시계열 분석을 이용한 Netflow 기반의 DDoS 공격 탐지

Netflow Based DDoS Attack Detection Using Time Series Analysis

저자 (Authors)
이상일, 김진, 최일준, 오창석
Sang-Il Lee, Jin Kim, Il-Jun Choi, Chang-Suk Oh

출처 (Source)
한국정보기술학회논문지 12(5), 2014.5, 115-121(7 pages)
The Journal of Korean Institute of Information Technology 12(5), 2014.5, 115-121(7 pages)

발행처 (Publisher)
한국정보기술학회
Korean Institute of Information Technology

URL
http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE02411893

APA Style
이상일, 김진, 최일준, 오창석 (2014). 시계열 분석을 이용한 Netflow 기반의 DDoS 공격 탐지. 한국정보기술학회논문지, 12(5), 115-121

Journal of KIIT. Vol. 12, No. 5, pp. 115-121, May 31, 2014. pISSN 1598-8619, eISSN 2093-7571 115
http://dx.doi.org/10.14801/kiitr.2014.12.5.115

시계열 분석을 이용한 Netflow 기반의 DDoS 공격 탐지

이상일*, 김진**, 최일준**, 오창석***

Netflow Based DDoS Attack Detection Using Time Series Analysis

Sang-Il Lee*, Jin Kim**, Il-Jun Choi**, and Chang-Suk Oh***

본 논문은 2013년도 충북대학교 학술연구지원사업의 연구비 지원에 의한 연구결과임.

요 약

오늘날 DDoS 공격이 급속도로 증가되고 규모 또한 커지고 있기 때문에 이에 대한 효율적인 탐지 기법이 요구된다. DDoS 공격 탐지 기법은 패턴 매칭 기법과 통계적 기법의 2가지로 구분되며 패턴 매칭 기법은 Rule에 포함되지 않은 새로운 공격은 탐지할 수 없고, 통계적 기법을 이용한 공격탐지 방법은 정상 사용자가 트래픽을 과도하게 발생시킬 경우 공격으로 오판하는 문제가 발생하게 된다. 이에 본 논문에서는 패턴분석 및 시계열 자료를 이용하여 패턴매칭 기법과 통계기반의 탐지기법을 혼합한 형태의 DDoS 공격 탐지기법을 제안한다. 제안시스템은 기존의 탐지기법과 비교하여 공격에 대한 탐지율이 약 10% 정도 높아져 전체적인 성능이 향상되고 개선되었음을 확인하였다.

Abstract

DDoS attack today increases rapidly for scale since larger detection efficient technique for this is required. Method of detecting DDoS attacks, is divided into two statistical techniques a pattern matching method, a new attack that is not included in the Rule can not be detected, the pattern matching method, attack using statistical techniques when generating a lot of traffic normal user is increased excessively, the detection method is, so that the problem of the faulty judgment aggressive occurs. Therefore, in this paper, is to provide a new method to detect DDoS attacks in the form of a mixture of detection techniques and statistical-based matching technique using time-series data of the pattern. By using the proposed method, compared to the detection method of the existing, performance improves overall detection rate is lowered ah increases, the detection rate of attack was identified was improved.

Keywords
distributed denial-of-service attack, flow, traffic analysis, false negative

* 충북대학교 컴퓨터공학과
** 중원대학교 컴퓨터시스템공학과
*** 충북대학교 컴퓨터공학과 교수(교신저자)
· 접 수 일: 2014년 04월 24일
· 수정완료일: 2014년 05월 06일
· 게재확정일: 2014년 05월 09일

· Received: Apr. 24, 2014, Revised: May 06, 2014, Accepted: May 09, 2014
· Corresponding Author: Chang-Suk Oh
Dept. of Computer Science, ChungBuk National University, 52 Naesudong-ro, Heungdeok-gu, Cheongju Chungbuk, 361-763, Korea,
Tel.: +82 43 261-2454, Email: csoh@chungbuk.ac.kr

Ⅰ. 서 론

과거에는 사용자나 관리자에게 해를 끼치지 않는 범위의 공격이 이루어졌는데, 최근에서의 웹 환경은 사용자의 시스템에 피해를 끼치는 바이러스 형태의 공격이 주류를 이루었고, 더 나아가 네트워크 자체를 공격하여 마비시키는 형태의 지능화된 공격으로 나날이 발전 하였다[1].

