2014년 5월 전자공학회 논문지 제 51권 제 5 호
Journal of The Institute of Electronics and Information Engineers Vol. 51, NO. 5, May 2014 http://dx.doi.org/10.5573/ieie.2014.51.5.127

논문 2014-51-5-15

상태기반 DRDoS 공격에 대한 탐지 및 방어기법

(A Detect and Defense Mechanism of Stateful DRDoS Attacks)

김 민 준*, 서 경 룡**

(Minjun Kim and Kyungryong Seo©)

요 약

DRDoS(Distributed Reflective Denial of Service)공격은 정상적인 동작을 하는 반사서버를 통해 이루어지며 공격을 위해 숙주를 필요로 하는 DDoS(Distributed Denial of Service) 에 비하여 훨씬 치명적이다. 유입되는 공격 패킷이 정상적 활동을 하는 반사서버로부터 오기 때문에 전통적인 방식인 소스패킷 분석법으로 DRDoS를 탐지하거나 막는 것은 매우 어렵다. 더욱이 최근에 관심이 대두되는 SCTP(Stream Control Transmission Protocol)의 멀티호밍(multihoming)같은 개선된 기능을 가진 전송프로토콜을 사용하여 공격하면 이에 대한 대처는 더욱 힘들게 되고 공격의 효과는 극대화 할 수 있다. 본 논문에서는 DRDoS가 상태기반 프로토콜의 특징을 활용하는데 착안하여 이에 대응하는 상태기반 탐지방법을 제안하였다. 제안된 방식은 상태기반 파이어 월과 연동하고 전송프로토콜에 따라 구성된 규칙테이블을 통하여 DRDoS공격을 탐지하고 공격에 대한 방어를 수행한다. 규칙테이블은 단순한 구조로 쉽게 갱신이 가능하며 특정한 프로토콜에 대한 제한을 받지 않고 모든 종류의 상태기반프로토콜의 DRDoS공격에도 대응할 수 있다. 실험을 통하여 공격대상이 알지 못하는 SCTP 같은 차세대 전송프로토콜을 활용한 공격에 대해서도 SCTP의 DRDoS 공격패킷을 잘 탐지하였으며 제안한 방어방식을 통하여 공격패킷의 수를 급격히 감소시키는 것을 확인하였다.

Abstract

In DRDoS(Distributed Reflective Denial of Service) attacks, the victim is bombarded by packets from legitimate reflector unlike DDoS(Distributed Denial of Service) attacks through zombie, which is more dangerous than DDoS attack because it is in stronger disguise. Therefore, the method of filtering packet method on router are useless. Moreover SCTP(Stream Control Transmission Protocol) multi-homing feature, such as with an improved transmission protocol allows detecting attacks is more difficult and the effect of the attack can be maximized. In this paper we propose a DRDoS detection mechanism based on DRDoS utilizing attention to the characteristics of stateful protocols. The proposed scheme is backed by stateful firewall, and detect DRDoS attacks through a rules table and perform a defense treatment against DRDoS attack. Rules table with a simple structure is possible to easily adapt for any kind of stateful protocol can used by DRDoS attack. The experimental result confirm that our proposed scheme well detect DRDoS attacks using SCTP, the next-generation transmission protocol which not known by victim, and reduce the attacking packets rapidly.

Keywords : DRDoS, stateful protocol, multihoming

Ⅰ. 서 론

서비스 거부(DoS), 분산 서비스 거부(DDoS) 공격은 인터넷상의 특정서버에 많은 접속시도를 만들고 서버의 자원을 고갈시켜 서비스 이용을 하지 못하게 한다. 2002년 과 2007년 DNS 루트 서버에 대한 DNS 백본 DDoS 공격은 인터넷 URL 주소 체계를 무력화시켜 인터넷 전체에 영향을 미친바 있다[1~3].

최근에 더욱 복잡한 형태의 반사 서비스 거부(DRDoS)공격은 “컴퓨터 한 대로 서버를 다운 시킨다.” 라고 알려진 공격법으로 상태기반 프로토콜의 특징을 이용하여 반사서버(reflector)를 통하여 대량의 패킷을 공격대상에 전송한다[4~6].

* 학생회원, ** 정회원, 부경대학교 컴퓨터공학과
(Dept. Computer Eng., Pukyong National University)
© Corresponding Author(E-mail: krseo@pknu.ac.kr)
※ 이 논문은 부경대학교 자율창의학술연구비 (2013년:C-D-2013-0553)에 의하여 연구되었음.
접수일자: 2014년2월 6일, 수정일자: 2014년3월13일
수정완료: 2014년4월28일

DDoS 공격으로부터 방어하는 일반적인 방법은 ISP 백본에서 탐지기를 구동하여 공격패킷을 탐지하고 탐지된 내용을 네트워크 라우터에 전달하면 네트워크 라우터가 정해진 규칙대로 패킷을 필터링하는 방법이 일반적이다.

