Journal of Knowledge Information Technology and Systems(JKITS), Vol. 9, No. 5, pp. 545~554, October 2014

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Prediction Model of Traffic Flooding in Limited Network Environments

Sang-Woo Lee[1], Hyun-Chul Baek[2], Suk-Won Hong[3], Sang-Bok Kim[*4]

[1]*Division of Information Service Center, Gyeongnam Provincial Namhae College*
[2]*Department of Intenet Information Technology, Gyeongnam Provincial Namhae College*
[3]*Division of Academic Affairs, Gyeongnam Provincial Geochang College*
[4]*Department of Computer Science, Gyeongsang National University*

ABSTRACT

The subjective of this study is to analyze a possibility of occurring traffic flooding in order to ensure stable services as bandwidth exhausting attacks are presented to users who use limited network bandwidths. Also, a model that can improve service availability and maintain service consistency through rapid responses is proposed. As abnormal traffics occur in a limited network environment, it makes possible to quickly response to traffic flooding attacks, which may occur in future, through estimating changes in subjective traffics. For achieving it, a traffic state model in normal users is extracted as samples of continuous and discrete values in a specific range and the error between these values and its transition process are also used as prediction and detection models. Then, the detection data extracted from normal users are compared and analyzed with the traffics in bandwidth exhausting attacks. Based on the results, the availability and consistency in Internet access services are improved through rapid responses for different unexpected traffics.

KEYWORDS: abnormal traffics, floodings, attacks, DDoS, analyzings

ARTICLE INFO: Received 30 July 2014, Revised 10 October 2014, Accepted 10 October 2014.

[*]Corresponding author is with the Department of Computer Science, Gyeongsang National University, 501, Jinju-daero, Jinju-si, Gyeongsangnam-do, 660-701, KOREA.
E-mail address: sbkim@gnu.ac.kr

1. 서 론

제한된 대역폭을 사용하는 환경에서의 트래픽 폭주는 시스템 또는 회선을 무력화 시킬 수 있다. 그러므로 이러한 트래픽 폭주에 대비하여 현재 다양한 분석 방법을 이용한 탐지와 대응 기법이 사용되고 있다.

이상트래픽 탐지를 위하여 일반적으로 사용하고 있는 패턴 매칭 기법은 가용중인 네트워크상의 해당 패킷을 정상적인 상태의 패킷과 패턴 비교를 한 후 이상트래픽을 탐지하는 기법이다[1]. 즉, 트래픽 수집 후 그 특성들을 분석하여 기존 정의된 트래픽 상태와의 편차 여부를 이용하여 폭주를 탐지한다. 하지만 이러한 패턴 매칭 기법은 기존 정의된 공격 탐지를 위한 데이터베이스 정보와 일치하는 경우에만 정확한 트래픽 폭주에 대한 탐지를 할 수 있다. 반면에 데이터베이스 정보에 포함되지 않은 새로운 이상트래픽이 발생하게 되면 이에 대한 탐지가 불가능한 상황이다. 그러므로 다양한 이상트래픽 탐지를 위하여 지속적인 데이터베이스의 업데이트가 반드시 필요하다[2]. 그렇지만 통계적 기법을 이용한 이상트래픽 탐지 기법은 일정 기간 탐지를 위한 다양한 실험을 통하여 탐지 임계값을 설정한 후 트래픽의 이상 여부를 분석한다[3].

이러한 기존의 이상트래픽 탐지기법들은 일반적으로 해당 트래픽이 발생한 이후에 탐지가 가능하고, 이미 공격 상황이 어느 정도 진행된 이후에 대응이 이루어진다. 아울러 이러한 탐지 후 대응 기법은 일반적으로 공격이 발생하면 즉각적인 연결에 대한 단절 처리를 먼저 수행하기 때문에 서비스 가용성을 저하시킬 수 있다. 그러므로 본 논문에서는 이상트래픽이 발생하는 경우 이상트래픽 예측 모델에 적용하여 해당 트래픽에 대한 분석을 실시한다. 이 과정에서 기존의 일반적인 서비스 단절 후 대응 처리하는 기법을 이용하지 않고, 제안하는 예측기법을 이용하여 네트워크 서비스 가용성을 최대한 보장할 수 있도록 한다. 이를 위하여 해당 트래픽을 분석한 후 정상 트래픽은 통과 시키고, 이상트래픽은 버퍼에 저장한다. 그 과정에 즉각적인 연결에 대한 단절을 시행하지 않기 때문에 연결에 대한 재설정 과정을 줄일 수가 있다. 그 다음 트래픽 예측 모델에서 해당 이상트래픽을 분석 예측하여 효과적인 대응을 할 수 있도록 했기 때문에 안정적인 서비스 보장이 가능하도록 하였다.

