(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0060655
(43) 공개일자 2012년06월12일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) *H04L 12/56* (2006.01)
(21) 출원번호 10-2010-0122263
(22) 출원일자 2010년12월02일
심사청구일자 없음

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
김학서
대전광역시 중구 서문로 96, 210동 1604호 (문화동, 센트럴파크)
강경순
대전광역시 유성구 노은동로 187, 608동 104호 (지족동, 열매마을6단지)
(뒷면에 계속)
(74) 대리인
양문옥

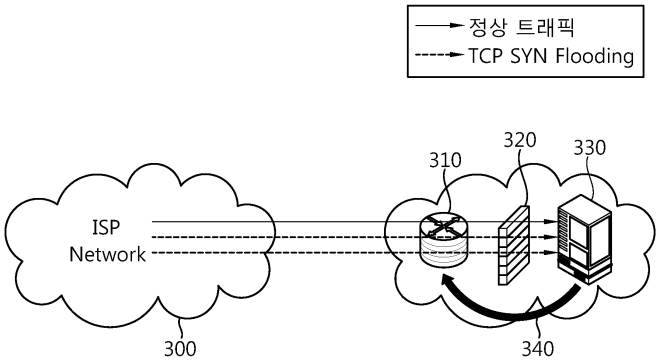
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **서버 공격을 탐지할 수 있는 라우팅 장치와 라우팅 방법 및 이를 이용한 네트워크**

(57) 요 약

본 발명은 서버 공격 탐지 기능을 갖는 라우팅 장치와 이 라우팅 장치에서 서버 공격을 탐지하는 방법으로서, 라우팅 장치는 네트워트상에서 전송되는 패킷을 수신하는 수신부, 패킷을 전송 경로를 따라 송신하는 송신부, 운용에 필요한 데이터 및/또는 정보를 저장하는 메모리부 및 네트워크상에서 패킷의 전송 경로를 설정하고 설정된 전송 경로에 따라서 패킷 스위칭을 수행하는 제어부를 포함하며, 수신부는 네트워크상의 서버들로부터 소정의 시간마다 서버의 상태 정보를 수신하고, 메모리부는 수신한 서버의 상태 정보를 저장하며, 제어부는 수신한 서버의 상태 정보를 기반으로, 서버의 상태 변화를 산출하고, 서버의 상태 변화가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단한다.

대 표 도 - 도3



(72) 발명자

황강욱

대전광역시 서구 둔산로 155, 크로바아파트 105동 703호 (둔산동)

조현제

경상북도 구미시 봉곡남로20길 15, 현대 I-Park 204동 1105호 (봉곡동)

이명우

부산광역시 동래구 쇠미로 198, 502호 (온천동, 한맥타운)

이 발명을 지원한 국가연구개발사업

과제고유번호	10035125
부처명	지식경제부/방송통신위원회
연구사업명	정보통신산업원천기술개발사업
연구과제명	엔터프라이즈용 Smart Border 라우터 개발
주관기관	한국전자통신연구원
연구기간	2010.03.01 ~ 2011.02.28

특허청구의 범위

청구항 1

네트워트상에서 전송되는 패킷을 수신하는 수신부;

상기 패킷을 전송 경로를 따라 송신하는 송신부;

운용에 필요한 데이터 및/또는 정보를 저장하는 메모리부; 및

네트워크상에서 패킷의 전송 경로를 설정하고 상기 설정된 전송 경로에 따라서 패킷 스위칭을 수행하는 제어부를 포함하며,

상기 수신부는 네트워크상의 서버들로부터 소정의 시간마다 서버의 상태 정보를 수신하고,

상기 메모리부는 수신한 서버의 상태 정보를 저장하며,

상기 제어부는 수신한 서버의 상태 정보를 기반으로, 서버의 상태 변화를 산출하고, 상기 서버의 상태 변화가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 서버 공격 탐지 기능을 갖는 라우팅 장치.

청구항 2

제1항에 있어서, 상기 서버의 상태 정보는 상기 서버의 CPU 부하에 관한 정보이며,

상기 제어부는 상기 서버의 CPU 부하 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 서버 공격 탐지 기능을 갖는 라우팅 장치.

청구항 3

제1항에 있어서, 상기 서버의 상태 정보는 상기 서버의 메모리 이용률에 관한 정보이며,

상기 제어부는 상기 서버의 메모리 이용량의 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 서버 공격 탐지 기능을 갖는 라우팅 장치.

청구항 4

제1항에 있어서, 상기 서버의 상태 정보는 백로그 큐(backlog queue)에 관한 정보이며,

상기 제어부는 상기 서버의 백로그 큐에 대기 중인 접속 요청의 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 서버 공격 탐지 기능을 갖는 라우팅 장치.

청구항 5

제1항에 있어서, 상기 서버의 상태 정보는 백로그 큐(backlog queue)에 관한 정보이며,

상기 제어부는 상기 서버의 백로그 큐에 대기 중인 접속 요청의 수가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 서버 공격 탐지 기능을 갖는 라우팅 장치.

청구항 6

제1항에 있어서, 상기 제어부는 서버가 공격을 받고 있다고 판단한 경우에, 해당 서버에 대한 트래픽을 조절하는 것을 특징으로 하는 서버 공격 탐지 기능을 갖는 라우팅 장치.

청구항 7

제1항에 있어서, 상기 제어부는 서버가 공격을 받고 있다고 판단한 경우에, 네트워크의 관리자 및/또는 해당 서버의 관리자에게 이를 통지하는 것을 특징으로 하는 서버 공격 탐지 기능을 갖는 라우팅 장치.

청구항 8

네트워크상의 서버들로부터 소정의 시간마다 서버의 상태 정보를 수신하는 단계;

상기 소정의 시간마다 수신한 서버의 상태 정보를 기반으로 서버의 상태 변화를 산출하는 단계;

상기 산출한 서버의 상태 변화를 기반으로 상기 서버가 공격당하고 있는지를 판단하는 단계; 및

상기 서버가 공격당하고 있다고 판단한 경우에는, 상기 서버에 대한 트래픽을 조정하는 단계를 포함하는 네트워크 라우팅 장치에서의 서버 공격 탐지 방법.

