엔터프라이즈 네트워크에서의 DDoS 공격의 예측 모델

하현태*, 백현철**, 김상복***

요약

본 논문은 네트워크를 이용하는 사용자들에게 서비스의 안정적인 보장을 위하여 DDoS 공격이 발생할 경우 그 시점에 대한 예측 가능한 모델을 제안한다. 본 논문에서 제안하는 모델은 이더넷 및 해당 노드의 부하 공격에 대하여 해당 공격을 예측 가능하도록 수학적 기준을 제시하였다. 더불어 공격 예측이 가능한 모델이 적용된 경우와 일반적인 탐지 후 대응이 이루어지는 모델과의 차이를 비교 분석하였다. 그 결과 본 논문에서 제안하고 있는 수학적 예측 모델이 일반적인 탐지 방식보다 신속하게 해당 공격에 대한 대응을 할 수 있기 때문에 안정적인 서비스 보장이 가능함을 알 수 있다.

Forecasting Model for DDoS Attacks in Enterprise Networks

Hyeon-tae Ha*, Hyun-Chul Baek**, Sang-Bok Kim***

ABSTRACT

In this paper, we propose a model that predict start time of DDoS attack to guarantee user reliable network services. The model presents a mathematical standard than can predict the DDoS attack on ethernet and each nodes. And, we do a comparative study on the predicting model and the general detecting and responding model. As a result, we could have a conclusion that the proposed mathematically predicting model can provide more secured services than the general detecting model do.

Key Words : DDoS attack, Forecast of attack, Traffic, Correlation coefficient, Statical detection

---

* 경상대학교 컴퓨터과학과 (✉hht0701@naver.com)
** 경남도립 남해대학
*** 경상대학교 컴퓨터과학과
· 제1저자(First Author) : 하현태 · 교신저자(Correspondent Author) : 김상복
· 접수일(2013년 5월 16일), 수정일(1차 : 2013년 5월 30일), 게재확정일(2013년 6월 13일)

Ⅰ. 서 론

서비스 거부 공격은 대상 시스템 또는 회선을 무력화 시킬 수 있는 다양한 공격 기법중 하나이다. 그리고 이러한 공격에 대한 방어를 위해서는 공격을 탐지하는 과정을 거친다. 탐지 과정은 크게 패턴 매칭의 기법을 사용하거나 통계적 기법을 이용하는 기법으로 나눈다.

패턴 매칭을 이용하는 기법은 네트워크상의 처리 패킷이 도착했을 때, 해당 패킷의 데이터를 룰의 시그니처와 비교하는 기법을 통하여 공격을 탐지하는 기법이다[1]. 이 기법은 트래픽을 수집하여 프로토콜 필드와 공격에 해당하는 데이터 필드의 내용을 수집 및 저장하여 기존 정의된 공격 탐지 정보와 일치하는지의 여부를 이용하여 공격을 탐지하는 기법이다. 패턴 매칭 기법은 정확한 공격 탐지가 가능하지만 탐지룰에 포함되지 않은 새로운 공격이 발생하면 이에 대한 탐지는 불가능하다. 그러므로 지속적인 업데이트를 위한 관리자의 노력과 설정이 수반되어야 한다. 이러한 패턴 매칭 기법의 문제점을 해결하기 위하여 통계적 기법을 이용한 기법이 제안되었다[2].

통계적 기법을 이용한 공격 탐지 기법은 네트워크상의 트래픽을 모두 저장하지 않는 특징을 보인다. 탐지를 위해 프로토콜별, 특정 필드의 카운트 값을 이용하여 일정 기간 동안의 실험을 통해 임계값을 설정하여 공격 여부를 판단한다. 이 공격 탐지 기법은 패킷을 수집하고 분류하는 수집 모듈, 탐지에 사용할 각종 요소를 추출 및 연산하여 임계값을 산출하는 분석 모듈, 그리고 임계값을 이용하여 공격 여부를 판단하여 처리하는 공격 판단 모듈로 구성되어 있다[3].

