



(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.

H04L 12/24 (2006.01)

H04L 12/28 (2006.01)

(11) 공개번호 10-2006-0130892

(43) 공개일자 2006년12월20일

(21) 출원번호 10-2005-0049207

(22) 출원일자 2005년06월09일

심사청구일자 2005년06월09일

(71) 출원인 한국과학기술원
대전 유성구 구성동 373-1

(72) 발명자 김세현
대전 유성구 구성동 한국과학기술원 산업공학과
김현우
대전 유성구 구성동 한국과학기술원 산업공학과
정석봉
대전 유성구 구성동 한국과학기술원 산업공학과

(74) 대리인 오병석

전체 청구항 수 : 총 5 항

(54) 광대역 네트워크에서의 분산 서비스 거부 공격 탐지 및 대응 방법

(57) 요약

본 발명은 광대역 네트워크에 있어서의 분산 서비스 거부(DDoS) 공격 탐지 및 대응 방법에 관한 것으로, 각 라우터에서 출력 큐의 패킷 손실 확률을 구하는 단계와, 출력 큐의 손실 확률이 소정의 임계치 이상이거나 또는 상기 출력 큐로 들어오는 패킷의 도착률과 출력 큐의 대역폭의 비가 1 이상인 경우, 상기 출력 큐의 라우터가 하류측 라우터들에게 혼잡 상황임을 알리는 경고 메시지를 보내는 단계와, 상기 경고 메시지를 공격 대상을 포함하고 있는 말단 라우터로 전송하는 단계와, 상기 말단 라우터가 상기 경고 메시지를 기초로 공격 경로를 재구성하는 단계 및 상기 말단 라우터가 상기 재구성된 공격 경로 중 상기 말단 라우터로부터 가장 멀리 떨어진 라우터들에게 패킷 여과를 요청하는 메시지를 보내는 단계를 포함한다.

대표도

도 1

특허청구의 범위

청구항 1.

광대역 네트워크에 있어서의 분산 서비스 거부(DDoS) 공격 탐지 및 대응 방법에 있어서,

- (1) 각 라우터에서 출력 큐의 패킷 손실 확률을 구하는 단계와,
- (2) 출력 큐의 손실 확률이 소정의 임계치 이상이거나 또는 상기 출력 큐로 들어오는 패킷의 도착률과 출력 큐의 대역폭의 비가 1 이상인 경우, 상기 출력 큐의 라우터가 하류측 라우터들에게 혼잡 상황임을 알리는 경고 메시지를 보내는 단계;
- (3) 상기 경고 메시지를 공격 대상을 포함하고 있는 말단 라우터로 전송하는 단계;
- (4) 상기 말단 라우터가 상기 경고 메시지를 기초로 공격 경로를 재구성하는 단계; 및
- (5) 상기 말단 라우터가 상기 재구성된 공격 경로 중 상기 말단 라우터로부터 가장 멀리 떨어진 라우터들에게 패킷 여과를 요청하는 메시지를 보내는 단계를 포함하는 방법.

청구항 2.

제1항에 있어서,

상기 단계(1)의 상기 출력 큐의 패킷 손실 확률은,

$$\pi_{MMIK}(\lambda_j) = \begin{cases} \frac{(1-\rho_j)\rho_j^K}{1-\rho_j^{K+1}}, & \text{if } \rho_j \neq 1 \\ \frac{1}{K+1}, & \text{if } \rho_j = 1 \end{cases}$$

여기서, $\rho_j = \frac{\lambda_j}{\mu_j}$, K는 j번째 출력 큐의 용량, λ_j 는 j번째 출력 큐에 들어가는 패킷의 도착률이고, μ_j 는 j번째 출력 큐의 대역 폭.

청구항 3.

제1항에 있어서,

상기 경고 메시지는 라우터의 네트워크의 주소를 포함하는 방법.

청구항 4.

제1항에 있어서,

상기 단계 (4)에서 상기 출력 큐의 패킷 손실 확률이 상기 소정의 임계치보다 작아질 때 까지 패킷 여과를 수행하고,

(5) 상기 출력 큐의 패킷 손실 확률이 상기 소정의 임계치보다 작아지면 패킷 여과가 종료되었음을 알리는 메시지를 주변 라우터로 전송하는 단계를 더 포함하는 방법.