이와 같이 DDoS 공격이 급속도로 증가되고 규모 또한 커지고 있기 때문에 이에 대한 효율적인 탐지 기법이 요구된다. 기존의 탐지 기법은 크게 두 가지로 나눌 수 있다. 첫 번째로 패턴 매칭은 네트워크 상의 모든 트래픽을 수집하여 기존에 정의된 공격과 일치하는지 여부로 공격을 탐지하는 방법이다. 이 방법은 정확한 공격 탐지는 가능하지만 탐지 Rule에 포함되지 않은 새로운 공격은 탐지할 수 없는 문제가 존재한다. 이와 같은 문제를 해결하기 위해서는 관리자가 수동적으로 많은 수의 공격 패턴을 시스템에 일일이 반영해야 하는 단점이 있다. 또한 적용된 수많은 패턴을 분석하고 처리하는데 있어 탐지 시스템에 과부하를 발생시켜 또 다른 문제점을 낳고 있다[2]. 두 번째, 통계적 기법을 이용한 공격 탐지 방법은 프로토콜별 특정 필드의 카운트 값만을 이용하여 일정 기간 동안의 실험을 통해 임계값을 설정하는 방법으로, 공격 여부는 임계값에 의해 판단한다. 그러나 이 방법도 정상 사용자에 의한 트래픽 증가를 공격으로 오판하는 문제가 발생할 수 있다. 통계적 기법은 탐지 시스템의 과부하 문제를 향상시킬 수는 있으나 초기 임계값을 설정하는데 상당한 시간이 소요되는 문제점이 있다[3].

따라서 본 논문에서는 패턴 매칭 탐지 기법과 통계 기반 탐지 기법을 혼합한 형태의 DDoS 공격 탐지 기법을 이용하여 공격에 대한 탐지율을 높이도록 하였다. NetFlow의 7-Tuple 정보인 출발지 IP, 목적지 IP, 출발지 포트, 목적지 포트, 레이어3 프로토콜, ToS, 라우터 또는 스위치 인터페이스를 분석하여 기존에 정의되어 있던 Rule DB의 데이터, 즉 정의된 패턴과 비교하여 기존에 정의되어 있던 패턴이면 이상으로 인식하여 공격으로 간주한다. 기존의 패턴을 통해 이상으로 감지되면 IP 블랙리스트 DB에 저장하고 차단한다. 패턴에 매칭 되어 지지 않은 정상 데이터는 2차 탐지 모듈의 지수평활법을 활용한 임계치 설정을 통하여 이상을 탐지한다. 최종적으로 이상으로 판단된 패킷에 대해서는 IP를 차단하고 패턴과 IP를 추출하여 Rule DB와 IP 블랙리스트 DB에 저장하는 방식으로 기존의 방법보다 오탐지율이 낮고 효율적인 탐지 기법을 제안한다. 본 논문의 구성은 2장에서는 관련 연구를 살펴보고, 3장에서는 시계열 분석을 이용한 DDoS 공격 탐지를, 4장에서는 실험 및 결과 고찰을 하고, 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1 NetFlow를 이용한 탐지 기법

