패턴 매칭 기법을 적용한 DDoS 공격 탐지

A Detection of DDoS Attack using Pattern Matching Method

김선영, 오창석
충북대학교

Kim Sun-Young, Oh Chang-Suk
Chungbuk Univ.

요약

현재의 해킹 기술은 네트워크상에 과도한 트래픽을 유발하여 단일 호스트 혹은 해당 네트워크 전체를 마비시키는 분산 서비스 거부 공격으로 변모하고 있다. 본 논문에서는 각 프로토콜별 평균 편차와 각 필드별 평균 편차에 이동성을 부여하고 패턴 매칭 기법을 적용하여 보다 정확하고 오탐율이 적은 DDoS 공격 탐지 기법을 제안하였다.

Abstract

Present hacking technology is undergone a change on the distributed DoS Attack which cause a lot of traffic to the network or single host. In this paper, with giving mobility to the mean deviation per protocol and it's field, and with adapting pattern matching approach to DDoS attack detection technique, we propose a method to detect the DDoS attack, to have less misdetection and to detect these attacks correctly.

Ⅰ. 서 론

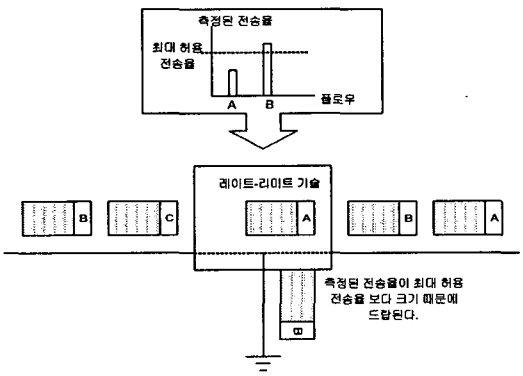
컴퓨터 네트워크 인프라 구축이 일반화되고 인터넷 사용자 수가 증가되면서 컴퓨터에 저장하고 있는 자료에 대한 접근이 쉬워짐으로 사용자들에게 많은 편이성을 제공하고 있다. 그러나 이런 편이성의 반대급부로, 컴퓨터 시스템에 대한 불법 접근 및 네트워크에 트래픽을 폭주시킴으로 정보 유출 및 제대로 된 서비스를 제공하지 못하게 하여 많은 경제적 피해가 야기되고 있다. 또한 공격 기법이 다양화, 지능화, 자동화 되고 있어 분석과 탐지가 어려워지고 있다. 이렇게 많은 피해를 야기하는 분산 서비스 거부 공격(Distributed DoS)은 많은 공격 에이전트를 이용하여 시스템 자원 및 네트워크의 대역폭을 차지하는 공격으로 TCP, UDP, ICMP등 다양한 형태의 패킷을 공격에 이용하기 때문에 공격자의 추적은 물론, 탐지와 방어에 어려움이 있다는 것이다. 또한 탐지를 하더라도 기존의 방법들은 많은 오탐율이 존재하여 대응에 많은 문제점을 가지고 있다. 따라서 본 논문에서는 기존의 DDoS 탐지 방법의 문제점을 개선하여 조기 탐지와 오탐율을 줄이는 이중 탐지 기법을 적용한 DDoS 탐지 알고리즘을 제안하고 구현하고자 한다[1],[2],[3].

Ⅱ. 기존의 DDoS 탐지 방법

1. 레이트-리미트 기술

레이트-리미트 기술[4],[5],[6]은 TCP SYN 플러딩 공격뿐만 아니라 DDoS공격 들을 탐지하고 차단하기 위하여 제안된 기술이다. 레이트-리미트 기술은 특정 플로우들의 대역폭을 측정하여 그 값이 관리자

