(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0020082
(43) 공개일자 2019년02월27일

(51) 국제특허분류(Int. Cl.)
H04L 12/721 (2013.01) *H04L 12/24* (2006.01)
H04L 12/46 (2006.01) *H04L 12/917* (2013.01)
H04L 29/08 (2006.01)
(52) CPC특허분류
H04L 45/38 (2013.01)
H04L 12/4641 (2013.01)
(21) 출원번호 10-2019-7001677
(22) 출원일자(국제) 2017년06월18일
심사청구일자 없음
(85) 번역문제출일자 2019년01월17일
(86) 국제출원번호 PCT/US2017/038053
(87) 국제공개번호 WO 2017/219009
국제공개일자 2017년12월21일
(30) 우선권주장
62/351,953 2016년06월18일 미국(US)

(71) 출원인
클레버넷 인코퍼레이티드
미국 캘리포니아 94159 샌프란시스코 차이나 베이 신 스트리트 #512 325
(72) 발명자
네미로브스키, 마리오
미국 캘리포니아 95030 로스 가토스 사우스 산타 크루즈 애비뉴 #105 20
세랄-그라시아, 르네
미국 캘리포니아 95030 로스 가토스 사우스 산타 크루즈 애비뉴 #105 20
(뒷면에 계속)
(74) 대리인
윤의섭, 김수진

전체 청구항 수 : 총 34 항

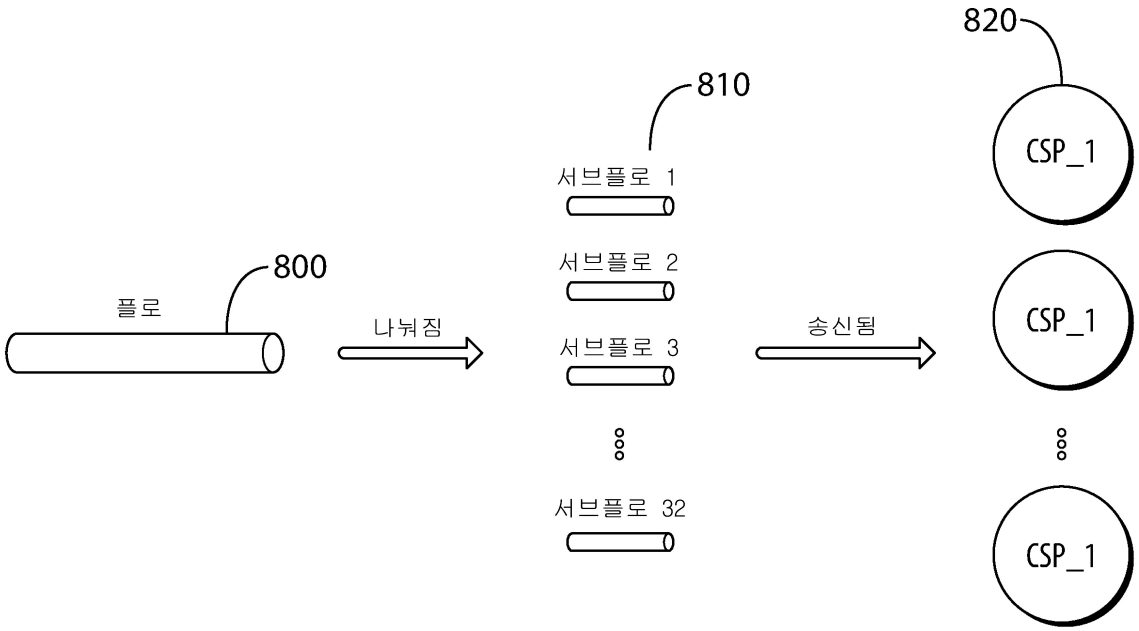
(54) 발명의 명칭 **다수의 채널을 사용하여 성능을 향상시키는 지능형 적응 전송 계층**

(57) 요 약

일련의 접속이 보다 효율적이고 제어된 방식으로 정보 플로를 송신하는 데 사용하기 위해 컴퓨터 네트워크 상의 호스트 간에 일련의 접속이 설정되고, 지속적으로 평가 및 유지 관리된다. 새로운 접속이 설정되고, 더 나은 성능 특성 및/또는 상이한 성능 특성을 가진 접속에 대한 지속적인 검색 시에 기존 접속은 종료된다. 각각의 접속

(뒷면에 계속)

대 표 도



은 네트워크를 통해 동일하거나 상이한 경로를 이용할 수 있으며 시간 경과에 따라 변경되는 성능 특성을 가질 수 있다. 주어진 정보 플로에 대해 여러 경로를 동시에 사용하여 처리량, 트랜잭션 시간, 데이터 일관성, 대기 시간, 및 패킷 손실을 포함하는 네트워크 메트릭을 개선시킬 수 있다. 정보의 플로는 하나 이상의 서브 플로로 분할될 수 있으며, 서브 플로는 하나 이상의 활성 접속에 할당될 수 있다. 또한, 플로가 어떻게 분할되고 접속에 할당되는지에 대한 동적 결정은 네트워크 조건에 응답하여 이루어질 수 있다. 이러한 접속의 사용을 통해, 비용을 절감하고 애플리케이션 QoS/QoE를 보장할 수 있으므로, 공용 인터넷과 같은 기존 네트워크가 기업급 접속을 제공할 수 있으며, 이는 현재 인터넷 인프라를 수정하지 않고도 기업 클라우드 채택을 가속화하는 데 사용될 수 있다.

(52) CPC특허분류
H04L 41/5019 (2013.01)
H04L 45/124 (2013.01)
H04L 47/76 (2013.01)
H04L 67/322 (2013.01)

(72) 발명자
시아치아, 프란체스코
미국 캘리포니아 95030 로스 가토스 사우스 산타 크루즈 애비뉴 #105 20

로메로 루이즈, 이반
미국 캘리포니아 95030 로스 가토스 사우스 산타 크루즈 애비뉴 #105 20

명 세 서

청구범위

청구항 1

네트워크 호스트를 연결하고 네트워크 호스트 간에 정보 플로를 통신할 수 있는 네트워크를 포함하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법에 있어서,

상기 복수의 접속 각각에 대해,

제1 네트워크 호스트와 제2 네트워크 호스트 간의 접속을 설정하는 하위 단계;

상기 접속과 연관된 적어도 하나의 성능 메트릭을 결정하기 위해 상기 접속을 반복적으로 평가하는 하위 단계; 및

상기 접속과 관련된 적어도 하나의 성능 메트릭에 기초하여, 복수의 상태 중에서 상기 접속에 대한 상태를 연관시키는 하위 단계 - 상기 복수의 상태 중에서 하나 이상의 제1 상태는 준비 상황을 나타내고, 상기 복수의 상태 중에서 하나 이상의 제2 상태는 준비되지 않은 상황을 나타냄 - 를 수행함으로써, 상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간에 복수의 접속을 유지하는 단계;

상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간의 정보 플로를 전송하라는 요청을 수신하는 단계;

상기 정보 플로를 상기 제1 상태 중 하나 이상과 연관된 상기 접속 중 하나 이상에 할당하는 단계; 및

상기 할당하는 단계에 기초하여 상기 복수의 접속 중 하나 이상을 통해 상기 정보 플로로부터의 데이터를 통신하는 단계;를 포함하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 2

제1항에 있어서,

상기 복수의 접속은 VPN 터널인 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 3

제1항에 있어서,

상기 적어도 하나의 성능 메트릭은 대기 시간, 처리량, 및 패킷 손실로 구성되는 세트로부터 취해진 하나 이상의 메트릭을 포함하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 4

제1항에 있어서,

상기 복수의 접속 중 하나에 대해 상기 네트워크를 통해 취해진 경로는 상기 복수의 접속 중 제2 접속에 대한 상기 네트워크를 통해 취해진 경로와 상이한 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 5

제1항에 있어서,

상기 제1 호스트는 복수의 엔드포인트를 가지고, 상기 복수의 접속 중 적어도 하나는 상기 복수의 접속 중 제2 접속과는 상이한 상기 엔드포인트 중 하나를 사용하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 6

제1항에 있어서,

상기 반복적으로 평가하는 단계는 상기 접속과 연관된 성능 메트릭을 규칙적인 간격으로 주기적으로 평가하는 단계를 포함하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 7

제1항에 있어서,

상기 하나 이상의 제2 상태는 대기 상황, 기다리는 상황, 강등 상황 및 탐색 상황을 나타내는 상태를 포함하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 8

제1항에 있어서,

상기 네트워크의 적어도 일부는 공용 인터넷의 일부를 포함하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 9

제1항에 있어서,

상기 복수의 접속 각각에 대해,

상기 접속의 상기 네트워크를 통한 경로를 결정하는 하위 단계를 더 포함하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 10

제1항에 있어서,

상기 정보 플로를 상기 제1 상태 중 하나 이상과 연관된 상이한 상기 접속 중 하나 이상에 재할당하는 단계 - 상기 재할당 단계는 상기 복수의 접속 중 적어도 하나와 연관된 적어도 하나의 성능 메트릭에 기초함 -; 및

상기 재할당하는 단계에 기초하여 상기 복수의 접속 중 하나 이상을 통해 상기 정보 플로로부터의 데이터를 통신하는 단계;를 더 포함하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 11

제1항에 있어서,

상기 복수의 접속 각각에 대해,

상기 접속이 상기 접속과 연관된 상기 적어도 하나의 성능 메트릭에 기초하여 기준을 충족시킬 때 상기 접속을 종료하는 하위 단계 - 상기 기준은 상기 접속과 연관된 적어도 하나의 성능 메트릭과 상기 복수의 접속 중 다른 것과 연관된 하나 이상의 다른 메트릭과의 비교에 기초함 - 를 더 포함하는 것을 특징으로 하는 시스템에서 네트워크 호스트 간의 복수의 접속을 이용하는 방법.

청구항 12

네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치에 있어서,

상기 장치는

프로세서 판독 가능 명령어를 저장하는 적어도 하나의 메모리와 통신하는 적어도 하나의 프로세서를 포함하는 제1 네트워크 호스트를 포함하고,

상기 적어도 하나의 프로세서는

상기 복수의 접속 각각에 대해,

제2 네트워크 호스트에 대한 접속을 확립하는 하위 단계;

상기 접속과 연관된 적어도 하나의 성능 메트릭을 결정하기 위해 상기 접속을 반복적으로 평가하는 하위 단계;

및

상기 접속과 연관된 적어도 하나의 성능 메트릭에 기초하여, 복수의 상태 중에서 상기 접속에 대한 상태를 연관시키는 하위 단계 - 상기 복수의 상태 중에서 하나 이상의 제1 상태는 준비 상황을 나타내고, 상기 복수의 상태 중에서 하나 이상의 제2 상태는 준비되지 않은 상황을 나타냄 - 를 수행함으로써, 상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간에 복수의 접속을 유지하는 프로세서 판독 가능한 명령어;

정보 플로를 상기 제2 네트워크 호스트로 전송하라는 요청을 수신하는 프로세서 판독 가능한 명령어;

상기 정보 플로를 상기 제1 상태 중 하나 이상과 연관된 상기 접속 중 하나 이상에 할당하는 프로세서 판독 가능한 명령어; 및

상기 할당하는 단계에 기초하여 상기 복수의 접속 중 하나 이상을 통해 상기 정보 플로로부터의 데이터를 통신하는 프로세서 판독 가능한 명령어;에 의해 동작 가능하게 구성되는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 13

제12항에 있어서,

상기 제1 호스트는 복수의 엔드포인트를 가지고, 상기 복수의 접속 중 적어도 하나는 상기 복수의 접속 중 제2 접속과는 상이한 상기 엔드포인트 중 하나를 사용하는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 14

제12항에 있어서,

반복적으로 평가하는 것은 상기 접속과 연관된 메트릭을 규칙적인 간격으로 주기적으로 평가하는 것을 포함하는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 15

제12항에 있어서,

상기 적어도 하나의 프로세서는

상기 정보 플로를 상기 제1 상태 중 하나 이상과 연관된 상이한 상기 접속 중 하나 이상에 재할당하는 프로세서 판독 가능한 명령어 - 상기 재할당하는 단계는 상기 복수의 접속 중 적어도 하나와 연관된 적어도 하나의 성능 메트릭에 기초함 -; 및

상기 재할당하는 단계에 기초하여 상기 복수의 접속 중 하나 이상을 통해 상기 정보 플로로부터의 데이터를 통신하는 프로세서 판독 가능한 명령어;에 의해 추가로 동작 가능하게 구성되는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 16

제12항에 있어서,

상기 적어도 하나의 프로세서는 상기 복수의 접속 각각에 대해,

상기 접속이 상기 접속과 연관된 상기 적어도 하나의 성능 메트릭에 기초하여 기준을 충족시킬 때 상기 접속을 종료하는 하위 단계 - 상기 기준은 상기 접속과 연관된 적어도 하나의 성능 메트릭과 상기 복수의 접속 중 다른 것과 관련된 하나 이상의 다른 메트릭과의 비교에 기초함 - 를 수행하는 프로세서 판독 가능한 명령어에 의해 추가로 동작 가능하게 구성되는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 17

제1항의 방법을 실행하도록 적어도 하나의 프로세서를 지시하기 위한 프로그램 코드로 인코딩된 비일시적 컴퓨

터 판독 가능 매체.

