(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0142544
(43) 공개일자 2014년12월12일

(51) 국제특허분류(Int. Cl.)
H04L 12/911 (2013.01)
(21) 출원번호 10-2013-0064110
(22) 출원일자 2013년06월04일
심사청구일자 없음

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
강경순
대전 유성구 노은동로 187, 608동 104호 (지족동, 열매마을6단지)
이경호
대전 유성구 어은로 57, 128동 403호 (어은동, 한빛아파트)
(뒷면에 계속)
(74) 대리인
제일특허법인

전체 청구항 수 : 총 20 항

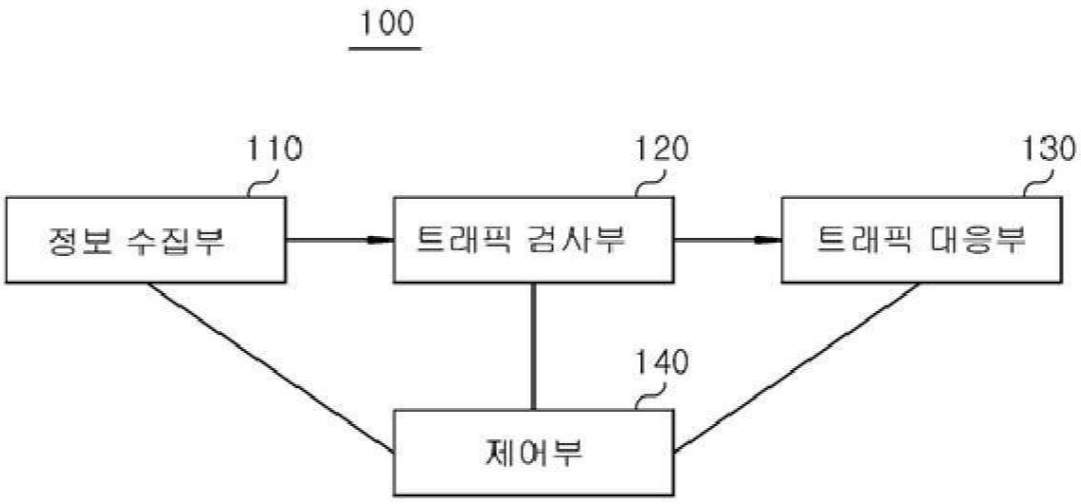
(54) 발명의 명칭 **공정성을 높이기 위한 네트워크 대역폭 할당 방법 및 장치**

(57) 요 약

본 발명은 IP 네트워크, 특히 라우터나 스위치와 같은 전송 장치에서 특정 사용자의 과도한 트래픽을 억제 함으로써 여러 사용자에게 공정하게 네트워크 대역폭을 할당할 수 있는 방법 및 장치에 관한 것으로서, 실시예는 네트워크 대역폭의 할당을 제어하는 제어부와, 상기 제어부에 의해 플로우(flow) 정보를 수집하는 정보 수집부와,

(뒷면에 계속)

대 표 도 - 도1



상기 수집된 플로우 정보의 트래픽을 검사하는 트래픽 검사부와, 상기 트래픽의 검사 결과에 따라 네트워크 대역폭의 통제를 수행하는 트래픽 대응부를 포함한다.

따라서, 사용자별로 프로파일을 설정하는 방법에 비하여 몇 개의 설정값과 사용자들의 이용 행태만을 가지고 특정 사용자의 네트워크 사용량 증가에 능동적으로 대처하여 공정한 네트워크 자원을 할당할 수 있고, 이러한 과정으로 인해 네트워크 대역폭 관리 비용이 감소하게 되며, 과도한 P2P, DDoS (Distributed Denial of Service) 공격으로 인하여 몇몇 사용자에게 네트워크 자원이 주로 사용되는 현상을 방지 할 수 있다.

(72) 발명자

안병준

대전 유성구 은구비남로 34, 807동 1501호 (노은동, 열매마을8단지)

전기철

대전 유성구 어은로 57, 121동 1001호 (어은동, 한빛아파트)

박혜숙

대전 유성구 어은로 57, 101동 1002호 (어은동, 한빛아파트)

특허청구의 범위

청구항 1

네트워크의 플로우(flow) 정보를 수집하는 정보 수집부와,

상기 수집된 플로우 정보의 트래픽을 검사하는 트래픽 검사부와,

상기 트래픽의 검사 결과에 따라 네트워크 대역폭의 통제를 수행하는 트래픽 대응부와,

상기 정보 수집부, 트래픽 검사부 또는 트래픽 대응부를 제어하는 제어부를 포함하는

네트워크 대역폭 할당 장치.