본 논문의 구성은 다음과 같다. 2장 관련연구에서는 이상트래픽 탐지 시스템의 종류와 특성을 분석하고 그 문제점을 기술한다. 3장에서는 제안 모델의 예측에 필요한 정보 수집과정을 기술 하고, 4장에서는 제안하는 예측 모델과 일반적인 기존 모델에 대한 비교 분석을 하였다. 마지막으로 5장에서는 성능평가표를 통하여 본 논문에서 제안하는 탐지 예측 모델과 기존 모델과의 성능 비교를 하였다.

2. 관련연구

2.1 이상트래픽 발생 유형

일반적으로 공격에 의한 이상트래픽 발생 유형은 다음과 같이 분류할 수 있다. 즉, 대역폭을 소진시켜 정상적인 네트워크 서비스를 할 수 없도록 하는 공격과 다른 하나는 서버의 처리 능력을 넘어서는 이상트래픽을 발생시켜 서비스 기능을 마비시키는 공격이 있다.

2.2 대역폭 소진 공격

이상트래픽을 발생시켜 대역폭을 소진시키는 대표적인 공격으로는 ICMP 플루딩 공격과 SYN 플루딩 공격이 있다. ICMP 플루딩 공격은 일반적으로 대형 네트워크를 형성하고 있는 특정 사이트를 이

용하여 대량의 패킷을 공격 목표인 특정 사이트로 전송하여 대역폭을 소진시켜 정상적인 서비스를 방해하는 공격 기법으로 대표적인 기법이 스머프 공격이다[4][5][6].

SYN 플루딩 공격은 TCP 3-Way 핸드셰이킹의 약점을 이용하여 대량의 SYN 패킷을 발송하여 서버의 자원을 소진시켜 정상적인 서비스를 할 수 없도록 하는 공격 기법이다[7][8][9][10].

2.3 기존 공격에 대한 방어기법들의 문제점

기존 자원 고갈형 공격에 대한 대응 기법들은 대부분 서비스 가용성에 대한 문제점을 안고 있다. 일반적으로 이들 공격에 대한 방어 시스템들은 공격 상황을 탐지하면 네트워크 서비스 연결을 단절한 후 대응 조치를 취하는 방식이다. 이러한 탐지 지향 기법은 정상적인 사용자일 경우에도 일정시간 트래픽 사용량이 정상 대역폭 정보를 초과 할 경우 1차적으로 네트워크 서비스에 대한 단절을 시도하는 문제점을 안고 있다. 이러한 기존 대응 방식은 서버와 클라이언트 간의 네트워크 서비스 안정성에 심대한 영향을 주게 된다. 또한 공격이 발생한 후 해당 공격에 대한 탐지 및 대응 시간이 촉박한 경우가 대부분이다. 그러므로 해당 공격에 대한 방어 및 처리가 지연되는 동안 이미 대역폭 소진이나 서비스 마비가 진행되는 상황이 발생 한다. 본 논문에서는 이러한 정상 사용자들의 네트워크 서비스의 안정적인 제공과, 공격에 대한 대응 시점의 지연 문제를 개선하기 위하여, 관찰이 필요한 이상트래픽이 발생했을 때, 그 해결을 위한 버퍼 개념을 도입하였다. 즉, 이상트래픽에 대한 즉각적인 단절보다 공격으로 의심되는 이상트래픽들을 해당 처리 버퍼에 저장한 후 일정 시간 동안 이상트래픽 발생 횟수, 해당 이상트래픽의 그래프 변화 정도를 나타내는 기울기 변이를 이용하여 공격에 대한 안정적이고 빠른 탐지와 예측, 그리고 방어가 가능하도록 하였다.

