단과 같은 방어방법이 효과적이지 않다. 이러한 DNS 증폭공격은 다음과 같은 3가지 특징을 갖고 있다.

첫째, DNS 증폭공격은 스푸핑된 IP주소를 사용하여 쿼리를 요청한다. 하지만, TCP 프로토콜과 같이 정보를 전달하기 전에 핸드셰이킹(handshaking)을 사용하는 프로토콜에서는 스푸핑된 IP주소의 사용이 어렵기 때문에 UDP 프로토콜의 53번 포트를 통해 공격이 이루어진다는 특징이 있다.



[그림 1] DNS 증폭공격

둘째, 큰 비용을 들이지 않고 대량의 네트워크 트래픽을 발생시킬 수 있다. DNS는 적은 양의 쿼리가 대량의 응답 트래픽을 발생시키는 특징을 갖고 있다. 이러한 특징은 공격자에 의해 생성된 쿼리가 정상적인 사용자에게 대량의 응답 트래픽으로 전달 될 수 있다.

셋째, DNS 증폭공격의 효과를 증가시키기 위해 봇넷을 이용하여 Open Recursive DNS 서버에 쿼리를 동시 다발적으로 요청하기 때문에 적은 비용으로 효과적인 공격이 가능해진다.

[그림 1]은 DNS 증폭공격의 예이다. (1)공격자가 봇넷에 공격 명령을 내리면, (2)다수의 봇넷들은 스푸핑된 타켓의 IP주소를 이용해 Open Recursive DNS 서버에 쿼리를 요청한다. (3)쿼리를 요청받은 서버에서는 타켓에 응답 트래픽을 전송한다. 동시에 대량의 응답패킷을 수신한 타겟은 DoS 공격으로 인해 원하는 인터넷 서비스를 이용할 수 없게 된다.

2.2 관련연구

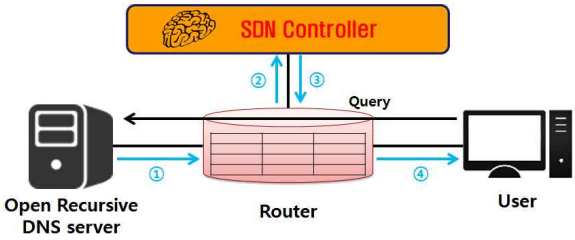
DNS 증폭공격을 탐지 및 방어하기 위해 많은 연구들이 진행되어 왔다. Kambourakis 등[3]은 쿼리 정보와 응답 정보를 일대일 매핑하

는 방법을 제안하였다. 정상적인 사용자의 경우 일반적으로 name resolution이 로컬 DNS 서버에서 수행되지만, DNS 증폭공격에서는 다수의 DNS 서버를 이용한다는 점을 이용한 탐지방법이다. 로컬 DNS 서버와 연결된 별도의 데이터베이스에 쿼리 정보를 저장하고, 응답 정보와 매핑한다. 매핑된 패킷은 사용자에게 전송하고, 매핑이 되지 않은 패킷은 드랍 시키는 방법을 제안하였다. 하지만, 데이터베이스에 저장된 데이터가 많아진다면, 성능이 저하된다는 단점을 갖고 있고, 로컬 DNS 서버와 데이터베이스 간 통신비용이 증가할 수 있다. Paola 등[4]은 라우터와 같은 네트워크 리소스에는 저장 공간이 크지 않기 때문에 블룸필터를 사용한 DNS 증폭공격 탐지 방법을 제안하였다. 블룸필터에 요청한 쿼리 정보를 해쉬값으로 저장하고, 응답 정보의 해쉬값과 비교하는 방식을 제안하였다. 그러나 블룸필터는 단방향 자료구조로 저장만 할 수 있고 삭제가 불가능한 단점을 갖고 있다. 이러한 문제를 해결하기 위해 2개의 블룸필터를 사용하고 교체하는 방식을 제안하였지만, 블룸필터가 교체되는 주기를 결정하기 어렵고, 필터가 교체될 때 공격이 발생한다면, 공격을 탐지가 어렵다는 단점을 갖고 있다. 따라서 제안한 방법은 정확도에 대한 문제를 갖고 있다.