이러한 특징을 가지는 탐지기법들의 경우 공격이 발생한 이후에 대응한다는 것이 일반적인 특징이다. 이에 본 논문에서는 신속하게 서비스 거부 공격에 대응하여 안정적인 서비스를 보장하기 위하여 공격이 발생하는 시점을 예측하는 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 DDoS 공격과 탐지 시스템의 종류와 특성을 분석하고 이들의 문제점에 대해 기술한다. Ⅲ장에서는 제안하는 시스템 모델에 대해 구체적으로 기술한다. Ⅳ장에서는 수학적 분석을 통해 제안하는 시스템 모델과 기존 시스템 모델에 대해 효율적인 방안을 제시하고 Ⅴ장에서는 성능평가 결과에 대하여 논하고 결론을 맺는다.

Ⅱ. 관 련 연 구

2.1 DDoS 공격의 종류

DDoS 공격은 크게 두 가지로 분류할 수 있는데, 첫 번째는 네트워크의 대역폭 소진 공격이 있으며 두 번째는 서비스(애플리케이션) 마비 공격이 있다. 이 두 가지 공격의 유형을 살펴보면 다음의 <표 1>과 같다[4].

표 1. DDoS 공격의 유형
Table 1. Type of DDoS attack

	대역폭 소진 공격	서비스 마비 공격
공격유형	UDP/ICMP Flooding, TCP Traffic Flooding	HTTP GET Flooding
공격의 형태	● UDP/ICMP Traffic Flooding UDP/ICMP Flooding, DNS Query Flooding 등 ●TCP Traffic Flooding SYN Flooding, SYN+ACK Flooding 등 ● IP Flooding IP Header Option 변조 (LAND Attack), IP Fragment Packet Flooding (Teardrop, HTTP Continuation) 등	● HTTP Traffic Flooding GET Flooding, GET with Cache-Control ● HTTP Header/Option Spoofing Slowris, Fragmented HTTP Header Attack(Slowloris/Pyloris) 등 ● TCP Traffic Flooding TCP Session, SYN Flooding, TCP Slow Read 등
프로토콜	Network,Transport Layer	Application Layer
공격대상	네트워크 플랫폼	서버
Spoofing 여부	사용 또는 미사용	미사용
특성	●회선 대역폭 고갈 ●동일 네트워크를 사용하는 모든 서비스에 대한 접속장애 발생	● HTTP 서버과다접속(또는 서비스 부하)으로 인한 장애발생 ●공격대상 시스템만 피해

2.2 대역폭 소진 공격

대역폭 소진 공격은 UDP/ICMP flooding 공격이 대표적인 공격으로 이는 공격자가 Spoofing 공격을 병행하거나 그렇지 않은 방법으로 UDP/ICMP 패킷을 대량으로 전송하여 대역폭을 소진하는 서비스 거부 공격 기법이다[5][6][7][8].

SYN flooding 공격은 공격자가 대량의 SYN 패킷을 발송하는 기법이 있고 TCP의 Flag 값을 임의로 조작하여 SYN, ACK, FIN, RST 등과 같이 여러 형태의 패킷을 생성한 후, 대량으로 전송을 하면 서버가 해당 패킷을 수신하여 검증하기 때문에 서버의 자원을 소진하는 공격 기법이다[5][6][7][8].

IP spoofing 공격 기법은 공격 대상에게 송신지 IP 주소와 수신지 IP주소를 위조하여 전송하는 공격 기법이다. 이를 통해서 서버 대역폭을 소진 시키는 공격기법이다[5][6][7][8].

2.3 서비스 마비 공격

서비스 마비 공격은 Http Traffic flooding 공격이 대표적인 공격으로 이는 공격자가 서버측에 Http 메시지 지시자중에서 GET/POST등의 지시자를 이용하여 메시지를 전송하여 TCP프로토콜 해석을 위해 서비스가 마비되는 공격 기법이다.

2.4 기존 공격 탐지 기법의 문제점

대역폭 소진 공격이나 서비스 마비 공격 모두 공격이 발생한 후의 증상으로 파악을 하는 탐지 지향의 기법이다. 이러한 탐지 지향 기법의 경우 공격이 발생한 후 이에 대한 탐지 및 대응을 하기에는 시간이 촉박한 경우가 대부분이거나 원활하게 대응이 되더라도 탐지 후 처리 시간이 지연되는 동안 대역폭이 소진 되거나 서비스 마비가 발생하는 문제점이 발생한다.