3. 공격 예측을 위한 정보 수집

본 논문에서는 이상트래픽에 대한 판정을 위하여 정상적인 상황 하에서 특정 시간대의 이상트래픽 발생 빈도수와 그 지속 시간을 측정하였다. 이는 정상적인 네트워크 서비스 상태에서도 이상트래픽은 항상 발생할 수 있기 때문에 일정 시간 동안 이상트래픽 발생 횟수를 측정한 것이다. 여기서 분석을 위한 전체 이상트래픽 측정 횟수를 T_{AC_MAX}로 정의하고 횟수에 대한 임계치는 $T_{AC_MAX}-1$로 정한다. 일반적으로 트래픽 폭주를 유발시키는 공격자는 사전 시뮬레이션 공격을 시도하기 때문에, 특정 시간대의 이상트래픽의 발생 빈도수를 측정하면 트래픽 폭주 공격에 대한 예측을 할 수 있기 때문이다. 그 다음 이상트래픽이 발생했을 때 해당 트래픽의 기울기 변이를 추적하여 정상적인 상황에서의 트래픽 변이에 대한 기울기 정보와 비교한다. 즉, 트래픽 폭주 공격 시 해당 공격에 대한 트래픽 변이 정보의 기울기가 급격하게 변하는 상황과 비교하기 위한 것이다. 이를 바탕으로 트래픽 폭주 공격에 대한 예측 시나리오를 다음과 같이 정의할 수 있다. 본 논문에서는 특정 시간대의 이상트래픽 빈도수를 T_{AC_n}으로, 이상트래픽이 발생했을 경우 해당 트래픽에 대한 기울기의 평균 변화율을 T_{GA_n}, 순간 변화율을 T_{GM_n}로 정의한다. T_{AC_n}은 발생하는 이상트래픽 빈도수가 임계치 $T_{AC_MAX}-1$이 될 때까지의 카운트를 위하여 사용하였다. 그리고 T_{GA_n}, T_{GM_n}은 빈도수가 임계치 $T_{AC_MAX}-1$이 될 때까지 각각의 빈도수에 대한 전체 누적 평균값 $T_{GA\_MAX-1\_AVG}$,

$T_{GM_MAX-1_AVG}$를 구하는데 사용하였다. 그리고 이상트래픽이 감지 될 경우 해당 빈도수 카운트를 위하여 AT_count_n을 사용하였다. AT_count_n에서의 각각의 평균 변화율 $AT_T_{GA_n}$과 순간 변화율 $AT_T_{GM_n}$을 사용하였다. 그러므로 $T_{GA\_MAX-1\_AVG}$, $T_{GM_MAX-1_AVG}$을 구하는 식은 다음과 같다.

$$T_{GA\_MAX-1\_AVG} = (AT\_T_{GA\_1} + AT\_T_{GA\_2} + \cdots\cdots AT\_T_{GA\_n})/n \quad (1)$$

$$T_{GM\_MAX-1\_AVG} = (AT\_T_{GM\_1} + AT\_T_{GM\_2} + \cdots\cdots AT\_T_{GM\_n})/n \quad (2)$$

본 논문에서는 이러한 트래픽 폭주 공격에 대한 예측과 네트워크 서비스의 안정적인 서비스를 위하여 다음과 같은 예측 시스템 모델을 제안하며, 그 순서도는 다음의 <그림 1>과 같다.

<그림 1>은 이상트래픽 발생 시점부터 해당 트래픽의 처리와 대응 과정을 순서도로 표현한 것이다. 먼저 이상트래픽이 발생하게 되면 해당 트래픽 빈도수를 저장할 AT_count_n 변수를 초기화 시키고, 이상트래픽이 감지되면 해당 빈도수 AT_count_n을 증가시킨다. 그 다음 시스템의 개방 포트를 탐색하고 인가된 트래픽 여부를 검사한 후 해당 트래픽만 통과 시킨다. 그리고 인가된 트래픽 측정 과정 중 일정시간 동일 포트에서 발생하는 비정상적인 트래픽 빈도수를 $T_{AC_MAX}-1$에 도달할 때 까지 구한다. 그런 다음 이상트래픽에 대한 빈도수가 최대값 T_{AC_MAX} 가 되면, 해당 이상트래픽의 기울기의 평균 변화율 T_{GA_MAX}, 순간 변화율 T_{GM_MAX}와 비교하여 해당 트래픽에 대한 네트워크 서비스 지속 여부를 결정한다. 즉 T_{AC_n}이 $T_{AC\_MAX}-1$ 이하의 상태를 유지하면 서비스를 계속 유지하고, T_{AC_MAX}상태이면 $T_{AC_MAX}-1$까지 에서 구한 $T_{GA\_MAX-1\_AVG}$, $T_{GM_MAX-1_AVG}$와 T_{AC_MAX}상태의 T_{GA_MAX}, T_{GM_MAX}와 비교한다.