청구항 18

호스트 간에 정보를 통신할 수 있는 네트워크에 연결된 복수의 네트워크 호스트를 포함하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법에 있어서,

상기 시스템은 상기 네트워크 호스트 간의 복수의 접속을 이용하고,

상기 방법은

제1 네트워크 호스트와 제2 네트워크 호스트 간의 정보 플로를 전송하라는 요청을 수신하는 단계 - 상기 요청은 성능 요구 사항 및 애플리케이션 특성과 연관됨 -;

상기 정보 플로를 패킷의 시퀀스를 각각 포함하는 복수의 서브 플로로 분할하는 단계 - 상기 나누는 단계는 성능 요구 사항 및 애플리케이션 특성 중 하나 이상에 기초함 -;

상기 복수의 서브 플로 각각을 상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간의 복수의 접속 중에서 한 접속에 할당하는 단계; 및

상기 할당하는 단계에 기초하여 상기 복수의 접속 중 하나 이상의 접속을 통해 상기 복수의 서브 플로로부터의 데이터를 통신하는 단계;를 포함하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 19

제18항에 있어서,

상기 복수의 접속은 VPN 터널인 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 20

제18항에 있어서,

상기 애플리케이션 특성은 패킷 크기, 플로 크기, 플로 지속 시간, 대기 시간 요구 사항, 및 우선 순위로 구성되는 세트로부터 취해진 하나 이상의 특성을 포함하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 21

제18항에 있어서,

지원 성능 요구 사항은 하나 이상의 서비스 레벨 협약(service level agreement, SLA)에 기초하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 22

제18항에 있어서,

상기 분할하는 단계는 네트워크 상태, 사용자 정보, 및 과거 이력의 결정으로 구성되는 세트로부터 취해진 하나 이상의 아이템을 포함하는 정보에 추가로 기초하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 23

제18항에 있어서,

상기 분할하는 단계는 상기 정보 플로의 전송 중에 상기 정보 플로가 상기 복수의 서브 플로로 어떻게 동적으로 나누어지는지를 변경하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 24

제18항에 있어서,

상기 할당하는 단계는 상기 정보 플로의 전송 중에 상기 복수의 접속 중에서 상이한 접속으로 하나 이상의 서브 플로의 할당을 변경하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 25

제18항에 있어서,

상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간의 제2 정보 플로를 전송하라는 제2 요청을 수신하는 단계;

상기 제2 정보 플로를 패킷의 시퀀스를 각각 포함하는 제2 복수의 서브 플로로 분할하는 단계;

상기 제2 복수의 서브 플로 각각을 상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간의 상기 복수의 접속 중에서 한 접속에 할당하는 단계; 및

상기 제2 복수의 서브 플로 각각을 할당하는 상기 단계에 기초하여 상기 제2 복수의 접속 중 하나 이상을 통해 상기 제2 복수의 서브 플로 각각으로부터의 데이터를 통신하는 단계;를 더 포함하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 26

제25항에 있어서,

상기 복수의 접속 중 적어도 하나는 상기 정보 플로 및 상기 제2 정보 플로 모두로부터의 데이터를 통신하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 27

제18항에 있어서,

상기 네트워크의 적어도 일부는 공용 인터넷의 일부를 포함하는 것을 특징으로 하는 시스템에서 복수의 이용 가능한 접속을 통해 복수의 패킷을 포함하는 정보의 플로를 통신하는 방법.

청구항 28

네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치에 있어서,

상기 장치는

프로세서 판독 가능 명령어를 저장하는 적어도 하나의 메모리와 통신하는 적어도 하나의 프로세서를 포함하는 제1 네트워크 호스트를 포함하고,

상기 적어도 하나의 프로세서는

정보 플로를 제2 네트워크 호스트로 전송하라는 요청을 수신하는 프로세서 판독 가능한 명령어 - 상기 요청은 성능 요구 사항 및 애플리케이션 특성과 연관됨 -;

상기 정보 플로를 패킷의 시퀀스를 각각 포함하는 복수의 서브 플로로 분할하는 프로세서 판독 가능한 명령어 - 분할하는 단계는 성능 요구 사항 및 애플리케이션 특성 중 하나 이상에 기초함 -;

상기 복수의 서브 플로 각각을 상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간의 복수의 접속 중에서 한 접속에 할당하는 프로세서 판독 가능한 명령어; 및

상기 할당하는 단계에 기초하여 상기 복수의 접속 중 하나 이상을 통해 상기 복수의 서브 플로로부터의 데이터를 통신하는 프로세서 판독 가능한 명령어;에 의해 동작 가능하게 구성되는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 29

제28항에 있어서,

상기 애플리케이션 특성은 패킷 크기, 플로 크기, 플로 지속 시간, 대기 시간 요구 사항, 및 우선 순위로 구성되는 세트로부터 취해진 하나 이상의 특성을 포함하는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 30

제28항에 있어서,

상기 프로세서는 상기 정보 플로의 전송 중에 상기 정보 플로가 상기 복수의 서브 플로로 어떻게 동적으로 나눠지는지를 변경하도록 동작 가능하게 구성되는 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 31

제28항에 있어서,

상기 프로세서는 상기 정보 플로의 전송 중에 상기 복수의 접속 중에서 상이한 접속으로 하나 이상의 서브 플로의 할당을 변경하도록 동작 가능하게 구성되는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 32

제28항에 있어서,

상기 적어도 하나의 프로세서는

상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간의 제2 정보 플로를 전송하라는 제2 요청을 수신하는 프로세서 판독 가능한 명령어;

상기 제2 정보 플로를 패킷의 시퀀스를 각각 포함하는 제2 복수의 서브 플로로 분할하는 프로세서 판독 가능한 명령어;

상기 제2 복수의 서브 플로 각각을 상기 제1 네트워크 호스트와 상기 제2 네트워크 호스트 간의 상기 복수의 접속 중에서 한 접속에 할당하는 프로세서 판독 가능한 명령어; 및

상기 제2 복수의 서브 플로 각각을 할당하는 단계에 기초하여 상기 제2 복수의 접속 중 하나 이상을 통해 상기 제2 복수의 서브 플로 각각으로부터의 데이터를 통신하는 프로세서 판독 가능한 명령어;에 의해 추가로 동작 가능하도록 구성되는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 33

제33항에 있어서,

상기 복수의 접속 중 적어도 하나는 상기 제1 정보 플로 및 상기 제2 정보 플로 양자 모두로부터의 데이터를 통신하는 것을 특징으로 하는 네트워크 호스트를 연결하는 네트워크를 통해 네트워크 호스트 간에 정보 플로를 통신하기 위한 장치.

청구항 34

제18항의 방법을 실행하도록 적어도 하나의 프로세서를 지시하기 위한 프로그램 코드로 인코딩된 비일시적 컴퓨터 판독 가능 매체.

발명의 설명

기 술 분 야

[0001] **관련 출원**

[0002] 본 출원은 본 명세서에 참조로서 포함된 2016년 6월 18일에 출원된 미국 가출원 제62/351,953의 우선권을 주장한다.

[0003] **기술분야**

[0004] 본 발명은 컴퓨터 네트워킹 분야에 관한 것으로, 보다 구체적으로, 패킷 교환 네트워크의 엔드포인트 간의 대기 시간, 플로 완료 시간(flow completion time, FCT) 및 처리량과 같은 네트워크 메트릭을 제어하는 것에 관한 것이다. 이는 공용 인터넷, 사설 네트워크, 및 3G/4G/5G 모바일 네트워크와 같은 네트워크를 포함한다.

배 경 기 술

[0005] 인터넷은 복원력(resilience), 분권화, 및 최선형 패킷 전달과 같은 속성을 보장하면서 탁월한 접속성을 제공한다. 그러나, 이러한 특성은 트래픽의 피크를 핸들링하기 위한 인터넷 코어의 낮은 활용도를 초래한다. 또한, 인터넷은 중요한 애플리케이션의 사용을 저해한다는 점에서 일반적으로 결정론적이지 않다. 기업은 일반적으로 처리량과 대기 시간을 포함하여 관심 대상 메트릭을 보장하기 위해 사설 네트워크를 배치한다. 그러나, 사설 네트워크는 운영비(operational expenses, OPEX)와 자본 지출(capital expenditure, CAPEX)이 커서 모든 기업이 비용을 감당할 수 있는 것은 아니다. 가상 사설 네트워크(Virtual Private Network, VPN)는 인터넷을 기본 기술로 사용하여 사설 네트워크의 이점을 모방한다. VPN은 공용 네트워크를 통한 보안 및 성능 보장을 위해 터널링 기술에 의존한다. 그러나, VPN은 통상적으로 기업의 중요한 측면인 네트워크 메트릭을 보장하지 않으면서 단일 터널을 사용하여 정보를 송신한다. 일부 시스템에서는 트래픽의 우선 순위를 지정하기 위해 MPLS(Multiprotocol Labeled System)와 같은 패킷 교환 계층을 적용하지만, 이는 특정 캐리어의 네트워크에서만 작동한다. 트래픽이 공용 인터넷을 통과할 때 서비스 품질(Quality of Service, QoS) 또는 체감 품질(Quality of Experience, QoE)을 보장하면서 처리량과 같은 메트릭을 제어하는 개선된 방법이 필요하다.

[0006] 인터넷 프로토콜 제품군(TCP/IP)은 한 지점에서 다른 지점으로 데이터가 전송되는 방법을 지정하는 통신을 위한 종단 간 프레임 워크를 제공한다. 이 모델은 일반적으로 OSI 7 계층 아키텍처 또는 4 계층 구조(링크, 인터넷, 전송, 애플리케이션)를 통해 제공된다. 이 시스템은 비용을 낮게 유지하면서 엔드포인트의 수가 급격히 증가함에 따라 인터넷을 확장할 수 있게 했다. 오늘날, 공용 인터넷은 방대한 양의 서비스와 애플리케이션이 의존하는 기본 시스템 중 하나이다. 많은 회사들이 서비스를 제공하고 인프라를 관리하기 위해 인터넷을 사용한다.

[0007] 공용 인터넷의 중요한 단점은 대기 시간 및 처리량과 같은 네트워크 메트릭을 보장하는 결정론적 서비스를 제공하는 것이 일반적으로 불가능하다는 것이다. 이 사실로 인해 여러 기관 및 회사에서 특정 서비스 품질(QoS)을 보장하는 사설 네트워크를 구축하게 되었다. 이러한 네트워크는 공용 인터넷에도 접속되지만 방화벽을 통해 중요하지 않은 서비스나 최소한의 목적으로만 접속된다. 이러한 시스템은 배치 및 유지 관리가 대규모 사설 회사에서 처리되므로 값비싼 배치이다. 반대로, 공용 인터넷은 통합 프로토콜로 운영되는 전 세계 공유 인프라를 갖춘 네트워크의 네트워크이다.

[0008] 이러한 사설 네트워크는 물리적이든 가상이든 상관없이 상이한 네트워크 프로토콜과 기술에 의존하여 엔드포인트를 상호 접속한다. 예를 들어, 본 명세서에 참조로 포함된 <Internet Engineering Task Force(IETF) Request for Comments(RFC) 3031>에 설명된 MPLS(Multiprotocol Label Switching)는 가상 전용 통신 채널 덕분에 표준 인터넷 접속과 비교하여 제어 가능한 성능과 안정성을 제공한다. 다른 최적화 기술 중에서도, 애플리케이션 유형과 같은 상이한 파라미터에 기초하여 트래픽의 우선 순위를 지정한다. 그러나, MPLS 배치는 통상적으로 Mbit당 100배 이상으로 훨씬 더 높은 비용이 소요된다. 예를 들어, 본 명세서에 참조로 포함된 <"What is the cost of MPLS?", Mushroom Networks Blog, August 20, 2015>를 참조하라.

[0009] 최근 몇 년 동안, 클라우드 컴퓨팅의 등장으로 인해 상호 접속 문제가 악화되었다. 예를 들어, 본 명세서에 참조로 포함된 <"A View of Cloud Computing," M. Armbrust 외>를 참조하라. 클라우드 컴퓨팅은 실제로 사용되는 리소스에 대한 비용을 지불하면서 주문형 서비스로 제공되는 유연한 인프라의 외부화를 제공한다. 그러나, 클라우드 컴퓨팅 모델에는 데이터가 생성되고 소비되는 기업과 데이터가 처리되고 저장되는 데이터 센터 간의 통신에 중요한 포인트가 있다. 이 사실은 클라우드 컴퓨팅 패러다임의 통합을 저해했다. 일부 업계 리더에 따르면, 작업 부하의 5%만이 공용 클라우드에 있다.

[0010] 주된 이유는 보안, 고정 비용, 데이터 프라이버시, 및 네트워크 비용이 IT 팀의 주저에 의해 악화되기 때문이다.

[0011] 중요한 애플리케이션을 관리할 수 있는 네트워크 사용 및 중요하지 않은 애플리케이션의 특정 경계를 보장해야 하는 필요성과 같은 클라우드 컴퓨팅의 잠재력을 달성하는 데 필요한 잃어버린 부분이 있다. 현재, 대기업만이 사설 광역 네트워크(Wide Area Network, WAN)에 필요한 전용 링크에 대한 비용을 지불할 수 있다. 또한, 이러한 네트워크는 패킷 교환 네트워크 대신 지점 간 접속에 의존하므로 공용 인터넷과 같은 네트워크의 주요 이점을 포기하기 때문에 확장성 문제가 존재한다. 최근에, 가장 큰 클라우드 서비스 제공업체는 사설 데이터 센터를 공용 클라우드에 접속하는 솔루션을 제공하여 이 문제를 해결했다. 예를 들어, Amazon Web Services는 Direct Connect를 제공하고 Microsoft Azure는 ExpressRoute를 제공한다. 그러나, 이러한 솔루션은 클라우드에 대한 사설 접속을 사용하여 문제를 해결한다. 따라서, 신뢰성을 유지하면서도 저비용 및 우수한 확장성을 갖는 네트워크 접속의 문제점은 여전히 해결되지 않고 있다.

발명의 내용

도면의 간단한 설명

[0012] 도 1은 기업 시나리오의 예를 도시한다.

도 2는 기업 시나리오의 예를 도시한다.

도 3은 클라우드 시나리오의 예를 도시한다.

도 4는 클라우드 시나리오의 예를 도시한다.

도 5는 글로벌 시나리오의 예를 도시한다.

도 6a는 간단한 MPTCP 예를 도시한다.

도 6b는 표준 TCP 및 MPTCP 프로토콜의 비교를 도시한다.

도 7은 기업 본사에 접속된 지사의 예시적인 실시예를 도시한다.

도 8은 다수의 CSP 내부의 플로로 나누는 것을 도시한다.

도 9a는 상이한 ISP와 인터넷의 코어를 통과하는 CSP를 도시한다.

도 9b는 인터넷 상의 상이한 경로를 도시한다.

도 10은 CSP 상태도를 도시한다.

도 11은 3 계층 CSP 관리 아키텍처를 도시한다.

도 12는 단일 기업 관점에서 시스템 아키텍처를 도시한다.

도 13은 2개의 상이한 기업을 갖는 글로벌 관점에서 시스템 아키텍처를 도시한다.

도 14a는 기업 간 중간 계층을 포함하여 2개의 상이한 기업을 갖는 글로벌 관점에서 시스템 아키텍처를 도시한다.

도 14b는 각각의 기업에 대한 특정 서브 계층과 결합된 서브 계층을 갖는 보다 복잡한 중간 계층을 도시한다.

도 15는 아키텍처 계층 내부의 학습 구성 요소를 도시한다.