그러므로 본 논문에서는 이러한 탐지를 위해 필연적으로 발생하는 지연시간의 문제를 해결하고자 하였다. 이를 위해 예측의 개념을 적용하여 문제가 발생할 가능성이 있는 시점을 중점 관리하여 공격을 예측한 후 미리 대응할 수 있도록 한다.

III. 제안하는 시스템 모델

DDoS 공격이 발생하는 시점에 트래픽에 대한 검사를 수행하는 기법은 다수의 논문에서 탐지의 영역으로 분류하여 많은 연구가 진행중이다. 그러나 공격의 예측을 판정하는 부분은 아직 연구가 부족한 상태이다. 본 논문에서는 DDoS공격의 예측 기법을 제안하고 이를 수학적 분석을 통해 분석하고 예측모델을 제안한다. 제안하는 시스템 모델의 순서도는 다음의 그림1과 같이 진행한다.

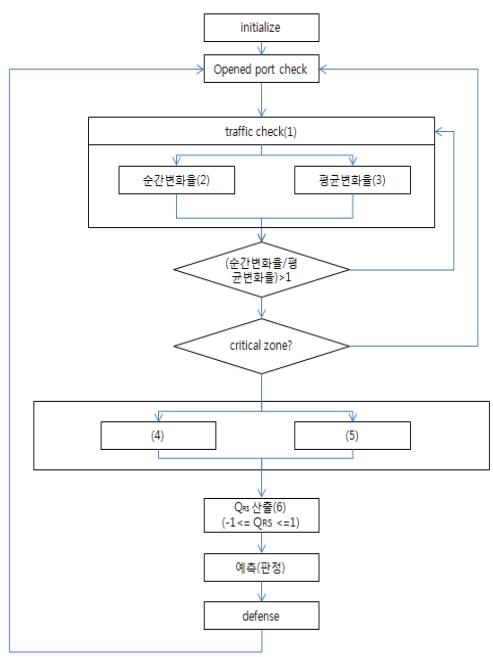

그림 1. 제안하는 시스템 순서도
Fig. 1. Proposed system flow

<그림 1>은 시스템의 초기화 이후에 개방되어 있는 포트를 탐색하여 트래픽을 측정하는 과정을 거치는데 이 과정에 패킷 단위로 순간 변화율과 평균 변화율을 측정한다. 기존의 연구는 임계값만을 설정하여 특정 시점이 임계치를 초과하여 분산 서비스 거부 공격의 발생여부를 판정하였다. 그러나 제안하는 시스템 모델은 임계값의 설정을 하지만 공격의 예측을 위한 임계구역을 추가하여 변화율을 측정하는 시점이 임계구역인지를 판단하게 된다. 이 임계구역의 판정은 순간 변화율이 평균 변화율을 초과하는 시점이면 임계구역인지를 판정하고 임계구역에 있을 경우에는 예측 시스템을 통해 분산 서비스 거부 공격의 여부를 판정하는 순서도이다.

Ⅳ. 수학적 분석

4.1 변화율 산출

제안하는 시스템 모델에서 우선 수행해야 하는 과정인 트래픽 측정은 개방된 포트에 한해서 할 수 있다. 이를 위해 개방된 포트를 OP_n이라 하고 해당 포트의 트래픽 양을 측정하기 위하여 도착하는 패킷의 길이를 측정하고 이 값을 $OP_{n(traffic_length)}$라 한다. $OP_{n(traffic_length)}$를 합한 후 단위 시간별로 누적하여 해당 노드의 전체 단위 시간별 트래픽 양으로 표시한다. 이 트래픽 양의 합산을 위해 $OP_{inspection}$을 정의하고 트래픽 양을 계산하는 식은 (1)과 같다.