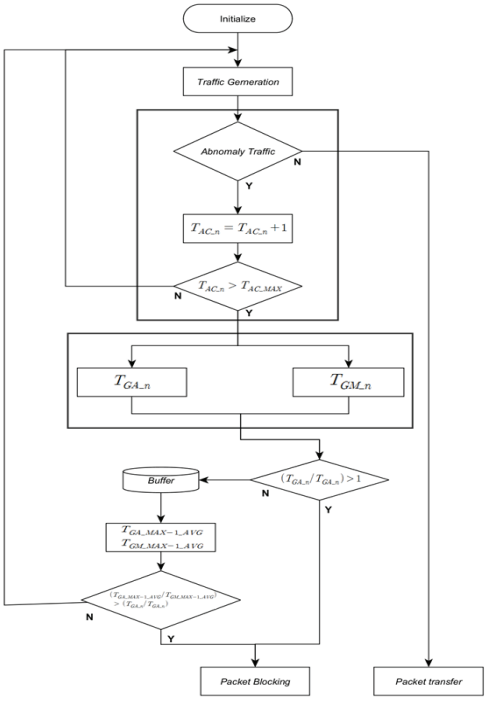

그림 1. 제안 시스템 순서도
Figure 1. Proposed System Flowchart

여기서 각각의 비교 결과가 그 이하이면 지속적인 관찰, 그 이상이면 즉각적인 침입예측 모드로 진입하고 해당 트래픽 폭주 공격을 예측하고 대응을 한다. 지속적인 관찰 상태의 작업에는 일시적인 과부하인지 웜/바이러스, 또는 대역폭 소진 공격 여부에 대한 분석을 한다. 만일 일시적으로 최대 빈도수를 넘어선 과부하인 경우는 정상적인 서비스 연결을 지속시키고, 웜/바이러스일 경우에는 치료 과정을 거친다. 하지만 지속적으로 클라이언트로부터 해당 웜/바이러스를 수신할 수 있기 때문에 이를 클라이언트로 통보하여 클라이언트 또한 해

당 웜/바이러스에 대한 치료를 할 수 있도록 한다. 만일 웜/바이러스가 아닌 대역폭 소진 공격으로 판단되면 즉각적인 차단을 한다. 차단을 위한 자료는 정상적인 상황에서 네트워크 상황을 분석하여 획득하게 되는데 그 정보는 다음과 같다. 먼저 특정 시간 영역당 발생하는 이상트래픽의 빈도수, 이상트래픽이 발생 했을 경우 그 변이를 나타내는 기울기의 순간 변화율과 평균 변화율에 대한 분석값들의 평균, 이상트래픽 발생 최종 시점일 때 해당 트래픽그래프에서 발생하는 기울기의 순간 변화율과 평균 변화율에 대한 측정값들을 필요로 한다. 현재 일반적인 트래픽 소진 공격에 대한 연구는 일정시간 동안 발생하는 트래픽 측정치를 공격 판정을 위한 임계값으로 설정하여 이용하고 있다. 즉, 특정 시점의 임계치 초과 여부만을 적용하여 이상트래픽에 대한 분석과 대응을 하고 있다.

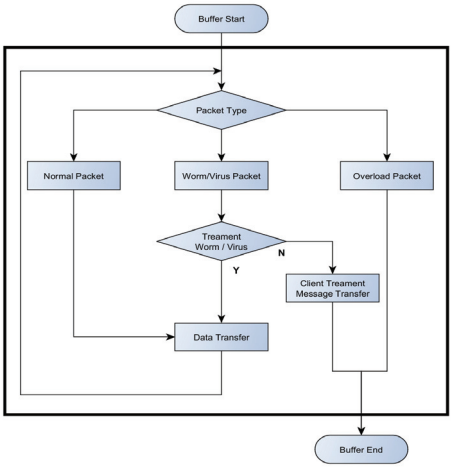

그림 2. 이상트래픽 처리 버퍼
Figure 2. Abnormal Traffic Process Buffer

본 논문에서 제안하는 대응 모델은 기존의 일반적인 대응 모델과 비교하여, 1차적으로 해당 이상트래픽의 빈도수를 이용하고, 이를 통한 이상트래픽 그래프의 기울기 변이가 급속하게 변하는 지점에서 즉각적인 대응 모듈의 동작을 한다. 그러므로 공격에 대한 신속한 대응과 안정적인 서비스 지속성을 유지할 수 있다. <그림 2>는 이상트래픽이 발생 했을 경우 기존의 즉각적인 연결에 대한 단절을 실행하지 않고, 해당 트래픽의 처리 과정을 도식화한 것이다.