III. SDN 기반 DNS 증폭공격 탐지

사용자가 요청한 쿼리 정보를 저장하기 위해 데이터베이스를 이용한 방법[3]은 큰 저장 공간을 확보할 수 있지만, 데이터베이스의 데이터를 읽을 때 추가적인 통신비용이 발생할 수 있고, 라우터에 있는 블룸필터를 이용한 방법[4]은 저장 공간이 부족하고 정확도가 떨어진다는 단점을 지니고 있다.

본 논문에서는 DNS 증폭공격을 탐지하기 위해 라우터와 SDN 컨트롤러의 저장 공간을 함께 사용하는 방법을 제안한다. 제안하는 방법은 라우터에 쿼리 정보를 저장하고, SDN 컨트롤러에 라우터에 저장된 데이터를 주기적으로 업데이트한다. 라우터의 데이터는 스케쥴링 알고리즘(예, FIFO)과 같은 방법으로 삭제 및 저



[그림 2] 제안하는 DNS 증폭공격 탐지 방법

장된다. SDN 컨트롤러에서는 사용자에 의해 발생된 모든 쿼리 정보를 저장하고, 라우터는 상대적으로 최근 데이터들만 저장한다.

제안하는 DNS 증폭공격 탐지 방법은 [그림 2]에서 볼 수 있으며, 다음과 같이 동작한다. 사용자가 요청한 쿼리 정보는 라우터에 저장된다. ① Open Recursive DNS 서버에서 응답 정보가 유입되면 라우터에 저장된 쿼리 정보와 비교한다. ④ 일치하는 쿼리 정보가 존재하면 사용자에게 응답 패킷을 전달한다. ② 일치하는 쿼리 정보가 존재하지 않으면 SDN 컨트롤러에 저장된 쿼리 정보를 요청하고, ③ SDN 컨트롤러에 쿼리 정보의 존재 유무를 라우터에 전달한다. 쿼리 정보가 존재하면 ④을 실행하고, 존재하지 않으면 드랍(drop)한다.

모든 쿼리 정보를 SDN 컨트롤러에 저장하기 때문에, 100%의 정확도를 달성할 수 있지만 ②,③에서 SDN 컨트롤러와의 추가적인 통신비용이 발생한다. 발생되는 통신비용이 크다면 라우터에 저장하는 방법을 사용해야 하고, 통신비용이 크지 않다면 저장 용량이 큰 SDN 컨트롤러를 이용하는 방법이 효율적이다. 따라서 본 논문에서 제안하는 방법은 정확도와 통신비용 사이의 트레이드오프(trade-off)가 존재한다.

3.1 정확도-통신비용 트레이드오프

Ⅲ장에서 논의한 바와 같이, SDN 컨트롤러는 사용자가 요청한 모든 쿼리 정보를 저장하기 때문에 100%의 정확도를 달성할 수 있지만 라우터와 SDN 컨트롤러 사이의 통신비용이 추가적으로 발생한다. 따라서 통신비용과 정확도 사이의 트레이드오프를 계산하여, 통신비용이 크다면 기존연구[4]와 같은 방법을 사용해야 하

[표 1] SDN 컨트롤러 이용에 따른 통신비용 증가

기호	설명
$_{MP}$	쿼리 정보 비교에 따른 오버헤드
C_{COMM_REQ}	통신비용 (to SDN 컨트롤러)
$C_{COMM-RSP}$	통신비용 (from SDN 컨트롤러)
$C_{COMM-TOT}$	전체 통신비용

고, 통신비용을 줄이기 위한 방법으로 라우터에서 사용하는 저장 공간에 대한 크기 확장이 요구된다. 라우터에서 SDN 컨트롤러에 저장된 쿼리 정보를 요청 시 발생하는 통신비용은 다음과 같이 계산할 수 있다.

$$C_{COMM-TOT} \quad O_{CMP} + C_{COMM-REQ} + C_{COMM-RSP}$$

따라서 $_{OMM\ TOT}$의 값과 탐지 정확도와의 트레이드오프를 계산하여, 적절한 라우터의 저장 공간 크기 및 SDN 컨트롤러와의 통신 주기 등을 설정해야 할 것이다.