청구항 9

제8항에 있어서, 상기 서버의 상태 정보는 상기 서버의 CPU 부하에 관한 정보이며,

상기 서버가 공격당하고 있는지 판단하는 단계에서는,

상기 서버의 CPU 부하의 증가량이 소정의 기준치보다 큰 경우에 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 네트워크 라우팅 장치에서의 서버 공격 탐지 방법.

청구항 10

제8항에 있어서, 상기 서버의 상태 정보는 상기 서버의 메모리 이용률에 관한 정보이며,

상기 서버가 공격당하고 있는지 판단하는 단계에서는,

상기 서버의 메모리 이용률의 증가량이 소정의 기준치보다 큰 경우에 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 네트워크 라우팅 장치에서의 서버 공격 탐지 방법.

청구항 11

제8항에 있어서, 상기 서버의 상태 정보는 상기 서버의 백로그 큐에 관한 정보이며,

상기 서버가 공격당하고 있는지 판단하는 단계에서는,

상기 서버의 백로그 큐에 대기 중인 접속 요청의 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 네트워크 라우팅 장치에서의 서버 공격 탐지 방법.

청구항 12

제8항에 있어서, 상기 서버의 상태 정보는 상기 서버의 백로그 큐에 관한 정보이며,

상기 서버가 공격당하고 있는지 판단하는 단계에서는,

상기 서버의 백로그 큐에 대기 중인 접속 요청의 수가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 네트워크 라우팅 장치에서의 서버 공격 탐지 방법.

청구항 13

네트워크상에서 패킷의 전송 경로와 트래픽을 제어하는 라우팅 장치; 및

상기 네트워크상의 서버들을 포함하며,

상기 라우팅 장치는,

상기 네트워크상의 서버들로부터 서버의 상태 정보를 수신하는 수신부;

수신한 서버의 상태 정보를 저장하는 메모리부; 및

수신한 서버의 상태 정보를 기반으로, 서버의 상태 변화를 산출하는 제어부를 포함하며,

상기 서버들은 소정의 시간마다 서버의 상태에 관한 정보를 상기 라우팅 장치에 송신하고,

상기 라우팅 장치의 제어부는 상기 서버의 상태 변화가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 네트워크.

청구항 14

제13항에 있어서, 상기 서버의 상태 정보는 상기 서버의 CPU 부하에 관한 정보이며,

상기 라우팅 장치의 제어부는 상기 서버의 CPU 부하 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공

격을 받고 있다고 판단하는 것을 특징으로 하는 네트워크.

청구항 15

제13항에 있어서, 상기 서버의 상태 정보는 상기 서버의 메모리 이용률에 관한 정보이며,

상기 라우팅 장치의 제어부는 상기 서버의 메모리 이용률의 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징을 하는 네트워크.

청구항 16

제13항에 있어서, 상기 서버의 상태 정보는 백로그 큐에 관한 정보이며,

상기 라우팅 장치의 제어부는 상기 서버의 백로그 큐에 대기 중인 접속 요청의 수가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 네트워크.

청구항 17

제13항에 있어서, 상기 서버의 상태 정보는 백로그 큐에 관한 정보이며,

상기 라우팅 장치의 제어부는 상기 서버의 백로그 큐에 대기 중인 접속 요청의 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단하는 것을 특징으로 하는 네트워크.

청구항 18

제13항에 있어서, 상기 라우팅 장치의 제어부는, 상기 서버 중의 어느 하나가 공격을 받고 있다고 판단한 경우에는 해당 서버에 대한 트래픽을 조정하는 것을 특징으로 하는 네트워크.

명 세 서

기 술 분 야

[0001] 본 발명은 네트워크상의 서버를 보호하기 위한 방법에 관한 것으로서, 더 구체적으로는 네트워크상의 라우팅 장치에서 서버들에 대한 공격을 탐지하고 이에 대응하는 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷을 비롯한 네트워크 기술이 발달함에 따라서, 네트워크상의 취약점을 노리는 공격도 증가하고 있다. 네트워크상의 공격은 점차 무차별적이고 자동화되어 가고 있다.

[0003] 이런 공격들의 유형은 크게 3 가지로, 시스템의 취약점을 이용하거나 소프트웨어로 구현되는 버그를 이용하는 방법, 공격 대상이 이용할 수 있는 자원을 모두 소모하게 하는 방법, 가용 대역폭을 모두 소모하게 하는 방법 등이 있다.

[0004] 특히 인터넷의 경우는 네트워크 보안이 상호 의존적이므로 보안이 침해된 곳을 통해 다른 호스트들을 공격하기 용이하다. 또한, 인터넷의 호스트, 네트워크 등은 모두 제한된 자원을 가지고 운용되기 때문에, 처리 대역폭, 작업 처리량, 저장 용량 등이 모두 제한되어 있어, 공격의 대상이 되기 쉽다. 비연결적인 IP(Internet Protocol)의 성질은 침입자를 추적을 어렵게 만든다.

[0005] 이와 함께, 네트워크상에서 서비스를 보장하기 위한 대부분의 기능이 종단의 호스트에 위치하며, 중간 노드는 패킷을 전달하는 등의 제한된 기능만을 가지고 있으므로, 네트워크 공격에 대한 부담은 대부분 종단의 호스트에 가중된다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 네트워크상의 서버에 대한 공격을 효과적으로 탐지하는 방법을 제공하고자 한다.

[0007] 본 발명은 네트워크상의 서버에 대한 공격을 네트워크 인입단(引入端)에 위치한 라우팅 장치에 탐지하여 효과적으로 대응할 수 있는 방법을 제공하고자 한다.