공격패킷을 탐지하기 위하여 주로 IP패킷 추적법이 사용되는데 해쉬기반 추적 법, ICMP 추적 법, 통계적 패킷 식별 법등의 등의 다양한 방법들이 제시되고 있다[7-10]. 하지만 DRDoS의 경우 특성상 정상적 동작을 하는 중요서버를 반사서버로 활용하기 때문에 근원지 주소를 통한 필터링방법은 효과를 거두기 어렵다[3, 6].

[6]에서는 단순히 요청패킷과 그 응답패킷의 상관관계를 조사하여 DRDoS 패킷을 탐지하는 방법을 제시하였다. 이 방법은 비교적 탐지 확률도 높고 적용이 용이하지만 SCTP에서의 멀티호밍같이 개선된 기능을 가진 프로토콜로 공격하는 경우에는 적응할 수 없다.

본 논문에서는 DRDoS가 상태기반 프로토콜의 특징을 활용하는데 착안하여 이에 대응하는 상태기반 탐지 방법을 제안한다. 상태기반 탐지는 프로토콜의 상태 변화 정보를 바탕으로 각 세션에 대한 상태 테이블을 유지하고 이후 유입되는 변화되는 상태 정보를 바탕으로 비정상인 상태의 패킷을 탐지한다. 탐지된 패킷을 분석하여 반사서버에게 더 이상의 공격이 계속되지 않도록 조치한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 DRDoS에 대한 공격원리와 상태기반프로토콜, 기존의 방어방법 등 관련된 연구내용을 서술한다. Ⅲ장에서 상태기반 방어기법을 제안하고 Ⅳ장에 그 시뮬레이션 결과를 보인다. 마지막 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 DDoS공격과 DRDoS 공격

DDoS는 공격대상(victim)인 대상서버에 무수히 많은 접속시도를 만들고 이를 통하여 네트워크자원이나 서버자원을 부족하게 하여 정상적인 서비스를 제공하지 못하도록 하는 공격법이다. 다양한 형태의 DDoS 공격법이 있으나 일반적으로 공격자(attacker)는 그림 1 과 같이 불특정 다수의 컴퓨터에 공격프로그램을 심어 숙주(zombie)로 만들고 이를 통하여 공격대상에 접속을 시도한다.

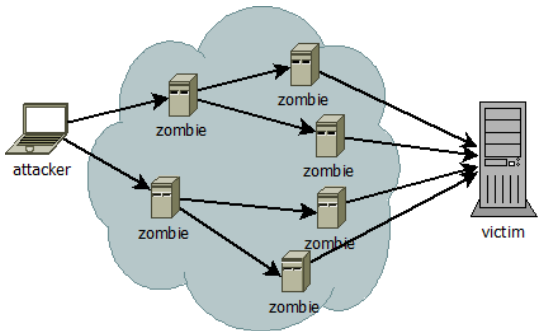

그림 1. DDoS 공격
Fig. 1. DDoS attack.

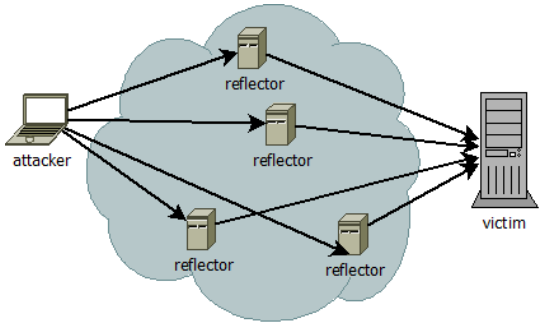

그림 2. DRDoS 공격
Fig. 2. DRDoS attack.

이와는 달리 DRDoS 는 그림 2와 같이 숙주를 만들지 않고 상태기반 프로토콜의 특징을 이용하여 정상적인 서버에 접속을 요청한다. 이때 발신주소를 공격대상의 주소로 변경하여 응답을 공격대상이 수신하도록 하여 공격이 이루어진다. 이때 변조된 패킷을 수신하여 공격에 가담하는 서버를 반사서버 라고 한다.

공격자는 다수의 반사서버를 확보하고 이를 통하여 공격을 시작하는데 공격을 위한 숙주를 확보하기 위하여 특별한 노력이 필요한 DDoS 에 비하여 훨씬 적은 노력으로 다량의 공격패킷을 만들 수 있다.