4. 제안 모델 분석

4.1 평균 트래픽 변화율 획득 과정

제안 시스템 모델의 탐지를 위한 정상 트래픽과 관련한 데이터베이스 정보는 방어 시스템에서 운용중인 개방된 포트의 측정을 통하여 획득하였으며 그 이름을 OP_n으로 정의하였다. 해당 포트들의 정상적인 트래픽 측정은 도착 패킷의 길이로 정하고 그 값은 OPt_length_re로 하여 이들의 합을 구한 후 단위 시간별로 누적하여 해당 노드의 전체 단위 시간별 트래픽 양으로 표시하고 그 식은 다음과 같다.

$$OPt\_tot\_x = OPt\_len\_re\_x1 + OPt\_len\_re\_x2 + \\ ..... + OPt\_len\_re\_xn \quad (3)$$

위의 식(3)에서 OPt_tot_x는 해당 포트의 정상적인 트래픽 발생에 대한 전체적인 합을 의미하고, x는 트래픽을 발생시키고 있는 포트를 의미한다. 특정 네트워크를 이용한 대역폭 소진 공격자들이 이용하는 공격 대상은 일반적으로 방어시스템에서 허용하고 있는 포트들이라고 할 수 있다. 이들 포트들을 본 논문에서는 OP_acc_x라 하고 이들 각각에 번호를 붙여 필요 정보를 획득한다. 예를 들어 웹서버와 관련한 포트를 방어시스템에서 허용한다고 가정하면 이 포트를 OP_acc_80으로 표현한 형식을 사용하여 각각의 포트에서 발생하는 트

래픽에 대한 공격여부를 판정하는 변수로 설정하였다. 그 다음 공격에 대한 판정 과정은 트래픽에 대한 임계값과 이상트래픽이 발생하는 빈도수를 이용하였다. 즉, 제한된 환경에서의 일반적인 트래픽 사용량과 특정 시간대의 이상트래픽 발생 빈도수를 분석하여 이상트래픽이 발생할 때 마다 해당 트래픽들의 순간, 평균값 들을 합산하여 전체 이상 빈도수들의 합에 대한 평균값을 구한다. 이후 임계값의 극한을 초과하는 순간변화율이 발생할 때 공격상태로 판정한다. 이를 위한 식은 다음과 같다.

$$OP\_acc\_x = \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x} = \lim_{x \to 0} \frac{G(a+\Delta x) - G(a)}{\Delta x} = \lim_{h \to 0} \frac{G(a+h) - G(a)}{h} \quad (4)$$

(4)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 $G(a)$가 $G(a+\Delta x)$까지 얼마나 변했는지 판정 가능하다. 또한 이 값은 x의 증분에 대한 변화율을 의미하므로 극한으로 표현할 수 있다. 그 다음 순간변화율로 발생한 미분계수를 시간의 구간별로 산정하여 이들의 평균변화율을 구한다.

$$OP\_acc\_x = \left| \frac{\sum_{\delta y}^{y'} \lim_{\gamma y \to b} \frac{G(lt-b) - G(kt-b)}{b}}{\sum_{\delta x}^{x'} \lim_{h \to 0} \frac{G(a-mh) - G(a+mh)}{h}} \right| \quad (5)$$