[0008] 본 발명은 네트워크상의 서버에 대한 공격을 효과적으로 탐지하고 대응할 수 있는 라우팅 장치를 제공하고자 한다.

과제의 해결 수단

[0009] 본 발명의 일 양태로서 서버 공격 탐지 기능을 갖는 라우팅 장치는 네트워트상에서 전송되는 패킷을 수신하는 수신부, 패킷을 전송 경로를 따라 송신하는 송신부, 운용에 필요한 데이터 및/또는 정보를 저장하는 메모리부 및 네트워크상에서 패킷의 전송 경로를 설정하고 설정된 전송 경로에 따라서 패킷 스위칭을 수행하는 제어부를 포함하며, 수신부는 네트워크상의 서버들로부터 소정의 시간마다 서버의 상태 정보를 수신하고, 메모리부는 수신한 서버의 상태 정보를 저장하며, 제어부는 수신한 서버의 상태 정보를 기반으로, 서버의 상태 변화를 산출하고, 서버의 상태 변화가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단한다.

[0010] 상기 서버의 상태 정보는 상기 서버의 CPU 부하에 관한 정보일 수 있으며, 제어부는 서버의 CPU 부하 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단할 수 있다.

[0011] 상기 서버의 상태 정보는 상기 서버의 메모리 이용률에 관한 정보일 수 있으며, 제어부는 서버의 메모리 이용량의 증가량이 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단할 수 있다.

[0012] 상기 서버의 상태 정보는 백로그 큐(backlog queue)에 관한 정보일 수 있으며, 제어부는 서버의 백로그 큐에 대기 중인 접속 요청의 증가량 또는 서버의 백로그 큐에 대기 중인 접속 요청의 수가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단할 수 있다.

[0013] 상기 제어부는 서버가 공격을 받고 있다고 판단한 경우에, 해당 서버에 대한 트래픽을 조절할 수 있다.

[0014] 상기 제어부는 서버가 공격을 받고 있다고 판단한 경우에, 네트워크의 관리자 및/또는 해당 서버의 관리자에게 이를 통지할 수 있다.

[0015] 본 발명의 다른 양태로서, 네트워크 라우팅 장치에서의 서버 공격 탐지 방법은 네트워크상의 서버들로부터 소정의 시간마다 서버의 상태 정보를 수신하는 단계, 소정의 시간마다 수신한 서버의 상태 정보를 기반으로 서버의 상태 변화를 산출하는 단계, 산출한 서버의 상태 변화를 기반으로 서버가 공격당하고 있는지를 판단하는 단계 및 서버가 공격당하고 있다고 판단한 경우에는 서버에 대한 트래픽을 조정하는 단계를 포함한다.

[0016] 본 발명의 또 다른 양태로서의 네트워크는, 네트워크상에서 패킷의 전송 경로와 트래픽을 제어하는 라우팅 장치 및 네트워크상의 서버들을 포함하며, 라우팅 장치는, 네트워크상의 서버들로부터 서버의 상태 정보를 수신하는 수신부, 수신한 서버의 상태 정보를 저장하는 메모리부 및 수신한 서버의 상태 정보를 기반으로, 서버의 상태 변화를 산출하는 제어부를 포함하며, 서버들은 소정의 시간마다 서버의 상태에 관한 정보를 라우팅 장치에 송신하고, 라우팅 장치의 제어부는 서버의 상태 변화가 소정의 기준치보다 큰 경우에는 해당 서버가 공격을 받고 있다고 판단한다.

발명의 효과

[0017] 본 발명에 의하면, 네트워크상의 서버에 대한 공격을 효과적으로 탐지할 수 있다.

[0018] 본 발명에 의하면, 네트워크상의 서버에 대한 공격을 네트워크 인입단(引入端)에 위치한 라우팅 장치에 탐지하여 효과적으로 대응할 수 있다.

[0019] 본 발명에 따른 라우팅 장치는 네트워크상의 서버에 대한 공격을 효과적으로 탐지하고 대응할 수 있다.

도면의 간단한 설명

[0020] 도 1은 DDoS 공격의 예를 개략적으로 도시한 개념도이다.

도 2는 TCP의 연결 설정 방법을 개략적으로 설명하는 순서도이다.

도 3은 본 발명에 따라서 분산 서비스 거부 방식의 공격을 탐지하고 트래픽을 조정하는 것을 개략적으로 설명하는 개념도이다.

도 4는 라우팅 장치에서 분산 서비스 거부 방식의 공격을 탐지하고 이에 대응하는 방법을 개략적으로 설명하는 순서도이다.

도 5는 본 발명에 따른 라우팅 장치의 기능적인 구성을 개략적으로 도시한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 본 발명은 서버들이 서비스를 제공하는 네트워크의 인입단에 위치한 라우팅 장치에서 각 서버들을 보호하는 방법에 관한 것이다.

[0022] 또한, 본 발명은 서버들이 서비스를 제공하는 네트워크에서 각 서버를 보고하기 위한 라우팅 장치에 관한 것이다.

[0023] 라우팅 장치는 네트워크상의 각 서버로부터 서버의 현재 상태에 관한 정보(이하, '서버의 상태 정보'라 함)를 수신한다. 라우팅 장치는 서버의 상태 정보를 이용하여 해당 서버가 현재 공격받고 있는지를 판단할 수 있다. 라우터는 공격받고 있는 것으로 판단한 서버에 대해서는 트래픽(traffic)을 조정할 수 있다. 라우터가 해당 서버에 대한 트래픽을 적정한 수준으로 감소시킴에 따라, 해당 서버는 원래의 서비스를 계속 수행할 수 있다. 라우터는 해당 서버가 공격당하고 있다는 것을 관리자에게 통지할 수 있다. 이에 따라서 관리자는 네트워크 운용을 위해 필요한 조치를 취할 수 있다.