$$OP_{inspection} = \sum_{n=1}^{\omega} OP_{n(traffic\_length)} \quad (1)$$

(1)에서 n은 노드의 포트 번호를 의미한다. 또한 노드 또는 회선 운영에서 서비스 거부 공격의 대상은 opened port인데 그 과정은 대부분 공격자가 개방된 포트를 찾아 공격 대상으로 선정한다. 이 opened port를 op라 하고 포트 번호를 붙여 관리를 한다. 일반적인 경우 웹서버 할당 포트가 opened port가 되므로 이를 op_{p_n}이라 하고 $op_{p_{80}}$으로 표현하고 트래픽에 대하여 공격여부를 판정하는 변수로 설정할 수 있다. 공격 여부의 판정을 위해 임계값을 설정하는데 이 값은 엔터프라이즈 환경의 일반적인 트래픽 사용량을 모니터링 하여 누적된 값을 사용한다. 이후 임계값의 극한을 초과하는 순간 변화율이 발생할 때 공격상태로 판정한다. 이는 (2), <그림 2>와 같이 수렴한다.

$$op_{p_n} = \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x} = \lim_{x \to 0} \frac{f(a+\Delta x) - f(a)}{\Delta x} \quad (2)$$
$$= \lim_{h \to 0} \frac{f(a+h) - f(a)}{h}$$

(2)에서 h는 x축의 특정 시간의 위치를 의미한다. 여기서 a는 순간변화율을 측정하기 위한 시점이고 시간축 x의 값이 a에서 Δx까지 변한다고 할 때 이는 $a+\Delta x$로 표현할 수 있다. 그리고 이 Δx가 0 즉 a의 극한에 도달할 때 종속변수 $f(a)$가 $f(a+\Delta x)$까지 얼마나 변했는지 판정할 수 있다. 또한 이 값은 x의 증분에 대한 변화율을 의미하므로 극한으로 표현할 수 있다.

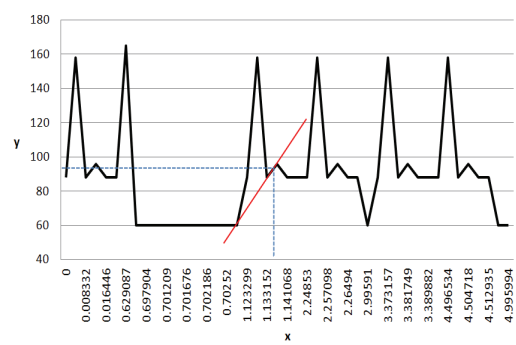

그림 2. 순간변화율 산정 그래프
Fig. 2. Differentiation and the derivative graph

이후 순간변화율로 발생한 미분계수를 시간의 구간별로 산정하여 이들의 평균변화율을 구한다. 평균 변화율 식은 (3)과 같이 수렴한다.

$$op_{p_n} = \left| \frac{\sum_{\delta y}^{y'} \lim_{\gamma y \to b} \frac{f(lt-b)-f(kt-b)}{b}}{\sum_{\delta x}^{x'} \lim_{h \to 0} \frac{f(a-mh)-f(a+mh)}{h}} \right| \quad (3)$$

(3)은 각 포트별로 시간의 지점마다 미분계수를 구하고 이를 이용하여 평균 변화율을 산정한다. (3)에 수렴하는 그래프는 <그림3>과 같다.

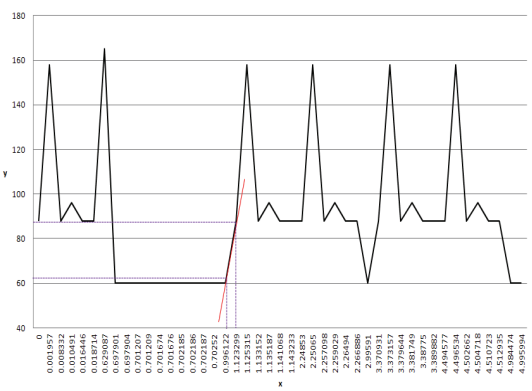

그림 3. 평균 변화율 산정 그래프
Fig. 3. The secant to curve

(1)과 (2), 그리고 (3)의 결과로 공격이 발생하는 포트는 특정 포트로 한정할 수 있으므로 해당 opened port에 대한 값으로 공격의 예측을 위한 관리 단계로 설정한다.

4.2 공격의 예측

공격 여부의 판정은 (2)와 (3)의 값이 극한에 도달하는 시점인데 공격의 예측을 위해서는 (2)와 (3)의 값이 극한에 도달하기 전에 임계구역을 설정한다. 임계구역의 설정 기준은 (2)의 결과로 산출한 순간 변화율이 (3)의 결과로 산출한 평균 변화율을 초과하는 경우로 설정하고 이 구역은 순간변화율의 극한에 도달할 때까지 유지한다.