청구항 5.

제4항에 있어서, (5-1) 상기 말단 라우터가 그로부터 가장 멀리 떨어진 라우터로부터 상기 패킷 여과가 종료되었음을 알리는 메시지를 수신하면, 공격 경로를 재구성하는 단계를 더 포함하는 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 통신 네트워크의 분산 서비스 거부(DDoS) 공격 탐지 및 대응 방법에 관한 것이다. 보다 구체적으로, 본 발명은 서비스거부 공격을 트래픽의 혼잡 현상으로 보고 이러한 비정상적 트래픽을 효율적으로 제어하는 DDoS 공격 탐지 및 대응 방법에 관한 것이다.

서비스 거부(Denial of Service; 이하 "DoS") 공격이란, 목적 망/서버에 유해 트래픽을 유입시켜 네트워크의 서비스 기능을 일시적으로 또는 완전히 정지시키는 공격 방식을 말한다. DoS 공격의 한 형태인 DDoS(Distributed Denial of Service) 공격은, 분산 설치된 다수의 공격 프로그램이 서로 통합된 형태로 목적 망/서버에 트래픽을 집중시키는 공격으로서 일반적인 DoS 공격에 비해 탐지가 어려울 뿐만 아니라 훨씬 더 강력한 파괴력을 가지고 있다. 이러한 DDoS 공격은 다량의 유해 트래픽으로 네트워크 전체의 자원을 고갈시키는 한편 네트워크에 심각한 부하를 주어 해당 네트워크를 마비시키기도 한다.

DDoS 공격을 탐지하고 예방하는 기존의 방법으로서, 패턴에 기반한 필터링(pattern-based filtering) 기술이나 큐 관리(queue management)와 같은 방법들이 있다. 이러한 기존의 방법들은 주로 네트워크 상의 트래픽을 관찰하고 트래픽의 손실량을 이용하여 DDoS 공격이 있는지를 탐지한다. 그러나, 공격 프로그램들은 공격 트래픽의 양과 패킷 내의 필드 정보를 쉽게 바꿀 수 있기 때문에, 필터링의 측정치가 될 수 있는 DDoS 패킷의 공통 특징을 찾아내기 어려울 뿐만 아니라, 공격자에게서 온 트래픽의 패턴을 감지할 수 있다 하더라도 공격에 능동적으로 대응하기는 어렵다는 문제점이 있다.

한편, DDoS 공격에 대한 기존의 대응 방법은 크게 푸시백(pushback) 기법과 공격 근원지 역추적(traceback) 기법으로 분류된다.

먼저, 푸시백 기법은, 라우터(router)가 공격으로 의심되는 집합적인 트래픽을 봉쇄하는 작업을 허용하는 방식의 기법으로서, 주로 속도 제한(rate limiting) 기법을 사용한 라우터 사이의 협업 과정을 통해 공격을 예방한다. 그러나, 이 기법은 DDoS 공격자들이 인터넷상에 잘 분포되어 있을 때는 효과적이지 않다는 사실이 이미 알려져 있다.

근원지 역추적 기법은, 패킷(packet)의 근원지 정보에 의존하지 않고 별도의 역추적 메시지를 생성하여 공격 주소지를 역추적하는 기법이다. 예컨대, 한국특허 제456635호는, 공격이 있음을 알리는 경보가 있는 경우 역추적 센서를 생성하여 파송함으로써 공격 호스트를 역추적하고 이 공격 호스트의 트래픽을 차단하는 DDoS 공격 대응 시스템과 그 방법을 개시하고 있다. 그러나, 이 기법은 네트워크의 부하를 증가시키고 DDoS 공격에 능동적으로 대응할 수 없다는 문제점이 알려져 있다. 또한, 상기 특허에는 DDoS 공격이 있음을 탐지하는 방법에 관하여서는 기재되어 있지 않다.

이와 같이, DDoS 공격을 신속하게 탐지하고, 이를 차단하거나 공격의 근원지를 역추적하는 등 DDoS 공격에 대한 효과적인 대응 방안은 매우 부족한 현실이다.