[0024] 일반적으로 분산 서비스 거부 공격(Distributed Denial of Service: DDoS, 이하 'DDoS'라 함)은 네트워크상의 각종 서버와 같은 공격 대상에 순간적으로 다량의 데이터를 송신함으로써 공격 대상이 정상적으로 동작하지 못하게 한다.

[0025] 도 1은 DDoS 공격의 한 예를 개략적으로 도시한 개념도이다.

[0026] 악성 바이러스 등에 감염된 PC들(100)은 ISP(Internet Service Provider) 네트워크(110)를 통해 대량의 트래픽을 발생시킨다. 일반적인 라우터(120)는 유입되는 트랙픽을 패킷의 전송 경로를 따라서 방화벽(130)과 공격 대상(140)이 위치한 네트워크로 보낸다.

[0027] 대량의 트래픽 유입으로 인해, 방화벽(130)과 공격 대상(140) 등은 부하(load)를 감당하지 못하고 다운되거나, 정상적으로 기능하지 못하게 된다.

[0028] DDoS 공격은 ICMP 플러딩(Flooding), UDP 플러딩, TCP 플러딩, TCP SYN 플러딩 등이 있다.

[0029] ICMP(Internet Control Message Protocol) 플러딩 방법은 ICMP 에코 요청(Echo Request) 메시지를 브로드캐스트 주소로 보냄으로써, 모든 시스템이 에코 응답 메시지를 공격 대상에게 전송하게 한다. 공격 대상은 모든 요청을 처리하기 위해 시스템 자원을 소모하게 되며, 결국 시스템이 기능을 상실한다.

[0030] UDP(User Datagram Protocol) 플러딩 방법은 대량의 UDP 패킷을 공격 대상의 IP로 전송하는 방법이다. 공격자는 목적지 포트를 지정하여 UDP 패킷을 전송한다. UDP 패킷을 수신한 호스트들은, 해당 포트에 대한 애플리케이션을 찾기 시작한다. 대응하는 애플리케이션을 찾지 못하면, UDP 패킷의 소스 주소로 설정된 공격 대상에게 도달 불능(unreachable) 메시지를 전송하며, 대량의 메시지로 인해 공격 대상의 시스템이 기능을 상실한다.

[0031] TCP(Transmission Control Protocol) 플러딩 역시 대량의 TCP 패킷을 공격 대상의 IP로 전송하는 방법으로서, 기본적으로 UDP 플러딩과 동일한 방법이다.

[0032] TCP SYN 플러딩 방법은 TCP 연결 설정 방식의 취약점을 이용한 방법이다. 공격자는 공격 대상에게 연결을 요청하는 TCP 패킷을 전송한 후, 연결 설정을 위한 ACK 메시지를 보내지 않는다. 공격 대상은 연결 설정을 위해 대기 상태에 머무르게 되며 연결 설정을 위한 메모리 공간인 백로그 큐의 용량이 모두 소진되게 된다.

[0033] 이하, 분산 서비스 거부(DDoS) 공격 방식의 가장 대표적인 예인 TCP SYN 플러딩을 통해 본 발명이 적용되는 일 예를 설명한다.

[0034] TCP는 소정의 규칙(3 Way Handshaking)에 따라서 연결 설정의 신뢰성을 유지한다. 도 2는 이 소정의 규칙(3 Way Handshaking)에 따른 TCP의 연결 설정 방법을 개략적으로 설명하는 순서도이다.

[0035] 클라이언트는 접속을 요청하는 SYN 메시지를 서버에게 전송한다(S210). 서버는 클라이언트의 SYN 메시지를 수신하고, 클라이언트의 SYN 메시지에 대한 ACK 메시지와 함께 접속을 요청하는 SYN 메시지를 클라이언트에게 전송한다(S220). 이때, 서버는 클라이언트로부터의 해당 접속 요청을 백로그 큐(backlog queue)에 대기시킨다.

[0036] 클라이언트는 서버로부터 ACK 메시지와 SYN 메시지를 수신하면, 서버와의 연결을 설정(connection establishment)한다(S230). 클라이언트는 서버로부터 수신한 ACK 메시지와 SYN 메시지에 대한 ACK 메시지를 서버에게 전송한다(S240). 서버는 클라이언트로부터 ACK 메시지를 수신하고, 클라이언트와의 연결을 설정한다

(S250).

[0037] 서버가 클라이언트에 ACK 메시지와 SYN 메시지를 전송하면, 클라이언트로부터의 ACK 메시지가 수신될 때까지 해당 접속 요청은 백로그 큐에 반 오픈(half-open) 상태로 대기한다. 서버가 클라이언트로부터 ACK 메시지를 수신하면, TCP 연결이 설정되고, 백로그 큐에서 해당 접속 요청이 삭제된다. 서버가 클라이언트로부터 일정 시간 동안 ACK 메시지를 수신하지 못하면, 해당 접속 요청은 백로그 큐에서 삭제되고 TCP 접속이 설정되지 않는다.

[0038] 이때, 공격자가 다수의 클라이언트 컴퓨터를 이용하여 SYN 메시지를 서버에 전송하고, SYN 메시지와 ACK 메시지를 수신한 뒤에, ACK 메시지를 전송하지 않고 계속해서 SYN 메시지를 전송하는 경우에는, 서버의 백로그 큐가 계속된 전송 요청에 의해 가득차게 된다. 따라서 서버는 더 이상의 서비스 접속 요청을 받아들일 수 없게 되므로, 서비스 거부 상태가 된다.

[0039] TCP SYN 플러딩은 TCP의 동작 특성을 이용하는 공격이다. 즉, TCP의 연결 방식을 그대로 따르고 있으므로, 네트워크상에서 공격을 미리 탐지하기 어렵다. 서버가 데미지를 받은 뒤에 공격이 있었던 것을 파악하게 되면, 대응은 그만큼 어려워지고 데미지는 커진다.