NetFlow 버전 중 가장 대중적으로 쓰이는 버전은 NetFlow v5 이지만 MPLS와 같은 프로토콜이 고려되지 않아 IPv4 트래픽만 모니터링이 가능하며, 고정된 Flow 통계 필드만 사용하기 때문에 다양한 분석 기능을 구현하기 어렵다. NetFlow v5의 단점을 보완하고 다양한 모니터링 기능의 구현이 가능한 NetFlow v9는 IP패킷의 구성이 가변적이고 확장 가능한 템플릿을 활용하며, 전송 프로토콜로 STCP / TCP를 기본으로 채택하고 있으며 IPv6를 지원한다. 하지만 현재 세계적으로 v5 버전이 가장 많이 쓰이고 있으며 버전 v5를 기준으로 Flow를 통해 제공되는 7-Tuple은 단방향성을 가지고 개별 Flow는 식별자 외에도 그 Flow의 시작 시각 및 지속시간, 패킷 수와 바이트수를 가지는 구조로 되어 있다. 이러한 정보를 바탕으로 이상탐지가 가능하며, 유해 트래픽을 탐지 할 수 있다.

2.2 Snort를 이용한 탐지 기법

Snort는 대표적인 공개용 네트워크 기반 침입 탐지 시스템 중에 하나이다. Snort는 경량화 네트워크 기반 침입 탐지 시스템으로서 실시간 트래픽 및 패킷의 내용을 분석하고, 버퍼 오버플로우, 포트 스캔 등 다양한 공격과 징후를 매칭 기법으로 탐지한다. 커뮤니티를 통해 지속적인 탐지 Rule의 업그레이드가 가능하며 다양한 OS에서 실행이 가능하다는 장점이 있다[4].

2.3 SNMP를 이용한 탐지 기법

SNMP를 이용한 탐지 기법은 SNMP의 MIB 정보를 이용한 방법으로 트래픽 폭주 공격 탐지는 MIB 데이터 수집을 위한 시스템 및 네트워크 리소스의 사용이 적고, 계층과 프로토콜을 기준으로 표준화된 네트워크 성능 데이터를 제공받을 수 있기 때문에 패킷 기반 탐지방법에 비해 빠르고 효과적인 탐지와 분류가 가능하다. 이는 대부분의 네트워크 기반 시스템들이 기본적으로 SNMP Agent를 탑재하고 있기 때문이다. 따라서 SNMP MIB 정보를 이용한 트래픽 폭주 공격 탐지는 고사양의 패킷 기반 탐지 시스템을 설치하기 힘든 소규모로 운영되는 곳에서의 침입 탐지 시스템으로 적합하고, 대규모의 네트워크에서도 적은 비용과 노력으로 탐지 시스템을 구축할 수 있는 대안이 될 수 있다[5].

2.4 기존 탐지 기법의 문제점

기존 Flow를 이용한 탐지 방법들 또한 헤더 위주의 정보제공 및 IANA에서 제공하는 포트 기반 응용 프로그램 탐지 및 점유율 기반 TOP 패킷들에 의해 이상 정도를 탐지하는 방법이다. 이런 경우 P2P를 이용한 응용들 같이 동적 포트 번호 사용과 Well-Know 포트를 사용한 공격에 대해서는 식별하기 어렵다. 이에 최근에는 Flow를 이용하여 NMS와 함께 중앙에서 트래픽을 분석/모니터링 하는 기법이 일반화 되고 있으며, 벤더별 NetFlow나 sFlow, cFlow 등과 같은 독자적인 포맷을 정의 하여 Flow를 제공하고 있다[6][7]. Snort를 이용한 탐지 기법은 사전에 정의된 공격 패턴과 패턴 매칭 기법으로 비교하는 방식을 취하므로 기존에 정의된 공격에 대한 탐지는 정확성이 뛰어나지만 기존에 패턴화 하여 저장되지 않은 정보에 대해서는 정확한 탐지가 어려운 단점이 있다. 그러한 문제점을 해결하기 위해 관리자는 꾸준한 시스템 관리와 패턴 업데이트를 해야 한다[8]. SNMP를 이용한 탐지 기법은 MIB 객체를 이용하여 탐지한다. IP, TCP, ICMP, UDP의 입출력에 해당되는 MIB객체의 로그값을 추출하여 사전에 정의된 임계치와 비교하여 공격을 감지하게 된다. 단순히 트래픽 정보를 가공하고 그래픽화 하여 보여주는 방식이기 때문에 호스트의 정보와 서비스 정보에 관한 사항은 미흡하거나 포함되어 있지 않아 정확한 측정이 불가능하다. 그리고 트래픽을 탐지하기 위해서 시스템에 많은 부하가 발생하여 사용자들이 적절한 서비스를 받지 못하게 되는 상황이 초래되기도 한다[9][10].