발명이 이루고자 하는 기술적 과제

본 발명은 큐잉 모델을 이용함으로써 신속하게 DDoS 공격을 탐지해 내고 공격의 근원지를 정확하게 역추적하는 DDoS 공격 탐지 방법을 제공하는 것을 목적으로 한다. 또한, 본 발명은 임계치를 조정하는 것만으로 근원지 추적의 정확도 및 필터링을 수행하는 라우터의 수 등을 조절할 수 있는 DDoS 공격 탐지 방법을 제공하는 것을 목적으로 한다.

본 발명의 다른 목적은, 말단(edge) 라우터가 혼잡이 최초로 발생한 라우터로 하여금 패킷 여과를 수행하도록 하고, 공격이 완화된 경우에는 패킷 여과를 중단함으로써 라우터들의 부담을 줄이는 DDoS 공격 대응 방법을 제공하는 것이다.

발명의 구성

본 발명에서는 네트워크의 병목현상 및 정상적인 서비스 제공 능력을 저하시키는 이러한 서비스 거부 공격을 트래픽 혼잡 현상으로 이해하고 이러한 비정상적 트래픽을 효율적으로 제어하기 위한 메커니즘을 제안한다. 이러한 메커니즘은 대기행렬 모형에 기초하여 개발되었다. 또한, 이러한 메커니즘을 이용하여 지역적으로 관찰되는 DDoS 공격의 탐지 결과를 네트워크의 각 라우터들이 서로 교환하고, 이를 이용한 전역적인 탐지 및 방어를 수행하는 DDoS 탐지 및 패킷 필터링 방법을 제안한다. 이하 본 발명의 바람직한 실시예에 관하여 상세히 설명한다.

도1은 네트워크 상에서의 DDoS 공격의 유형을 설명한다. 일반적으로 DDoS 공격은 깔대기 모양의 트래픽 흐름을 갖게 된다. 공격의 근원지들은 마치 깔대기의 입구와 같이 네트워크 상에 넓게 분포되어 있으며, 이러한 근원지들로부터 발생한 공격 패킷들은 네트워크 중간의 경유 라우터를 거치면서 공격 대상을 포함하고 있는 말단(edge) 라우터로 집중된다.

이와 같은 공격 유형을 고려하여, 본 발명은 말단 라우터로 하여금 공격의 발생 여부 및 특성을 파악하도록 한다. 말단 라우터가 공격 패킷들을 모두 관찰할 수 있기 때문에, 말단 라우터로 하여금 공격의 발생 여부 및 특성을 파악하도록 하는 것이 가장 효과적이기 때문이다. 한편, 본 발명은 공격의 대응 기법인 패킷 여과가 공격 근원지 네트워크에서 일어나도록 한다. 이렇게 함으로써, 공격 패킷이 네트워크로 유입되는 것 자체를 차단하여 네트워크 자원이 낭비되는 것을 방지할 수 있다.

즉, 본 발명은 DDoS 공격의 특성을 이용하여 말단 라우터에서 공격을 탐지하고, 말단 라우터에서 가장 멀리 떨어진, 즉, 공격 근원지와 가장 가까운 라우터에서 패킷 여과를 수행할 수 있도록 한 것이다.

광대역 네트워크에서 DDoS 공격을 탐지하기 위해서는 네트워크 상의 각 라우터가 트래픽을 관찰할 필요가 있다. 본 발명은 트래픽의 손실 정도를 파악하기 위해 패킷(packet) 손실량이 아닌 패킷 손실 확률을 이용한다. 또한, 각 라우터에서의 출력 큐(queue)의 패킷 손실 확률을 측정하기 위해 본 발명에서는 출력 큐를 싱글 서버(single-server) 큐잉 모델인 M/M/1/K 큐잉 모델로 디자인한다.