DRDoS를 탐지하거나 막는 것은 상당히 어렵다. 공격대상의 관점에서는 유입되는 공격 트래픽이 공격자가 아닌 정상적 활동을 하는 반사서버로부터 오기 때문이다.

2.2 상태기반 프로토콜활용 DRDoS공격

TCP는 대표적인 상태기반 프로토콜로 인터넷의 시작부터 현재까지 광범위 하게 사용되고 있다.

TCP를 사용한 DRDoS 공격의 한 예를 그림 3으로 설명한다. 여기서 공격자는 TCP 접속요청 SYN 패킷을 반사서버로 전송한다. 물론 이때 발신주소를 공격대상

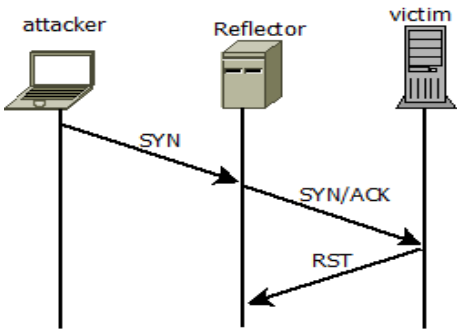

그림 3. TCP를 활용한 DRDoS공격
Fig. 3. DRDoS attack under TCP.

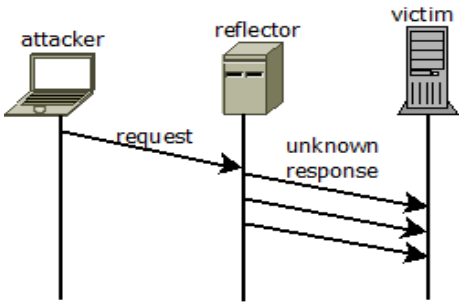

그림 4. SCTP를 활용한 DRDoS공격
Fig. 4. DRDoS attack under SCTP.

으로 변경한다. SYN패킷을 수신한 반사서버는 공격대상에 SYN/ACK패킷을 전송한다. TCP의 상태변화로는 SYN을 보내지 않은 상태에서는 SYN/ACK를 수신할 수 없다. 이 경우 공격대상은 RST 패킷을 전송하고 종료한다. 1대의 반사서버만을 사용하는 예를 보였지만 실제 공격에는 수많은 반사서버를 사용한다.

SCTP는 TCP 의 단점을 개선하고 멀티호밍, 멀티스트리밍 같은 새로운 기능을 추가한 상태기반 프로토콜이다[11-14]. 멀티호밍은 차세대 전송프로토콜의 주목받고 있는 특징으로 호스트는 복수의 주소로 접속을 할 수 있다. 따라서 한 개의 주소에 문제가 생겼을 때 다른 주소로 접속을 유지할 수 있다.

그림 4는 [13]에서 소개한 Bombing공격의 예이다. 여기서 반사서버는 SCTP를 사용하여 공격하는데 공격대상은 SCTP를 알지 못한다. 이에 따라 TCP의 RST와 같이 종료역할을 하는 SCTP ABORT 패킷을 보낼 수 없다. 따라서 반사서버는 DATA에 대한 ACK를 받지 못해 다음 상태로 진행하지 못하고 다량의 재전송 패킷을 공격대상에게 보낸다.

이와 같이 개선된 기능을 가진 상태기반 프로토콜을 DRDoS 공격에 이용할 경우 더욱 복잡한 형태의 공격이 가능해지고 공격의 효력도 극대화 할 수 있다.

2.3 기존 방어 대책

기존에 존재하는 DRDoS 방어 기법들에는 포트 번호로 차단하는 방법, 서버에서 SYN_SENT 상태의 지속시간을 줄이는 방법, ISP 업체에서 자신들이 관리하지 않는 소스 IP가 적힌 패킷이 아웃바운드 되지 못하게 하는 방법 등이 있으나 비효율적이거나 멀티호밍기능을 활용하는 공격에는 대응하기 어렵다.

[6]의 방법이 탐지 확률도 높고 적용이 용이하지만 여기에도 문제점이 있다. 멀티호밍 기능을 지원하는 SCTP 프로토콜이 해당 솔루션의 규칙에 존재하고 솔루션이 관리하는 호스트 중 다중 인터페이스를 갖는 노드가 존재할 경우라면 해당 노드가 정상적인 SCTP 세션을 갖는 도중 경로상의 우선순위 변경에 따라 거짓양성(false positive) 오류를 일으킬 수 있다.