청구항 2

제 1항에 있어서,

상기 제어부는

상기 트래픽의 전송량이 기 설정된 임계값(TH)이상인 경우, 상기 네트워크 대역폭의 할당을 제어하는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 3

제 1항에 있어서,

상기 플로우 정보는

소스 IP주소, 목적지 IP주소, 소스포트, 목적지포트 또는 프로토콜을 포함하는것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 4

제 3항에 있어서,

상기 정보수집부는

상기 제어부의 제어에 따라 상기 수집된 플로우 정보를 바탕으로 상기 소스IP 주소로 플로우 정보를 집합화하는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 5

제 4항에 있어서,

상기 집합화된 플로우 정보는 단위시간당 플로우 수, 단위 시간당 바이트(byte)수 및 초당 패킷 전송수를 포함하는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 6

제 5항에 있어서,

상기 정보수집부는

상기 제어부의 제어에 따라 상기 소스IP 주소가 기 설정된 화이트 리스트(White List) 그룹, 블랙 리스트(Black List) 그룹 또는 일반 그룹 중 어느 것에 속하는지를 판단하는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 7

제 6항에 있어서,

상기 제어부는

상기 소스IP 주소가 상기 화이트 리스트 그룹에 속하는 경우, 상기 트래픽 대응부가 상기 네트워크 대역폭의 통제를 수행하지 않도록 제어하는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 8

제6항에 있어서,

상기 제어부는

상기 상기 소스IP 주소가 상기 블랙 리스트 그룹에 속하는 경우,

상기 트래픽의 네트워크 진입을 차단하는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 9

제6항에 있어서,

상기 트래픽 검사부는

상기 소스IP주소가 상기 일반 그룹에 속하는 경우, 상기 제어부의 제어에 따라 상기 단위시간당 플로우 수, 단위 시간당 바이트(byte)수 및 초당 패킷 전송수의 각각이 중간값(Median)을 초과 하는지를 판단하는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 10

제 9항에 있어서,

상기 트래픽 대응부는

상기 판단 결과 상기 단위 시간당 바이트(byte) 수가 상기 중간값을 초과 하는 경우, 상기 제어부의 제어에 따라 해당 소스IP 주소에 대해 상기 트래픽 전송량을 상기 중간값까지 감소 시키고,

상기 판단결과 상기 단위시간당 플로우 수가 상기 중간값을 초과 하는 경우, 상기 제어부의 제어에 따라 해당 소스IP 주소에 대해 신규 플로우 생성을 억제하고 기존 플로우 수를 상기 중간값까지 감소 시키고,

상기 판단 결과 상기 초당 패킷 전송수가 상기 중간값을 초과 하는 경우, 상기 초당 패킷 전송수가 기 설정된

상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단하는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 11

제 9항에 있어서,

상기 트래픽 대응부는

상기 초당 패킷 전송수가 기 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는 경우, 상기 제어부의 제어에 따라 DDoS (Distributed Denial of Service)공격 발생 가능성을 알리고, 해당 소스IP 주소를 상기 블랙 리스트 그룹으로 이동시키는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 12

제 11항에 있어서,

상기 트래픽 대응부는

상기 초당 패킷 전송수가 상기 기 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)이하인 경우, 상기 초당 패킷 전송수를 상기 중간값까지 감소시키는 것을 특징으로 하는

네트워크 대역폭 할당 장치.

청구항 13

제어부가 트래픽의 전송량이 미리 정해진 임계값(TH)이상인지를 판단하는 과정과,

정보수집부가 플로우(flow) 정보를 바탕으로 소스IP 주소에 플로우 정보를 집합화하는 과정과,

상기 정보수집부가 상기 소스IP 주소가 기 설정된 화이트 리스트(White List) 그룹, 블랙 리스트(Black List) 그룹 또는 일반 그룹 중 어느 것에 속하는지를 판단하는 과정을 포함하는 것을 특징으로 하는

네트워크 대역폭 할당 방법.

청구항 14

제 13항에 있어서

상기 정보수집부가 어느 것에 속하는지를 판단하는 과정은

상기 소스IP 주소가 상기 화이트 리스트 그룹에 속하는 경우, 상기 네트워크 대역폭의 통제를 수행하지 않고,

상기 소스IP 주소가 상기 블랙 리스트 그룹에 속하는 경우, 상기 트래픽의 네트워크 진입을 차단하는 것을 특징으로 하는

네트워크 대역폭 할당 방법.

청구항 15

제 13항에 있어서,

상기 정보수집부가 어느 것에 속하는지를 판단하는 과정은

상기 소스IP주소가 상기 일반 그룹에 속하는 경우, 상기 트래픽 검사부가

단위시간당 바이트(byte) 수가 중간값(Median)을 초과 하는지를 판단하는 과정과,

단위시간당 플로우(flow) 수가 상기 중간값을 초과 하는지를 판단하는 과정과,

초당 패킷 전송수가 상기 중간값을 초과 하는지를 판단하는 과정을 포함 하는 것을 특징으로 하는

네트워크 대역폭 할당 방법.