도 16은 각각의 레벨에 대한 입력 및 출력을 포함하는 계층적 학습 아키텍처를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 발명의 실시예는 현재의 인프라를 사용하여 애플리케이션의 서비스 품질(QoS) 또는 체감 품질(QoE)을 보장하기 위해 공용 인터넷을 지능적으로 사용한다. 서비스 품질(QoS)은 서비스 파라미터(예컨대, 패킷 손실률이나 평균 처리량)를 객관적으로 측정하는 반면, 체감 품질(QoE)은 고객의 서비스 경험(예를 들어, 웹 브라우징, 전화 통화, TV 방송, 또는 콜센터 호출)을 측정하는 것과는 다르지만 관련 개념이다. 핵심 전제는 보장된 QoS/QoE를 제공하는 동시에 감소된 가격 및 확장성을 유지하는 것이다.

[0014] 본 발명의 실시예를 이용하면, 보다 효율적이고 제어된 방식으로 정보를 송신하기 위해 다수의 엔드포인트 간에 일련의 접속이 설정된다. 이러한 접속을 통해 감소된 비용이 제공될 수 있으며, 처리량, 패킷 손실, 및 대기 시

간과 같은 네트워크 메트릭에 대해 애플리케이션 QoS/QoE가 보장될 수 있다. 본 발명의 실시예를 이용하는 것은 공용 인터넷과 같은 기존의 네트워크가 현재 인터넷 인프라를 수정하지 않고서도 기업 클라우드 채택을 가속화하는 데 사용될 수 있는 기업급 접속을 제공할 수 있게 한다.

[0015] 본 발명의 실시예는 대부분의 네트워크, 특히 인터넷에서 사용되지 않는 용량이 있다는 관찰에 기초한다. 트래픽 피크를 흡수하기 위해, 코어의 라우터가 과도하게 프로비저닝되므로 낮은 사용률 레벨로 실행된다. 이는 정체 기간을 제외하고는 사용되지 않은 대역폭이 많이 있음을 의미한다. 이 여분의 대역폭을 사용하기 위해 이용된 도구와 기술은 다중 경로 프로토콜을 사용할 수 있다. 처리량, 트랜잭션 시간, 데이터 일관성, 대기 시간, 및 패킷 손실을 포함하여 상이한 네트워크 메트릭을 개선시키기 위해 여러 경로가 동시에 사용된다. 또한, 네트워크 조건에 따라 동적 결정이 이루어진다.

[0016] 다음과 같은 약어가 본 명세서에서 사용된다:

[0017] CSP Certified Starflow™Path

[0018] QoE Quality of Experience

[0019] ASP Aggregated Secured Paths

[0020] BW Bandwidth

[0021] QA Quality Assurance

[0022] LCI Local Contextual Information

[0023] GCI Global Contextual Information

[0024] 이 명세서에서 인터넷이라는 용어는 공용 인터넷, 또는 공용 또는 사설 여부에 관계없이 인터넷 프로토콜을 사용하는 임의의 다른 패킷 교환 네트워크를 의미하는 데 사용된다. 본 발명의 실시예는 다양한 상이한 시나리오 하에서 이용될 수 있다. 아래에 몇 가지 시나리오가 설명되어 있다.

[0025] 시나리오 1: 기업: 사무실 상호 접속

[0026] 도 1에 도시된 이 시나리오에서는 지사(100, 110, 120, 130)가 본사(140)와 접속을 설정한다. 공용 인터넷(150) 상의 다수의 라우터(예를 들어, 160)는 접속을 설정하는 데 사용된다. 본 발명의 실시예가 QoE 보증을 제공하기 때문에 현재 사용되는 사설 링크가 더 이상 필요하지 않다. 지능형 정책은 사설 링크에 의존하기보다는 인터넷, 3G/4G/5G 모바일 네트워크 및/또는 다중 경로 기술을 사용하는 사설 네트워크의 기존의 과다한 용량을 활용한다. 이 솔루션은 회사가 고성능을 경험하면서 OPEX 및 CAPEX를 줄이는 가상 사설 WAN을 만든다.

[0027] 도 2에서, 기업 시나리오는 모바일 디바이스를 갖춘 것으로 도시되어 있다. 지사(200, 210)와 모바일 디바이스(220, 230, 240)는 라우터(260)를 통해 공용 인터넷(250)에 그리고 본사(HQ)(270)에 연결된다. 모바일 디바이스는 사무실 상호 접속 시나리오에 새로운 차원을 추가한다. 이 경우, 디바이스는 물리적 위치의 경계 내에 한정되지 않지만 상이한 이동성 패턴을 갖는다. 예를 들어, 모바일 디바이스는 특정 지사에 머무르는 동안 HQ와의 접속을 설정한다. 이어서, 그 직원은 그 디바이스를 가지고 다른 위치에 있는 고객을 방문할 수 있다. 본 발명은 접속을 끊거나 QoE를 저하시키지 않으면서 이러한 상황을 핸들링한다. 또한, 기업 구내를 기반으로 추가 제약 조건이 적용될 수 있다. 한 회사 정책은 방화벽을 사용하기 위해 모든 디바이스가 먼저 한 사무실에 접속되어야 한다고 명시할 수 있다. 다른 회사는 모바일 디바이스가 HQ에 직접 접속하는 것을 허용할 수 있다. 이들은 고레벨 상황이지만, 모바일 디바이스의 수 및 이들의 이동성 패턴이 본 발명에 의해 제시된 솔루션에 영향을 미친다는 것은 명백하다.

[0028] 시나리오 2: 클라우드: 클라우드 데이터 센터를 클라이언트와 접속시키기

[0029] 도 3은 클라우드를 수반하는 시나리오를 도시한다. 본사에 지사를 접속시키는 대신, 라우터(360)를 통해 공용 인터넷(350)을 통해 공용 클라우드 데이터 센터(340)에 다수의 클라이언트(300, 310, 320, 330)가 연결된다. 클라우드 공간에는 두 가지 주요 사상 학파가 있다. 일부 주요 기업(예를 들어, Amazon 및 Google)은 모든 처리를 실행하고 데이터를 저장하는 공용 클라우드에만 전념한다. 대조적으로, 다른 회사(예를 들어, Microsoft)는 공용 클라우드와 사설 기업 클라우드 간에 작업 부하 및 스토리지를 분할할 수 있는 하이브리드 클라우드 모델을 옹호한다.

[0030] 본 발명의 실시예는 기업 시나리오에서와 같이 클라우드 시나리오에서 동일한 기본 기술을 사용한다. 각각의 엔

드포인트(클라이언트 또는 클라우드)는 다중 경로 기술을 사용하여 다수의 경로를 동시에 가능하게 하므로, 필요한 액세스 QoE를 보장한다.

[0031] 모바일 디바이스는 클라우드 클라이언트로 간주될 수도 있다. 도 4는 모바일 디바이스가 통합된 클라우드 시나리오를 도시한다. 라우터(460)를 통해 공용 인터넷(450)을 사용하여 클라우드 데이터 센터(470)에 클라이언트(400, 410, 420)와 모바일 클라이언트(430, 440)가 함께 연결된다. 클라우드와 기업 시나리오 간의 주요 차이점에는 특히 다양한 애플리케이션 유형, 트래픽 패턴, 리소스 공유, 및 이러한 리소스의 관리가 포함된다.

[0032] 시나리오 3: 글로벌 시나리오

[0033] 도 5는 글로벌 또는 전체-전체 시나리오를 도시한다. 이 시나리오는 모바일 디바이스를 포함하여 기업 시나리오와 클라우드 시나리오가 결합된 결과이다. 기업 본사(570) 및 클라우드 데이터 센터(580)와 함께 클라이언트(500, 520, 530, 540) 및 모바일 클라이언트(510, 550)는 라우터(560)를 통해 공용 인터넷(590)에 연결된다. 이 시나리오에서, 본 발명의 실시예는 클라이언트의 요구에 기초하여 상이한 QoE를 보장하면서 엔드포인트(예를 들어, 사무실, HQ, 모바일 디바이스, 공용 클라우드 등) 사이의 상이한 접속을 지원한다.

[0034] 도입

[0035] 인터넷 전송 프로토콜은 원래 복원력, 견고함, 및 안정성을 염두에 두고 설계되었다. 또한, 각각의 라우터의 가시성이 인접 라우터로 제한되므로 링크별로 작동한다. 따라서, 라우팅 결정은 전체 네트워크의 상태를 고려하기보다는 로컬 조건에 기초한다. 이러한 아키텍처 결정은 인터넷 확장성에 크게 기여하지만 처리량 및 대기 시간과 같은 다른 메트릭에 대한 성능에는 불리하다.

[0036] 클라우드와 같은 모델은 공용 인터넷에 의존하여 서비스를 제공하므로, 네트워크 메트릭은 전반적인 성능에 큰 영향을 준다. 또한, 데이터에 대한 제어 부족과 같은 새로운 문제가 발생한다. 이러한 영향에도 불구하고, 회사는 공용 클라우드를 사용하여 설치 용이성, 유연한 인스턴스, 비용 효율성, 및 가용성과 같은 요소를 활용하도록 동기가 유발될 수 있다.

[0037] 본 발명의 실시예는 기존의 공용 인터넷 인프라를 사용하여 우수한 성능을 제공하는 네트워크 솔루션을 이용한다. 이를 위해, 최종 사용자에게 체감 품질(QoE)을 보장하기 위해 상이한 접속 유형에 대한 로컬 및 글로벌 맥락(context) 정보를 활용하여 최적화된 라우팅 기법이 활용된다.

[0038] 채택된 핵심 기술은 정보 패킷을 지능적인 방식으로 전송하기 위해 다수의 경로를 이용하는 것이다. 통합 경로의 역량에는 처리량 증가, 향상된 보안, 대기 시간 감소, 패킷 손실 감소, 및 신뢰성 향상이 포함된다.

[0039] 프로토콜

[0040] 위에 논의된 시나리오에 직면한 회사를 위한 바람직한 솔루션은 공용 인터넷을 기본 인프라로 사용하지만 사설 네트워크의 이점을 얻는 것이다. 이러한 접근 방식은 배치 및 관리 비용을 줄여줄 것이다. 이러한 성과를 가능하게 하는 기술은 부분적으로 터널 구현에 의존한다. 이들은 공용 인터넷을 통해 전송된 트래픽에 견고성, 무결성, 및 보안을 추가한다.

[0041] 본 발명의 실시예는 가상 사설 네트워크(VPN)를 사용하여 터널을 구현한다. VPN은 본 명세서에 참조로 포함된 <Internet Engineering Task Force(IETF) Request for Comments(RFC) 2764>에서 논의된다. 본 발명의 일 실시예에서는, OpenVPN(https://openvpn.net/)이 사용된다. 대안적인 실시예에서는, IPSEC 구현이 사용된다. IPSEC는 본 명세서에 참조로 포함된 <Internet Engineering Task Force(IETF) Request for Comments(RFC) 6071>에서 논의된다.

[0042] 본 발명의 실시예는 VPN 터널을 사용하여 암호화를 사용하여 기밀 방식으로 데이터를 전송한다. 대안적인 실시예에서, 터널은 암호화된 패킷을 생성하고 성능을 증가시키는 데 요구되는 계산 시간을 줄이기 위해 안전하지 않다.

[0043] 본 발명의 실시예는 기본 인터넷 인프라를 유리하게 이용한다. 인터넷은 패킷 교환 네트워크로 설계되고 작동하며, 따라서 잠재적으로 소스와 목적지 사이에 많은 수의 경로가 존재한다. 본 발명의 실시예는 터널링을 이용하여 다수의 경로를 발견하고 유지하지만, 대안적인 실시예는 접속 풀링과 같은 다른 기술을 이용한다. 접속 풀링은 접속 풀을 항상 활성으로 유지하고 애플리케이션 데이터를 전송하기 위해 그것을 재사용하는 것으로 구성된다. 접속 풀링과 터널링의 차이점은 터널이 수정되지 않은 패킷을 헤더와 함께 전송하는 반면 접속 풀링은 패킷의 페이로드를 전송하며 추가 세부 정보가 대역 외 또는 사용자 정의 프로토콜을 통해 전송되어야 할 수도 있다

는 것이다. 본 발명의 일 실시예에서, TCP 폴링은 인터넷을 통해 TCP 데이터를 전송하는 데 사용된다.

[0044] 다중 경로 전송은 네트워크 장비를 수정하거나 재구성하는 것을 필요로 하지 않으면서 상이한 경로 세트를 사용하는 것을 허용한다. 즉, 다중 경로 전송은 라우터에 투명하다. 본 발명의 실시예는 다중 경로 전송의 이점을 VPN과 결합하여 미리 설정된 특성화된 터널 세트를 통해 데이터를 동시에 전송한다. 이들 VPN 터널은 이더넷, ARP, ICMP, IP, TCP 또는 UDP와 같은 OSI 데이터 링크 계층 이상의 특성에 적합한 임의의 프로토콜의 패킷을 전달할 수 있다.

[0045] 복제 및 분산과 같이, 다수의 경로를 이용할 수 있는 많은 기술이 정의될 수 있다. 복제는 정보 플로를 복제하고 그것을 상이한 경로를 통해 전송하여 최상의 성능을 획득한다. 증가된 신뢰성은 비용이 든다. 이 기술은 여러 번 전송된 동일한 트래픽이 서로 간섭하고 라우터를 정체시키기 때문에 큰 오버헤드를 갖는다. 대조적으로, 분산은 정보 플로를 서브 플로로 분해하여 그것들을 상이한 경로를 통해 전송한다. 이 기술은 정체를 줄이지만 잠재적으로 순서가 틀리는 문제를 악화시킬 수 있다. 전송된 트래픽의 특정 요구 사항에 따라 경로가 지능적으로 사용되면, 성능이 향상될 수 있다. 두 기술 모두 다수의 경로를 생성하기 위해 공통의 오버헤드를 공유한다.

[0046] 본 발명의 실시예는 인터넷의 다중 접속성을 이용함과 동시에 VPN 및 TCP 프로토콜 파라미터를 조정하여 일반적으로 처리량 및 성능을 개선시킨다. 예를 들어, 일 실시예는 거대한 최대 전송 유닛(Maximum Transmission Unit, MTU) 값(심지어 이더넷 9KB 점보 프레임보다 큼, 예를 들어 48KB MTU)을 사용하여 LAN을 시뮬레이션하기 위해 VPN 터널에 의해 제공되는 추상성(abstraction)을 이용할 수 있다; 그 다음에, TCP 최대 세그먼트 크기(Maximum Segment Size, MSS)가 이 조정에 적응되어 터널 가상 인터페이스에서 큰 프레임의 주입을 허용할 것이다; 그 다음에, 이러한 거대한 프레임은 경로 상의 라우터에 의해 또는 그것을 생성하는 동일한 물리적/가상 호스트에 의해 다수의 IP 조각으로 조각날 것이다. 이러한 방식으로, 발신자의 TCP 정체 제어 알고리즘은 보내는 창 값의 빠른 증가를 보여 지속적으로 증가하는 처리량을 가져올 것이다.