4.2 트래픽 소진 공격 예측

공격 여부의 판정은 이상트래픽에 대한 빈도수가 최대값 T_{AC_MAX}에 도달하는 시점에서 이루어진다. 이때 T_{AC_MAX}에서의 평균 변화율 T_{GA_MAX}와 순간 변화율 T_{GM_MAX}, $T_{AC_MAX}-1$까지 구한 $T_{GA_MAX-1_AVG}$와 $T_{GM_MAX-1_AVG}$간의 비교를 한다. 그 결과 각각의 비교 값이 $T_{AC_MAX}-1$에서의 평균값을 넘어서면 공격으로 예측한다. 아울러 T_{AC_MAX}에 도달하는 시점의 평균 변화율 T_{GA_MAX}와 순간 변화율 T_{GM_MAX}가, $T_{AC_MAX}-1$에서의 $T_{GA\_MAX-1\_AVG}$ 와 $T_{GM\_MAX-1\_AVG}$ 이하일 경우 지속적 관찰을 위하여 이에 대한 영역 설정을 한다. 관찰 영역에서는 분석을 일정시간 진행하게 되는데, 이때 해당 비교 값이 $T_{GA_MAX-1_AVG}$와 $T_{GM\_MAX-1\_AVG}$ 을 넘어서게 경우 공격으로 예측한다.

5. 시뮬레이션 및 결과 비교

5.1 시뮬레이션

제안하는 논문은 시뮬레이션을 통하여 결과를 살펴보고자 한다. 시뮬레이션 환경은 OPNET 과 VC++ 6.0 커맨드라인 컴파일러를 사용하였으며 1Hour의 시뮬레이션 시간을 사용하였다. 시뮬레이션 레이아웃은 <그림 3>과 같다.

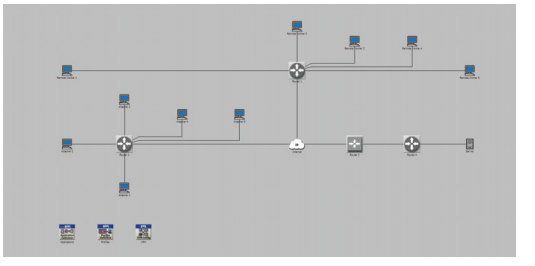

그림 3. 시뮬레이션 레이아웃
Figure 3. Simulation Layout

시뮬레이션 레이아웃은 Attacker 스테이션을 5대, Remote Worker 스테이션 5대를 각각 배치하고 시뮬레이션 결과 분석은 각 1대씩을 선택하여 분석하였다.

제안하는 시스템은 Router3에서 구현하였으며 각각의 트래픽은 Client Http 측에서 측정하였다. Client Http 측의 측정값 중 Attacker1에 해당하는 트래픽 차트는 다음의 <그림 4>와 같다.

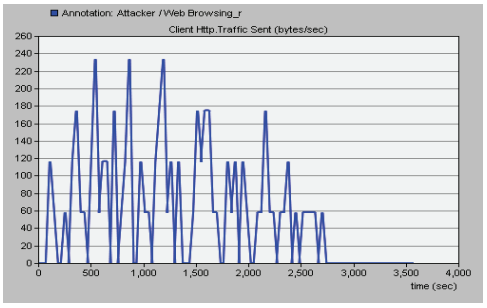

그림 4. Attacker 1 시뮬레이션 결과
Figure 4. Attacker 1 Simulation result

Attacker 1이 전송하는 트래픽에서 공격의 임계값으로 설정한 150byte/sec초과 트래픽은 총 10회 동안 발생하였다. 그리고 $T_{GA\_MAX-1\_AVG}$ 와 $T_{GM\_MAX-1\_AVG}$ 값에 대한 예측 임계값을 넘어서는 시각이 2160초 지점이다. 이후 공격의 차단이 완료되는 시각은 2700초 지점이다.

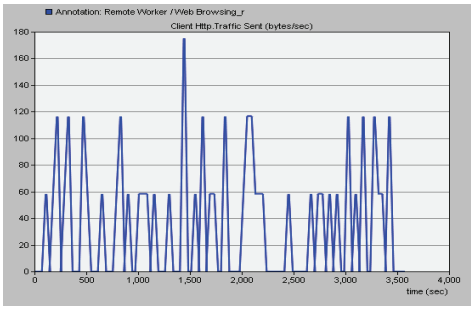

그림 5. Remote Worker 1 시뮬레이션 결과
Figure 5. Remote 1 Simulation Result

이에 반해 동일한 1Hour 시뮬레이션 시간동안 Remote Worker 1이 전송하는 트래픽이 일시적으로 이상트래픽을 발생시키더라도 <그림 5>와 같이 즉각적인 차단 없이 정상 운영되는 형태를 보이고 있다.