청구항 16

상기 제15항에 있어서,

상기 단위시간당 바이트(byte) 수가 상기 중간값을 초과 하는지를 판단하는 과정에서,

상기 단위시간당 바이트 수가 상기 중간값을 초과하는 경우, 상기 트래픽의 전송량을 상기 중간값까지 감소시키는 것을 특징으로하는

네트워크 대역폭 할당 방법.

청구항 17

제 15항에 있어서,

상기 단위시간당 플로우 수가 상기 중간값을 초과 하는지를 판단하는 과정에서,

상기 단위시간당 플로우 수가 상기 중간값을 초과 하는경우, 해당 소스IP 주소에 대해 신규 플로우 생성을 억제하고 기존 플로우 수를 상기 중간값까지 감소 시키는 것을 특징으로 하는

네트워크 대역폭 할당 방법.

청구항 18

제 15항에 있어서,

상기 초당 패킷 전송수가 상기 중간값을 초과 하는지를 판단하는 과정은

상기 초당 패킷 전송수가 상기 중간값을 초과하는 경우, 상기 초당 패킷 전송수가 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단하는 과정을 포함하는 것을 특징으로 하는

네트워크 대역폭 할당 방법.

청구항 19

제 18항에 있어서,

상기 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단하는 과정에서

상기 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과하는 경우, 트래픽 대응부는 DDoS (Distributed Denial of Service)공격 발생 가능성을 알리고, 해당 소스IP 주소를 상기 블랙리스트 그룹으로 이동시키는 것 특징으로 하는

네트워크 대역폭 할당 방법.

청구항 20

제 18항에 있어서,

상기 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단하는 과정에서

상기 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS) 이하인 경우, 상기 초당 패킷 전송수를 상기 중간값까지 감소시키는것을 특징으로하는

네트워크 대역폭 할당 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 네트워크의 대역폭 할당(통제) 에 관한 것으로, 특히 IP(Internet Protocol) 네트워크, 특히 라우터나 스위치와 같은 전송 장치에서 특정 사용자의 과도한 트래픽을 억제 함으로써 여러 사용자에게 공정하게 네트워크 대역폭을 할당할 수 있는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 고화질 동영상 유통 경로 이용되는 P2P(Peer-to-peer) 프로그램의 경우와 같이 많은 대역폭을 요구하는 서비스들이 생겨나고 있으며, 이러한 서비스들의 이용 행태를 볼 때 특정 사용자의 과도한 트래픽 집중 현상이 발생하고 있다. 이 때문에 나중에 접속하는 사용자는 네트워크 자원을 할당 받지 못하거나 최소한의 대역폭만을 보장받게 됨으로써 서비스 품질에 차이가 발생하게 된다.

[0003] 이와 같은 문제를 해결하기 위하여 개별 사용자별로 프로파일을 생성하여 해당 프로파일에 따른 QoS (Quality of Service)를 제공하도록 하는 방법이 사용될 수 있으나, 이는 많은 유지보수 비용이 필요하게 되며, 그 프로파일의 개수에도 제한이 발생 함으로써 많은 사용자에 대한 설정이 어렵게 된다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 대한민국 등록특허번호 10-0519962호 등록일자 2005년 09월 30일에는 집단 흐름간 공평 대역폭 할당을 위한 에지-대-에지 흐름 제어방법에 관한 기술이 개시되어 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명의 실시예는, 이와 같은 종래 기술의 문제점을 해결하기 위한 것으로서, 특히 IP 네트워크 상의 라우터나 스위치 단에서 특정 사용자의 과도한 트래픽을 탐지하고 트래픽을 제어하여 다른 사용자들의 요청 서비스가 유지되도록 함으로써 네트워크 자원의 사용에 공정성을 제공할 수 있는 방법 및 장치를 제공하고자 한다.

[0006] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 본 발명이 속하는 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0007] 본 발명의 일 관점에 의하면, 네트워크의 플로우(flow) 정보를 수집하는 정보 수집부와, 상기 수집된 플로우 정보의 트래픽을 검사하는 트래픽 검사부와, 상기 트래픽의 검사 결과에 따라 네트워크 대역폭의 통제를 수행하는 트래픽 대응부와, 상기 정보 수집부, 트래픽 검사부 또는 트래픽 대응부를 제어하는 제어부를 포함한다.

[0008] 또한, 상기 제어부는 상기 트래픽의 전송량이 기 설정된 임계값(TH)이상인 경우, 상기 네트워크 대역폭의 할당을 제어할수 있다.