Ⅲ. 제안 방어 기법

우리는 상태기반 탐지 개념을 이용하여 DRDoS를 정확하게 탐지해내고 완화시키는 방법을 제안 한다. 상태기반 탐지는 상태기반 파이어 월에서 제공하는 상태 변화 정보를 바탕으로 각 세션에 대한 테이블을 갖고 이후 유입되는 트래픽에 따라 해당하는 세션의 상태 정보를 테이블과 함께 변경해 나간다. 만약 해당 세션의 상태 조건에 위배되는 패킷이 온다면 해당 패킷은 통과되지 않으며 통과된 패킷은 바로 전달되거나 다음 장비에 의해 추가로 검사를 받을 수 있다.

이러한 방식을 사용하면 상태기반 프로토콜을 활용한 DRDoS공격을 쉽게 탐지하고 완화할 수 있다. 상태기반 정보를 탐지시스템에서 유지 관리 할 수도 있지만 이 경우 상태테이블을 유지하기 위하여 과도한 자원을 소모하게 되므로 이를 지원하는 파이어 월[15-16]에 연동하는 형식으로 쉽게 구성할 수 있도록 하였다.

제안 방어 기법은 다음의 세 가지 절차에 따라 이루어진다.

DRDoS와 관련된 상태정보 확보

DRDoS를 일으키는 상태정보를 주기적으로 업데이트하고 그에 따른 종료 패킷을 준비한다.

(ex: protocol=TCP,
current_state=SYN,ACK,
last_state=None)

상태기반 파이어 월로부터 상태정보를 제공받고 상태정보 테이블을 구성하고 유지한다. 이 정보는 패킷이 유입되었을 경우 공격 여부의 판단에 결정적인 역할을 한다. 확보 절차는 표준화 및 비표준화 프로토콜 분석을 통해 이루어진다. 중요한 것은 이것으로부터 확보한 정보는 단순한 패턴이 아닌 상태로서의 의미를 가져야 한다.

공격 판단

유입되는 패킷 중 패턴과 일치하는 패킷이 있으면 상태정보 테이블로부터 공격 여부를 판단한다.(last_state가 None이면 테이블이 존재하지 않는 경우로 한다.)

유입되는 패킷에 대하여 DRDoS 상태정보를 포함하면 검사를 진행한다. 패킷이 유입되었을 때 이에 합당한 상태정보가 상태정보테이블에 존재하느냐 여부이다. 존재한다면 공격이 아닌 정상 세션이므로 해당 세션이 종료될 때까지는 관련 패킷에 대하여 추가 검사를 진행하지 않는다. 공격이라고 판단될 경우에는 공격 완화 단계를 수행하고 검사에 사용된 패킷은 포워딩하지 않고 폐기한다.

공격 완화

공격이 아니면 패킷을 허용하고 공격이면 공격 완화 단계를 수행한다.

DRDoS 공격이라고 판단한 경우 패킷을 폐기하는 것만으로는 부족하다. 추가조치를 하지 않는다면 그림 4에서 보인바와 복잡한 프로토콜을 활용하는 경우에는 계속적인 공격이 이루어진다. 따라서 DRDoS 공격 완화를 위하여 최종적으로 공격자에게 종료패킷 송신 단계를 수행한다.

이를 기반으로 한 방어알고리즘을 그림 5에 기술하였다.

1~3 : 유입된 패킷이 탐지시스템에서 지원하지 않거나 이전 검사에서 통과 가능 판정을 받은 패킷이면 아무작업도 실행하지 않는다.

4~5 : 규칙파일로부터 규칙을 갱신하고 패킷에 해당하는 DRDoS 성립 규칙이 있는지 검사한다.

```
1:while(pkt = listen()):
2:    if not pkt.isSupport() and not (pkt in whiteTable):
3:        continue
4:    rules = get(open("ruleFile").read())
5:    if rules[pkt]:
6:        if pkt in blackTable:
7:            send(rules[pkt].output)
8:            continue
9:        state = readState(state_Table).find(pkt)
10:       if state is pkt.last_state:
11:           send(rules[pkt].output)
12:           blackTable.add(pkt)
13:           drop(pkt)
14:       else:
15:           whiteTable.add(pkt)
16:           forward(pkt)
```

그림 5. 제안 방어 알고리즘
Fig. 5. Proposed defence Algorithm.