M/M/1/K 큐잉 모델에서, 출력 큐의 대역폭이 μ_j 이고, 큐에 들어가는 패킷의 도착률이 λ_j 이고, 큐의 용량이 K라고 할 때, j 번째 출력큐의 패킷 손실 확률은 다음과 같이 정의된다.

$$\pi_{MM1K}(\lambda_j) = \begin{cases} \frac{(1-\rho_j)\rho_j^K}{1-\rho_j^{K+1}}, & \text{if } \rho_j \neq 1 \\ \frac{1}{K+1}, & \text{if } \rho_j = 1 \end{cases}$$

여기서, $\rho_j = \frac{\lambda_j}{\mu_j}$ 이다. j번째 큐는 $\pi(\lambda_j) \geq \alpha$ 이거나 $\rho_j \geq 1$ 인 경우 혼잡한 상황으로 간주되고, 상기 큐에 직접 연결된 하류측 라우터로 경고 메시지를 전달한다. 상기 임계치 α 를 조정함으로써 공격 탐지 수준을 제어할 수 있고, 이에 따라 네트워크의 상황에 맞는 DDoS 공격 탐지가 가능하도록 하며 공격에 대한 대응 수준도 조절할 수 있다.

아래의 표1은 본 발명에서 사용하는 알고리즘에 사용하는 몇가지 시스템 변수를 설명한다.

[표 1]

표시법	설명
-----	----

I_n	AM을 보내고, 직접적으로 라우터의 입력 큐에 연결되어 있는 상위 라우터들의 집합.
J	특정 경유 라우터의 출력 큐의 집합.
J_C	특정 라우터의 혼잡한(congested) 출력 큐들의 집합. ($J_c = \{j \in J \mid \pi(\lambda_j) \geq \alpha \text{ or } \rho \geq 1\}$)
J_N	특정 라우터의 정상적인 상태의 출력 큐의 집합. ($J_N = J - J_C$)
DR_j	j 번째 출력 큐에 직접적으로 연결되어 있는 하류측 라우터.
UR_i	i 번째 입력 큐에 직접적으로 연결되어 있는 상류측 라우터.
T_{sleep}	라우터가 혼잡을 확인하지 않는 시간 주기.
P_n	RAP(Reconstructed Attack Paths), 즉, 공격 경로를 구성하는 라우터들의 집합. 아래 첨자는 RAP의 인덱스.
U	P_n 의 인덱스의 집합.
t_n	P_n 을 구성하는 라우터 중 말단 라우터로부터 가장 멀리 떨어져 있는 라우터.
λ_j^F	j 번째 출력 큐로 송신되는 패킷들의 여과율.
$\lambda_j^{\overline{F}}$	j 번째 출력 큐에 대해서 라우터가 패킷 여과를 할 때, j 번째 출력 큐로 입력되는 패킷의 비율.

한편, 표2는 본 발명이 제안하는 알고리즘에 있어서 라우터들 사이에 교환되는 메시지들을 설명한다. 표2의 메시지들은 ICMP(Internet Control Message Protocol) 패킷을 통해 구현 가능하다.

[표 2]

메시지 이름	설명
AM (Alarm Message)	라우터가 혼잡을 감지했을 때 하류측 라우터들에게 보내는 경고(alarm) 메시지. 라우터가 AM을 하류측 라우터들로 전송할 때, 이 AM에는 AM을 보내는 라우터의 네트워크 주소가 붙는다.
IM (Ignore Message)	주변 라우터들에게 혼잡을 무시해야 한다는 것을 알리는 메시지.
RPFM (Message for Requesting Packet Filtering)	말단 라우터가 경유 라우터에게 공격 패킷을 여과하도록 요청하는 메시지. 이 메시지는 말단 라우터에서 수행하는 전역적 탐지 결과인 공격 패킷의 특성을 포함한다.
APFM (Message for Accepting Packet Filtering)	RPFM을 받은 라우터가 RPFM을 보낸 말단 라우터에게 패킷 여과 요청을 수용함을 알리는 메시지이며, 이 메시지를 보낸 후 패킷 여과를 수행.
SPFM (Message for Stopping Packet Filtering)	말단 라우터가 경유 라우터에게 패킷 여과를 중단하도록 요청하는 메시지.
IPFM (Message for Ignoring Packet Filtering)	경유 라우터가 말단 라우터에게 패킷 여과가 필요없거나 패킷 여과가 중지되었음을 알리는 메시지.