[0047] 이러한 이점을 이용하기 위해, TCP와 UDP가 주된 전형임에도 불구하고 상이한 프로토콜이 사용될 수 있다. 본 발명의 실시예는 터널을 통해 패킷을 전송한다. 터널 선택 및 패킷 스케줄링은 패킷 우선 순위 요구 사항과 일치하는 터널 메트릭에 기초한다.

[0048] MPTCP

[0049] 다중 경로 전송, 다중 경로 TCP에 대한 한 가지 접근법은 본 명세서에 참조로 포함된 <Engineering Task Force(IETF) Request for Comments(RFC) 6182>에서 기술된 <Architectural Guidelines for Multipath TCP Development>에 기술되어 있다. 다중 경로 TCP(Multipath TCP, MPTCP)는 다중 경로를 가능하게 하는 TCP의 확장이다. 도 6a는 MPTCP의 간단한 예를 도시한다. 두 개의 접속(A1, A2)은 호스트 A(600)를 인터넷(610)에 연결하고, 두 개의 접속(B1, B2)은 호스트 B(620)를 인터넷(610)에 연결한다. 호스트 A에서 호스트 B까지의 각각의 경로는 IP 소스 및 목적지 주소, IP 소스 및 목적지 포트 번호, 및 사용된 프로토콜로 구성된 5 튜플로 고유하게 식별된다.

[0050] 전술한 바와 같이, 인터넷을 통한 경로가 반드시 분리되어 있는 것은 아니다. 예를 들어, A1-B1 및 A1-B2는 네트워크 내에서 공통 링크를 공유할 수 있으며, 이 경우 지능형 선택은 정체 및 상호 간섭을 방지할 것이다.

[0051] MPTCP는 (i) 다수의 경로의 동시 사용을 통해 처리량을 개선시키고, (ii) 경로를 통해 세그먼트를 전송할 수 있으므로 복원력을 개선시키는 두 가지 주요 목표를 갖고 있다. 두 가지 목표는 독립적이지 않다. 노드 장애는 MPTCP의 복원력이 중요한 극단적인 경우이다. 일부 조건에서는 MPTCP가 TCP 성능을 능가할 수 있다. 실제에서는 구현 세부 사항이 고려되어야 한다. 예를 들어, MPTCP의 오버헤드 비용은 작은 파일을 전송할 때 이점에 반대로 작용할 수 있다.

[0052] MPTCP의 사용이 일반화되면, 여분 용량의 더 나은 사용을 통해 정체된 병목 현상에서 트래픽을 이동시켜 전체 인터넷의 정체를 줄일 수도 있다.

[0053] MPTCP 아키텍처 스택의 개요가 도 6b에 도시되어 있다.

[0054] 표준 TCP(630)가 왼쪽에 도시되어 있고 MPTCP(640)가 오른쪽에 도시되어 있다. MPTCP 계층은 경로 관리, 패킷 스케줄링, 서브 플로 인터페이스, 및 정체 제어를 핸들링한다. 서브 플로는 각각의 경로에 기본 전송을 제공하는 표준 TCP 세션이다. 이러한 모든 세부 사항은 애플리케이션에 투명하다.

[0055] Linux용 기준 MPTCP 구현은 커널 공간에서 실행된다.

[0056] 본 발명의 실시예는 기존 Linux 구현의 특정 MPTCP 커널 모듈에 대한 수정을 수반한다. 이 모듈은 사용자 공간에 구현된 프로세스에서 MPTCP 접속을 최적화하기 위해 Netlink를 통해 명령을 수신한다.

[0057] 일 실시예에서, 디폴트 풀 메시 토폴로지를 사용하는 대신 클라이언트(예를 들어, 지사)와 서버(예를 들어, HQ) 사이의 포인트-포인트 접속을 개선시키는 새로운 커널 모듈이 이용된다. 이 모듈은 (예를 들어, 같은 사무실에 있는 동일한 디바이스의 두 IP 포트 사이의) 사용되지 않는 접속을 제거하여 다중 경로 전송의 오버헤드를 줄인다. 일 실시예에서, 기존 MPTCP Linux 구현의 인터페이스 제한이 증가되었다. 이 수정으로, 이제 플로는 원래 구현에서 부과된 한계인 8개가 아니라 최대 32개의 인터페이스를 사용할 수 있다. 대안적인 실시예에서, 인터페이스 및 서브 플로의 최대 수는 더 클 수 있다.

[0058] 대안적인 실시예에서, 사용자 공간 패킷 I/O(예를 들어, DPDK)와 함께 완전한 사용자 공간 구현이 이용될 수 있다. 이 실시예는 하이브리드 커널-사용자 공간 솔루션보다 더 효율적이다. 이는 프로토콜 구현 및 성능 최적화를 제어하면서 커널에서 사용자 공간으로 또는 그 반대로 통신하는 것과 연관된 오버헤드를 줄이는 것을 가능하게 한다. 다른 대안적인 실시예에서는, 전체 커널 공간 구현이 이용될 수 있다.

[0059] 본 발명의 실시예에서, 2개의 MPTCP 서브 모듈의 새로운 버전인 경로 관리자 및 패킷 스케줄러가 이용된다. 경로 관리자는 설정할 서브 플로 수를 결정한다. 새 버전은 서브 플로를 동적으로 생성하고 닫을 수 있으며 아래 설명된 다른 수정도 가능하다. 스케줄러는 서브 플로에 패킷을 할당한다. 새로운 스케줄러 알고리즘은 서브 플로와 애플리케이션 간의 부하의 균형을 조정한다.

[0060] 다중 경로 UDP(Multipath UDP, MPUDP)

[0061] UDP는 다른 주요 전송 프로토콜이다. MPUDP를 지원하기 위한 UDP 확장은 아직 표준화되지 않았지만, UDP 접속이 다수의 경로를 동시에 이용할 수 있도록 하기 위한 기본 개념은 동일하다. TCP와는 달리, UDP는 신뢰성 있는 전송 프로토콜이 아니며, 즉 드롭된 패킷, 순서가 틀린 패킷, 및 복제된 패킷의 문제를 애플리케이션에 남겨둔다.

[0062] MPUDP는 UDP 특성인 신뢰할 수 없는 전송, 정체 제어와 패킷 순서 보증의 부족을 이어받는다. 현재, 3개의 표준 프로토콜인 UDP, DCCP 및 SCTP만이 신뢰할 수 없는 전송을 구현한다. UDP에는 정체 제어가 없기 때문에, 주로 처리량이 낮은 전송의 경우에 사용된다. 애플리케이션 요구 사항에 따라, 상이한 주요 메트릭이 최적화되어야 한다. 예를 들어, 일부 애플리케이션에서는 패킷 손실을 줄이는 것이 매우 중요하지만 다른 애플리케이션에서는 한 방향 지연을 줄이는 것이 더 중요하다. 다중 경로는 이 주제에서 상당히 도움이 될 수 있다. 예를 들어, 패킷 손실을 줄이기 위해, UDP 트래픽은 덜 정체한 경로로 이동될 수 있다. 한 방향 지연을 줄이기 위해, UDP 트래픽은 복제되고 동시에 여러 경로로 전송될 수 있다. 후자의 경우, 수신자 측에서 복제를 제거하는 것이 중요하다. 이는 UDP 전송을 DCCP 전송으로 변경하여 달성될 수 있다.

[0063] 데이터 그램 정체 제어 프로토콜(Datagram Congestion Control Protocol, DCCP)은 (세션 핸드 쉐이킹 및 시퀀스 번호를 사용하여) TCP와 유사한 정체 제어를 통해 신뢰할 수 없는 전송을 구현한다. DCCP는 본 명세서에 참조로 포함된 <Internet Engineering Task Force(IETF) Request for Comments(RFC) 4340>에서 기술된다.

[0064] 스트림 제어 전송 프로토콜(Stream Control Transmission Protocol, SCTP)은 만료된 데이터의 재송신을 방지하는 부분 신뢰도(Partial Reliability, PR)를 확장했다. SCTP는 본 명세서에 참조로 포함된 <Internet Engineering Task Force(IETF) Request for Comments(RFC) 4960>에서 기술된다.

[0065] 이 세 가지 프로토콜 중에서 DCCP와 SCTP만이 정체 제어 기능이 있으며, SCTP만이 다중 스트림 및 다중 홈(다중 경로)을 지원한다. 따라서, 효율적인 MPUDP를 위한 두 가지 가능한 후보는 다중 경로 DCCP(경로 관리자 및 패킷 스케줄러를 수동으로 구현), 또는 부분 신뢰성 및 다중 홈을 구비한 SCTP일 것이다. 전자와 같은 접근 방식은 본 명세서에 참조로 포함된 <"Packet Scheduling and Congestion Control Schemes for Multipath Datagram Congestion Control Protocol", C. Huang, Y. Chen, 및 S. Lin>에 제시되어 있다. 후자와 같은 접근 방식은 본 명세서에 참조로 포함된 <"Partially Reliable- Concurrent Multipath Transfer(PR-CMT) for Multihomed Networks" C. Huang 및 M. Lin>에 제시되어 있다.

[0066] 또한, 일부 UDP 기반 애플리케이션은 다중 경로 전달을 통해 악화될 수 있는 패킷 순서에 민감하다. DCCP와 SCTP는 이 문제를 피하기 위해 패킷 재순서화를 지원한다.

[0067] 메트릭

[0068] 본 발명의 실시예에서 이용되는 터널은 네트워크 메트릭의 측면에서 평가된다. 그들 중 일부는 다음과 같다:

[0069] 대역폭(Bandwidth, BW): 대역폭은 고정된 시간 양 내에 송신될 수 있는 이론적인 최대 데이터 양으로 정의된다. 따라서, 대역폭은 데이터 전송을 지원하기 위한 네트워크 접속의 용량을 나타낸다. 대역폭은 종종 초당 비트 수(bps, Kbps, Mbps, Gbps)로 표시된다.

[0070] 패킷 손실: 패킷 교환 시스템에서, 패킷 손실은 의도한 목적지에 도착하지 못한 패킷의 수를 말한다. 패킷 손실을 유발하는 주요 요인은 링크 정체, 버퍼 과부하와 같은 디바이스 성능(라우터, 스위치 등), 네트워크 디바이스 상에서의 소프트웨어 문제, 및 하드웨어 결함이다. 버리는 것은 패킷을 의도적으로 폐기하는 것이다.

[0071] 신뢰성: 신뢰성은 특정 시간 기간 동안 명시된 조건 하에서 기능하는 시스템 또는 구성 요소의 역량을 기술한다.

[0072] 처리량: 처리량이란 실제로 "채널"을 통해 실제로 얼마나 많은 데이터가 이동하는지이다. 이것은 대기 시간, 패킷 손실, 및 어떤 프로토콜이 사용되는지를 포함하여 상이한 것들에 의해 제한될 수 있다. 처리량은 일반적으로 초당 비트 수(bps, Kbps, Mbps, Gbps)로 측정된다.

[0073] 대기 시간: 대기 시간은 애플리케이션이 송신할 일부 데이터를 생성한 이후로 그러한 데이터가 처리된 목적지 애플리케이션에 도착할 때까지의 시간으로 정의된다. 패킷 교환 네트워크의 대기 시간은 많은 상이한 요인, 특히 처리 지연, 버퍼 팽창, 및 대기열 지연과 같은 장거리 네트워크의 운영 환경에 영향을 받을 수 있다.

[0074] 지터: 지터는 동일한 스트림에 속하는 두 개의 연속하여 수신된 패킷의 전달 지연 간의 차이의 절대 값이다. 지터는 네트워크 정체, 타이밍 드리프트, 및 경로 변경으로 인해 발생한다. 본 명세서에 참조로 포함된 <Internet Engineering Task Force(IETF) Request for Comments(RFC) 3393>에서 보고된 바와 같이, 패킷 교환 네트워크에서 지터라는 용어는 패킷 지연의 변화를 식별하기 위해 완전히 정확하지 않다. 패킷 지연 변화(Packet Delay Variation, PDV)는 이 맥락에서 사용하기에 더 좋은 용어일 수 있다.

[0075] 왕복 시간(Round Trip Time, RTT): 왕복 시간은 왕복 지연이라고도 하며, 특정 소스에서 특정 목적지까지 패킷이 이동하고 반송 패킷이 소스로 다시 이동하는 데 필요한 시간이다.

[0076] 패킷 간 시간(Inter Packet Time, IPT): 패킷 간 시간은 플로 내에서 두 개의 연속된 패킷 사이에 경과된 시간이다. 패킷 간 도착 시간(Inter Packet Arrival Time, IPAT)는 패킷 간 방출 시간(Inter Packet Emission Times, Emission Time)과 비교되며, 지터를 계산하기 위한 편리하고 효율적인 방법을 제공한다. 경험적 방법을 통해 IPAT를 평가하는 것만으로도 지터를 예측할 수 있다.

[0077] 플로 완료 시간(Flow Completion Time, FCT): 플로 완료 시간은 네트워크 플로를 사용하여 성공적인 트랜잭션을 수행하는 데 필요한 시간이다. 트랜잭션 유형 및 정확성은 애플리케이션에 따라 다르다.

[0078] 관찰 가능한 접속 경로: 관찰 가능한 접속 경로는 플로의 구성 패킷이 통과하는 측정 가능한 노드 세트(예를 들어, 두 개의 엔드포인트 간의 영구 터널 접속)이다.

[0079] Certified Starflow™ Path

[0080] 본 발명의 실시예에 대한 중요한 개념은 "Certified Starflow™ Path" 또는 CSP이다. CSP는 네트워크의 두 개의 엔드포인트 간에 열린 지속적인 접속이다. 본 발명의 실시예에서, 이러한 지속적인 접속은 VPN 터널에 의해 구현된다. 접속이 열리고 살아있도록 유지되면, 위에서 설명한 것과 같은 메트릭이 모니터링되기 시작한다. 터널이 원하는 간격 동안 특정 임계치를 통과하면, 터널은 "Certified Starflow™ Path" 또는 CSP의 상태로 승격된다. 마찬가지로, 원하는 간격 동안 특정 임계치를 유지하지 못하면, CSP는 강등될 수 있다. 상이한 알고리즘이 다른 요인뿐만 아니라 요구되는 바람직한 QoE에 따라 승격 및 강등 과정을 관리한다. 예를 들어, 한 회사가 10Mbps 보다 높은 처리량을 요구하는 QoE를 가지면, 이 임계치를 초과하는 VPN 터널만이 CSP로 승격될 것이다. 대안적인 실시예에서, CSP는 보안 또는 암호화를 사용하지 않는다. 이들은 임의의 터널링 기술로 구현될 수 있다.