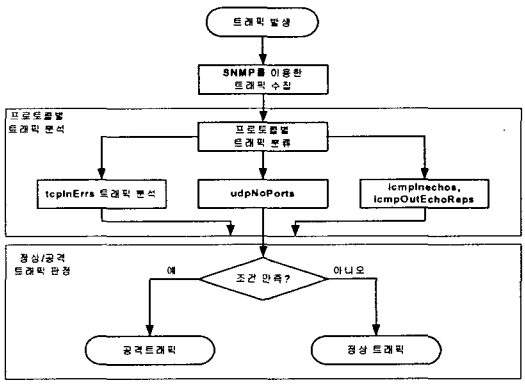
가 정한 최대 허용 대역폭을 초과하면 탐지하여 드랍시키는 기술이다. 이 기술은 두 가지 문제점을 가지고 있다. 첫 번째는 관리자가 최대 허용 대역폭을 정하기 위하여 일정 시간동안 망의 트래픽을 측정해야 하는 문제점이 발생한다. 두 번째는 DDoS 공격을 효과적으로 차단하기 어렵다는 것이다. DDoS 공격의 파괴력과 피해 규모는 수많은 공격 사이트들이 한 곳으로 집중하여 모아진 엄청난 트래픽 때문이다. 즉 공격 사이트와 정상 사이트에서 발생 시키는 트래픽의 차이가 크지 않은 DDoS 공격에서는 최대 허용 대역폭을 정하는 것이 매우 어려운 단점을 가지고 있다. [그림 1]은 레이트-리미트의 구조를 도시하였다.



▶▶ 그림 1. 레이트-리미트 구조

2. SNMP-MIB를 이용한 탐지 방법

SNMP를 이용한 DDoS 공격 탐지 방법[7],[8]은 관리 객체들의 집합인 MIB(Management Information Base)를 이용하여 트래픽을 수집하고 임계값을 적용하여 유해 트래픽을 분석하는 방법이다. 관리 대상 에이전트는 자신의 정보를 메니져시스템으로 전송하게 된다. 전송된 MIB 정보는 로그값으로 저장되며 이 값을 토대로 트래픽을 분석하게 된다. 로그값은 수집된 시간, MIB를 통해 얻어진 트래픽의 평균값, 수집된 트래픽의 최대값으로 저장된다. 이러한 특징을 이용하여 일정 기간의 트래픽 정보를 수집하여 임계값을 산출한 후 임계값과 비교하여 서비스 거부 공격을 탐지하는 방법이다. 그러나 유해 트래픽을 분석하기 위해 현재의 트래픽량과 이전의 트래픽량을 비교하기 때문에 분석하는데 많은 시간이 소요된다는 단점이 있다[9],[10] [그림 2]는 SNMP를 이용한 기존의 공격 탐지 흐름도를 도시하였다.



▶▶ 그림 2. SNMP를 이용한 공격 탐지 흐름도

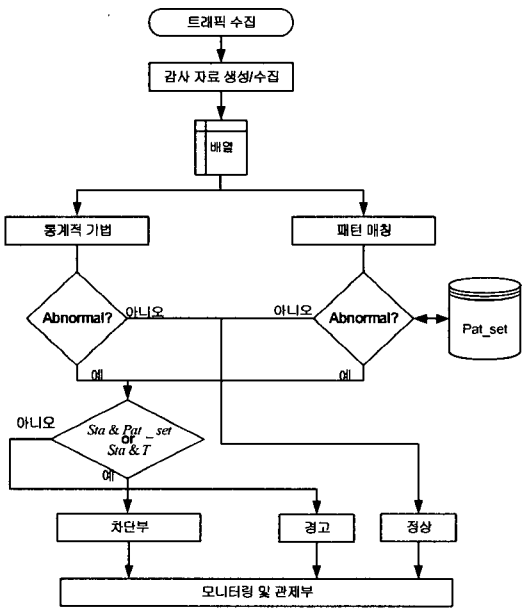
Ⅲ. 패턴 매칭 기법을 적용한 DDoS 공격 탐지

1. 기본 개념

본 논문에서 제안하는 패턴 매칭 기법을 적용한 DDoS 탐지 방법은 기존에는 공격을 탐지하기 위해 일정 기간의 트래픽을 수집하여 평균을 내어 평균값을 기준으로 임계값을 설정하였다. 이로 인해 임계값에 도달하기 전의 트래픽에 대해서는 공격이어도 정상으로 판정하거나 혹은 임계값을 넘었을때 공격과 유사한 정상 트래픽도 공격으로 간주하는 오탐율이 많이 존재하였다. 이러한 기존 방법의 문제점을 해결하기 위해 본 논문에서는 패턴 매칭[11],[12] 기법을 적용하여 DDoS 공격을 탐지하였다. 탐지 방법은 임계값을 고려하는 통계적인 방법과 공격 트래픽의 특성을 패턴으로 가지고 있어 두 조건의 상관관계를 이용하여 공격 및 정상으로 판정하는 방법이다.