III. 시계열 분석을 이용한 DDoS 공격 탐지

3.1 NetFlow 기반의 탐지 모델

제안하는 DDoS 탐지 기법은 웹 서버로 전달되는 모든 네트워크 정보를 수집한 후, NetFlow를 통해 제공되는 대용량의 Flow를 7-Tuple의 정보를 기반으로 분석한다. 기존 패턴 매칭 기법의 문제점은 정의되지 않은 패턴에 대해서는 탐지가 불가능한 문제점이 있다. 이는 False Negative가 높아지는 문제점이 발생한다. 이러한 문제점을 해결하기 위해 제안 시스템은 새로 수집된 정보를 기존에 정의 되어진 패턴과 비교하여 기존에 이미 정의 되어진 패턴이면 이상으로 판단하고 정의되지 않은 패턴은 통계적 기법의 하나인 임계치를 이용한 이상 판단을 다시 한 번 실행한다. 제안 시스템의 흐름도는 그림 1과 같다.

3.2 시계열 분석에 의한 임계치 설정

본 논문에서 제안하는 통계 기반의 임계치 설정 알고리즘은 시계열 자료를 분석하여 동적인 임계치를 설정하는 방식이다. 시계열 자료 분석의 대표적인 방법인 평활법 중에 지수평활법을 이용하였다. 이동평균법은 과거의 데이터를 포함하여 임계치를 설정하는 반면 지수평활법은 오래된 자료일수록 비중을 적게 두어 미래의 예측값을 산출해 낼 수 있다는 장점이 있다. 지수평활법은 시점의 실제치 X_t가 입력되면 식 (1)을 이용하여 t+1 시점에 대한 예측치 Y_{t+1}을 계산하게 된다.