[0081] 인터넷과 같은 패킷 교환 네트워크 내의 경로는 두 개의 엔드포인트 간에 교환되는 패킷에 의해 가로지르는 홉 세트로 정의될 수 있다. 이 세트는 각각의 홉에 의해 행해진 전달 결정에 따라 다르다. 인터넷의 라우터는 그것을 고유하게 식별함으로써(예를 들어, 플로 식별자로서 5개의 튜플), 그리고 활성인 동안 그들의 대응하는 라우팅 상태를 유지함으로써, 동일한 플로에 속하는 패킷을 전달하는 경향이 있다; 이것을 플로 점착(flow stickiness)이라고 한다.

[0082] 본 발명의 실시예는 인터넷에 의해 제공되는 동적 다수의 경로를 이용한다. 본 발명의 실시예에서, 다수의 ISP가 두 개의 엔드포인트를 접속시키는 데 사용되어, 암묵적으로 이들이 별개의 관리 도메인을 통과할 때 그들 사이에 다수의 경로를 제공할 수 있다. 엔드포인트 당 단일의 ISP가 있더라도, 이 두 엔드포인트 사이를 흐르는 트래픽은 별개의 경로를 통과할 수 있다. 이는 경로 상의 일부 라우터가 동일한 목적지를 향한 다수의 나가는 루트를 갖고 있기 때문이다. 이러한 다음 홉의 다중성은 트래픽을 부하 밸런싱하여 성능을 개선시키고 정체를 줄이기 위해 라우터에 의해 이용될 수 있다. 다중 경로 라우팅 상황에서 접속 지향 프로토콜(예컨대 TCP)이 손상되지 않도록 하기 위해, 라우터는 동일한 플로에 속하는 패킷을 동일한 다음 홉으로 보내 경향이 있어, 플로 점착을 강화한다. 본 발명의 실시예는 "경로 낚시(Path Fishing)"로 정의된 프로세스에서 이러한 접속을 설정한 에이전트에 관계없이 엔드포인트 간의 접속을 사전에 유지한다.

[0083] 동일한 두 엔드포인트 간에 별개의 경로를 지닌 CSP를 발견하는 것은 라우터가 플로별 부하 밸런싱을 강화하는 방법에 따라 다르다. 특정 플로에 속한 패킷을 구별하고 그것을 동일한 다음 홉으로 라우팅하기 위해, 보통 일부 플로별 불변 필드에 대해 해싱 값을 계산한다. UDP/TCP 플로 패킷의 5 튜플인 IP 소스, IP 목적지, 포트 소스, 포트 목적지, 및 전송 프로토콜 식별자가 그 예이다. 본 발명의 실시예에서는, UDP 터널이 사용된다. 다른 실시예는 IPsec 또는 다른 터널링 기술을 사용할 수 있다. 일부 경우에는, 소스 또는 목적지 포트가 없다(예를 들어, 터널 모드에서 IPsec의 가장 일반적인 구성인 ESP 헤더가 있는 터널링 모드에서 작동하는 IPsec 패킷). 이 경우, 헤더의 다른 바이트가 동일한 IPsec 터널에 속하는 모든 패킷에 대해 안정된 경로를 유지하기 위해 경로 상의 라우터에 의해 소스 IP 및 목적지 IP와 함께 해싱 값으로 사용될 수 있다.

[0084] 발견된 CSP는 관련 메트릭 세트에 기초하여 특징지어지며, 경로는 관련 메트릭 중 하나이다. 특성화는 활성(active)일 수도 있고 패시브(passive)일 수도 있다. 전자는 활성 탐색을 이용하여 측정치를 검색하는 반면, 후자는 전송되는 실제 트래픽에서 측정치를 수집한다. 동등한 경로를 가진 다수의 CSP가 발견되더라도, 다른 메트릭의 관점에서 별개의 거동을 가질 수 있다. 두 사이트 간의 CPS 수는 필요한 QoE에 따라 동적이며 지능적으로 관리된다.

[0085] 본 발명의 일 실시예에서, CSP의 수는 부분적으로 고유 터널 식별자의 수에 의해 제한된다. 예를 들어, 5 튜플 기술이 사용된다면, 주어진 소스로부터 주어진 목적지까지의 CSP의 수는 엔드포인트 사이에 설정될 수 있는 고유한 5 튜플의 수에 의해 결정된다.

[0086] 도 7은 기업 본사에 접속된 지사의 예시적인 실시예를 도시한다. 이 예에서 지사는 2개의 상이한 ISP 접속을 갖는데, 하나의 ISP(700)에는 이용 가능한 두 개의 전송 포트가 있는 단일 IP 주소를 가지고, 다른 ISP(710)는 각각 세 개의 전송 포트와 두 개의 전송 포트가 있는 두 개의 IP 주소를 갖는다. 접속의 다른 측면에서, 본사는 하나의 IP 주소와 두 개의 전송 포트를 지닌 단일 ISP(720)를 갖는다.

[0087] 이 네트워크 설정 위에는 위치 간에 가능한 모든 CSP(730)가 또한 도시되어 있다. 지사 내의 모든 CSP는 표시되지는 않았음에 유의한다. 이것은 단순한 네트워크 토폴로지이지만, 기업은 사무실을 상호 연결하기 위해 더 복잡한 토폴로지를 요구할 수 있다. 결과적으로, 토폴로지는 CSP 수를 결정할 것이다.

[0088] 이 예에서, IP 전송 포트 제한은 지사에서 이용 가능한 총 IP 전송 포트 쌍 수와 본사에서 이용 가능한 총 IP 전송 포트 쌍 수의 합으로 표현될 수 있는 14개의 가능한 CSP를 허용한다. 따라서, 본 발명의 실시예는 이들 14개의 CSP를 통해 트래픽을 잠재적으로 전송할 수 있다.

[0089] 네트워크 구성이 CSP 수를 제한하는 반면, 송신 중인 플로 수는 사용자 및 애플리케이션에 따라 다르다. 또한, 플로 수는 각각의 접속의 대역폭인 CSP의 용량으로 제한된다. 또한, 플로는 서브 플로로 나뉘어져 시스템의 세분성을 향상시키면서 이용 가능한 CSP에 걸쳐 트래픽을 분산시킨다.

[0090] 본 발명의 일 실시예에서, 플로는 최대 32개의 상이한 CSP를 동시에 사용할 수 있으며, 여기서 각각의 CSP는 그 플로의 서브 플로의 총 수의 서브 세트를 핸들링할 수 있다. 대안적인 실시예에서, 사용될 수 있는 상이한 CPS의 수는 32보다 클 수 있다. 이것은 도 8에 도시되어 있다. 단일 플로(800)는 최대 32개의 서브 플로(810)로 나누어지고 최대 6 개의 CSP(820)를 통해 송신된다.

[0091] 본 발명의 일 실시예에서, 원래의 MPTCP 프로토콜이 이용되고, 따라서 그것은 모든 엔드포인트 간에서 풀 메시 접속을 설정한다. 대안적인 실시예에서, 사용되지 않는 터널의 오버헤드를 제거하고, 가능한 서브 플로의 수를 증가시키며, CSP 할당에 대한 플로의 한계를 극복하기 위해 포인트-투-포인트 토폴로지가 사용된다.

[0092] CSP 방향성

[0093] 본 발명의 일 실시예에서, CSP는 터널들로부터 상속된 특성으로서 양방향성이다. 두 CSP 방향 모두 동일한 네트워크 경로를 사용하는지 여부는 네트워크 인프라에 따라 다르다. 예를 들어, IP 기반 터널의 경우 양방향이 반드시 동일한 네트워크 경로를 통과하지는 않는다. 이것은 터널의 각각의 방향이 (예를 들어, 대기 시간 또는 대역폭 면에서) 잠재적으로 상이한 특성을 갖게 한다.

[0094] 그러나, 일부 애플리케이션 및/또는 프로토콜은 두 플로 방향의 특성에서 이러한 비대칭성으로 어려움을 겪을 수 있다. 예를 들어, TCP 접속은 새로운 데이터를 전달하기 전에 프로토콜이 반환되는 확인 응답 패킷(ACK)에 종속되어 있기 때문에 글로벌 종단 간 QoE를 보장하기 위해 RTT(양방향의 결합 대기 시간)에 크게 의존한다.

[0095] 본 발명의 일 실시예에서, 각각의 데이터 패킷은 그 순간에 애플리케이션의 특성 또는 시스템의 정책에 더 잘 맞는 CSP를 통해 전송될 수 있다. 예를 들어, TCP 접속은 초기에 주어진 CSP를 통해 설정될 수 있지만, 데이터 패킷은 더 높은 대역폭과 같은 더 나은 특성을 가진 동일한 목적지에 도달하는 대안적인 CSP를 통해 이후에 전송될 수 있다. 또한, 대응하는 ACK 패킷은 대기 시간과 같은 다른 특성에 기초하여 데이터 패킷과 반드시 동일하지는 않은 이들 CSP 중 임의의 것을 통해 반환될 수 있다. 이러한 결정은 동적이며 시간 경과에 따라 그리고 각각의 패킷마다 변경될 수 있다.

[0096] 본 발명의 일 실시예에서, CSP는 전술한 메트릭에 의해 분류될 것이다. 또한, 플로는 이러한 동일한 메트릭 및 이러한 플로를 여는 애플리케이션에 의해 정의된 특정 특성(예를 들어, 트래픽 유형, 파일 전송 크기 등)에 대한 요구 사항 세트를 가질 것이다. 시스템은 플로의 패킷을 전달하는 데 가장 필요한 애플리케이션을 최적화하는 CSP(예를 들어, 대량 데이터 전송을 위해 이용 가능한 대역폭이 큰 VoIP 또는 CSP와 같은 대기 시간이 중요한 애플리케이션의 대기 시간이 짧은 CSP)를 선택할 수 있다.

[0097] CSP를 분류하기 위해, 터널이 몇 가지 기준을 위반할 때 동적으로 반응하는 터널을 지속적으로 모니터링한다. 예를 들어, CSP는 처리량에 따라 분류될 수 있다. 대체 분류에서, CAP는 패킷 손실 메트릭에 따라 분류될 수 있다. 예를 들어, 범주 A는 처리량이 특정 임계치보다 높은 CSP를 포함하는 반면, 범주 B는 처리량이 그 임계치 아래이지만 패킷 손실이 낮은 CPS를 갖는다.

[0098] 또한, 분류 패턴은 CSP를 특정 유형의 트래픽과 연관시킬 수 있다. 예를 들어, 큰 파일이 전송되는 경우, 원하는 CSP는 우수한 처리량을 가져야 한다. 또는, 데이터 수신 확인 응답이 전송되는 경우, 감소된 대기 시간이 처리량보다 바람직하다. 또한, 플로는 사용자 및 애플리케이션 유형에 따라 상이한 우선 순위를 가질 수 있다. 예를 들어, 분류는 실시간 또는 심지어 QoE와 같은 특성을 손상시키지 않고 우선 순위를 보장하는 데 기여할 수 있다.

[0099] 배치

[0100] 본 발명의 실시예는 임의의 디바이스 또는 네트워크 장비에 배치될 수 있는 가상 머신(Virtual Machine, VM) 내에서 실행되는 "에이전트"로서 배치된다. VM이 실행되는 곳이 CSP의 소스와 목적지를 결정한다. 시스템 성능에 영향을 미치는 세 가지 VM 배치 옵션이 있다: 1. LAN과 WAN을 접속시키는 네트워크 장비에서 VM을 실행한다; 2. LAN 내부의 특정 집계 포인트에서 VM을 실행한다; 그리고 3. LAN 내의 각각의 디바이스에서 VM을 실행한다.

[0101] 대안적인 실시예에서, 에이전트는 VM 대신에 컨테이너를 사용하여 배치된다. 컨테이너는 운영 체제에서 제공하는 가벼운 가상화 메커니즘으로 프로세스 그룹 또는 시스템 리소스 그룹을 분리할 수 있게 한다. 예를 들어, Linux에서는 애플리케이션과 네트워크 디바이스가 네임 스페이스로 분리될 수 있다.

[0102] 일부 경우에, CSP는 인터넷 코어의 라우터를 포함하여 상이한 네트워크 도메인(예를 들어, 별개의 AS(Autonomous Systems))을 통과할 수 있다. 또한, 위의 세 번째 옵션을 선택되는 경우, CSP도 LAN을 통과할 것이다. 도 9a가 이러한 상황을 도시하고 있다. 2개의 ISP 연결(910)을 갖는 하나의 엔드포인트(900)는 인터넷 코어(920)를 통해 2개의 ISP 연결(930)을 또한 갖는 다른 엔드포인트(940)에 연결된다. 각각의 CSP는 엔드포인트 중 하나에서 하나의 IP/전송 포트 쌍에서 시작하여 다른 하나의 IP/전송 포트 쌍에서 종료된다.

[0103] 에이전트 배치 장소는 총 CSP 수에 기여한다. 이 결정은 접속될 엔드포인트의 수를 결정한다. 예를 들어, 위의 첫 번째 옵션을 사용하여 LAN의 입구와 출구에서 VM을 배치할 경우, 입구 지점과 출구 지점에서 사용할 수 있는 CSP 식별자 수가 제한되어 CSP 수가 줄어들 수 있다. 이 제한은 열려 있는 포트에 대한 보안 문제가 있기 때문에 엔드포인트에 의해 공개적으로 열려 있는 이용 가능한 전송 포트 수에 기인한다. 대조적으로, VM이 LAN 내의 모든 디바이스에 배치되는 경우, 일반적으로 더 많은 CSP 식별자가 이용 가능할 것이기 때문에 CSP의 수가 더 커질 수 있다. 이 선택은 또한 계산 용량, 보안, 및 회사 정책과 관련이 있다. LAN을 보호하기 위해 방화벽을

사용하는 것을 선호하기 때문에 일부 회사에서는 각각의 디바이스에서 VM을 실행하는 것이 바람직하지 않을 수 있다.