[0009] 또한, 상기 플로우 정보는 소스 IP주소, 목적지 IP주소, 소스포트, 목적지포트 또는 프로토콜을 포함할 수 있다.

[0010] 또한, 상기 정보수집부는 상기 제어부의 제어에따라 상기 수집된 플로우 정보를 바탕으로 상기 소스IP 주소로 플로우 정보를 집합화 할 수 있다.

[0011] 또한, 상기 집합화된 플로우 정보는 단위시간당 플로우 수, 단위 시간당 바이트(byte)수 및 초당 패킷 전송수를 포함할 수 있다.

[0012] 또한, 상기 정보 수집부는 상기 소스IP 주소가 기 설정된 화이트 리스트(White List) 그룹, 블랙 리스트(Black List) 그룹 또는 일반 그룹 중 어느 것에 속하는지를 판단할 수 있다.

[0013] 또한, 상기 제어부는 상기 소스IP 주소가 상기 화이트 리스트 그룹에 속하는 경우, 상기 트래픽 대응부가 상기 네트워크 대역폭의 통제를 수행하지 않도록 제어할 수 있다.

[0014] 또한, 상기 제어부는 상기 상기 소스IP 주소가 상기 블랙 리스트그룹에 속하는 경우 상기 트래픽의 네트워크 진입을 차단할 수 있다.

[0015] 또한, 상기 트래픽 검사부는 상기 소스IP주소가 상기 일반 그룹에 속하는 경우, 상기 제어부의 제어에 따라 상기 단위시간당 플로우 수, 단위 시간당 바이트(byte)수 및 초당 패킷 전송수의 각각이 중간값(Median)을 초과하는지를 판단할 수 있다.

[0016] 또한, 상기 트래픽 대응부는 상기 판단 결과 상기 단위 시간당 바이트(byte) 수가 상기 중간값을 초과 하는 경우, 상기 제어부의 제어에 따라 해당 소스IP 주소에 대해 상기 트래픽 전송량을 상기 중간값까지 감소 시키고, 상기 판단결과 상기 단위시간당 플로우 수가 상기 중간값을 초과 하는 경우, 상기 제어부의 제어에 따라 해당 소스IP 주소에 대해 신규 플로우 생성을 억제하고 기존 플로우 수를 상기 중간값까지 감소 시키고, 상기 판단결과 상기 초당 패킷 전송수가 상기 중간값을 초과 하는 경우, 상기 초당 패킷 전송수가 기 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단할 수 있다.

[0017] 또한, 상기 트래픽 대응부는 상기 초당 패킷 전송수가 기 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는 경우, 상기 제어부의 제어에 따라 DDoS (Distributed Denial of Service)공격 발생 가능성을 알리고, 해당 소스IP 주소를 상기 블랙 리스트 그룹으로 이동시킬 수 있다.

[0018] 또한, 상기 트래픽 대응부는 상기 초당 패킷 전송수가 상기 기 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)이하인 경우 상기 초당 패킷 전송수를 상기 중간값까지 감소시킬 수 있다.

[0019] 본 발명의 다른 관점에 의하면, 네트워크 대역폭 할당 방법은 제어부가 트래픽의 전송량이 미리 정해진 임계값(TH)이상인지 판단하는 과정과, 정보수집부가 플로우(flow) 정보를 바탕으로 소스IP 주소로 플로우 정보를 집합화하는 과정과, 상기 정보수집부가 상기 소스IP 주소가 화이트 리스트(White List) 그룹, 블랙 리스트(Black List) 그룹 및 일반 그룹 중 어느 것에 속하는지를 판단하는 과정을 포함한다.

[0020] 또한, 상기 정보수집부가 어느 것에 속하는지를 판단하는 과정은 상기 소스IP 주소가 상기 화이트 리스트 그룹에 속하는 경우 상기 네트워크 대역폭의 통제를 수행하지 않고, 상기 소스IP 주소가 상기 블랙 리스트 그룹에 속하는 경우 상기 트래픽의 네트워크 진입을 차단할 수 있다.

[0021] 또한, 상기 정보수집부가 어느 것에 속하는지를 판단하는 과정은 상기 소스IP주소가 상기 일반 그룹에 속하는 경우 상기 트래픽 검사부는 단위시간당 바이트(byte) 수가 중간값을 초과 하는지를 판단하는 과정과, 단위시간당 플로우(flow) 수가 상기 중간값을 초과 하는지를 판단하는 과정과, 초당 패킷 전송수가 상기 중간값을 초과 하는지를 판단하는 과정을 포함할 수 있다.

[0022] 또한, 상기 단위시간당 바이트(byte) 수가 상기 중간값을 초과 하는지를 판단하는 과정에서, 상기 단위시간당 바이트 수가 상기 중간값을 초과하는 경우 상기 트래픽의 전송량을 상기 중간값까지 감소시킬수 있다.