2. DDoS 탐지 알고리즘

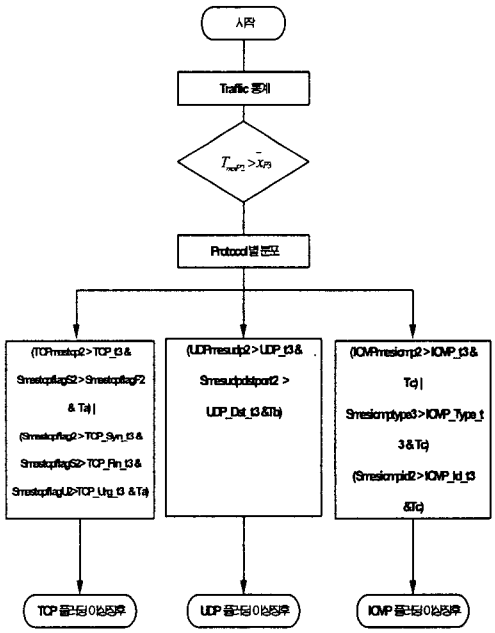
이중 탐지 기법을 이용한 DDoS 공격 탐지의 전반적인 흐름도는 [그림 3]과 같다. 먼저 트래픽 수집시 모든 트래픽을 수집하지 않고 동일한 트래픽이 반복적으로 유입되는 DDoS의 특성을 고려하여 시간 딜레이를 두고 트래픽을 샘플링하여 수집한다. 다음 단계에서는 샘플링된 데이터들 중 필요한 감사 자료만을 추출하여 이중 링크드 리스트 구조에 저장하였다. 저장된 데이터는 지속적으로 통계값[13]을 산출하며 적용하게 된다. 다음단계에서는 저장된 데이터를 기준으로 하여 통계적 기법과 패턴 매칭 기법을 적용하게 된다. 통계적 기법을 만족하는 경우를 Sta라고 하고 패턴 매칭 기법을 만족하는 경우는 Pat_set라고 한다. Sta와 Pat_set를 만족하는 일정시간 T를 만족하는 경우는 최종적으로 만족할 경우 공격으로 간주하는 구조이다.



▶▶ 그림 3. 전체 알고리즘 흐름도

2.1 통계적 기법

통계적 기법은 네트워크에서 수집된 트래픽에 평균과 표준 편차를 산출하여 임계값을 구하여 탐지에 적용하는 방법을 말한다. [그림 3]의 전체 흐름도에서 통계적 기법과 패턴 매칭 기법을 이용하여 공격을 탐지하게 된다. 통계적 기법의 흐름도는 [그림 4]와 같다.



▶▶ 그림 4. 통계적 기법 알고리즘 흐름도

단계 1: 감사 자료에서 정의된 트래픽 선정 항목을 기준으로 링크드 리스트 배열에 있는 데이터를 기준으로 Traffic 통계를 산출하게 된다. Traffic 통계는 각 파라메타별 평균과 표준편차를 산출하는 것이다.

단계 2: 산출된 Traffic 통계를 이용하여 $T_{mesP2} > \overline{x}_{P3}$이면 일단 공격 이상 징후라 판단하게 된다. T_{mesP2}는 링크드 리스트 배열에 입력된 100개의 패킷을 말한다. $\overline{x}_{P3}$는 링크드 리스트 배열 1,000개가 모두 기록되었을 경우 평균을 의미한다. 즉 입력된 100개에 대한 측정값이 평균값 이상이

라면 일단 프로토콜별 분석을 통해 정확한 공격 여부를 가름할 수 있다.