[0040] 하지만, 상술한 TCP SYN 플러딩에 관한 설명에서 확인할 수 있듯이, 소위 분산 서비스 거부 방식의 공격이 있는 경우에는 시스템의 상태, 특히 서버의 상태가 변화한다. 예를 들어, TCP SYN 플러딩의 경우에는 공격 대상의 백로그 큐의 상태가 급격히 증가하게 된다. 또한, 공격 대상에 대한 트래픽 내지는 공격 대상이 처리해야 하는 프로세스를 급격히 증가시키게 되므로, CPU 부하나 메모리 이용률과 같은 공격 대상의 상태가 크게 변하게 된다.

[0041] 따라서 일정 주기로 또는 정해진 조건에 따른 시기에 서버의 CPU 부하, 서버의 백로그 큐의 접속 요구 대기량, 서버의 메모리 이용률 등과 같은 상태 정보를 확인하여, 분산 서비스 거부 방식의 공격을 탐지할 수 있다.

[0042] 본 발명에서는 네트워크의 인입단에 위치하는 라우팅 장치에서 네트워크상의 각 서버로부터 서버의 현재 상태에 관한 정보를 수신하고 이를 이용하여 공격을 받고 있는 서버가 있는지를 탐지할 수 있다. 또한, 공격받고 있는 서버가 있다고 판단한 경우에는, 라우팅 장치에서 해당 서버로 나가는 트래픽을 감소시키거나 차단함으로써 해당 서버가 지속적으로 기능을 유지하도록 할 수 있다.

[0043] 따라서 라우팅 장치의 후단에 위치하는 각종 방화벽 또는 방어 시스템의 정상적인 작동을 유도할 수 있고, 공격 대상이 기능을 상실하지 않도록 보호할 수 있다.

[0044] 특정 대상에 대한 공격 때문에, 전체 트래픽을 모두 감소시키거나 차단하지 않고, 라우팅 장치가 공격 대상으로 나가는 트래픽만을 감소시킬 수 있으므로, 네트워크상의 다른 서버들이 공격에 의해 영향을 받지 않도록 할 수 있다.

[0045] 이하, 도면을 참조하여 본 발명의 일 실시 형태에 대하여 구체적으로 설명한다. 각 도면의 구성 요소들에 참조 부호를 부가함에 있어서, 동일한 구성 요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 명세서의 실시예를 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 명세서의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0046] 또한, 본 명세서의 구성 요소를 설명하는데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다. 어떤 구성 요소가 다른 구성 요소에 "연결", "결합" 또는 "접속"된다고 기재된 경우, 그 구성 요소는 그 다른 구성요소에 직접적으로 연결되거나 접속될 수 있지만, 각 구성 요소 사이에 또 다른 구성 요소가 "연결", "결합", "접속"될 수도 있다고 이해되어야 할 것이다.

[0047] 또한 본 명세서에서 설명하는 내용 중, 통신 네트워크에서 이루어지는 작업은 해당 통신 네트워크를 관할하는 시스템(예를 들어 서버 또는 미디어 센터)에서 네트워크를 제어하고 데이터를 송신하는 과정에서 이루어지거나, 해당 네트워크에 결합한 단말에서 작업이 이루어질 수 있다.

[0048] 아울러, 본 발명에서 특정 구성을 "포함"한다고 기술하는 내용은 해당 구성 이외의 구성을 배제하는 것이 아니며, 추가적인 구성이 본 발명의 실시 또는 본 발명의 기술적 사상의 범위에 포함될 수 있음을 의미한다.

[0049] 도 3은 본 발명에 따라서 분산 서비스 거부 방식의 공격을 탐지하고 트래픽을 조정하는 것을 개략적으로 설명

하는 개념도이다.

[0050] 네트워크상에서 서비스를 제공하는 서버(330)는 라우팅 장치(310)를 통해 ISP 네트워크(300)에 연결되어 있다. 라우팅 장치(310)와 서버(330) 사이에는 보안을 위한 방화벽(320)이 존재한다.

[0051] 도 3에서 보는 바와 같이, 분산 서비스 거부 방식의 공격이 있을 때, ISP 네트워크(300)를 통해 전달되는 트래픽에는 공격을 위한 트래픽, 예컨대 TCP SYN 플러딩과 함께, 정상적인 트래픽도 있다. 즉, 서비스 사용자들의 정상적인 트래픽이 라우팅 장치(310)와 방화벽(320)을 거쳐 서버(330)에 전달될 때, 분산 서비스 거부 방식의 공격, 예컨대 TCP SYN 플러딩 역시 동일하게 서버(330)에 전달된다. 따라서, 서버(330)의 부하가 많아져서 서비스 중단에 이르게 된다.

[0052] TCP SYN 플러딩처럼 적은 양의 트래픽을 일으키면서 서비스 중단에 이르게 하는 경우에는, 일반적으로 네트워크상에서 트래픽의 흐름만으로 공격을 탐지하는 것이 용이하지 않다.

[0053] 이때, 서버(330)로부터 주기적으로 또는 정해진 조건에 따른 시기에 서버(330)의 상태 정보(340)가 라우터 장치(310)로 송신되면 서버의 상태 변화를 라우팅 장치(310)에서 탐지할 수 있다.

[0054] 공격 대상이 될 수 있는 서버(330)는 주기적으로 또는 정해진 조건에 따른 시기마다 서버(330)의 상태에 관한 정보를 라우팅 장치(310)로 전송한다. 여기서 정해진 조건에 따른 시기는, 미리 설정된 비주기적인 시간 간격일 수도 있고, 해당 서버가 자신의 상태에 대한 급격한 변화를 감지한 있는 때일 수도 있다. 라우팅 장치(310)는 서버(330)의 상태에 관한 정보를 수신하고, 이를 저장한다. 서버(330)의 상태에 관한 정보는 서버의 CPU 부하, 서버의 메모리 이용량, 서버의 백로그 큐 상태에 관한 정보 등과 같이 서버의 상태를 반영하는 다양한 정보가 가능하다.