[0023] 또한, 상기 단위시간당 플로우 수가 상기 중간값을 초과 하는지를 판단하는 과정에서, 상기 단위시간당 플로우 수가 상기 중간값을 초과 하는경우 해당 소스IP 주소에 대해 신규 플로우 생성을 억제하고 기존 플로우 수를 상기 중간값까지 감소 시킬 수 있다.

[0024] 또한, 상기 초당 패킷 전송수가 상기 중간값을 초과 하는지를 판단하는 과정은 상기 초당 패킷 전송수가 상기 중간값을 초과하는 경우 상기 초당 패킷 전송수가 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단하는 과정을 포함할 수 있다.

[0025] 또한, 상기 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단하는 과정에서 상기 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과하는 경우 트래픽 대응부는 DDoS (Distributed Denial of Service)공격 발생 가능성을 알리고, 해당 소스IP 주소를 상기 블랙 리스트 그룹으로 이동시킬 수 있다.

[0026] 또한, 상기 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단하는 과정에서 상기 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS) 이하인 경우 상기 초당 패킷 전송수를 상기 중간값까지 감소시킬 수 있다.

발명의 효과

[0027] 본 발명의 실시예에 따른 공정한 네트워크 대역폭 할당 방법 및 장치는 사용자별로 프로파일을 설정하는 방법에 비하여 몇 개의 설정값과 사용자들의 이용 행태만을 가지고 특정 사용자의 네트워크 사용량 증가에 능동적으로 대처하여 공정한 네트워크 자원을 할당할 수 있다. 또한, 이러한 과정으로 인해 네트워크 대역폭 관리 비용이 감소하게 되며, 과도한 P2P, DDoS (Distributed Denial of Service) 공격으로 인하여 몇몇 사용자에게 네트워크 자원이 주로 사용되는 현상을 방지 할 수 있다.

도면의 간단한 설명

[0028] 도 1은 본 발명의 실시예에 따른 공정성을 높이기 위한 네트워크 대역폭 할당 장치의 블록 구성도이다.

도 2는 도1의 공정성을 높이기 위한 네트워크 대역폭 할당 장치에 사용되는 트래픽 정보의 블록 구성도이다.

도 3은 본 발명의 실시예에 따른 네트워크 대역폭 할당 과정을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 이하, 첨부된 도면을 참조하여 본 발명의 동작 원리를 상세히 설명한다. 하기에서 본 발명을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0030] 도 1은 본 발명의 실시예에 따른 공정성을 높이기 위한 네트워크 대역폭 할당 장치(100)의 블록 구성을 도시한 것으로, 정보 수집부(110), 트래픽 검사부(120), 트래픽 대응부(130) 또는 제어부(140) 등을 포함 할 수 있다.

[0031] 또한, 도 2는 도1의 공정성을 높이기 위한 네트워크 대역폭 할당 장치(100)에 사용되는 트래픽 정보(200)의 블록 구성도이다. 도2에 도시된 바와 같이, 본 발명의 실시예에 따른 네트워크 대역폭 할당 장치(100)에 사용되는 트래픽 정보(200)는 사용자 단말(210), 소스IP 주소 #1…#N(220), 플로우 수(230), 바이트(byte) 수(240) 및 초당 패킷수(250)등을 포함할 수 있다.

[0032] 이하, 도 1 및 도 2를 참조하여 본 발명의 실시예에 따른 공정성을 높이기 위한 네트워크 대역폭 할당 장치의 각 구성요소에서의 동작을 상세히 설명하기로 한다.

[0033] 먼저, 제어부(140)는 상기 정보 수집부(110), 트래픽 검사부(120) 또는 트래픽 대응부(130)를 제어하여 네트워크 대역폭의 할당을 제어하는 것으로서, 네트워크 트래픽의 전송량이 기 설정된 임계값(TH) 이상인 경우, 네트워크 대역폭의 할당을 제어한다.

[0034] 정보 수집부(110)는 제어부(140)의 제어에 따라 소스 IP주소, 목적지 IP주소, 소스포트, 목적지포트 또는 프로토콜을 포함하는 네트워크의 플로우(flow) 정보를 수집하고, 수집된 플로우 정보를 바탕으로 소스IP 주소에 플로우 정보를 집합화하고, 소스IP 주소가 화이트 리스트(White List) 그룹, 블랙 리스트(Black List) 그룹 또는

일반 그룹 중 어느 것에 속하는지를 판단한다. 여기서, 집합화된 플로우 정보는 도2에 도시된 단위시간당 플로우 수(230), 단위 시간당 바이트(byte)수(240) 또는 초당 패킷 전송수(250)를 포함할 수 있다.