[0104] 모든 디바이스에서 VM을 실행하면 종단 간 QoE가 발생하지만, QoE는 두 포인트 사이에서만 보장되므로 LAN의 출구/입구 포인트에서 실행하면 성능이 불확실해질 수 있다. 또한, 내부 라우팅 옵션이 통상적으로 제한되어 있기 때문에 회사 내부의 CSP는 대부분의 링크를 공유한다. 이 사실은 상호 간섭 및 정체로 인해 성능에 영향을 줄 수 있다.

[0105] 위에서 논의된 세 번째 옵션은 이전 두 가지 사이의 중간 솔루션이다. 모든 LAN 디바이스에서 VM을 실행하는 대신, 특정 핵심 집계 포인트만이 VM을 실행할 것이다. 이 기술은 두 번째 옵션만큼 공격적이지 않으며 LAN 내에서도 QoE를 보증할 수 있다.

[0106] CSP 할당

[0107] 공용 인터넷을 통해 두 개의 엔드포인트를 접속시키는 경로의 수는 매우 클 수 있다. 에이전트는 CSP로 승격되고 이용될 적절한 터널 세트를 결정할 책임이 있다. 스케줄링 및 패킷 전송을 위한 CSP 선택은 동적이다. 이 결정 프로세스는 트래픽 요구 사항과 CSP 특성이라는 두 가지 기준에 기초한다. 전자는 전송되는 트래픽의 유형을 분류하는 반면, 후자는 CSP의 사전 모니터링의 결과이다. 이는 통해 트래픽을 동적으로 조정하고 네트워크의 변화에 반응하게 한다. 이는 에이전트가 트래픽 요구 사항과 일치하는 더 우수한 메트릭을 가진 CSP를 사용하게 하며, 트래픽 요구 사항 중 하나는 관찰 가능한 경로이다; 예를 들어, 상이한 CSP가 (양자 모두 전체적으로 관찰 가능한) 별개의 네트워크 경로를 통과할 수 있고, 시스템은 신뢰성을 향상시키기 위해 이러한 별개의 CSP에서 패킷을 복제하기로 결정할 수 있다.

[0108] VM이 실행되는 위치와는 독립적으로, 도 9b는 터널 세트와 CSP 풀 사이의 관계를 도시한다. 엔드포인트 A(950) 및 엔드포인트 B(970)는 일련의 중간 라우터(960)를 통해 인터넷을 통해 통신한다. 이 시나리오에는 아래 표의 처음 네 행에 도시되어 있는 네 개의 고유한 경로가 있다.

[0109] 또한, VM을 실행하기 위한 상이한 옵션이 설명된다. 일 실시예에서, VM은 엔드포인트 장비(980)에서 실행되는 반면, 다른 실시예에서는 VM은 회사의 출구 라우터(950)에서만 실행된다.

[0110] 아래 표는 여섯 개의 가능한 경로와 각각이 통과하는 노드를 보여준다.

[0111]

	통과한 노드						
경로 1	0	1	2	3	5	6	7
경로 2	0	1	2	3	6	7	
경로 3	0	1	2	4	6	7	
경로 4	0	1	2	z	4	6	7
경로 5	0	1	2	3	6	7	
경로 6	0	1	2	3	5	6	7

[0112] 두 개의 상이한 CSP가 동일한 경로를 통과하는 것이 가능하므로, 추가 터널이 다른 터널 중 하나와 동일한 노드를 통과할 수 있음에 유의한다. 예를 들어, 터널 5는 터널 2와 동일한 노드를 통과하고 터널 6은 터널 1과 동일한 노드를 통과한다. 두 개의 상이한 CSP가 동일한 노드를 통과하더라도, 상이한 성능 특성을 가질 수 있다.

[0113] 이 예에서, 에이전트는 하나의 활성 CSP(터널 1), 대기 CSP(터널 2), 및 탐색 CSP(터널 3)를 가질 수 있다. 고려된 CSP 상태 및 상태 전환 중 하나의 가능한 세트가 이하에 상세히 설명된다. CSP의 활성 관리 및 모니터링은 특정 임계치에 대해 각각을 평가하고 이에 따라 조치를 취한다(예를 들어, 성능이 저조한 CSP를 제거한다). 탐색 CSP가 활성 CSP 및/또는 대기 CSP보다 성능이 좋지 않은 경우, 그것은 폐기될 수 있고, CSP 식별(5 튜플)이 다른 터널을 위해 재사용될 것이다. 그 다음에, 이 새 터널은 탐색 CSP가 되어 그 성능이 사용되고 있는 다른 두 개를 개선시키는지를 분석한다. CSP 상태와 이들 사이의 전환에 대해서는 하기에서 자세히 논의된다.

[0114] 본 발명의 일 실시예에서, CSP의 풀은 이들 중 하나 이상이 CSP를 탐색하는 곳에서 사용된다. 여기서, 성능은 예를 들어 5분마다 주기적으로 평가된다. 대안적인 실시예에서, 측정 간의 시간은 다른 로직 또는 거동 패턴에 기초할 수 있다. 측정 오버헤드를 줄이기 위해, 실제 트래픽이 송신되는 경우 패시브 측정이 사용되거나, 해당

CSP에 트래픽이 없는 경우 활성 측정이 사용될 수 있다.

[0115] 일부 실시예에서, 임의의 다른 CSP를 능가하지 않는 탐색 CSP/터널의 다수의 연속적인 테스트는 시스템으로 하여금 CSP를 폐기하고 더 나은 CSP를 대신 선택하게 한다. CSP를 폐기하기 위한 테스트 기준은 시간이 분산된 연속적인 테스트로 구성될 수 있다. CSP에 활성 플로가 있는 경우, 플로가 완료될 때까지 활성으로 유지되지만 새 플로가 할당되지 않는다. 이로 인해 새로운 5개 튜플로 CSP/터널이 다시 시작되며, 새로운 5개 튜플은 이전 5개 튜플과 동일할 수 있다. 새로운 CSP는 소스 전송 포트에서 상이할 수 있으며, 소스 전송 포트는 이제 소스에서 이용 가능한 포트 세트에서 무작위로 선택된다. 이 포트 수정은 동일한 폐기된 경로를 재사용할 가능성을 최소화하기 위해 수행된다. 이 변경에도 불구하고, "새" 터널이 폐기된 터널이나 활성 터널과 상이한 속성을 갖는 것이 보장되지는 않는다. 이러한 이유로, 에이전트는 속성이 상이한지 여부를 검사한다.

[0116] 대안적인 실시예에서, 동일한 기본 경로를 사용하는 다수의 CSP가 유지된다. 이는 네트워크 경로가 동일하더라도 두 CSP에 대해 상이한 성능이 발생할 수 있기 때문이다. 이러한 차이점은 라우터 및 큐잉, 라우팅 및/또는 내부 부하 밸런싱 전략에서 발생할 수 있다.

[0117] 일부 실시예에서, 에이전트는 CSP를 열린 상태로 유지하기 위해 VPN 소프트웨어의 옵션을 통해 킵-얼라이브(keep-alive)를 전송한다. 이 기술은 터널을 열린 상태로 유지하기 위해, 주기적으로 네트워크 메시지를 생성한다, 예를 들어 비활성 상태인 경우 매 10초마다 ICPM "ping" 패킷을 생성한다.

[0118] 대안적인 실시예에서, 정책은 동적 알고리즘으로 새로운 터널을 탐색할 시기를 결정하고 승격/강등 프로세스를 안내하는 데 사용된다. 또한 CSP를 테스트하기 위해 샘플링 주파수에 영향을 미치며 네트워크 상태에 적절하게 적응하기 위해 세분성이 요구된다.

[0119] 루트 식별

[0120] CSP를 구별하는 한 가지 방법은 CSP가 통과하는 경로를 이용하는 것이다. 이 정보가 이용 가능한 경우에, 공용 인터넷에서 또 다른 주요 관심사를 충족시켜 가시성을 얻는다. 사용자는 트래픽이 통과하는 노드(예를 들어, IP 주소 세트)에 대한 제어 또는 최소한 지식을 얻고자 할 것이다. 본 발명의 실시예는 이 가시성을 제공하기 위해 2개의 상이한 기술을 이용한다.

[0121] 첫 번째 방법은 "추적 루트" 기술이다. 이 기술은 증가하는 TTL(Time To Live)로 일련의 패킷을 전송한다. 각각의 패킷이 특정 라우터에서 최대 홉 수에 도달하는 경우, 해당 라우터는 도달한 노드를 나타내는 패킷을 소스로 반환한다.

[0122] 예를 들어, 전송된 첫 번째 패킷은 TTL = 1을 갖는다. 첫 번째 라우터가 이 패킷을 수신하면, TTL을 1씩 감소시킨다. 결과 값이 0이므로, 이 라우터는 자신의 주소 또는 식별을 나타내는 패킷을 반환한다.

[0123] 추적 루트 방법은 완전히 정확하지는 않다. 첫째, 라우터는 응답할 의무가 없으며, 이 경우 라우터는 자신에 대한 정확한 정보를 전송하지 않을 수 있다. 라우터는 그들의 ISP를 나타내는 일반적인 대답을 전송하거나 심지어 잘못된 IP 주소를 제공할 수도 있다. 이것은 의도적으로 행해질 수 있지만, 일반적으로는 그렇지 않다. 추적 루트 이상(anomalies)은 본 명세서에 참조로 포함된 <"Avoiding traceroute anomalies with Paris traceroute," B. Augustin 외>에서 분석되고 설명된다. 추적 루트 이상은 일반적으로 토폴로지 자체 또는 라우터 부하 밸런싱 정책과 관련된다.

[0124] 또한, 추적 루트 기술은 패킷 교환 네트워크에서 항상 만족되는 것은 아니라는 가정을 한다. 하나의 패킷은 특정 경로를 사용할 수 있고, 다음 패킷은 상이한 경로를 사용할 수 있다. 이 경우, 증가하는 TTL 패킷은 동일한 경로 내의 라우터 식별을 제공하지 않는다. 이 사실은 잠재적인 잘못된 링크 식별을 초래할 수 있다.

[0125] 일 실시예에서, 변경된 TTL 값을 갖는 프로브(probe)가 추적하고자 하는 접속 플로의 실제 트래픽으로 가장하는 추적 루트 기술을 수정하는 대안적인 방법이 사용된다. 패킷은 접속 플로 패킷 중 하나와 동일한 5 튜플과 특정 프로브로 라우터 응답과 일치하도록 지문이 찍힌 랜덤 페이로드를 갖도록 위조된다. 이 수정된 추적 루트 기법은 종래의 추적 루트 기법보다 더 신뢰할 만한데, 프로브에 대한 잘 알려진 포트 또는 랜덤 포트를 사용하지 않고 실제 트래픽 플로를 시뮬레이션하기 때문이다.

[0126] 플로 점착 효과(일반적으로 부하 밸런서를 통과할 때에도 보장됨)와 함께, 시간 경과에 따른 루트 변경 검출을 포함하여 경로 발견의 측면에서 반복 가능한 결과가 달성될 수 있다. 그러나, 이 기술은 모든 추적 라우팅 기술에 영향을 미치는 단점을 가지고 있다: (i) 사설 네트워크에서 NAT 주소 재작성, (ii) TTL이 만료된 경우 ISP

무응답.

[0127] 수정된 추적 루트 기술에 특유한 특정 단점은 5 튜플이 그 포트 상의 청취 서비스(예를 들어, OpenVPN 서비스)로 전달되는 실제 유효한 튜플이기 때문에 최종 홉으로부터 어떠한 응답도 수신하지 않을 가능성이다. 그 다음에, 터널 서비스는 내부 프로토콜 요구 사항을 따르지 않기 때문에 패킷을 삭제할만큼 똑똑하다; 해당 특정 프로브에 대한 ICMP 시간 초과 메시지는 아직 생성되지 않았다. 이를 위해, 툴은 종료 전의 어느 시점에 대해 TTL 값을 증가시키는 어떠한 응답도 수신하지 못한 후 프로브를 계속 전송하고 접속의 끝에 도달했다고 결론을 내린다. 루트 발견을 위한 대안적인 기술이 가능하며, 대안적인 실시예에서는 다른 루트 발견 메커니즘이 사용된다.

[0128] 일단 터널을 따라 통과하는 네트워크 노드에 관한 정보를 제공할 수 있는 기술이 설정되면, 노드 세트를 포함하는 정보가 유지될 수 있고, 각각의 경로에 대한 다른 관심 메트릭이 수집될 수 있다. 따라서, 대형 CSP 풀을 관리하는 대신에, 감소된 CSP 세트가 사용될 수 있다. 이러한 최적화는 CSP 관리 단순화로 인해 오버헤드를 감소시킨다.

[0129] CSP 상태

[0130] 네트워크 변동은 CSP의 성능에 영향을 미치며, 이는 에이전트가 초기화될 때 정적 구성을 방지한다. 오히려, CSP는 지속적으로 변화하는 인터넷 상태에 적응해야 한다. 이 문제를 해결하기 위해, 각각의 CSP는 CSP 역할과 메트릭(예를 들어, 처리량, 대기 시간 등)에 기초하여 상이한 상황을 반영하는 가능한 상태 세트를 갖는다.

[0131] 최종 사용자에게 시스템은 안정적이지만, 사용된 CSP 세트는 원하는 QoE를 유지하기 위해 동적으로 변경된다. 도 10은 CSP의 가능한 상태의 예를 도시한다. 일 실시예는 활성(131), 대기(111), 기다림(141), 강등(121), 및 탐색(101)의 5 가지 상태를 사용한다. 다른 실시예는 이들 상태를 수정할 수 있는데, 예를 들어 대기 상태를 제거할 수 있다. 도 10에 도시된 상태 다이어그램은 이러한 상태 간의 전환을 나타낸다. 이러한 상태가 아래에서 보다 자세히 설명된다.

[0132] 활성: 이는 CSP가 트래픽을 전송할 수 있거나 현재 트래픽을 전송하는 것이다.

[0133] 대기: 이 CSP 상태는 활성으로 승격될 경우 사용될 자격이 있음을 의미한다. 이 승격은 CSP 메트릭(대역폭, 대기 시간 등)에 기초한다. 승격되면, 대기 CSP가 활성이 된다. 품질이 특정 기준을 위반하는 경우 대기 CSP가 제거될 수도 있다.

[0134] 기다림: 열려 있고, 성능이 특정 한계를 초과하거나 더 많은 자원이 필요할 경우 대기로 승격될 수 있는 CSP. 예를 들어, 대기 CSP는 때로는 성능이 좋지만 다른 기간에는 성능이 좋지 않을 수 있다.