$$Y_{t+1} = \alpha X_t + (1-\alpha)\, Y_t, \quad 0 < \alpha \leq 1 \qquad (1)$$

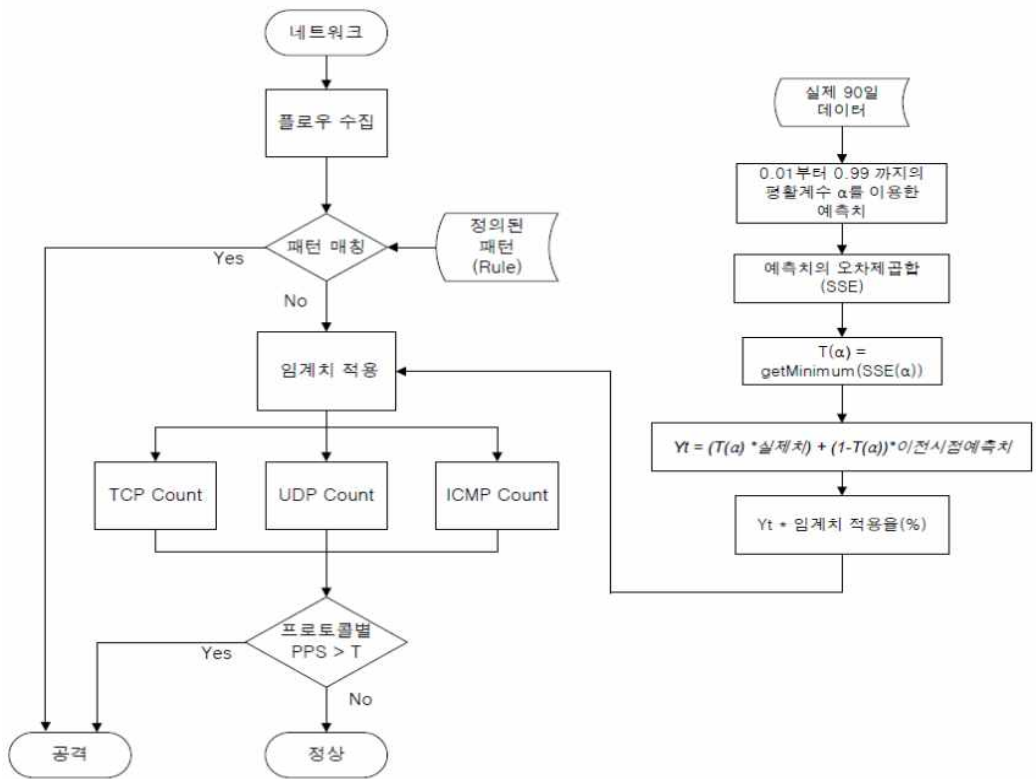

그림 1. 공격탐지 흐름도
Fig. 1. Attack detection flowchart

α는 평활계수를 나타내며 시간에 따라서 변하지 않는 상수로서 0.05 ~ 0.3 사이의 값을 주로 사용한다. 평활계수는 실제치를 이용하여 다음 시점의 예측치에 대한 가중치가 된다. X_t는 t시점의 실제치이고 Y_t는 t시점에서 X_t와 Y_{t-1}을 이용하여 $t+1$ 시점에 수요를 예측한 예측치이다. 이와 같은 임계치 설정에 앞서 선행되어야 할 부분은 적절한 평활계수 α의 선택이다. α는 시간에 따라서 변하지 않는 상수로서 0.05 ~ 0.3으로 정해주는 것을 권장하고는 있지만 시스템의 방식과 여러 환경에 많은 영향을 받는 것을 감안해 직접 표본 데이터를 추출, 최소제곱법(method of least square)을 이용하여 예측오차의 제곱 합인 SSE(sum of squares error)를 평활계수 α를 0.1부터 0.99까지 시뮬레이션 하여 오차 제곱합이 가장 적은 가중치를 선택한다.

$$SSE = \sum_{t=1}^{n}(X_t - Y_t)^2 = \sum_{t=1}^{n} e_t^2 \quad (2)$$

그림 2는 0<α<1 의 평활계수 α에 대한 예측오차의 제곱합을 시뮬레이션 하여 그래프로 나타낸 것이다.

이 결과를 바탕으로 최근 90일 동안의 일별 최고 PPS의 평균 $PPS^{(1)}$을 식 (2)와 같이 도출해 내고 최근 90일 동안의 일별 PPS의 평균 $PPS^{(2)}$를 식 (3)과 같이 도출하여 식 (4)와 같이 $PPS^{(1)}$과 $PPS^{(2)}$를 이용하여 임계치 적용률을 산출해 내도록 하였다.