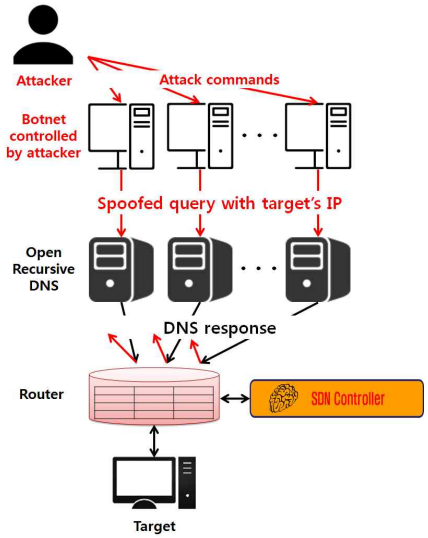
3.2 탐지 방법의 예

[그림 3]에서 볼 수 있듯이, 공격자는 봇넷을 통해 스푸핑한 타겟 IP주소를 이용하여 다수의 Open Recursive DNS 서버에 쿼리를 요청한다. DNS 서버는 타겟에서 요청한 쿼리로 인식하고 응답 패킷을 타겟에게 보낸다.

라우터에서는 쿼리 정보를 비교하지만 쿼리 정보가 저장되어 있지 않기 때문에 SDN 컨트롤러에 해당 응답 정보를 요청한다. SDN 컨트롤러에서는 저장된 모든 쿼리 정보와 비교하고 존재하지 않는 쿼리 정보이기 때문에 라우터에 해당 메시지를 전송한다. 라우터에서는 해당 패킷을 공격으로 판단하여 드랍시킨다.

IV. 결론

본 논문에서는 DDoS 공격 유형 중 하나인 DNS 증폭공격을 탐지하기 위한 기존 연구를 살펴보고, 기존 연구의 한계를 개선할 수 있는 SDN 기반의 DNS 증폭공격 탐지 방법을 제안하였다. SDN 컨트롤러를 이용해 저장 공간에 제약 없이 쿼리 정보를 저장하기 때문에 높은 정확도(100%)를 달성할 수 있지만, SDN 컨트롤러와 라우터간의 통신비용이 발생하기 때문



[그림 3] SDN 기반 DNS 증폭공격 탐지 방법

에 트레이드오프를 계산하여 합리적인 설정이 요구된다.

향후 연구에서는 제안한 시스템을 구현한 후, 라우터의 저장 공간 크기 및 라우터와 SDN 컨트롤러 간 통신 주기 등에 대한 합리적인 설정을 찾고, 시스템의 안정성 및 타당성을 검증할 계획이다.

[참고문헌]

[1] 이기택, 백승수, 김승주, “DNS 증폭공격 탐지를 위한 근실시간 DNS 질의 응답 분석 시스템에 관한 연구”, 한국정보보호학회 논문지 제25권 제2호, 2015.4, pp 303-311.

[2] Rozekrans, Thijs, Konning, Javy de, and Mekking, Matthijs, “Defending against DNS reflection amplification attacks”, University of Amsterdam, Technical report, 2013.

[3] Kambourakis, Georgios, Moschos, Tassos, Geneiatakis, Dimitris, and Gritzalis, Stefanos, “Detecting DNS Amplification Attacks”, Lecture Notes in Computer Science, Volume 5141, 2008, pp 185-196.

[4] Paola, Sebastiano Di, and Lombardo, Dario, “Protecting against DNS Reflection Attacks with Bloom Filters”, Lecture Notes in Computer Science, Volume 6739, 2011, pp 1-16.