5.2 시뮬레이션 결과 비교 분석

본 논문에서는 대역폭 소진 공격과 관련하여 기존 일반적 대응 방식의 특징과 제안하는 방식의 특징을 테이블 형태로 <표 1>에서 비교 분석하였다.

표 1. 탐지 및 대응속도 측면
Table 1. Aspect of Detection and Response Time

구분	일반적인 탐지/대응 모델	제안 모델
분석 임계값 이하	연결 서비스 가능	연결 서비스 가능
임계값 이상 트래픽 발생 시 대응	일시적 이상트래픽일 경우에도 즉각 단절	이상트래픽에 대한 빈도수 이용으로 즉각 단절 없음
필요 탐지 정보	판정에 필요한 임계값 및 분석 시간 요구	이상트래픽 빈도수, 트래픽 그래프의 기울기 변화 정보
대응 속도	탐지에 필요한 일정시간 경과 후 대응	최종 빈도수일 경우 즉각적인 대응이 이루어지므로 빠른 대응 가능
탐지 오류 빈도수	빈번	감소

<표 1>의 탐지 및 대응 속도 측면을 보면 기존 모델은 탐지를 위하여 항상 일정 탐지 시간을 요구하고 있다. 그러므로 탐지를 하더라도 해당 대역

폭 소진 공격에 대응하기에는 이미 늦은 경우가 많다. 그렇지만 본 논문에서 제안하는 모델은 탐지를 위한 일정 시간을 요구하지 않고 이상트래픽에 대한 발생 빈도수를 분석 한 후 이를 넘어서는 경우 즉각적인 대응이 이루어지므로 기존 탐지 및 대응 모델보다 보다 빠른 탐지 및 대응이 가능하다. 그리고 일시적으로 트래픽이 폭주하는 경우에도 이상트래픽 빈도수를 이용하여 즉각적인 단절보다 서비스 안정성을 고려하고 있다.

6. 결론 및 향후 과제

본 논문에서는 대역폭 소진 공격이 발생할 경우 제한된 네트워크 환경에서의 노드 상호간 연결 서비스의 안정성을 위하여 이상트래픽 빈도수와 트래픽 그래프를 이용하고 있다. 이를 통하여 일반적인 공격 탐지 및 대응 기법과 비교했을 때 제안 모델이 안정적인 서비스, 탐지에 대한 오류 감소, 빠른 탐지 및 대응 기능이 있음을 알 수 있다. 또한 본 논문에서 제안하는 모델은 제한된 특정 네트워크 환경에서 일정시간 정상적으로 운영한 자료를 분석하여 사용하기 때문에 탐지 및 대응에 대한 효율성이 높다고 할 수 있다. 그리고 본 논문에서 제안하는 모델은 일반적인 대역폭 소진 공격에 대한 방어 시스템에 쉽게 응용이 가능하다. 그러므로 다양한 네트워크 플랫폼 환경에도 적용이 가능하다고 본다. 향후 연구과제로는 좀 더 다양한 네트워크 환경과 새로운 공격 기법에 능동적으로 대응할 수 있는 방어 시스템 연구가 요구되어진다.

References

[1] T.-W. Kim, J.-I. Jung, and J.-Y. Lee, *DoS/DDoS attacks detection algorithm and system using packet counting*, Journal of The Korea Society For Simulation, Vol. 19, No. 4. pp. 151-159, 2010.

[2] Y,-J. Ma, H.-C. Baek, C.-G. Kim, and S.-B. Kim, *Prevention of DDoS attacks for enterprise network based on traceback and network traffic analysis*, Journal of information and communication convergence engineering, Vol. 7, No. 2. pp. 157-163, 2009.

[3] J.-W. Kim, I.-J. Choi, T.-Y. Shim, and C.-S. Oh, *Flow based traffic flooding attack detection for reducing false negative*, Journal of The Korean Institute of Information Technology, Vol. 10, No. 3, pp. 149-159, 2012.

[4] J.-W. Seo, and J. Kwak, *The design of Anti-DDos system using defense on depth*, Journal of Korea Institute of Information Security and Cryptology, Vol. 22, No. 3. pp. 679-689, 2012.

[5] J.-I Lee, J.-W. Kim, and C.-S. Oh, *DDoS attack detection algorithm using dynamic threshold*, Journal of The Korea Entertainment Industry Association, Vol. 2, No. 2. pp. 57-63, 2008.