규칙파일에는 공격에 사용되는 프로토콜에 대한 판단 규칙이 기록되어 있다. TCP의 경우 SYN공격에 대하여 다음과 같은 규칙을 추가한다.

protocol : TCP
current_state : SYN,ACK
last_state : None

정상적인 TCP 연결이 발생하면 이 규칙에 상태정보 확인 전까지 대하여 제안 알고리즘이 동작한다. 그러나 정상적인 연결인 경우에 상태정보 테이블에는 SYN SENT 상태를 갖는 연결 정보가 저장되어 있을 것이고 제안 알고리즘은 정상적인 경우로 간주한다.
SCTP도 유사하게 아래와 같은 규칙을 구성한다.

protocol : SCTP
current_state : DATA or HEARTBEAT
last_state : None

이와 같이 규칙테이블은 단순히 구성되어 있으며 새로운 프로토콜에 대하여 쉽게 확장이 가능하다.

6~8 : 이전에 검사하여 공격이라 판단되는 세션에 대해서는 종료패킷만 전송해주고 아무 작업을 하지 않는다. 이전에 전달한 종료패킷이 제대로 작동하지 않을 경우를 대비한 루틴이다.

9~13 : 만약 패킷이 현재 가지는 상태와 기존에 존재하는 상태 정보가 DRDoS를 일으키는 경우에 해당하면 공격으로 간주하여 종료패킷 전송, 블랙리스트에 세션 추가, 해당 패킷을 제거한다.

14~16 : 정상적인 패킷에 대하여 화이트리스트에 세션 추가 및 해당 패킷을 포워딩한다.

화이트리스트를 사용하는 이유는 정상적인 연결임을 확인한 상태에서 추가적인 검사를 진행하지 않기 위해서이다. 제안 방어 시스템은 정상적인 경우의 거짓양성(false positive) 오류도 존재하지 않는다.

정상적인 경우 DATA 패킷이 왔을 때 상태기반 테이블 조회 시 해당 세션에 대하여 연결 완료 상태로 존재하는 테이블이 존재하므로 공격이라고 판단하지 않는다.

Ⅳ. 시뮬레이션

4.1 실험환경

본 논문에서 제안한 DRDoS방어 시스템을 구현하고 동작과 성능을 평가하기 위하여 시뮬레이션을 실시하였다. 그림 6은 시뮬레이션을 위하여 구현된 시스템으로 공격에 사용되는 외부의 시스템으로 3대의 반사서버와 공격자로 구성하였다. 여기서 반사서버 R1, R2, R3는 모두 SCTP프로토콜을 이해하는 서버들로 DDoS에서와 같이 공격을 위한 특별한 프로그램이 설치되어 있지 않고 정상적으로 동작하는 서버들이다.

공격대상은 보호되어야할 내부시스템으로 상대기반 방화벽으로 분리되는 내부 네트워크에 접속되어 있다. 일반적으로 내부네트워크에는 다수의 컴퓨터가 접속되어 있지만 본 실험환경에서는 목적서버만 있는 것으로 하였다.

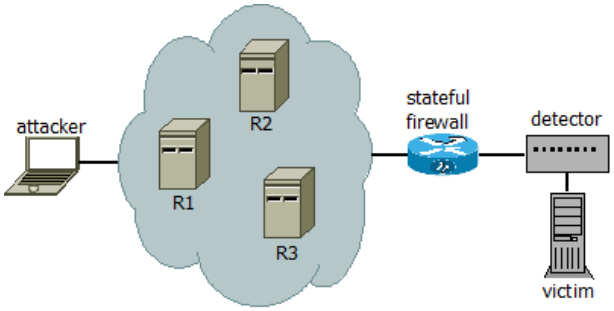

그림 6. 시뮬레이션 환경
Fig. 6. Simulation environment.

탐지장치는 상태기반 파이어 월과 연동하여 동작을 수행한다. 본 논문에서는 실험을 위하여 별도의 파이어 월을 사용하지 않고 상태정보를 저장하고 유지하는 상태기반 함께 구현하여 실험하였다.

4.2 DRDoS 공격과 방어 실험

제안한 시스템은 일반적인 상태기반공격에 모두 적용할 수 있지만 제안된 방법의 장점을 잘 설명할 수 있는 SCTP를 사용한 DRDoS공격에 대하여 실시하였다. 이때 공격방법은 RFC 5062에 정의된 SCTP Bombing 공격[14]을 기준으로 한다.

공격자는 반사서버 R1, R2, R3에 멀티홈드 SCTP 연결을 시도한다. 이 때 발신지 주소에 공격대상의 주소를 추가한다. 연결을 완료한 공격자는 반사서버 R1,R2,R3 에게 데이터 요청을 하는 동시에 선호 경로로 공격대상으로 정한다. 이를 수신한 반사서버는 공격대상에 데이터를 전송하게 되고 대상서버는 원하지 않는 다량의 패킷을 받게 되어 DRDoS 공격이 이루어지게 된다.