[0135] 강등: 활성 CSP가 저하되면, 강등 상태가 된다. 이 상태는 시스템이 새로운 플로 또는 트래픽을 해당 CSP에 할당할 수 없음을 의미한다. 또한, 강등된 CSP를 통해 진행 중인 트래픽을 핸들링하기 위한 상이한 옵션이 있다. 예를 들어, 공격적인 옵션은 CSP를 자르고 TCP가 (송신되고 있거나 버퍼 상의 패킷에 대한) 패킷 손실을 핸들링하도록 하는 것이다. 또 다른 옵션은 패킷을 손실시키지 않고 CSP 간에 소프트 전환을 구현할 것이다. 이 옵션은 진행 중인 패킷이 전송되고, 그 다음에 CSP가 완전히 강등되게 한다.

[0136] 탐색: 탐색 CSP는 유효 CSP로 승격되거나 제거되기 전에 (관심 네트워크 메트릭에 따라) 분석 하에 있는 터널이다.

[0137] 삭제된 CSP는 관련된 모든 것이 지워지기 때문에 상태로 간주되지 않는다. 도 10의 십자 기호는 CSP 제거를 나타낸다.

[0138] 상이한 상태 전환을 결정하는 조건은 처리량, 대기 시간, 및 패킷 손실을 포함하는 네트워크 메트릭에 따라 다르다. 본 발명의 일부 실시예에서, 이들 전환은 정적이고 수동이다. 대안적인 실시예에서, 프로세스는 더 많은 메트릭을 고려하여 자동화된다.

[0139] 에이전트는 CSP ID를 포함하는 각각의 상태에 대한 대기열을 관리한다. 에이전트가 새 CSP를 송신할 필요가 있는 경우, 활성 대기열로 이동하여 원하는 메트릭으로 CSP ID를 선택한다. 또한, 이러한 대기열에 우선 순위를 적용하여 CSP 선택 프로세스를 최적화할 수 있다.

[0140] CSP 할당에 대한 플로

[0141] 정책은 주어진 플로로부터의 최대 서브 플로 수와 사용할 수 있는 CSP 수를 명시한다. 이러한 파라미터 외에, CSP 할당에 대한 플로가 구현되어 성능을 최적화한다.

[0142] 일 실시예에서, 새로운 플로가 VM에 도착하는 경우, 그것은 활성 CSP의 수만큼의 서브 플로로 나누어진다. 그 다음에, 하나의 서브 플로가 각각의 활성 CSP를 통해 전송된다. 이 프로세스는 정적이며 새로운 플로가 에이전트에 도착할 때마다 행해진다.

[0143] 대안적인 실시예에서, 트래픽 특성화 및 네트워크 상태에 기초한 동적 플로/서브 플로 분할이 이용된다. 하나의 플로 분할 및 CSP 할당이 특정 순간에는 좋은 성능을 갖지만 다른 시간에는 성능이 좋지 않을 수 있기 때문에, 동적 솔루션이 이점을 갖는다. 일부 실시예에서, 서브 플로의 수는 가변적이며, CSP 할당은 동적으로 변할 수 있다. CSP도 동적이며, 동적 할당은 애플리케이션 유형, 하루 중 시간, 사용자 유형 등에 따라 달라질 수 있다.

[0144] 아키텍처

[0145] 상이한 엔드포인트 사이의 많은 수의 CSP를 관리하고 네트워크 조건에 대해 CSP 할당에 플로를 적응시키고, 종단 간 QoE를 보장하는 것은 확장성 및 복잡성 관점에서 중요한 작업이다. 이 관리는 네트워크 상태(예를 들어, 정체, 장애 등), 교차 트래픽 간섭과 같은 실시간 정보에 따라 행동하고, 공용 인터넷의 확률론적 특성을 다루는 것을 포함한다. 계층적 아키텍처가 이러한 문제를 해결하기 위해 정의되었다. 도 11은 이 아키텍처를 도시하고 있다. 일 실시예는 상위 계층이 글로벌 계층(151)이고, 중간의 계층이 중간 계층(161)이고, 최하위 계층이 데이터 계층(171)인 3 계층의 계층적 시스템을 사용한다. 아키텍처의 맨 아래에는 정보, 측정, 및 패킷을 관리하는 데이터 레벨이 있다. 데이터 레벨 위에는 중간 레벨이 있으며, 중간 레벨은 상이한 서브 레벨로 분해되어 다수의 레벨의 집합을 관리할 수 있다. 범위는 기업 요구 사항(예를 들어, 부서별 부문, 사용자 정책 등) 및 네트워크 토폴로지(예를 들어, ISP 수, 포트 수 등)를 포함하는 LCI(Local Contextual Information)를 포함한다. 이 레벨은 LCP를 CSP에 대한 규칙 및 LCI에 기초한 CSP 할당에 대한 플로를 포함하는 정책을 핸들링한다. 아키텍처의 상위에는 사회 정치적 상황, 치명적인 재해, 스포츠 게임 등과 같은 세계적 규모의 이벤트를 다루는 글로벌 레벨이 있다. 이 글로벌 맥락 정보(Global Contextual Information, GCI)는 하위 레벨을 안내하는 정책을 생성하는 데 사용된다. 인터페이스는 이러한 레벨 간의 통신 및 정보 교환을 핸들링한다. 주요 특징은 반(semi) 독립적 운영 체제이다. 데이터 계층 이 상위 계층에서 접속 해제되는 경우에, 이용 가능한 정보에 기초하여 계속 작동할 수 있다.

[0146] 본 발명의 실시예는 상이한 맥락 정보를 이용하여 그 기능을 최적화하기 위해 각각의 계층에 분산 학습 알고리즘을 갖는다. 각각의 계층이 상이한 유형의 정보를 다룬다는 점은 공용 인터넷을 통해 QoE를 보장하기 위한 확장 가능한 솔루션을 제공하는 데 기여한다.

[0147] 레벨이 높을수록 추상성과 시스템 범위는 커지지만 세분성은 더 거칠어진다. 이 레벨은 또한 상이한 시간 스케일을 반영한다. 데이터 레벨은 실시간으로 작동할 수 있지만 중간 및 글로벌 레벨은 그렇지 않다. 이러한 상이한 운영 체제는 엔드포인트에서 실행되는 에이전트(데이터 레벨) 및 구내 또는 클라우드에서 실행되는 중간 및 글로벌 레벨을 갖는 분산 아키텍처에서 초래된다.

[0148] 단일 기업 관점

[0149] 기업이 본 발명의 실시예를 사용하여 종단 간 QoE를 보장하기를 원할 경우, 그들의 사무실에서 에이전트를 배치하는 것이 첫 번째 액션이다. 이러한 에이전트를 조합하면 데이터 계층이 구현된다. 각각의 에이전트는 CSP를 관리하는 것을 책임지고, 일련의 정책에 기초하여 CSP에 플로를 할당한다.

[0150] 이 정책은 LCI에 기초하여 정책을 생성하는 중간 계층의 결과물이다. 동시에, 중간 계층은 GCI를 고려하는 글로벌 계층으로부터 정책을 수신한다. 단일 기업을 갖는 경우에, 중간 계층 및 글로벌 계층은 QoE를 보장하기 위해 전용된다. 도 12는 이러한 상황을 도시하고 있다. 기업 엔드포인트에서 데이터 계층(221, 261, 251)을 이용하는 에이전트는 ISP(231)를 통해 공용 인터넷(241)에 연결된다. 중간 계층(211) 및 글로벌 계층(201)은 또한 공용 인터넷(241)에 연결되고 서로 및 데이터 계층(221, 261, 251)과 통신한다.

[0151] 글로벌 관점

[0152] 데이터 계층에 대한 본 발명의 실시예는 중간 레벨 내부의 서브 계층의 일부와 함께 각각의 클라이언트에 대해 복제된다. 글로벌 레벨은 공동 분석 및 트래픽을 활용하기 위해 모든 고객 사이에서 공유된다. 집합 정보에도 불구하고, 각각의 기업 도메인은 분리되어 데이터와 통신의 보안과 개인 정보 보호를 보장한다.

[0153] 아키텍처의 글로벌 관점은 도 13에 제시되어 있다. 첫 번째 기업인 "회사 A"(321, 331, 371) 및 두 번째 기업인 "회사 B"(341, 361)에서 데이터 계층을 이용하는 에이전트는 ISP(351)를 통해 공용 인터넷(391)에 연결된다. 회사 A(311)와 회사 B(381)에 대한 중간 계층이 또한 공용 인터넷(391)에 연결되고, 서로 그리고 데이터 계층

(321, 331, 371, 341, 361)과 통신한다.

[0154] 이 경우, 두 개의 기업이 있다. 각각의 사무실은 다른 사무실과의 접속을 설정하고 핸들링하는 에이전트를 갖는다. 이 에이전트는 클라우드에서 실행되는 각각의 중간 계층에서 정책과 명령을 수신한다. 동시에, 중간 계층 소프트웨어는 GCI를 고려하는 글로벌 계층으로부터 정책을 수신한다. 글로벌 계층 소프트웨어는 전세계 분산 클라우드에서 실행될 수 있다.

[0155] 이 예시적인 예에서, 동일한 기업 내의 사무실만 그들 간에 접속될 수 있다. 대안적인 실시예에서, 상이한 기업의 사무실을 상호 연결하기 위한 보다 복잡한 솔루션이 구현된다. 이 토폴로지는 정책의 복잡성을 증가시킬 수 있다. 중간 레벨 내의 상이한 서브 계층은 특정 시나리오에 적응된 이러한 복잡성 생성 정책을 핸들링하도록 구성될 수 있다.

[0156] 대안적인 실시예에서, 각각의 기업에 대한 특정 중간 레벨 서브 계층 외에 기업 간 접속을 핸들링하기 위한 보다 높은 서브 계층이 사용된다. 이 구성은 도 14a와 도 14b에 도시되어 있다. 회사 A(421, 431, 471) 및 회사 B(441, 461)의 데이터 계층을 이용하는 에이전트는 ISP(451)를 통해 공용 인터넷(491)에 연결된다. 글로벌 계층(401)뿐만 아니라 기업 간 중간 계층(483)에 더해, 회사 A(411) 및 회사 B(481)에 대한 중간 계층이 또한 공동 인터넷(491)에 연결되고, 서로 그리고 데이터 계층(421, 431, 371, 441, 461)과 통신한다. 개념적으로 회사 A 중간 계층(413) 및 회사 B 중간 계층(423) 외에 A-B 회사 간 계층(403)의 세 개의 중간 계층을 볼 수 있다. 이 상황에서, 중간 레벨은 두 개의 상이한 하위 계층을 갖는다.

[0157] 중간 레벨 내에 상이한 하위 계층을 만드는 한 가지 이점은 기업 간의 로컬 인식 및 공동 특성을 활용하는 것이다. 상이한 기업으로부터의 LCI를 결합하여 설계된 정책은 성과를 개선시킬 수 있다. 중간 레벨 서브 계층과 글로벌 계층 양자 모두는 클라우드에서 실행된다. 계층화된 아키텍처는 복잡성을 다루고 한편 최종 사용자에게는 완전히 투명하다.

[0158] 데이터 계층

[0159] 데이터 계층은 사용자 데이터에 액세스하고 이에 따라 행동하며 패킷과 플로를 다룬다. 이 계층은 데이터 플레인과 제어 플레인의 두 가지 주요 구성 요소를 갖는다. 데이터 플레인은 교환 및 라우팅 정책 세트에 기초하여 패킷을 전달하는 것을 담당한다. 이 플레인은 플로와 해당 서브 플로를 핸들링한다. 또한 데이터 플레인은 트래픽 쉐이핑 및 우선 순위를 위한 곳이다. 대조적으로, 제어 플레인은 CSP 관리, CSP 할당에 대한 플로, 서브 플로 정책 시행, 및 학습 알고리즘에 중점을 둔다.

[0160] 핵심 작업은 CSP 메트릭의 측정 및 수집이다. 본 발명의 실시예는 전술한 바와 같이 대역폭, 패킷 손실, 및 대기 시간을 포함하는 메트릭 세트를 수집한다. 이러한 분석의 목적은 시스템의 성능을 실시간으로 모니터링하고 QoE를 유지하고 개선하기 위한 의사 결정을 내리는 것이다.

[0161] 중요한 기능은 여러 네트워크 메트릭 및 핵심 성과 지표(key performance indicator, KPI)의 추출, 변환, 및 로딩(Extraction, Transformation, and Loading, ETL)이다. 본 발명의 일 실시예에서, 이러한 모든 데이터는 큐레이팅된 다음 그 세분성에 기초하여 중간 계층으로 전송된다. 이상적으로 엄격하게 필요한 정보만 한 계층에서 다른 계층으로 가는 것이 이상이다.

[0162] 이러한 계층 간 통신의 빈도는 주기적인 분포를 따를 수 있다. 예를 들어, 매초마다 한 세트의 데이터가 데이터 계층에서 중간 계층으로 전송될 수 있다. 이 간격의 값은 반응형 시스템을 가능하게 하고 확장성을 위태롭게 하지 않기 위해 중요해진다. 간격이 짧을수록 처리 및 송신 노력에서 큰 오버헤드가 발생하지만 미세한 세분성을 얻는다. 긴 간격은 비용을 피하지만 반응 시간을 줄인다. 따라서, 시스템의 세분성을 제어하기 위해 정확성과 리소스 사용 간에 상충이 있다. 이 실시예에서, 데이터 계층 대 중간 계층 통신의 간격은 대략 1초이다. 대안적인 실시예에서는, 다른 간격이 구현된다.

[0163] 일 실시예에서, 고성능 비동기 메시징 라이브러리인 ZeroMQ 및 컴퓨터 데이터 교환 포맷인 MessagePack이 이계층 간 통신을 가능하게 한다. 또한, 데이터 플레인의 실시예는 MQTT(Message Queue Telemetry Transport)를 지원하며, 이는 TCP/IP 외에 사용하기 위한 ISO 표준 발행-구독-기반 경량 메시징 프로토콜이다.

[0164] 반응 시간을 개선시키기 위해 예외(이벤트 기반) 메커니즘이 이용된다. 데이터 계층에서 CSP의 갑작스러운 변경을 검출하는 경우, 간격 기반 통신 외부의 중간 계층에 예외를 전송한다. 이 예외는 중간 계층에서 이러한 변화에 반응하는 방식을 결정할 상이한 이벤트를 트리거할 것이다. 이 기술은 시스템 확장성을 개선하는 한편, 작은 오버헤드로 예기치 않은 변경을 관리하는 반응 시간을 향상시킨다. 이 기능은 최종 사용자 및 애플리케이션에

대한 투명성을 강화한다.