본 발명의 DDoS 탐지 및 대응 방법은, 네트워크의 라우터들이 출력 큐의 패킷 손실 확률을 통해 네트워크의 혼잡 상황을 감지하고, 이를 네트워크에 존재하는 다른 라우터들에게 알려서 최종적으로 말단(edge) 라우터가 DDoS 공격의 근원지에 가장 가까운 라우터에게 패킷 여과(filtering)를 지시하여 네트워크의 혼잡 상황을 피하는 과정을 포함한다.

이러한 과정을 각 상황별로 살펴보면 다음과 같다.

<경유 라우터에서 특정 출력 큐에서 혼잡이 발생했을 때의 처리 과정>

단계1. 만약 혼잡이 $j^* \in J_N$ 인 곳에서 감지되면 J_C 를 $J_C \cup \{j^*\}$ 로 갱신한다. 그렇지 않은 경우에는 갱신을 중단한다.

단계2. 만약 $I_A \neq \emptyset$ 이면, $i \in I_A$ 인 UR_i 로부터의 모든 AM들을 DR_{j^*} 로 전송하고 단계4를 수행한다. 그렇지 않은 경우에는 단계3을 수행한다.

단계3. 모든 AM들을 DR_{j^*} 로 보낸 후, 단계4를 수행한다.

단계4. T_{sleep} 동안 j^* 의 혼잡 검사를 중단한다.

<경유 라우터가 UR_{i^*} 로부터의 AM을 받았을 때의 처리 과정>

단계1. 만약 라우터가 패킷 여과를 수행하고 있다면, $j \in J_C$ 인 것에 대해 AM을 DR_j 로 전송한다. 만약, $J_C \neq \emptyset$ 이면, 여과된 패킷의 목적지인 말단 라우터로 AM을 전송하고 단계3을 수행한다. 그렇지 않은 경우에는 단계2를 수행한다.

단계2. $J_C = \emptyset$ 이면, UR_{i^*} 로 IM을 보내고 중단한다.

단계3. UR_{i^*} 로부터 $j \in J_C$ 인 모든 DR_j 들에게 AM을 전송한다.

단계4. I_A 를 $I_A \cup \{UR_{i^*}\}$ 로 갱신한다.

<경유 라우터가 DR_{j^*} 로부터 IM을 받았을 때의 처리 과정>

단계1. J_C 를 $J_C - \{j^*\}$ 로 갱신한다.

단계2. T_{sleep} 동안 j^* 의 혼잡 검사를 중단한다.

<경유 라우터에서 $j^* \in J_C$ 인 곳의 혼잡이 사라졌을 때의 처리 과정>

단계1. J_C 를 $J_C - \{j^*\}$ 로 갱신한다.

단계2. DR_{j^*} 로 IM을 보낸다.

<경유 라우터가 UR_{i^*} 로부터 전송된 IM을 받았을 때의 처리 과정>

단계1. I_A 를 $I_A - \{UR_{i^*}\}$ 로 갱신한다.

<경유 라우터가 DR_{j^*} 로부터 전송된 RPFM을 받았을 때의 처리 과정>

단계1. 만약 j^* 가 J_C 에 속하지 않으면 IPFM을 말단 라우터로 보낸다. 그렇지 않은 경우에는 단계2를 수행한다.

단계2. 만약 라우터가 RPFM의 목적지였다면 단계2-1을 수행하고, 그렇지 않은 경우에는 단계3을 수행한다.

단계2-1. APFM을 말단 라우터로 보낸다.

단계2-2. $\pi(\lambda_{j^*}^F + \lambda_{j^*}^{\bar{F}}) \geq \alpha$ 가 될 때까지, 공격 특성을 가지고 말단 라우터로 전송되는 패킷의 여과를 수행한다.

단계2-3. IM을 DR_{j^*} 로 보내고, J_C 를 $J_C - \{j^*\}$ 로 갱신한다.

단계2-4. $\pi(\lambda_{j^*}^F + \lambda_{j^*}^{\bar{F}}) \geq \alpha$ 가 된 후, IPFM을 말단 라우터에게 보낸다.