이 공격은 다음의 세 가지 제약조건을 만족하면 성공할 수 있다.

* 공격대상 V는 SCTP 프로토콜을 알지 못한다.
* 공격자는 충분한 공격 패킷이 V에 도달하면 지속적인 공격을 위해 Acknowledgement를 전송해주어야 하는데 이 패킷을 보낼 시간적 여유가 있어야 한다.
* 공격자는 Acknowledgement를 보낼 때 TSN 값을 정확하게 예측하여야 한다.

공격 시뮬레이션에서는 방어기법 테스트의 공정성을 위해 RFC에 정의된 SCTP 프로토콜 재전송 정책을 토대로 시뮬레이션 프로그램을 제작하여 테스트를 진행하였다. 이 공격은 SCTP의 멀티호밍 기능과 재전송 정책의 허점을 이용한 공격으로 재전송되는 데이터의 크기와 공격에 이용되는 반사서버의 개수에 따라서 공격대상이 받는 피해는 증가하게 된다. 또한 DATA 세그먼트들은 전송하고자 하는 추가적인 데이터를 포함할 수 있고 데이터의 크기에 따라 만약 하위 계층에서 단편화 과정을 거치면 그 피해는 더욱 커지게 된다.

공격시나리오를 방어시스템이 없이 구동하였을 때 대상서버가 수신하는 패킷의 변화를 표 1에서 볼 수 있다. 본 시뮬레이션에서 공격자는 반사서버에 지속적인

표 1. DRDoS 공격에 의한 패킷.
Table 1. Packets through DRDoS attack.

패킷방향 / 단위시간(s)	R1 ⇨ V (A ⇨ R1)	R2 ⇨ V (A ⇨ R2)	R3 ⇨ V (A ⇨ R3)	(R1,R2,R3) ⇨ V
0~4	2	2	2	6
5~9	2(1)	1	2(1)	5
10~14	3(1)	0	3(1)	6
15~19	3(1)	1(1)	3(1)	7
20~24	2(1)	2	1	5
25~29	3(1)	4(2)	0	7
30~34	4(2)	5(3)	2(1)	11
35~39	1	3(1)	0	4
40~44	0	1	0	1
45~49	0	1	3(1)	4
50~54	0	1	0	0
합계	20(7)	21(7)	16(5)	57

* Rn ⇨ V : 단위시간 동안 반사서버n에서 공격 대상으로 반사되어 향하는 패킷 수
* A ⇨ Rn : 단위시간 동안 재전송 상태 유지를 위해 공격자가 반사서버 Rn으로 전달해주어야 할 응답 패킷 수
* (R1,,Rn) ⇨ V : 단위시간 동안 공격에 이용된 모든 반사서버에서 공격 대상으로 향하는 패킷 수

표 2. 방어시스템 구동시 DRDoS 공격으로 수신한 패킷
Table 2. Packets through DRDoS attack under defence system.

패킷방향 / 단위시간(s)	R1 ⇨ V (A ⇨ R1)	R2 ⇨ V (A ⇨ R2)	R3 ⇨ V (A ⇨ R3)	(R1,R2,R3) ⇨ D
0~4	1	1	1	3
5~9	0(1)	0	0(1)	0
10~14	0(1)	0	0(1)	0
15~19	0(1)	0(1)	0(1)	0
20~24	0(1)	0	0	0
25~29	0(1)	0(2)	0	0
30~34	0(2)	0(3)	0(1)	0
35~39	0	0(1)	0	0
40~44	0	0	0	0
45~49	0	0	0(1)	0
50~54	0	0	0	0
합계	1(7)	1(7)	1(5)	3

* Rn ⇨ V : 단위시간 동안 반사서버Rn에서 공격 대상으로 반사되어 향하는 패킷 수
* A ⇨ Rn : 단위시간 동안 재전송 상태 유지를 위해 공격자가 반사서버Rn으로 전달해주어야 할 응답 패킷 수
* (R1,,Rn) ⇨ D : 단위시간 동안 공격에 이용된 모든 서버에서 공격 대상으로 향하는 패킷 수. 공격 대상 앞단에 존재하는 DRDoS 탐지 시스템 D가 먼저 수신하게 됨.
* V는 D에 의해 공격이라고 판단되는 패킷은 수신하지 않으므로 생략

공격을 할 수 있도록 반사서버 n 에 (A ⇨ Rn)의 패킷을 전송하는데 실험에서는 (A ⇨ R1)=7, (A ⇨ R2)=7, (A ⇨ R3)=5로 총 19개의 패킷을 전송한다. 공격이 성공하면 대상서버는 세대의 반사서버로부터 1분 동안 총 57개의 패킷을 수신한다.