$$PPS^{(1)} = (\sum_{t=1}^{n} \text{일일최고} PPS)/n \quad (3)$$

$$PPS^{(2)} = (\sum_{t=1}^{n} \text{일일평균} PPS)/n \quad (4)$$

$$\text{임계치 적용율}(\%) = \frac{PPS^{(1)}}{PPS^{(2)}} \times 100(\%) \quad (5)$$

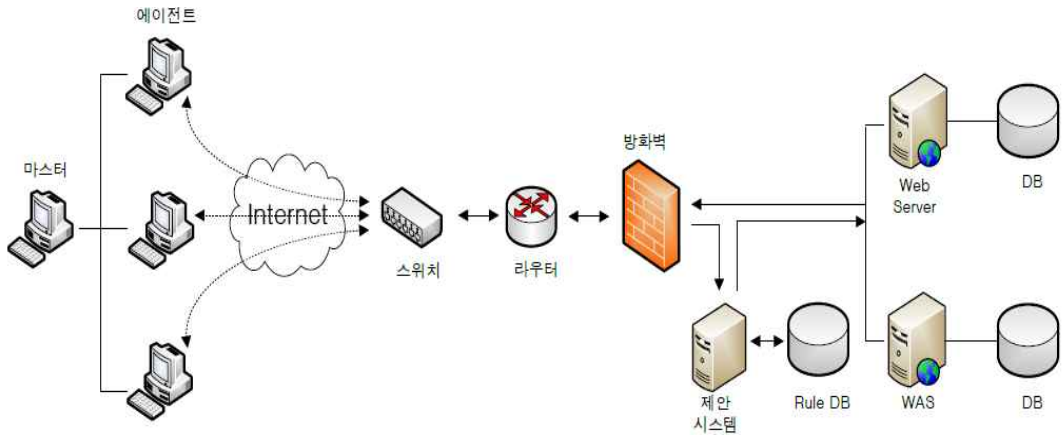

그림 2. 실험 환경 구성도
Fig. 2. Experiment enviroment diagram

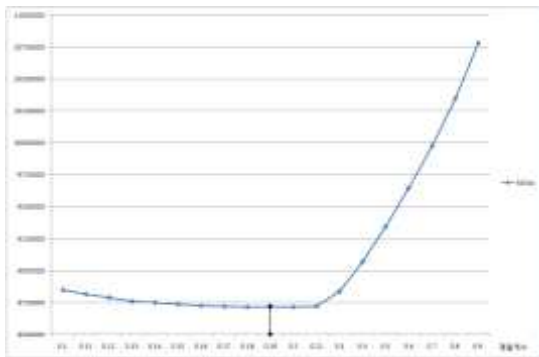

그림 3. 예측 오차의 제곱합
Fig. 3. Sum of squars error

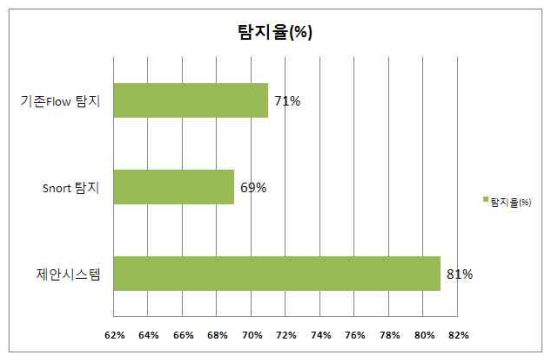

그림 4. 성능 평가 결과
Fig. 4. Experimental result

IV. 실험 및 결과 고찰

4.1 실험 환경

본 논문에서는 DDoS 공격 탐지와 차단을 시험하기 위해 사용된 실험 망 구성도는 그림 2와 같다. DDoS 공격 탐지와 차단을 시험하기 해당 사이트에 접근하는 모든 트래픽에 대해 방화벽 정책을 적용하여 웹 트래픽만 시스템으로 전달 되도록 하였다. 방화벽을 거친 패킷은 1차로 스위치와 라우터를 거치면서 1차 탐지를 위해 Flow를 수집하고 룰에 의해 먼저 탐지 되며 이후 지수평활법을 이용한 임계치를 거치면서 최종 탐지 된다.

4.2 결과 고찰

제안한 시스템은 성능 평가를 위해 트래픽 폭주 상태를 가장하여 실험을 실시하였다. 실험에서 사용된 공격 에이전트들은 Bot 및 웜 감염 좀비 PC와 같은 폭주트래픽을 생성하기 위해 트래픽 제너레이터와 전형적인 DDos공격 도구 Trinn00, TFN2K가 설치하여 이와 같은 공격도구를 이용하여 100회에 걸쳐 트래픽 폭주를 유발 시켜 그림 4와 같은 결과를 얻을 수 있었다. 실험방법은 최초 Flow 데이터를 수집하여 Rule DB 기반의 패턴 매칭을 실시하여 1차 필터링을 실시한 후 지수평활법을 이용하여 임계치 설정에 의한 통계 기반의 2차 공격탐지를 실시함으로써 전체 트래픽의 모니터링 결과 81% 탐지율을 보였다. 특히 정확한 임계치의 예측으로

False Negative를 기존의 방법들보다 효율적으로 감축 시킬 수 있었다.