[0055] 라우팅 장치(310)는 수신한 서버(330)의 상태 정보에 따라서 각 서버(330)의 상태 변화량을 산출할 수 있다. 이 변화의 양을 소정의 기준치(threshold)와 비교하여, 기준치를 넘는 경우에는 해당 서버가 공격을 받고 있는 것으로 판단할 수 있다. 이때 소정의 기준치는, 각각의 상태 정보마다 상이하게 설정된다. 소정의 기준치는 네트워크 관리자 등에 의해 미리 설정될 수 있다. 또한, 소정의 기준치는 서버의 상태에 따라서 변경될 수 있다. 예컨대, 해당 서버의 서비스 인기가 갑자기 급증하거나 해당 서버의 서비스에 대한 관심이 높아지는 경우에는, 해당 서버에 트래픽이 몰릴 수 있으므로, 이 경우에는 각각의 상태 정보 변화량에 대한 소정의 기준치를 높게 변경할 수도 있다.

[0056] 서버(330)에 대한 공격을 탐지한 라우팅 장치(310)는 미리 정해진 정책(policy)에 따른 조치를 수행한다. 예컨대, 라우팅 장치(310)는 서버에 대한 공격 사실과 함께, 공격을 받고 있는 서버에 대한 정보를 네트워크 관리자 및/또는 서버 관리자에게 전송할 수 있다. 라우팅 장치(310)는 공격을 받고 있는 서버에 대한 트래픽을 차단할 수도 있다. 또한, 라우팅 장치(310)는 공격을 받고 있는 서버에 대한 트래픽을 차단하는 대신, 적정한 수준, 예컨대 미리 정해진 소정 양의 트래픽으로 제한함으로써 해당 서버가 제공하는 서비스가 중단되지 않도록 할 수도 있다.

[0057] 도 4는 라우팅 장치에서 분산 서비스 거부 방식의 공격을 탐지하고 이에 대응하는 방법을 개략적으로 설명하는 순서도이다.

[0058] 라우팅 장치는 네트워크상의 서버로부터 주기적으로 또는 정해진 조건에 따른 시기마다 서버의 상태에 관한 정보를 수신한다(S410). 여기서 정해진 조건에 따른 시기는, 미리 설정된 비주기적인 시간 간격일 수 있다. 또한 정해진 조건에 따른 시기는, 해당 서버가 자신의 상태를 스스로 체크하도록 하고, 자신의 상태에 대해 소정의 기준치를 넘는 변화를 감지할 때, 상태 정보를 라우팅 장치에 송신하도록 할 수도 있다.

[0059] 서버의 상태 정보는 상술한 것처럼, 서버의 CPU 부하, 서버의 메모리 이용량, 서버의 백로그 큐 상태에 관한 정보 등과 같이 서버의 상태를 반영하는 다양한 정보가 가능하다. 라우팅 장치는 수신한 상태 정보를 메모리부에 저장한다.

[0060] 라우팅 장치는 서버로부터 상태 정보를 수신하면, 수신한 상태 정보와 메모리부에 저장된 상태 정보를 기반으로 서버의 상태 변화량을 산출한다(S420). 서버의 CPU 부하의 증가량, 서버의 메모리 이용량의 증가량, 서버의 백로그 큐에 대기 중인 접속 요청의 증가량 등과 같이 서버의 상태 변화를 반영하는 다양한 정보의 변화량을 활용할 수 있다.

[0061] 라우팅 장치는 산출한 서버의 상태 변화량을 미리 설정된 기준치(threshold)와 비교한다(S430). 라우팅 장치는 서버의 상태 변화량이 미리 설정된 소정의 기준치보다 큰 경우에는 해당 서버가 현재 공격을 받고 있다고

판단할 수 있다.

[0062] 소정의 기준치는 소정의 기준치는, 각각의 상태 정보마다 설정된다.

[0063] 예컨대, 라우팅 장치에서 수신하는 서버의 상태 정보가 서버의 CPU 부하에 관한 것이면, 소정의 기준치는 부하의 변화량에 대하여 미리 결정된 값이 된다. 라우팅 장치는 산출된 서버의 CPU 부하의 증가량이 미리 정해진 부하의 변화량보다 큰 경우에, 해당 서버가 공격을 받고 있다고 판단할 수 있다.

[0064] 라우팅 장치에서 수신하는 서버의 상태 정보가 서버의 메모리 이용량에 관한 것이면, 소정의 기준치는 메모리 이용량의 변화량에 대하여 미리 결정된 값이 된다. 라우팅 장치는 산출된 서버의 메모리 이용량의 증가량이 미리 정해진 메모리 이용량의 변화량보다 큰 경우에, 해당 서버가 공격을 받고 있다고 판단할 수 있다.

[0065] 마찬가지로, 라우팅 장치에서 수신하는 서버의 상태 정보가 서버의 백로그 큐에 대기 중인 접속 요청에 관한 것이면, 소정의 기준치는 접속 요청의 변화량에 대하여 미리 결정된 값이 된다. 라우팅 장치는 산출된 서버의 백로그 큐에 대기 중인 접속 요청의 증가량이 미리 정해진 접속 요청의 변화량보다 큰 경우에, 해당 서버가 공격을 받고 있다고 판단할 수 있다.

[0066] 소정의 기준치는 네트워크 관리자 등에 의해 미리 설정될 수 있다. 또한, 소정의 기준치는 서버의 상태에 따라서 변경될 수 있다. 예컨대, 해당 서버의 서비스 인기가 갑자기 급증하거나 해당 서버의 서비스에 대한 관심이 높아지는 경우에는, 해당 서버에 트래픽이 몰릴 수 있으므로, 이 경우에는 각각의 상태 정보 변화량에 대한 소정의 기준치를 높게 변경할 수도 있다.