[6] K. Choudhary, Meenakshi, and Shilpa, Smurf Attacks: Attacks using ICMP, International Journal of Computer Sci ence and Technology, Vol. 2, No. 1. pp. 75-77, 2011.

[7] H.-T. Ha, H.-C. Baek, and S.-B. Kim, *Forecasting model for DDoS attacks in enterprise networks*, Journal of Knowledge Information Technology and Systems, Vol. 8, No. 3. pp. 57-64, 2013.

[8] H.-D. Lee, H.-T. Ha, H.-C. Baek, C.-G. Kim, and S.-B. Kim, *Efficient detction and defence model against IP spoofing attack through cooperation of trusted hosts,* Journal of the

Korea Institute of Information and Communication Engineering, Vol. 16, No. 12. pp. 2649-2656, 2012.

[9] H.-T. Ha, H.-D. Lee, H.-C. Baek, and S.-B. Kim, *Queueing model for traffic loading improvement of DDoS attacks in enterprise networks*, Journal of The Korean Institute of Maritime Information and Commucation Sciences, Vol. 15, No. 1. pp. 107-114, 2011.

[10] H.-S. Choi and M.-S. Jun, *DDoS TCP syn flooding backscatter analysis algorithm*, Journal of The Korea Society of Computer and Information, Vol. 14, No. 9. pp. 55-66, 2009.

제한된 네트워크 환경에서의 트래픽 폭주 예측 가능 모델

이상우[1], 백현철[2], 홍석원[3], 김상복[4]

[1]*경남도립남해대학 정보지원센터*
[2]*경남도립남해대학 인터넷정보기술과*
[3]*경남도립거창대학 교무부 정보지원팀*
[4]*경상대학교 컴퓨터과학과*

요 약

본 논문은 제한된 네트워크 대역폭을 이용하는 사용자들에게 대역폭 소진 공격이 발생 했을 경우, 서비스의 안정적인 보장을 위하여 트래픽 폭주가 발생할 가능성을 예측 분석한다. 그리고 신속한 대응 조치를 통하여 서비스 가용성을 향상 시키고 서비스 지속성을 유지할 수 있는 모델을 제안한다. 본 논문은 제한된 네트워크 환경 하에서 이상트래픽이 발생할 경우 해당 트래픽 변이를 분석 예측하여 향후 발생 가능한 트래픽 폭주 공격에 대하여 신속한 대응을 할 수 있도록 하였다. 이를 위하여 정상적인 사용자들의 트래픽 상태 모형을 일정 영역 범위에서 연속적인 값과 이산적인 값으로 표본 추출하여 이들 간의 편차와 변이 과정을 예측과 탐지 모델로 이용하였다. 그런 다음 대역폭 소진 공격이 발생하게 되면 이들 해당 트래픽과 정상 사용자들로부터 표본 추출한 탐지 자료와 비교 분석을 한다. 이를 통하여 다양한 이상트래픽 발생 상황에 대하여 보다 빠르게 대응함으로써 인터넷 접속 서비스의 가용성과 지속성을 향상시킬 수 있도록 하였다.

Sang Woo Lee received the Master´s degree in the Department of Computer Science from Gyeongsang National University in 2012. His current research interests include network architecture, network security.

E-mail address: swlee@namhae.ac.kr

Hyun Chul Baek received the Ph.D. degree in the Department of Computer Science from Gyeongsang National University in 2003. He was a chairman in the Committee of Computer System technology at The Korea Association of Regional Public Hospital in 2007. He has been a professor in the Department of Intenet Information Technology, Gyeongnam Provincial Namhae College since 2013. His current research interests include network, network security, encryption, bigdata security, cloud computing. He is a member of the KKITS.

E-mail address: dosi_gas@lycos.co.kr

Suk Won Hong received the Ph.D. degree in the Department of Computer Science from Gyeongsang National University in 2011. His current research interests include network, multimedia.

E-mail address: swhong@gc.ac.kr

Sang Bok Kim received the Ph.D. degree in the Department of Electronics Engineering from Chung-ang University in 1989. He was a director in the Department of Education Information Computer Center at The Gyeongsang National University from 2007 to 2010. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1984. He has been a researcher in the Computer Data Communication Research Institute at The Gyeongsang National University since 1984. His current research interests include computer network and security, computer system architecture. He is a member of the KKITS.

E-mail address: sbkim@gnu.kr