[0035] 트래픽 검사부(120)는 수집된 플로우 정보의 트래픽을 검사하는 것으로서, 소스IP주소가 일반 그룹에 속하는 경우, 제어부(140)의 제어에 따라 단위시간당 플로우 수(230), 단위 시간당 바이트(byte)수(240) 또는 초당 패킷 전송수(250)의 각각이 중간값(Median)을 초과 하는지를 판단한다.

[0036] 트래픽 대응부(130)는 트래픽 검사부(120)의 트래픽 검사 결과에 따라 네트워크 대역폭의 통제를 수행하는 것으로서, 트래픽 검사부(120)의 판단 결과 단위 시간당 바이트(byte) 수(240)가 중간값을 초과 하는 경우, 제어부(140)의 제어에 따라 해당 소스IP 주소에 대해 트래픽 전송량을 중간값까지 감소 시킨다. 또한, 트래픽 대응부(130)는 트래픽 검사부(120)의 판단 결과 단위시간당 플로우 수(230)가 중간값을 초과 하는 경우, 제어부(140)의 제어에 따라 해당 소스IP 주소에 대해 신규 플로우 생성을 억제하고 기존 플로우 수를 상기 중간값까지 감소 시킨다. 또한, 트래픽 대응부(130)는 트래픽 검사부(120)의 판단 결과 초당 패킷 전송수(250)가 중간값을 초과하는 경우, 초당 패킷 전송수(250)가 기 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단하고, 만약 초과 하는 경우, 제어부(140)의 제어에 따라 DDoS (Distributed Denial of Service) 공격 발생 가능성을 알리고, 해당 소스IP 주소를 상기 블랙 리스트 그룹으로 이동시킨다. 반면에, 초당 패킷 전송수(250)가 기 설정된 소스IP 주소별 최대 초당 전송수(PPS)이하인 경우, 초당 패킷 전송수(250)를 중간값까지 감소시킨다.

[0037] 또한, 제어부(140)은 소스IP 주소가 화이트 리스트 그룹에 속하는 경우, 트래픽 대응부(130)는 네트워크 대역폭의 통제를 수행하지 않도록 제어하고, 소스IP 주소가 블랙 리스트 그룹에 속하는 경우, 트래픽의 네트워크 진입을 차단한다.

[0038] 도1의 본 발명의 실시예에 따른 공정성을 높이기 위한 네트워크 대역폭 할당 장치(100)는 네트워크의 공정성을 높이기 위해 소스IP 주소 #1…#N(220)별로 대역폭을 할당(통제)하며, 하나의 사용자 단말(210)이 하나의 소스IP 주소를 갖는 환경에 적합하다. 그러나, 공정성을 높이기 위한 네트워크 대역폭 할당 장치(100)는 각 소스IP 주소 #1…#N(220)을 합산하여 사용자 단말(210)이 사용하는 대역폭을 집합화 하여 계산함으로써 하나의 사용자 단말(210)이 여러 개의 소스IP 주소 #1…#N(220) 을 갖는 경우에도 적용이 가능하다.

[0039] 도 3은 본 발명의 실시예에 따른 네트워크 대역폭 할당 과정을 설명하기 위한 흐름도이다.

[0040] 이하, 도 3을 참조하여 본 발명의 실시예에 따른 공정하게 네트워크 대역폭을 할당할 수 있는 방법에 대해 설명하기로 한다.

[0041] 먼저, 제어부(140)는 트래픽의 전송량이 기 설정된 임계값(TH)이상인지 판단하고(S300), 트래픽의 전송량이 임계값(TH)이상인 경우, 정보 수집부(110)가 플로우(flow) 정보를 바탕으로 소스IP 주소로 플로우 정보를 집합화한다(S310).

[0042] 정보 수집부(110)는 소스IP 주소가 화이트 리스트 그룹, 블랙 리스트 그룹 또는 일반 그룹 중 어느 것에 속하는지를 판단하고(S320), 판단결과 소스IP 주소가 화이트 리스트 그룹에 속하는 경우, 트래픽 대응부(130)는 네트워크 대역폭의 통제를 수행하지 않으며(S330), 소스IP 주소가 블랙 리스트 그룹에 속하는 경우, 트래픽의 네트워크 진입을 차단한다(S340).

[0043] 또한, 정보 수집부(110)의 판단 결과 소스IP주소가 일반 그룹에 속하는 경우, 트래픽 검사부(120)는 단위시간당 바이트(byte) 수가 중간값을 초과 하는지를 판단하고(S350), 단위시간당 플로우(flow) 수가 중간값을 초과 하는지를 판단하며(S370), 초당 패킷 전송수가 중간값을 초과 하는지를 판단한다(S390).