[0067] 여기에서는 서버의 상태에 대한 변화량에 대하여 설명하였으나, 본 발명은 이에 한정되지 않으며, 서버의 상태를 나타내는 수치를 소정의 기준값과 비교하여 해당 서버가 공격을 받고 있는지 판단할 수도 있다. 예컨대, 라우팅 장치는 서버의 CPU 부하, 서버의 메모리 이용량, 서버의 백로그 큐에 대기 중인 접속 요청의 수 등에 대한 기준값(threshold)을 미리 설정하고, 상기 상태 값들이 소정의 기준값을 넘는 경우에는 해당 서버가 공격을 받고 있다고 판단할 수도 있다.

[0068] 공격을 받고 있지 않는 정상적인 상태라고 판단한 경우에는, 라우팅 장치는 서버로부터 계속해서 상태 정보를 수신한다(S410).

[0069] 해당 서버가 공격을 받고 있다고 판단한 경우에, 라우팅 장치는 미리 정해진 정책(policy)에 따른 대응 조치를 수행한다(S440). 예컨대, 라우팅 장치는 서버에 대한 공격 사실과 함께, 공격을 받고 있는 서버에 대한 정보를 네트워크 관리자 및/또는 서버 관리자에게 전송할 수 있다. 라우팅 장치는 공격을 받고 있는 서버에 대한 트래픽을 차단할 수도 있다. 또한, 라우팅 장치는 공격을 받고 있는 서버에 대한 트래픽을 차단하는 대신, 적정한 수준, 예컨대 미리 정해진 소정 양의 트래픽으로 제한함으로써 해당 서버가 제공하는 서비스가 중단되지 않도록 할 수도 있다.

[0070] 대응 조치를 수행한 후, 예컨대, 공격 대상 서버에 대한 트래픽을 차단하거나 경감시킨 뒤에, 라우팅 장치는 일정한 조건에 따라서 트래픽을 다시 복구시킬 수 있다. 또한 라우팅 장치는 트래픽을 복구시키지 않고, 네트워크 관리자 및/또는 서버 관리자의 직접적인 지시나 조치를 기다릴 수도 있다.

[0071] 도 5는 본 발명에 따른 라우팅 장치의 기능적인 구성을 개략적으로 도시한 블록도이다.

[0072] 라우팅 장치(500)는 수신부(510), 송신부(520), 메모리(530) 및 제어부(540)를 포함한다.

[0073] 수신부(510)는 라우팅 장치(530)로 들어오는 패킷의 입력 포드 역할을 수행함과 동시에 네트워크상의 각 서버로부터 서버의 상태 정보를 수신한다.

[0074] 송신부(520)는 라우팅 장치(530)로부터 나가는 패킷의 출력 포드 역할을 수행함과 동시에 네트워크상의 각 서버에 대한 메시지를 송신한다.

[0075] 메모리(530)는 네트워크 운용에 필요한 정보/데이터와 함께, 각 서버로부터 수신한 서버의 상태 정보와 이 상태 정보에 대한 기준치를 저장한다.

[0076] 제어부(540)는 데이터 패킷의 출발지로부터 목적지까지의 경로를 설정하며, 경로 설정에 따라 데이터 패킷의 스위칭을 수행한다. 또한, 제어부(540)는 각 서버로부터 수신한 서버의 상태 정보와 메모리부(530)에 저장된 상태 정보로부터 서버의 상태 변화량을 산출한다. 제어부(540)는 산출한 서버의 상태 변화량 또는 수신한 서버의 상태값과 소정의 기준치를 비교하여, 해당 서버가 공격을 받고 있는지를 판단한다. 해당 서버가 공격을 받고 있는 것으로 판단한 경우에, 제어부(540)는 해당 서버에 대한 트래픽을 조정한다.

[0077] 서버가 공격을 당하고 있다고 제어부(540)가 판단한 경우에, 송신부(520)는 서버가 공격받고 있다는 사실과 공격을 받고 있는 서버에 관한 정보를 네트워크 관리자 및/또는 해당 서버의 관리자에게 송신할 수 있다.

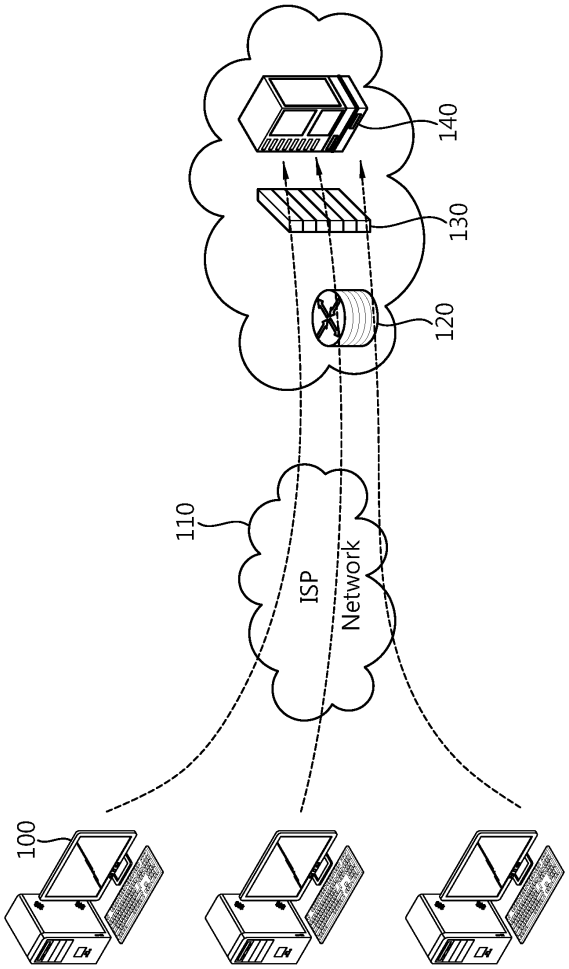
[0078] 본 발명에 의하면 현재 공격 대상이 어떤 서버인지 라우팅 장치가 파악하고 있으므로, 많은 트래픽 중에서 공격 대상으로 가는 트래픽만을 감소시키거나 차단하고, 공격당하지 않는 서버들에게는 아무런 영향을 주지 않을 수 있다. 이렇게 공격 대상 서버로 가는 트래픽의 양을 라우팅 장치에서 감소시켜줄 수 있으므로, 공격 대상 서버도 자신의 서비스를 중단없이 사용자에게 제공할 수 있다.