단계 3: 단계 2에서 공격으로 의심되는 패킷들에 한하여 좀 더 세부적인 공격 여부를 판단하는 부분으로 TCP의 경우에는 측정값 TCPmestcp2 값이 TCP_t3보다 클 때 즉 평균값에 표준편차의 k 배한 값보다 큰경우에 해당하면 공격으로 판단하게 된다.

공격 이상 징후로 판단하기 위한 임계값은 다음과 같이 구한다.

$$T\_t = S_{P3} + kS_{P2} (k = 1, 2, 3, 4 \cdot \cdot \cdot \cdot) \quad \text{(식 1.)}$$

Sp3는 전체 평균 편차: Sp2는 측정값의 평균 편차 식 1.을 이용하여 각 해당 감사 항목에 대하여 각각의 임계값을 설정하여 공격을 탐지하게 된다.

2.2 패턴 매칭 기법

패턴 매칭 기법은 DDoS 공격을 탐지할 때 가장 큰 관건이 오탐율을 줄이는 문제이다. 이러한 문제를 해결하기 위해 본 논문에서는 통계적 기법에 공격 트래픽의 패턴 일치 여부를 비교하여 오탐율을 줄이는 패턴 매칭 기법을 적용하였다. 공격에 대한 각각의 패턴들은 프로토콜별로 다음과 같은 특징을 가지고 있다.

- IP의 경우
  - 대부분의 DDoS 공격의 경우 공격 에이전트들의 출발지 주소는 동일 네트워크이다.
  - 일부 공격툴의 경우 IP 스프핑으로 출발지 주소와 목적지 주소를 피해 호스트로 세팅하여 전송한다.
  - 공격자가 에이전트를 통해 공격을 시도할 때 출발지 주소를 브로드캐스팅 주소로 세팅하여 전송한다.
- ICMP의 경우
  - DDoS 도구중 TFN의 경우 ICMP 플러딩 공격을 수행시 외부 에이전트를 통해 내부 피해호스트를 공격하기 전에 마스터가 에이전트에게 ICMP 헤더의 type 필드 값이 8로 echo request를 요청하는 메시지이다. 이런 경우 TFN이 사용하는 ICMP id 필드값은 678로 세팅되어 데이터에는 "1234"가 포함되어 전송된다. 이외의 패턴에는 표 1과 같다.

[표 1] ICMP를 이용한 공격 패턴

필드 / 공격도구	Type	Code	ID	DATA
TFN	0	0	456	
TFN	0	0	666	
stacheldraft	0	0	667	ficken
stacheldraht	0	0	1000	gesundheit
stacheldraht	0	0	666	skillz
stacheldraht	0	0	9015	niggahbitch
stacheldraht	0	0	6666	skillz
stacheldraht	0	0	6667	ficken

- TCP의 경우
  - DDoS 공격 도구 중 shaft 도구는 출발지 포트번호가 20432로 고정되고 DATA에는 "login|3A| 값이 포함되어 공격 에이전트는 핸들러에 로그인을 하게 된다. 이 외에도 TCP 플러딩 공격을 탐지하기 위한 패턴들은 표 2와 같다.

[표 2] TCP를 이용한 공격 패턴

필드 / 공격도구	출발지 포트	목적지 포트	Syn	Fin	Urg	DATA
trin00	-	27665	-	-	-	gOrave
trin00	-	27444	-	-	-	|44ads|
mstream	-	12754	-	-	-	>
mstream	12754	-	-	-	-	>
mstream	-	15104	1	-	-	-
mstream	15104	-	-	-	-	>

• UDP의 경우

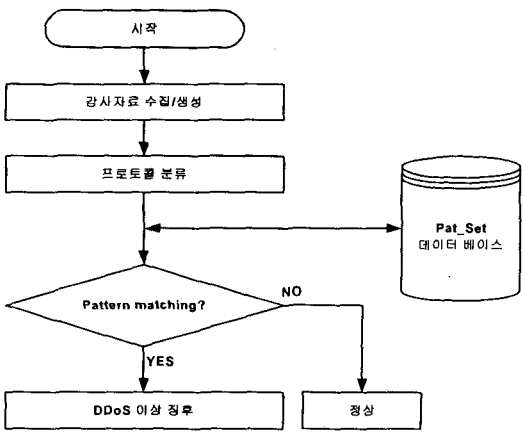
- DDoS 공격 도구중 trin00는 데몬이 마스터에게 Pong 메시지를 보내어 통신을 하게 된다. 이런 경우에는 목적지 포트가 31335 이고 DATA에는 "PONG"이 포함되어 있다. 이외에 UDP 플러딩 공격을 위한 패턴은 [표 3]과 같다.

