한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

# x86 컴퓨터 기반 저 대역폭 DoS 방어 시스템

박성현[O], 서정환[*], 박성준[*], 이상곤[*]
[O*]동서대학교 컴퓨터공학부
e-mail: {mrolgood[O],ribatel,qoogam}@naver.com, nok60@dongseo.ac.kr

# Low-bandwith DoS Defense System Based on x86 Computers

Sang-Gon Lee[O], Sung-Hyun Park[*], Jung-Hwan Seo*, Seong-Jun Park*
[O*]Div. of Computer Engineering, Dongseo University

● 요 약 ●

DoS 공격은 증가하고 있지만 비용이 많이 들다보니 제대로 된 방어를 하지 못 하고 공격을 당하는 경우도 많다. 저렴한 DoS 방어 시스템의 필요성이 절실하다. 본 논문에서는 저 대역폭 DoS 공격을 방어하는 시스템 개발을 하고자 한다. 방어시스템의 물리적 구조는 듀얼 홈 게이트웨이 구조를 사용하며, DoS 탐지 방법으로는 일반적인 상황에서의 인 바운드되는 프로토콜별 패킷의 값을 세어 그 값을 평균값과 비교하여 탐지하며, 1초 단위로 IP와 SYN, FIN 플래그 값을 세어 그 값을 평균값과 비교하여 탐지하며, 2초 단위로 IP와 SYN, FIN 플래그 값을 세어 임계값을 넘어서면 차단하는 방식을 사용한다.

**키워드:** 임계값(threshold value); 평균값(average value); DoS 공격(Denial of Service attack)

## I. Introduction

2016년 1분기 동안 한국이 세계 2번째로 DoS 및 DDoS 공격을 많이 받는 국가에 이름을 올렸다[1,2].점차 고도화된 공격 방법이 개발되어 지고, 이를 이용한 공격에 대한 피해 또한 막심해 지고 있다. 하지만 중소기업이나 개인과 같은 저 대역폭을 인터넷 사업자로 회선 임대하여 서버를 운영하는 사용자 또한 DoS 공격에 노출 되어 있지만 방어를 위한 시스템을 유지하기 위해 소요되는 비용이 많이 들다보니 제대로 된 방어를 하지 못하고 공격을 당하는 경우도 많다[3].

## II. The proposed low-bandwith DoS defence system

본 논문에서는 저 대역폭 DoS 방어 시스템을 개발하고자 한다. 개발하고자 하는 시스템의 동작설명은 다음과 같다.

서버와 방어 시스템이 듀얼 홈 게이트웨이 방식으로 연결된 네트워크 구조에서 실시간으로 유입되는 패킷들을 1초 단위로 나누고, 먼저 TCP, UDP, ICMP 별로 나누어 각 프로토콜별 패킷 수를 카운팅 한다.

해당 카운팅 값은 초 단위 평균값으로 계산 후 저장을 하며, 이 평균값을 넘어서는 순간 DoS 공격이라 판단하고 방어 함수를 작동시킨다. 방어 함수에서는 실시간으로 인바운드 되는 패킷의 IP와 SYN 플래그를 1초 단위 카운팅하여 그 값을 누적시키고, 해당 카운팅 값이 미리 설정해둔 임계값을 넘어서는 IP와 사전에 공격 패턴(LAND, Ping of Death)을 넣어둔 채 들어오는 패킷의 임의의 부분과 비교를 통해 판단 후 차단 함수로 넘겨 IP를 차단하는 형태이다. 매 카운트는 1초 후 초기화 한다. 차단 방식은 리눅스 기본 방화벽을 이용하여 정책에 추가하는 방식을 사용한다.

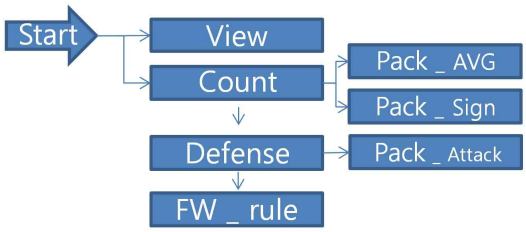


Fig. 1. DoS defense system data processing

그림 1은 제안된 DoS 방어시스템의 데이터 처리과정을 나타낸다. 표 1은 방어시스템 서버모듈의 기능을 나타낸다.

Table 1. The function of the system submodules

| Sub-module | Function description |
|---|---|
| View | 프로그램 동작화면 표시 |
| Count | 패킷의 평균값과 이상 패턴 유입을 판단하여 공격 유/무 판단 |
| Pack_AVG | TCP, UDP, ICMP 패킷의 평균값 카운트 |
| Pack_Sign | 사전 정의된 패턴과의 일치여부 판단 |
| Defense | 공격 판단 시 실행 공격 패킷의 세부정보 불러와 차단 |
| Pack_attack | 공격 패킷이라 판단 시 세부내용 저장 |
| FW_rule | 공격 IP주소를 방화벽 리스트에 추가시킴 |

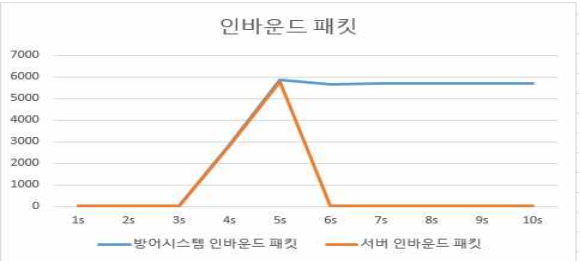


Fig. 2. DoS defense simulation results

그림 2는 시뮬레이션 결과를 나타낸다. 제안된 DoS시스템을 테스트하기 위해 SYN, Flooding 공격을 사용하여 허용유입패킷 평균값을 초과하는 트래픽을 주입하였다. 방어시스템 외부에서 TCP 공격 트래픽을 주입하는 공격호스트 3대와 ICMP 정상 트래픽을 주입하는 호스트 2대를 사용하여 내부에 있는 공격 목표 호스트 1대에 트래픽을 주입하였다. ICMP 정상 트래픽은 초당 10개의 패킷이 주입되었으며, TCP 공격 패킷은 초당 액 6000개의 패킷이 주입되었다. 그림에서 보는 바와 같이 DoS 방어 시스템이 잘 작동함을 알 수 있다.

## III. Conclusions

본 논문에서는 저 대역폭용 DoS 방어시스템을 개발하였다. 개발된 시스템에 DoS 공격 패킷을 주입하여 성능을 검증해 본 결과 DoS 공격을 잘 방어함이 확인되었다.

## References

[1] Kaspersky Lab Korea, "Kaspersky Disaster inteligence Report for the first quarter of 2016". URL:http://news.kaspersky.co.kr/news2016/05n/160502.htm

[2] FORTINET. "DDoS : A brief history". URL : https://www.fortinet.com.

[3] KISA Korea Internet Promotion Agency "2015 Review KISA Report". URL:https://www.etnews.com/20160711000038.

[4] KS, hosting service statistics URL : cs.ksidc.net/sub/qna.