기존의 NetFlow 탐지 기법은 71%의 탐지율을 보였고, Snort는 69%의 공격 탐지율을 보였다. Snort의 경우 공격이 계속 일어날수록 패턴을 업데이트해주면서 탐지율이 상승하는 것을 볼 수 있었다. 마지막으로 제안 시스템은 다른 기법에 비해 약 10% 정도 공격 탐지율이 높아 효과적인 False negative 감축을 할 수 있었다.

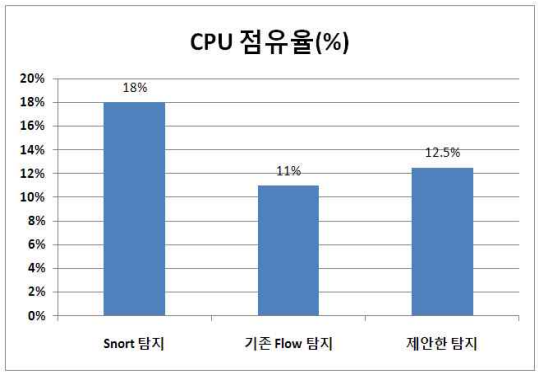

그림 5. CPU 점유율
Fig. 5. CPU occupancy rate

제안 시스템의 리소스 사용면에서의 비교는 Snort와 NetFlow를 이용한 방식에 따라 큰 차이를 보였다. Snort의 경우 예상했던 것과 같이 패킷 캡처와 Rule 매칭 분석 시 평균 18%의 CPU 점유율을 보였고 기존 NetFlow를 이용한 방법은 Snort를 이용한 방법보다는 적은 11% CPU 점유율 보였다. 이에 비해 제안한 시스템은 패턴매칭 구간에서는 snort를 이용한 방법과 유사한 CPU 점유율인 약 16%의 CPU 점유율을 보이다가 2차 탐지 구간에서는 9%의 CPU 점유율을 나타내며 약 12.5%의 CPU 점유율을 보여 비교적 적절한 수준의 탐지율을 보였다.

V. 결론 및 향후 과제

본 논문에서는 기존의 DDoS 탐지 기법의 문제점을 보완하고자 Netflow 기반의 패턴 매칭 기법과 통계적 기반의 혼합된 형태의 DDoS 탐지 기법을 제안하였다. 기존의 패턴 매칭 기법은 정의되지 않은 공격에 대해 공격으로 인지하지 못하는 False Negative가 높았고 기존의 통계적 기법의 이상 탐지는 임계치 설정에 대한 단순 평균을 이용하여 정확한 임계치 설정이 어려워 이상을 탐지하기 어렵다는 단점이 있었다.

따라서 본 논문에서는 1차적으로 NetFlow를 기반으로 Flow의 정보를 분석하여 패턴 매칭을 실시하여 이상을 탐지 하였다. 정상으로 판단된 트래픽에 대해 2차적으로 지수평활법을 이용한 정확한 트래픽 추정치를 산출하여 임계치를 설정하는 방식의 기법을 제안 하였다. 제안 기법의 비교를 위해 패킷 캡처 기반의 Snort를 이용한 탐지기법과 기존 포트 기반의 Flow 분석 방법을 통하여 제안 시스템의 성능을 비교 테스트 하였다. 2중 탐지를 실시하기에 CPU 점유율이 Snort를 이용한 기법보다 10% 정도 탐지율이 향상 되었다. Snort를 이용한 방법은 기존에 정의 되어진 패턴에 대해서는 정확한 탐지가 가능했으나, 새로운 공격일수록 탐지율이 낮은 것을 볼 수 있었다. 그리고 기존의 Flow 기반의 탐지 기법은 False Negative는 높았으나 CPU점유율 즉 시스템 부하율이 제안 시스템에 비해 낮았다. 향후 과제로는 시스템 부하를 줄이고 최근에 발생되는 새로운 형태의 DDoS 공격에 대한 정확하고 효율적인 공격 대응을 할 수 있는 기술적 연구가 이루어져야 하겠다.