[0044] S350 단계에서의 판단결과 단위시간당 바이트(byte) 수가 중간값을 초과 하는경우, 트래픽의 전송량을 상기 중간값까지 감소시키고(S360), S370 단계에서의 판단결과 단위시간당 플로우 수가 상기 중간값을 초과 하는 경우, 해당 소스IP 주소에 대해 신규 플로우 생성을 억제하고 기존 플로우 수를 상기 중간값까지 감소 시키며(S380), S390 단계에서의 판단결과 초당 패킷 전송수가 상기 중간값을 초과하는 경우, 상기 초당 패킷 전송수가 기 설정된 상기 소스IP 주소별 최대 초당 전송수(PPS)를 초과 하는지를 판단 한다(S400). S400 단계에서의 판단결과 초당 패킷 전송수가 기 설정된 소스IP 주소별 최대 초당 전송수(PPS)를 초과하는 경우, 트래픽 대응부(130)는 DDoS (Distributed Denial of Service)공격 발생 가능성을 알리고(S410), 해당 소스IP 주소를 블랙 리스트 그룹으로 이동시킨다(S420).

[0045] 한편, S400 단계에서의 판단결과 초당 패킷 전송수가 상기 미리 설정된 상기 소스IP 주소별 최대 초당 전송수

(PPS) 이하인 경우, 트래픽 대응부(130)는 초당 패킷 전송수를 상기 중간값까지 감소시킨다(S430)본 발명에 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0046] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들 또는 단계들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0047] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0048]