임계구역에서는 관리 단계를 설정하여 공격 예측과정을 2회차로 설정하고 지속적으로 모니터링한다.

1차 단계는 시간과 opened port를 검사하는 과정을 거치는데 시간을 T_{time}으로 하고 트래픽 양을 검사하는 opened port는 (1)에서 산출한 값인 $OP_{inspection}$을 (4)에 적용한다.

$$R_{T_{time} OP_{inspection}} = \frac{1}{N} \sum_{i=1}^{N} T_{time \cdot i} OP_{inspection \cdot i} \quad (4)$$

여기서 i는 <표 2>로 정리할 수 있는데 이는 각 시간대 별로 평균 트래픽을 산출하기 위한 시간의 구간으로 표현한다.

2차 단계는 시간과 회선에 session 개방된 유저수의 관계를 검사하는데 시간은 동일하게 T_{time}, 유저수는 U_{user}라 하고 검사과정은 (5)와 같이 적용한다.

$$S_{T_{time} U_{user}} = \frac{\sum_{i=1}^{N} T_{time \cdot i} U_{user \cdot i}}{N} \quad (5)$$

(4)와 (5)에서 i는 표2와 같으며, 1차와 2차의 T_{time}은 측정 시간의 구간으로 산정하는데 그 내용도 <표 2>와 같으며 각 구간의 평균값으로 산출한다. 이는 일반 업무에서는 급격한 트래픽 변동이 발생하지 않으므로 이를 기준으로 측정을 한다.

표 2. 트래픽 측정 시간 구간
Table 2. Traffic measuring time section

i	측정시간구간
1	08~12
2	12~13
3	13~18
4	18~19
5	19~24
6	24~08

(4)와 (5)의 결과 값은 (6)을 통하여 일반화를 수행하는데 이는 (4), (5)의 결과 값을 기반으로 적률값을 산출한다.

$$Q_{RS} = \frac{\sum_{i=1}^{N} r_i s_i}{N\sigma_r \sigma_s} = \frac{\sum_{i=1}^{N} Z_{r_i} Z_{s_i}}{N} \quad (6)$$

(6)의 결과로 산출한 적률값 Q_{RS}는 항상 (7)의 범위에 있다.

$$-1 \leq Q_{RS} \leq 1 \quad (7)$$

(7)의 적률값은 음의영역이 발생할 수 있으나 이 경우는 정상범위에 수렴하고, 공격 예측에 대한 판정이 불필요하므로 판정대상에서 제외한다.

(7)의 적률값을 음의 영역까지 포함하면 공격 예측의 판정 범위가 더 넓어지나 음의 영역에 대한 부분은 판정이 불필요하다 했으므로 값의 수렴 범위가 표 3으로 귀결된다.

이를 통해 (7)의 적률값으로 <표 3>에 해당하는 판정이 가능하다.

표 3. DDoS 공격의 판정
Table 3. Determine of the DDoS attack

QRS	판 정
1.0~0.7	공격 가능성 70% 이상
0.7~0.4	공격 가능성 40% 이상
0.4~0.1	공격 가능성 40% 미만

V. 성 능 평 가

본 장에서는 시뮬레이션을 통한 성능 평가 결과를 기술한다. 시뮬레이션에서는 제안하는 방안을 활용하여, 서비스 거부 공격의 예측을 수행한 후 공격에 대응한 경우, 탐지를 수행한 후 공격에 대응한 경우에 대하여 각각의 대응 시간을 비교 및 평가를 한다.

그림4는 이더넷 환경의 시뮬레이션에서 정상 상태의 트래픽양을 측정한 결과 값으로 측정 시간 34초와 92초의 시점에 일시적으로 트래픽이 폭주하는 현상이 있으나 이는 정상적인 범주이므로 서비스 거부 공격의 예측단계로 들어가지 않음을 확인할 수 있다.

<그림 5>와 <그림 6>에서 분산 서비스 거부 공격이 발생하는 시점은 시뮬레이션 환경의 트래픽 발생 시점을 나타내는 것으로 실험 결과와는 상관이 없다.