References

[1] Eung-Jun Jo, Jin-ho Kim, and Choong-Seon Hong, "LoWPAN based Botnet Traffic Detection Method Using Characteristics", Information Science Society, Vol. 17, No. 1, 33-41, Feb. 2011.

[2] Jonatan Gomez, Fabio Gonzakez, and Dipankar Dasgupta, "An Immuno-Fuzzy Approach to Anomaly Detection", in Proc, IEEE, Vol. 2, pp. 1219-1224, May 2003.

[3] Young-Jin Yoon, "Traffic DDoS Attack Detection Method Using The Average Rate of Change", Master Thesis, Chungbuk National University.

[4] Jong-Won Kim, Il-Jun Choi, Tae-Yong Shim, and Chang-seok Oh, "False Negative Flow for Reducing Traffic Congestion Based Attack Detection",

Journal of KIIT, Vol. 10, No. 3, 149-159, March 2012.

[5] Jae-hak Yu, Jun-Sang Bak, Han-Seong Yi, and Dae-hee Park, "SVDD Using SNMP MIB Traffic Congestion and Attack Detection", Information Processing Society No. 15-C XIV Article 122, Issue 5, pp. 351-358, Oct. 2008.

[6] Cisco NetFlow, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/netflct/tech/napps_ipfix¬charter.html

[7] Cisco Systems, White Papers, "Introduction to Cisco IOS NetFlow", May 2007.

[8] A. Valdes and K. Skinner, "Probabilistic alert correlation", RAID, pp. 54-68, May 2001.

저자소개

이 상 일 (Sang-Il Lee)

2014년 2월 : 충북대학교 컴퓨터공학과(공학석사)
2014년 ~ 현재 : 충북대학교 컴퓨터공학과 박사과정
2014년 ~ 현재 : 한국특허정보원 재직중
관심분야 : 정보보안, 네트워크

김 진 (Jin Kim)

2005년 2월 : 울산대학교 컴퓨터공학과(공학사)
2010년 2월 : 인천대학교 컴퓨터공학과(공학석사)
2013년 2월 : 충북대학교 컴퓨터공학과(공학박사)
2009년 ~ 2013년 : 중원대학교 전산정보센터 팀장
2013년 ~ 현재 : 중원대학교 컴퓨터시스템공학과 조교수
관심분야 : 컴퓨터네트워크, 정보보안

최 일 준 (Il-Jun Choi)

1997년 2월 : 충주대학교 컴퓨터공학과 (공학사)
2003년 8월 : 충북대학교 전기전산공학과 (공학석사)
2008년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
2013년 ~ 현재 : 중원대학교 컴퓨터시스템공학과 겸임교수
2013년 ~ 현재 : (주)NSworks 기술이사
관심분야 : 정보보안, 네트워크

오 창 석 (Chang-Suk Oh)

1978년 2월 : 연세대학교 전자공학과(공학사)
1980년 2월 : 연세대학교 전자공학과(공학석사)
1988년 8월 : 연세대학교 전자공학과(공학박사)
1985년 ~ 현재 : 충북대학교 컴퓨터공학과 교수
1982년 ~ 1984년 : 한국전자 통신연구소 연구원
1990년 ~ 1991년 : Stanford 대학교 객원교수
2007년 8월 ~ 2009년 8월 : 충북대학교 전산정보원장
2007년 7월 ~ 2010년 7월 : 한국엔터테인먼트산업학회 회장
2010년 7월 ~ 현재 : 한국엔터테인먼트산업학회 명예회장
관심분야 : 컴퓨터네트워크, 뉴로컴퓨터, 정보보호