[0079] 상술한 예시적인 시스템에서, 방법들은 일련의 단계 또는 블록으로써 순서도를 기초로 설명되고 있지만, 본 발명은 단계들의 순서에 한정되는 것은 아니며, 어떤 단계는 상술한 바와 다른 단계와 다른 순서로 또는 동시에 발생할 수 있다. 또한, 당업자라면 순서도에 나타낸 단계들이 배타적이지 않고, 다른 단계가 포함되거나 순서도의 하나 또는 그 이상의 단계가 본 발명의 범위에 영향을 미치지 않고 삭제될 수 있음을 이해할 수 있을 것이다.

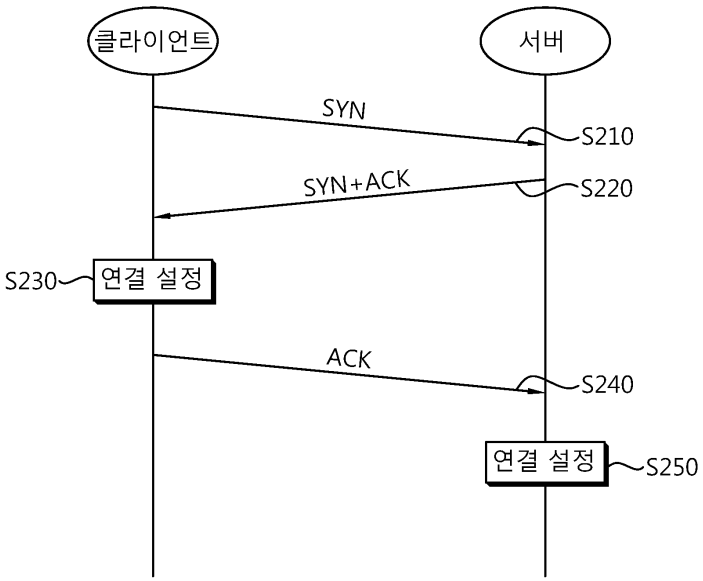
[0080] 상술한 실시예는 다양한 양태의 예시들을 포함한다. 다양한 양태들을 나타내기 위한 모든 가능한 조합을 기술할 수는 없지만, 해당 기술 분야의 통상의 지식을 가진 자는 다른 조합이 가능함을 인식할 수 있을 것이다. 따라서, 본 발명은 이하의 특허청구범위 내에 속하는 모든 다른 교체, 수정 및 변경을 포함한다고 할 것이다.

도면

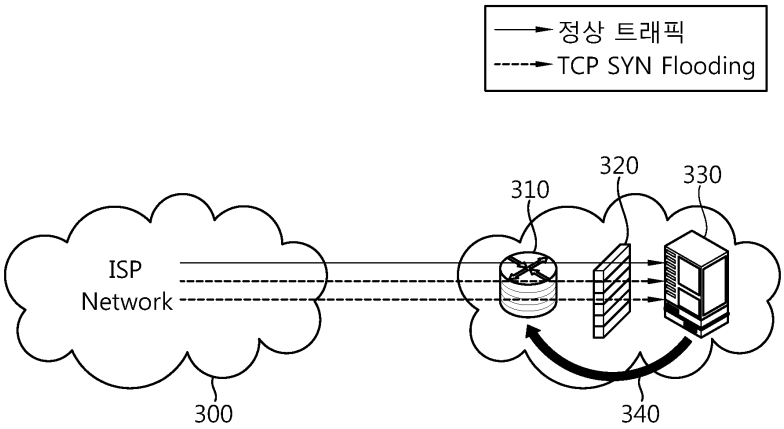
도면1



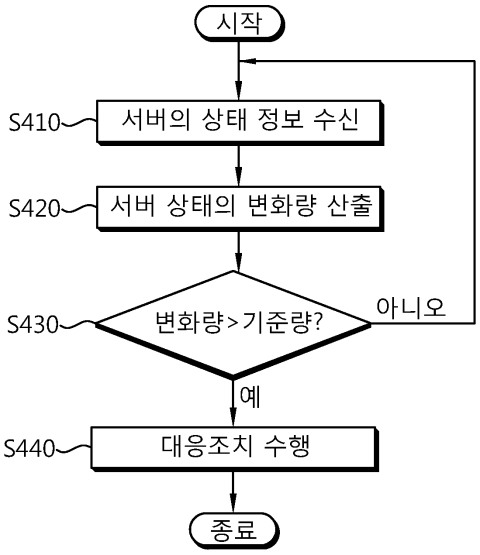
도면2


클라이언트
서버
SYN
S210
SYN+ACK
S220
S230
연결 설정
ACK
S240
연결 설정
S250

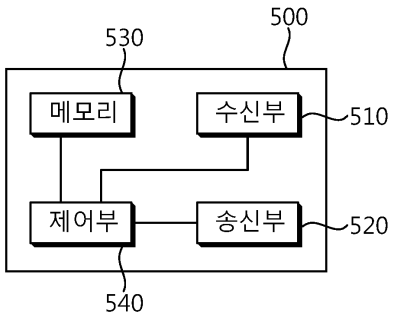
도면3


정상 트래픽
TCP SYN Flooding
ISP
Network
300
310
320
330
340

도면4


시작
S410
서버의 상태 정보 수신
S420
서버 상태의 변화량 산출
S430
변화량>기준량?
아니오
예
S440
대응조치 수행
종료

도면5


500
530
메모리
수신부
510
제어부
송신부
520
540