제안된 시스템을 적용하였을 때 대상시스템이 수신하는 패킷은 표 2에서 확인할 수 있다.

제안 방어 시스템 D는 규칙테이블에 따라 허용된 패킷에는 아무런 조치를 취하지 않는다. SCTP의 DATA나 HEARTBEAT 패킷에는 상태정보테이블을 참조하고 이 패킷들이 접속이 이루어지지 않은 상태에서 전송된 패킷으로인식하고 DRDoS 공격 패킷임을 검출하게 된다. 따라서 대상서버로 보내야할 패킷을 폐기하고 추가적인 공격을 막도록 연결 종료 패킷을 만들어 각 반사서버에게 전달한다.

연결종료패킷을 수신한 반사서버는 더 이상 공격패킷을 전송하지 않고 공격자가 전송하는 패킷의 수는 변화가 없는데 목표시스템이 위치하고 있는 네트워크로 도달하는 공격패킷의 수는 57개의 패킷에서 3개의 패킷으로 급격히 감소한다.

이상의 결과에서와 같이 제안시스템은 상태기반테이블을 참조하여 정상적인 접속이 아닌 경우의 패킷을 검출할 수 있을 뿐 아니라 지속적인 공격을 방어하는 역할을 잘 수행함을 확인할 수 있다.

4.3 비교검토

제안 방어기법의 장점은 상태기반 정보를 바탕으로 보다 신뢰적인 대처가 가능하다는 것이다. 추가된 정보로 유입 패킷이 정상패킷인지 DRDoS패킷인지를 정확하게 판단할 수 있다. 특히 [6]에서 멀티호밍 연결 시 발생할 수 있는 오류가 제안 방어기법에서는 나타나지 않는다.

또한 방어방법에서도 단순히 패킷을 필터링하는 것에 비하여 적극적으로 공격패킷을 보내는 반사서버에 공격을 감소하도록 작용함으로 공격을 완화할 뿐 아니라 반사서버의 부하도 줄일 수 있어 DRDoS 공격완화에 큰 기여를 할 수 있다.

시뮬레이션에서는 SCTP 의 경우만 수행하였지만 상태기반의 프로토콜을 사용한 공격에 모두 동일하게 적용될 수 있다. 일반적인 DRDoS공격인 TCP SYN 공격에 대해서도 마찬가지다. 동일한 실험 환경에서 유입되는 SYN/ACK 패킷에 대하여 상태 테이블이 존재하지 않으면 공격으로 간주하는 규칙이 존재하고 SYN/ACK가 유입되었을 때 상태 테이블 조회만으로 공격 유무 판단이 가능하다. 단 이 경우 는 공격대상이 TCP프로

토콜을 알고 있어 TCP 종료패킷을 반사서버로 보낼 수 있어 공격완화의 효과는 반감된다.

V. 결 론

DRDoS 공격은 상태기반 프로토콜의 특성을 이용하여 정상적인 서버를 반사서버로 하여 대상시스템을 공격하므로 손쉽게 공격목적을 달성할 수 있다.

또한 멀티호밍, 멀티스트리밍 같은 새로운 기능을 추가한 새로운 형태의 상태기반 프로토콜들이 발표되고 있으며 이들의 사용이 일반화 되면 더욱 강력하고 다양한 형태의 DRDoS 공격이 가능해진다.

본 논문에서는 DRDoS가 상태기반 프로토콜의 특징을 활용하는데 착안하여 이에 대응하는 상태기반 탐지방법을 제안하였다. 상태기반 탐지는 프로토콜의 상태변화 정보를 바탕으로 각 세션에 대한 상태 테이블을 유지하고 이후 유입되는 변화되는 상태 정보를 바탕으로 준비된 규칙테이블을 참조하여 비정상인 상태의 패킷을 탐지한다. 간단한 규칙테이블을 구성할 수 있도록 하여 특정한 프로토콜에 대한 제한을 받지 않고 일반적인 모든 종류의 상태기반프로토콜의 DRDoS공격에도 쉽게 대응 할 수 있다. 따라서 제안된 방법은 TCP 같은 전통적인 프로토콜을 이용한 DRDoS 공격뿐 아니라 공격대상이 알지 못하는 SCTP 같은 차세대 전송프로토콜을 활용한 공격에도 쉽게 대응할 수 있다.

제안된 방식의 동작과 성능을 실험으로 확인하였다. 실험결과 이미 작성된 규칙테이블로부터 SCTP의 DRDoS 공격패킷을 잘 탐지하였으며 제안한 방어방식을 통하여 공격패킷의 수를 급격히 감소시키는 것을 확인하였다.