단계3. RPFM을 목적지 라우터로 전송한다.

단계4. J_C 를 $J_C - \{j^*\}$ 로 갱신하고 T_{sleep} 동안 j^* 의 혼잡 검사를 중단한다.

<경유 라우터가 DR_{j^*} 로부터 전송된 SPFM을 받았을 때의 처리 과정>

단계1. 만약 라우터가 SPFM의 목적지이면 단계2를 수행하고, 그렇지 않은 경우에는 그 목적지로 전송한다.

단계2. 말단 라우터를 향하고 공격 성향이 있는 패킷에 대한 여과를 중단한다.

단계3. J_C 를 $J_C - \{j^*\}$ 로 갱신한다.

단계4. T_{sleep} 동안 j^* 의 혼잡 검사를 중단한다.

<말단 라우터가 UR_{i^*} 로부터 전송된 AM을 받았을 때의 처리 과정>

단계1. 기존의 ACC(Aggregated-based Congestion Control) 방식을 사용하여 전역적 탐지를 수행하고, 만약 현재 공격이 진행 중라고 판단되면 단계2를 수행한다. 그렇지 않은 경우에는 중단한다.

단계2. 전송된 AM을 기초로 P_n 을 재구성한다.

단계3. $P_n = P_u$ 인 $u \in U$ 가 존재한다면, AM을 무시하고 중단한다. 그렇지 않은 경우에는 단계4를 수행한다.

단계4. $P_n \supseteq P_u$ 인 $u \in U$ 가 존재한다면, P_n 을 구성하는 라우터들을 통해 RPFM을 t_n 으로, SPFM을 t_u 로 보낸다. 그렇지 않은 경우에는 단계5를 수행한다.

단계5. P_n 을 구성하는 라우터들을 통해서 RPFM을 t_n 으로 보낸다.

<말단 라우터가 t_n 으로부터 전송된 APFM을 받았을 때의 처리 과정>

단계1. U 를 $U \cup \{n\}$ 으로 갱신한다.

<말단 라우터가 t_n 으로부터 전송된 IPFM을 받았을 때의 처리 과정>

단계1. U를 $U-\{n\}$ 으로 갱신한다.

이상 살펴본 바와 같이, 본 발명은 DDoS 공격을 대량의 트래픽으로 인한 혼잡 상황으로 보아 출력 큐를 싱글 큐잉 모델로 디자인하고 출력 큐의 패킷 손실 확률을 이용하여 DDoS 공격을 탐지하기 때문에, 패킷 손실율을 이용하는 기존의 방법에 비해 빠른 공격 탐지가 가능하다. 또한, 네트워크 상의 라우터들이 정보를 서로 공유하고 협업함으로써 공격 근원지를 보다 정확하게 찾을 수 있다.

또한, 임계치인 α 를 조정함으로써 공격 탐지의 정도 및 필터링을 수행하는 라우터의 숫자 등을 조절할 수 있다.

발명의 효과

본 발명은 DDoS 공격의 특성을 이용하여 말단 라우터에서 공격을 탐지하고, 말단 라우터에서 가장 멀리 떨어진, 즉, 공격 근원지와 가장 가까운 라우터에서 패킷 여과를 수행할 수 있도록 함으로써, DDoS 공격을 효과적이면서 정확히 탐지하고 네트워크의 자원 손실을 최소화하면서 DDoS 공격에 대응할 수 있다.

또한, 본 발명에 의하면, 단일 서버 큐잉 모델을 이용함으로써, 기존의 패킷 손실율을 이용한 다른 기법들에 비해, 네트워크의 패킷 손실이 일어나거나 네트워크가 마비되기 전에 보다 빠른 공격 탐지가 가능하다.

또한, 네트워크 상의 라우터들이 정보를 서로 공유하고 협업함으로써 실질적인 공격 근원지를 보다 정확하게 추적하는 것이 가능하고, 간단한 파라미터를 조정하는 것만으로 공격 근원지 탐색 및 방어 수준을 조절하는 것이 가능하다.

도면의 간단한 설명

도1은 네트워크 상에서의 DDoS 공격의 유형을 설명하는 간략도.

도면