<그림5>는 이더넷 환경의 분산 서비스 거부 공격에 대하여 룰 기반의 실시간 탐지 기법을 적용한 탐지 및 차단 시스템의 차단 시점을 실험한 시뮬레이션 결과이다. 본 실험에서는 분산 서비스 거부 공격의 차단을 위한 임계값을 시간과 트래픽의 양에 대한 교차값의 범위를 설정하고 패킷 분석을 수행하였다. 분산 서비스 거부 공격을 탐지하는 시점은 56초, 73초, 88초, 91초에 해당하는 지점이며 차단하는 시점은 60초, 77초, 91초, 95초로 총 4회에 걸쳐 공격 시스템을 차단하는 과정을 보인다. 탐지후 차단까지 소요된 시간은 각 건별 4초에서 5초 정도 소요되는 것을 확인할 수 있다.

<그림 6>의 제안하는 시스템의 분산 서비스 거부 공격 상태의 트래픽을 살펴보면 공격의 예측이 4회에 걸쳐 발생하는데 그 시점은 16초, 17초, 19초, 23초가 해당한다. 예측단계에서 공격을 판정하는 시점은 1초 이내이며 이후 차단할 때까지의 시간은 2초가량 소요된다.

제안하는 시스템의 시뮬레이션 실험 결과는 예측단계에서 차단단계까지의 전체 소요 시간기준으로 20%이내에서 향상된 것으로 판정할 수 있다.

기존 분산서비스 거부공격의 탐지 실험에 해당하는 그림5의 결과로 파생하는 특징은 86초의 시점에 공격이 발생한 후 89초에 한 번의 공격이 더 발생한 경우에 차단 완료시점인 97초까지 11초의 시간이 소요되는 것을 확인할 수 있었는데 반해 제안하는 시스템의 분산서비스 거부 공격의 예측 기법을 적용한 경우에는 19초에 3차 공격, 23초에 4차 공격이 발생했음에도 차단 완료 시점이 29초 인 것을 확인할 수 있었다. 이는 동시 공격에 대하여 예측을 통해 공격에 대비할 수 있는 가용성을 확보하여 차단 완료까지 10% 이내에서 향상된 성능을 보임을 알 수 있다. 이는 네트워크가 대형화가 된다면 더욱 향상된 성능을 보임을 입증하는 것이다.

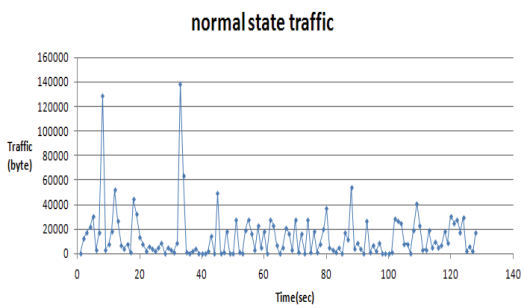

그림 4. 정상상태의 트래픽
Fig. 4. Normal state traffic

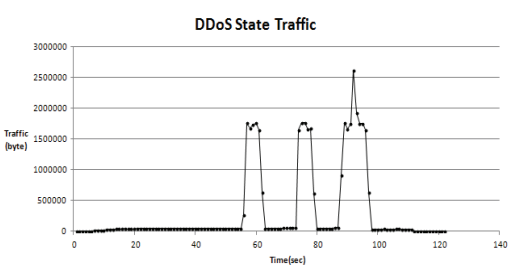

그림 5. 일반 탐지 기법 시스템을 적용한 분산 서비스 거부공격 상태의 트래픽
Fig. 5. DDoS attack state traffic of generally detect technique system

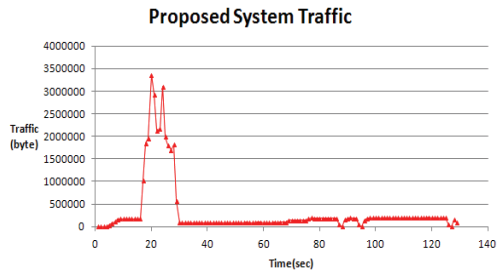

그림 6. 제안하는 시스템의 분산 서비스 거부공격 상태의 트래픽
Fig. 6. DDoS attack state traffic of proposed system