100 : 네트워크 대역폭 할당 장치　　110 : 정보 수집부

120 : 트래픽 검사부　　130 : 트래픽 대응부

140 : 제어부　　200: 트래픽 정보

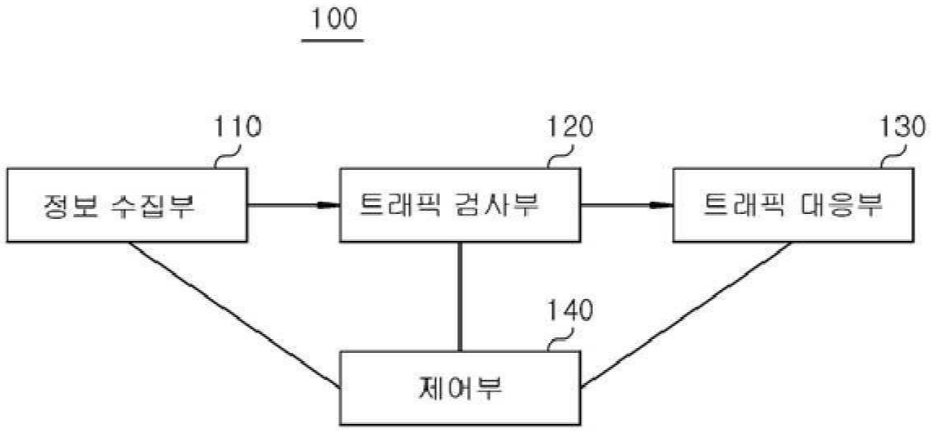
210 : 사용자 단말　　220: 소스IP주소 #1…#N

230: 플로우 수　　240: 바이트 수

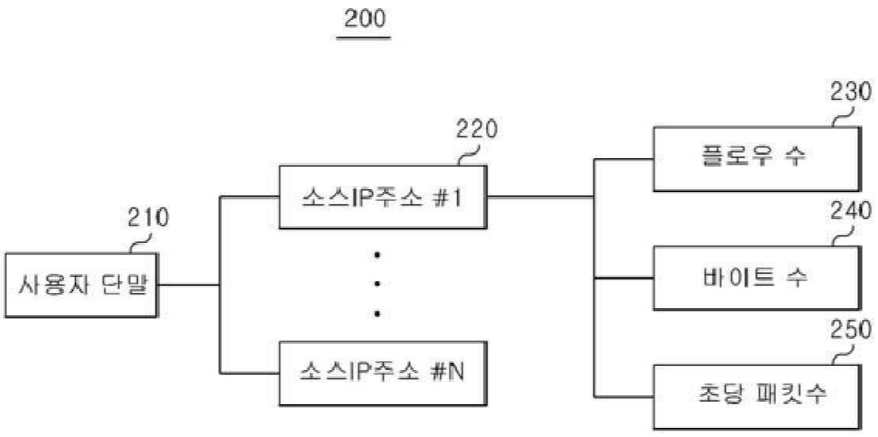
250: 초당 패킷수

도면

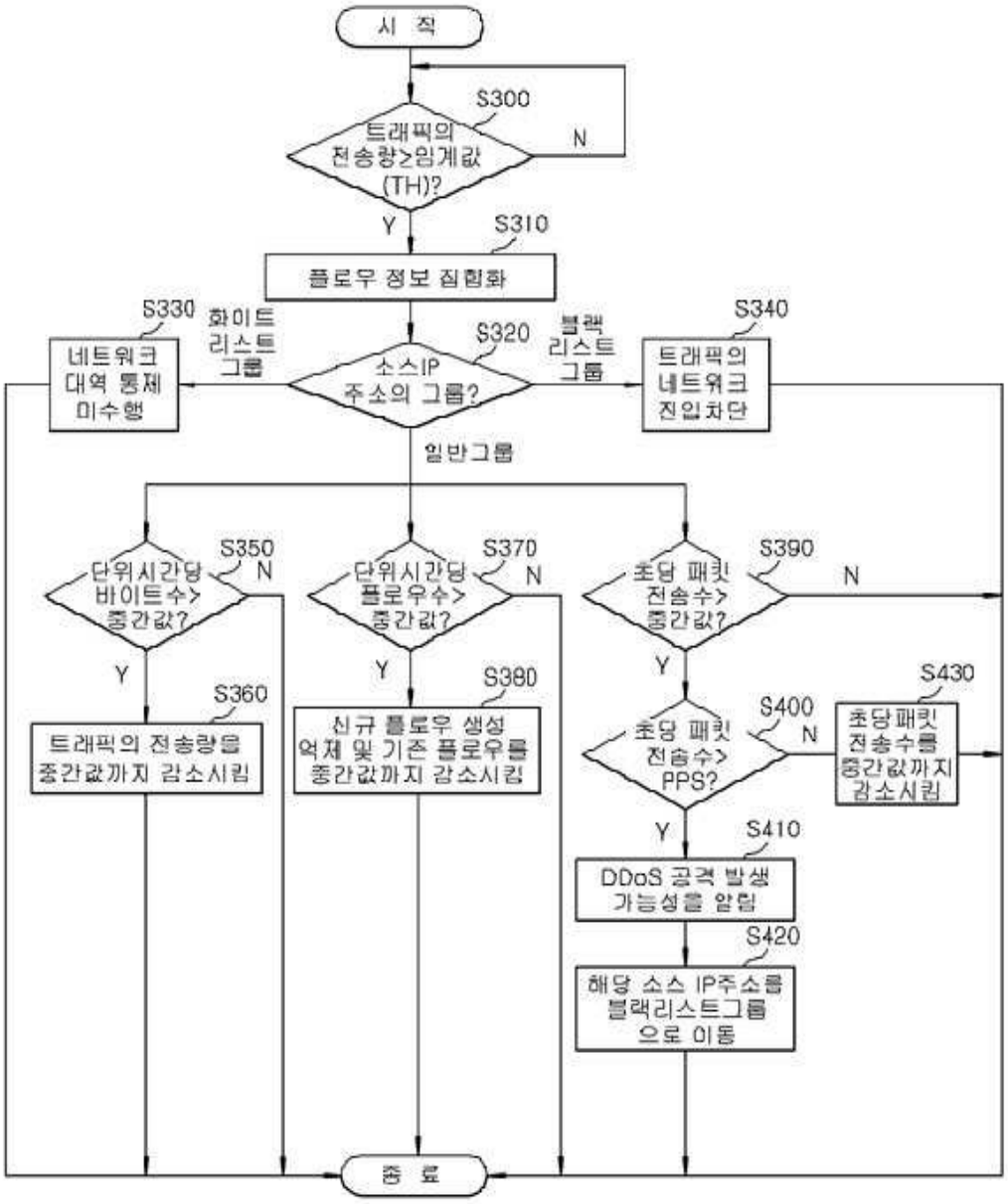
도면1


100
110
120
130
정보 수집부
트래픽 검사부
트래픽 대응부
140
제어부

도면2


200
230
220
플로우 수
소스IP주소 #1
210
240
사용자 단말
바이트 수
250
소스IP주소 #N
초당 패킷수

도면3


시 작
S300
트래픽의 전송량≥임계값(TH)?
N
Y
S310
플로우 정보 집합화
S330
네트워크 대역 통제 미수행
화이트 리스트 그룹
S320
소스IP 주소의 그룹?
블랙 리스트 그룹
S340
트래픽의 네트워크 진입차단
일반그룹
S350
단위시간당 바이트수> 중간값?
N
Y
S360
트래픽의 전송량을 중간값까지 감소시킴
S370
단위시간당 플로우수> 중간값?
N
Y
S380
신규 플로우 생성 억제 및 기존 플로우를 중간값까지 감소시킴
S390
초당 패킷 전송수> 중간값?
N
Y
S400
초당 패킷 전송수> PPS?
N
Y
S410
DDoS 공격 발생 가능성을 알림
S420
해당 소스 IP주소를 블랙리스트그룹으로 이동
S430
초당패킷 전송수를 중간값까지 감소시킴
종 료