기존의 방어시스템이 복잡하거나 거짓양성탐지의 여지가 있는 반면 상태기반 파이어 월과 연동하여 간단히 구현이 가능하고 멀티호밍등 차세대 프로토콜의 기능으로부터 발생하는 거짓양성탐지가 발생하지 않는다.

본 논문에서 제안한 방법을 채택하여 방어를 위해 탐지시스템이 보낸 종료패킷을 반사서버가 수신하고 이를 공격자에 대응하도록 한다면 DRDoS 공격에 대한 획기적인 대처방안이 될 것이다. 이에 관한 내용은 외부시스템인 반사서버를 포함한 전송프로토콜과 관련된 것으로 계속된 연구과제로 남긴다.

REFERENCES

[1] J. Mirkovic and P. Reiher, “A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms.” ACM SIGCOMM Computer Communication Review, Vol. 32, no. 2, pp. 39-53, 2004.

[2] M. McDowell, “Understanding Denial-of-Service Attacks.” Security Tip (ST04-015), US-CERT, http://www.us-cert.gov/ncas/tips/st04-015.

[3] Douligeris C., and Mitrokotsa A., DDoS Attacks and Defense Mechanisms.“ A Classification Signal Processing and Information Technology, 2003. ISSPIT 2003. Proceedingsof the 3rd IEEE International Symposium, pp. 190-193, 2003.

[4] S. Gibson, “DRDOS: Distributed Reflection Denial of Service.” http://grc.com/dos/drdos.htm, 2002.

[5] J. J. A. Hamilton, Denial of Service: Distributed Reflection DOS Attack, Auburn Information Assurance Laboratory, 2012.

[6] H. Tsunoda, K. Ohta, A. Yamamoto, N. Ansari, Y. Waizumi and Y. Nemoto, “Detecting DRDoS attacks by a simple response packet confirmation mechanism.” Computer Communications, Vol. 32, no. 14, pp. 3299-3306, 2008.

[7] Wei Zhou, Lina Wang, Huanguo Zhang, Jianming Fu, “A New DDoS Attack and Countermeasure against It.” Computer Engineer and Application, Vol. 1, pp. 144-146, 2003.

[8] Tao Peng, Leckie C., Ramamohanarao K., “Protection from Distributed Denial of Service Attacks Using History-based IP Filtering.” 2003. ICC'03, IEEE International Conference on Communications, pp. 482-486. 2003.

[9] Fan Y., Hassanein H., Martin P., “Proactively Defeating Distributed Denial of Service Attacks.” Vol. 2, IEEE CCECE 2003. Canadian Conference on Electrical and Computer Engineering, pp. 1047-1050, 2003.

[10] X. Yang, W. Yang, Y. Shi and Y. Gong, “The Detection and Orientation Method to DRDoS Attack Based on Fuzzy Association Rules.” Journal of Communication and Computer, Vol. 3, no. 8, pp. 1-10, 2006.

[11] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang and V. Paxson, “Stream Control Transmission Protocol.” rfc2960, 2000.

[12] Jong Shik Ha, Seok Joo Koh and Jung Soo Park, “SCTP versus TCP.” 대한전자공학회,

ITC-CSCC : 2005 Proceedings Vol. 4, pp. 1477-1478, 2005.
[13] R. Stewart, M. Tuexen and G. Camarillo, “Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures.” rfc5062, 2007.
[14] E. P. Rathgeb, C. Hohendorf and M. Nordhoff, “On the Robustness of SCTP against DoS Attacks.” Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on, pp. 1144-1149, 2008.
[15] H. Kim, J.-H. Kim, I. Kang and S. Bahk, “Preventing session table explosion in packet inspection computers.” Computers, IEEE Transactions on, Vol. 54, no. 2, pp. 238-240, 2005.
[16] Mohamed G Gouda, and Alex X Liu, “A Model of Stateful Firewalls and Its Properties,” in Dependable Systems and Networks, DSN 2005. Proceedings. International Conference on (IEEE, 2005), pp. 128-37, 2005.

저 자 소 개

김 민 준(학생회원)
2014년 부경대학교 컴퓨터공학과 졸업.
<주관심분야 : 컴퓨터보안>

서 경 룡(정회원)-교신저자
1983년 부산대학교 전기기계 공학과 학 사졸업.
1990년 한국과학기술원(KAIST) 전자공학과 석사 졸업.
1995년 한국과학기술원(KAIST) 전자공학과 박사 졸업.
1991년~현재 부경대학교 컴퓨터공학과 교수.
<주관심분야 : 분산시스템, 컴퓨터 네트워크>