[표 3] UDP를 이용한 공격 패턴

필드 / 공격도구	출발지 포트	목적지 포트	DATA
trin00	-	31335	144
trin00	-	31335	Hello
mstream	-	27444	l44adsl
mstream	-	6838	newserver
mstream	-	10498	stream/
mstream	-	10498	ping
mstream	-	10498	pong

위와 같은 DDoS 공격에 사용되는 패턴들을 데이터베이스에 저장하여 네트워크에서 감사자료를 수집한 후 프로토콜을 판별하여 데이터베이스에 있는 필드의 레코드에 해당하는 항목만을 비교하게 된다.

[그림 5]는 패턴매칭 기법에 관한 흐름도를 도시하였다.



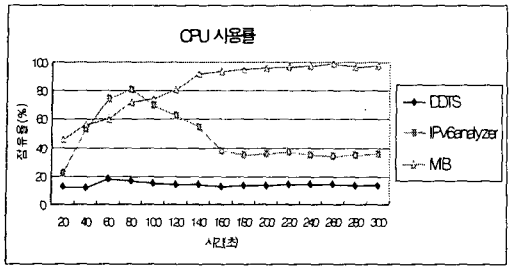
▶▶ 그림 5. 패턴 매칭 알고리즘 흐름도

이러한 통계적 기법과 패턴 매칭 기법을 이용하여 두 조건을 모두 만족하는 경우 공격으로 판단하게 된다.

Ⅳ. 실험 및 결과 고찰

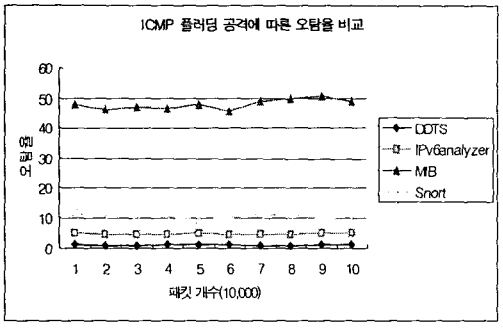
본 논문에서 제안한 알고리즘을 적용한 DDoS 공격 탐지 시스템의 성능을 실험하기 위하여 공격 도구로는 Trin00, TFN등을 사용하였다. 이러한 통계적 기법과 패턴 매칭 기법을 이용하여 두 조건을 모두 만족하는 경우 공격으로 판단하게 된다.

제안한 이중 탐지 도구의 성능을 비교하기 위해 기존의 IPv6alalyzer와 MIB를 이용하였을 경우 CPU 점유율을 비교하였다. [그림 6]에서 보듯이 이중 탐지 도구를 이용한 방법의 경우 CPU 사용률 및 탐지 시간을 감소시키고, 모든 트래픽을 수집하지 않고 0.02초마다 샘플링을 통해 패킷을 수집함으로써 CPU의 점유율을 MIB와 비교해서는 약 30.4%, IPv6analyzer와 비교해서는 약 12.5%의 점유율을 감소시켰다. 또한 탐지 시간을 기존의 방법보다 감소시킴으로써 탐지 후 차단되는 시간이 감소되게 된다. 기존 방법중 IPv6analyzer는 탐지 시간이 60초 즉 1분정도 소요되고, 차단이 이루어지는 처리시간도 20초정도 소요되고, 실제 공격이 처음 이루어지는 순간부터 차단까지 1분 20여초가 소요되게 된다. 이렇게 됨으로써 총 80여초 사이의 CPU는 점차 상승하게 되고 실질적으로 차단이 이루어짐으로써 CPU가 감소되게 된다. 그러나 제안된 시스템에서는 시간에 따른 임계값을 적용한 방법이 아니라 샘플링한 패킷의 개수에 의해 임계값을 적용함으로써 탐지 시간은 약 20초, 처리 시간은 약 10초가 소요되어, 총 탐지 후 차단까지 30초가 되어 초기 약 10초정도만 CPU 점유율이 상승하고 원래의 CPU 점유율을 유지할 수 있다. 즉 빠른 탐지 및 차단으로 공격이 들어와도 CPU 점유율을 평상시처럼 유지할 수 있었다.