VI. 결론 및 향후 과제

본 논문에서는 이더넷 및 노드의 서비스 가용성 확보를 위해 분산 서비스 거부 공격이 발생했을 때 해당 공격의 예측을 통해 기존의 공격 탐지 기법에 비해 제안하는 모델의 탐지 성능이 향상된 것을 볼 수 있다. 특히 제안하는 예측 모델에서는 분산 서비스 거부 공격에 대하여 공격의 예측을 할 수 있는 수학적 기준을 제시하였다. 제안하는 예측모델은 특정 네트워크 환경에서 장시간 운영하여 자료의 축적량이 방대해 질수록 그 효율을 더욱 증가시킬 수 있다고 본다.

또한 본 논문의 예측 모델은 기존의 분산 서비스 거부 공격 탐지 시스템의 상위 노드에 탑재하여 사용하더라도 네트워크 플랫폼에 큰 변형없이 적용이 가능하므로 이더넷을 포함한 범용 네트워크에 활용이 가능하리라 기대된다. 향후 공격의 예측 구간에 대한 세분화에 대한 연구가 병행되어야 할 것이다.

참고문헌

[1] 이영실, 김낙현, 이훈재, “고성능 침입방지 시스템을 위해 개선한 시그니처 해싱 기반 패턴 매

칭 기법", *한국정보통신학회 추계학술대회* 2010, pp.434-437, 2010.

[2] Yun-Ji Ma, Hyun-Chul Baek, Chang-Geun Kim, and Sang-Bok Kim, "Prevention of DDoS Attacks for Enterprise Network Based on Traceback and Network Traffic Analysis," *Journal of information and communication convergence engineering*, v.7, no.2, pp. 157-163, 2009.

[3] 국윤주, 김용호, 김점구, 김귀남, "통계 기반 분산 서비스거부(DDoS)공격 탐지 모델에 관한 연구", *한국사이버테러정보전학회 정보·보안논문지*, v.9 no.2, pp.41-48, 2009.

[4] 인터넷침해사고대응지원센터, *DDoS 공격대응 가이드*, 한국인터넷진흥원(KISA), 2012.

[5] 이태진, 임채수, 임채태, 정현철, "웹서비스 대상 경량화 된 응용계층 DDoS 공격 대응 메커니즘", *한국정보보호학회논문지*, v.20, no.3, pp.99-110, 2010.

[5] 정은희, 이병관, "DDoS 공격 탐지 기법인 IPCW-IDS 설계", *한국통신학회논문지*, 제35권 제10호, pp.1443-1450, 2010.

[6] 김홍일, "제한된 트래픽 영역에서의 분산 서비스 거부(DDoS) 방어 기법", *한국엔터테인먼트산업학회논문지*, 제8권, pp.19-24, 2010.

[7] 이해동, 하현태, 백현철, 김창근, 김상복, "신뢰 호스트 상호 협력을 통한 IP 스푸핑 공격의 효율적 탐지 및 방어 모델 설계", *한국정보통신학회논문지*, v.16, no.12, pp.2649-2656, 2012.

[8] 하현태, 이해동, 백현철, 김상복, "엔터프라이즈 네트워크에서 DDoS 공격의 부하개선을 위한 큐잉 모델", *한국정보통신학회논문지*, 제15권 제1호, pp.107-114, 2011.

저자소개

하현태(Hyeon-tae Ha)

2011년 경상대학교 (공학석사)

현재 경상대학교 컴퓨터과학과 박사과정
경남과학기술대학교 컴퓨터정보센터 연구원
※ 관심분야 :네트워크, 네트워크보안

백현철(Hyun-chul Baek)

2003년 경상대학교 (공학박사)
2007년 전국지방의료원 전산기술위원장

현재 경남도립남해대학 산학협력중점교수
※ 관심분야 : 네트워크, 네트워크보안, 암호화

김상복(Sang-Bok Kim)

1989년 중앙대학교 (공학박사)
2007. 12 ~ 2010. 8 경상대학교 교육정보전산원장

1984년~현재 경상대학교 컴퓨터과학과 교수,
경상대학교 컴퓨터정보통신연구소원
※ 관심분야 : 컴퓨터네트워크 및 보안, 컴퓨터구조