▶▶ 그림 6. 공격 차단 전,후의 CPU 사용률

[그림 7]은 동일한 조건으로 ICMP 플러딩 공격시 전체 패킷에 따른 오탐율을 비교하였다. 제안된 시스템의 경우 약 1.2%대에서 안정한 오탐율을 기록한 반면에 IPv6analyzer의 경우 약 3.5%의 오탐율을 기록하고 있다. 기존시스템과의 오탐율 차이는 약 2%가량 제안된 시스템의 성능이 개선된 것을 확인할 수 있다.



▶▶ 그림 7. ICMP 플러딩 공격에 따른 기존 시스템과의 오탐율 비교

V. 결 론

기존의 공격 탐지 방법에서는 공격이 발생할 때 조기 탐지가 어려워 탐지를 하더라도 이미 피해를 입어 대응을 할 수 없는 문제가 발생하였다. 이것은 기존 방법이 일정기간 동안의 트래픽을 수집하여 임계값을 설정하였기 때문이다. 본 논문에서는 일정 기간 동안의 트래픽 수집에 의한 방법이 아니라 단위 패킷에 의해 트래픽을 수집한 결과를 통계적 기법과 패턴 매칭 기법을 적용한 DDoS 공격 탐지 알고리즘을 제안하였고 구현한 결과, DDoS 공격의 가장 큰 관건인 조기 탐지와 오탐율 및 CPU 점유율에 있어서 성능이 향상되는 것을 확인 할 수 있었다. 향후 연구과제로는 다양한 공격 패턴을 추가한다면 성능이 개선되리라 사료된다.

▌참 고 문 헌▐

[1] 오창석, 데이터 통신, 영한 출판사, 1999.
[2] H. Wang, D. Zhang, K. G. Shin, "Detecting SYN Flooding Attacks", Univ. of Michigan, 2002.
[3] 유대성, 오창석, "공격 탐지를 위한 트래픽 수집 및 분석 알고리즘", 한국콘텐츠학회 논문지, 제4권 4호 (pp.33-43), 2004.12
[4] 유대성, 박원주, 김선영, 서동일, 오창석, "DDoS 공격을 검출하기 위한 트래픽 분석 알고리즘", 한국콘텐츠학회 2003 추계 종합학술대회, (pp.105-108), 2003.11
[5] D. Dittrich, "Distributed Denial of Service attacks/tools resource page" University of Washington, 2000.
[6] Joseph S. Sherif, and Tommy G. Dearmond. "Intrusion Detection: Systems and Models." Proceedings of Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure of Collaborative Enterprises. 2002.
[7] 김선영, 박원주, 유대성, 서동일, 오창석, "SNMP를 이용한 트래픽 폭주 공격 검출", 한국콘텐츠학회 논문지, 제3권 4호, pp.48-54, 2003.12
[8] Rocky K. C. Chang, "Defending against Flooding-Based Distributed Denial of Service Attack," IEEE Communications Magazine, 10, Oct 2002.
[9] Ed Skoudis, Counter Hack, "A Step-by-Step Guide to Computer Attacks and Effective Defenses, Prentice Hall PTR, 2003.
[10] S. Jha, K. Tan, and R. Maxion. "Markov chains, Classifiers, and Intrusion Detection, " Computer Security Foundations Workshop, June 2001.
[11] David Moore, Geoffrey M. Voelger and stefan savage, "Inferring Internet Denial-of-Service Activity", Usenix Security symposium, pp.9-22, August 2001.
[12] L. Garber, "Denial of Service Attacks rip the Internet", IEEE Cpmputer pp. 12-17, April 2000
[13] 정휘석, 이철호, 최경희, 정기현, "트래픽 분석을 통한 효과적인 DDOS 공격탐지방법", 정보과학회 가을 학술발표논문집, pp.574-576, 2002.10.