[0165] 터널과 CSP를 모니터링하는 것 외에도, 데이터 계층은 상이한 CSP에 걸쳐 플로를 분배하는 데 필요한 작업을 실행하는 것도 담당한다. 이 기능은 패킷 캡슐화, 선택적 암호화, 및 다중 경로 전송을 가능하게 하는 플로에 대한 분기/결합 작업의 실행이 포함한다.

[0166] 또한, 데이터 계층은 이용 가능한 대역폭, 패킷 손실, 및 대기 시간과 같은 물리적 또는 가상 인터페이스의 특성을 측정한다. 병행하여, 데이터 계층은 터널 및 CSP를 통해 기본 작업을 수행한다. 예를 들어, 데이터 계층은 CSP 상태와 독립적으로 CSP를 열어 유지하는 킵-얼라이브 메시지를 담당한다. 동일한 원칙이 터널에도 적용된다. 트래픽이 터널을 통해 전송되지 않으면, 터널은 CSP가 되거나 터널은 폐기된다.

[0167] 위의 설명은 데이터 계층의 상이한 기능과 중간 계층에 전송하는 것과 관련된다. 반대 방향으로, 중간 계층은 데이터 계층에 대한 정책을 전송하여 강화한다. 정책은 정보 상태를 액션에 매핑하는 것이다. 시스템의 상태를 고려하여, 정책은 어떤 CSP가 어떤 유형의 트래픽을 전송하는 데 이용될 수 있고 다른 기능과 함께 트래픽이 어떻게 서브 플로로 나누어지는지를 결정한다. 정책은 또한 상이한 CSP 상태 간의 전환(예를 들어, CSP가 활성에서 대기로 진행됨), 뿐만 아니라 CSP로의 터널의 승격/강등을 트리거한다. 정책은 또한 데이터를 캡처하는 방식과 같은 상이한 이벤트를 제어한다.

[0168] 본 발명의 일 실시예에서, CSP는 전달-반환 쌍으로 존재한다. 전달 경로와 반환 경로가 일치할 필요는 없지만, 독립적으로 선택되지는 않는다. 따라서, CSP의 선택은 헤드 포인트(소스)와 테일 포인트(목적지)가 공동으로 책임을 져야 한다. 중요한 정보는 여전히 로컬(입구 및 출구 링크에서의 액세스 정체에 주로 관심이 있지만)이지만, 두 엔드포인트에서 로컬이다(또는, 통신에 다른 목적지가 포함된 경우에는 더 많음). 이는 왜 중간 계층에서 CSP 선택을 해야 하는지를 정당화한다. 두 경우 모두, 중간 계층은 브로커로서 작용하여 상이한 에이전트에 영향을 미치는 결정을 내린다.

[0169] 정책 외에도, 중간 계층은 데이터 계층에서 전송한 분석에 기초하여 특정 터널을 CSP로 승격시키거나 특정 메트릭을 요청하는 명령을 또한 전송할 수 있다. 명령의 수신 시에, 데이터 계층은 바람직한 액션을 실행한다. 다른 예시적인 명령은 터널을 탐색하는 것이다. 따라서, 데이터 계층은 상태에 관계없이 모든 CSP를 관찰하지만, 그에 따라 행동하기 위해서는 중간 계층으로부터의 정책을 필요로 한다. 이 경우 제어는 확장성 문제로 인해 데이터 계층으로부터 로드되지 않는다.

[0170] 정책은 데이터 계층이 활용할 수 있는 자유도가 다를 수 있다.

[0171] 예를 들어, 정책은 10Mbps를 초과하는 처리량을 가진 CSP만이 사용될 수 있다고 나타낼 수 있다. 이 상황에서, 데이터 계층은 이 조건을 충족시키는 CSP 중 어느 것이 사용되는지 결정할 수 있다. 일부 실시예에서, 조건문에 기초한 제어 알고리즘으로서 동작하는 엄격한 정책이 이용된다. 또 다른 실시예에서, 중간 계층 정책에 의해 보다 많은 유연성이 허용된다. 지능형 알고리즘은 이러한 자유도를 활용하여 성능을 최적화 할 수 있다. 예를 들어, 중간 계층 정책을 유지하면서 어떤 CSP를 통해 데이터가 전송되었는지를 결정하기 위해 반응 정보(즉, 각각의 CSP에 대한 테스트)를 활용하기 위해 기계 학습 알고리즘이 사용될 수 있다.

[0172] 본 발명의 일 실시예에서, 데이터 계층의 모든 기능은 각각의 엔드포인트에 위치한 에이전트에서 가상 머신(Virtual Machine, VM) 상에서 실행된다. 하나의 VM이 하나의 엔드포인트에 있는 물리적 포트 세트를 관리할 수 있다. 데이터 계층은 전체 아키텍처의 기초를 구성하기 때문에 중요하다. 다중 경로 최적화 및 학습 알고리즘은 데이터 계층 위에 구축된다.

[0173] 요약하면, 바람직한 실시예에서, 데이터 층은 다음 기능을 수행한다: 1. 간격 기준으로 CSP 및 터널을 통한 메트릭을 측정한다; 2. 분석을 큐레이팅한다; 3. CSP를 얼라이브로 유지한다; 4. 중간 계층 정책 및 명령을 실행한다; 5. 실시간 제어 작동; 및 6. 애플리케이션 디코딩 및 분류(정책에 의해 제어될 수 있음).

[0174] 바람직한 실시예에서, 데이터 계층은 다음의 입력을 갖는다: 1. 중간 계층 정책; 및 2. 터널, CSP, 및 플로 관리에 대한 명령, 그리고 다음 출력을 갖는다; 1. RTT, 단방향 지연, 처리량, 용량, 및 추적 루트와 같은 큐레이팅된 분석(CSP 및 터널); 및 2. 극한 상황(예를 들어, 이용 가능한 BW와 같은 특정 기능의 갑작스러운 상실)에 예외를 핸들링한다.

[0175] 데이터 계층의 실시예 중 일부는 다음의 모듈로 구성된다: 1. 서브 플로 관리자; 2. 애플리케이션 분류기; 3. 네트워크 제어기; 및 4. 보고 에이전트. 대안적인 실시예에서, 데이터 계층은 또한 중간 계층 정책에 의해 허용된 자유도를 활용하기 위해 기계 학습 알고리즘을 구현하고, 새로운 네트워크 메트릭 및 서로 간의 관계를 발견

한다.

[0176] 중간 계층

[0177] 중간 계층은 각각의 회사의 관점에서 시스템을 이해하고 제어하는 계층이다. 본 발명의 일 실시예에서, 이 정보는 ISP, 물리적 인터페이스, IP 주소, 전송 포트, 토폴로지 등에 관한 세부 사항을 포함한다. 이 정보는 로컬 맥락 정보(Local Contextual Information, LCI)라고 불리는 것을 포함한다. 또한, LCI는 그 중에서도, 상이한 애플리케이션 간의 우선 순위, 새로운 정책을 안내하는 패턴을 생성하는 애플리케이션 및 플로 범주, 및 교차 트래픽에 관한 정보를 포함한다. 따라서, 이 계층의 범위는 각각의 기업 내부에 시스템의 그림을 만든다.

[0178] 또한 중간 계층은 데이터 계층에 터널 식별자를 전달하는 상이한 터널을 탐색하라고 한다. 데이터 계층이 네트워크 측정치를 다시 전송하면, 중간 계층은 정책 또는 명령을 통해 CSP로 수준을 승격 또는 강등할지 여부를 결정할 수 있다. 그 다음에, 이러한 지시는 원하는 정책이나 명령을 실행하는 데이터 계층으로 다시 전송된다. 다른 명령은 이용 가능한 대역폭, 대기 시간, CSP 상태 간 전환 측정, 데이터 계층에서 ETL을 수행할 빈도 수정, 및 로컬 맥락 인식(기업 수준)을 사용하는 정책 정의를 포함할 수 있다.

[0179] 또한, 중간 계층에는 큐레이팅된 분석과 함께 정책을 안내하는 애플리케이션 및 사용자 요구 사항이 입력된다. 중간 계층은 논리적 계층이기 때문에, 플로 또는 애플리케이션 데이터를 볼 수 없다. 일부 실시예에서, 네트워크 구성(전송 포트, IP 주소, 인터페이스 등)은 각각의 기업의 IT 직원에 의해 GUI를 통해 이 계층에 입력된다. 다른 실시예에서, 이 정보는 자체 발견 프로세스의 결과이다.

[0180] 상위 계층의 출력으로서, 중간 계층은 (모든 중간 레벨 서브 계층으로부터) 예기치 않은 상황으로 인한 성능 병목 현상 및 접속 상태에 관한 정보를 글로벌 계층에 전송한다. 상태 테스트 및 데이터 분석은 보다 상위 레벨로 이동하기 전에 다시 큐레이팅되어 세분성을 줄이는 한편 더 나은 확장성을 위해 추상성을 얻는다. 반대 방향에서, 중간 계층은 글로벌 계층으로부터의 정책 및 명령을 수신한다. 이 규칙은 보다 상위 계층에서부터 나오므로, 정치적 상황을 피하기 위해 특정 국가를 가로 지르는 네트워크 경로를 사용하지 말라는 것처럼 더 추상적이다. 데이터 계층, 중간 계층, 및 글로벌 계층 간의 관계는 군대 조직에 비유할 수 있다. 군인(데이터 계층)은 대령(중간 계층)으로부터 지시를 받는 동시에 장군(글로벌 계층)으로부터의 지시에 따른다. 정책을 시작한 계층이 높을수록 세분성은 줄어들지만 보다 낮은 레벨에 의해 더 높은 우선 순위가 보장된다.

[0181] 기계 학습 알고리즘은 로컬 맥락 정보(LCI)를 활용하여 솔루션의 성능을 개선시키는 새로운 정책을 동적으로 적응시키거나 만들 수 있다. 글로벌 계층 정책에 의해 남겨진 자유도는 중간 계층에 대한 개선 영역을 결정한다. 이는 학습 아키텍처가 또한 각각의 계층에서 이용 가능한 정보에 따라 계층적 구조를 따르는 것을 나타낸다.

[0182] 바람직한 실시예에서, 중간 계층은 에이전트가 아닌 클라우드 상에서 실행된다.

[0183] 상이한 서브 계층이 역시 계층적 방식으로 구성되는 중간 계층을 형성할 수 있다. 서브 계층의 수는 핸들링할 맥락 정보, 구현할 인텔리전스의 양, 및 다른 기업 간의 관계에 따라 달라질 것이다.

[0184] 요약하면, 바람직한 실시예에서, 중간 층은 다음 기능을 수행한다: 1. (회사 측면에서) 시스템 뷰를 핸들링한다; 2. CSP 및 터널 관리한다; 3. 정책 및 명령을 데이터 계층에 전송한다; 4. 글로벌 데이터 계층으로부터의 정책 및 명령을 실행한다; 및 5. 데이터 플레인 및 보다 낮은 중간 계층의 측정치를 수집하고 처리한다.

[0185] 바람직한 실시예에서, 중간 계층은 다음의 입력을 갖는다: 1. 글로벌 계층으로부터의 정책; 및 2. 데이터 계층으로부터의 큐레이팅된 데이터 분석, 그리고 다음의 출력을 갖는다: 1. 글로벌 계층에 대한 큐레이팅된 데이터 분석; 2. 데이터 계층에 대한 정책 및 명령; 3. LCI; 및 4. GUI 사용자 데이터.

[0186] 대안적인 실시예에서, 중간 계층은 기계 학습 알고리즘을 이용하여 정책을 동적으로 만들고 트래픽 패턴을 분류한다.

[0187] 글로벌 계층

[0188] 글로벌 계층에는 모든 기업, 글로벌 공용 인터넷, 및 사회 정치적 이벤트, 뉴스 등과 같은 외부 요인을 포함하여 시스템에 대한 전체적인 시각이 있다. 따라서, 이 레벨 내의 맥락 정보는 중간 계층에 대해서는 단일 기업의 초점을 넘어서기 때문에 글로벌 맥락 정보(GCI)이다.

[0189] 글로벌 계층도 중간 계층으로부터 수신된 큐레이팅된 분석에 따라 정책 및 결정을 안내한다. 이러한 정책은 규칙의 제약과 자유도에 따라 보다 낮은 계층에서 최적화할 여지를 남겨 둔다. 글로벌 정책의 예는 특정 국가 링크를 사용하지 않거나, 스포츠 이벤트로 인한 정체를 피하거나, 휴일 또는 야간 시간이므로 사용률이 낮은 지역

을 통과하는 CSP를 사용하는 것일 것이다.

[0190] 요약하면, 바람직한 실시예에서, 글로벌 계층은 다음의 입력을 사용한다: 1. 중간 계층으로부터의 큐레이팅된 분석; 2. 사회 정치적 사건에 대한 외부 정보; 3. 정보에 대한 크롤링, 그리고 다음의 출력을 갖는다: 1. 중간 계층에 대한 정책 및 명령.

[0191] 대안적인 실시예에서, 글로벌 계층은 기계 학습을 적용하여 정책을 동적으로 만들고 월드 이벤트와 네트워크 메트릭 사이의 관계를 설정한다.

[0192] 학습

[0193] 상이한 레벨로 구성된 시스템 아키텍처가 위에서 설명되었다. 또한 각각의 레벨에서 일부 실시예는 더 나은 결정을 내리기 위해 이용 가능한 정보를 활용하여 전체 시스템의 성능을 최적화하는 학습 알고리즘을 이용한다는 사실이 상기에 언급되었다. 아래에는 주요 과제, 필요한 입력과 출력, 및 최종 목표를 포함하여 각각의 레벨에서의 학습이 기술되어 있다.

[0194] 이 실시예를 위한 학습 솔루션은 3개의 상이한 계층인 (i) 데이터 계층, (ii) 중간 계층, 및 (iii) 글로벌 계층에 적용된다. 이 세 계층은 세 가지 학습 단계로 변환된다. 데이터 계층부터 시작하여 CSP 및 송신되는 패킷에 대한 정보에 기초하여 반응 단계가 있다. 중간 계층에는 기업 내 교차 트래픽과 같은 LCI에 의존하는 로컬 단계가 있다. 마지막으로, 글로벌 계층에는 더 높은 추상성(예를 들어, 한 국가 밖으로의 트래픽)으로 트래픽 플로를 다루는 글로벌 단계가 있다.

[0195] 계층이 높을수록 대기 시간이 길어 지므로 가시성이 향상되어 실시간 기능이 저하된다. 도 15는 아키텍처 프레임워크 내의 이러한 상이한 단계를 도시한다. 학습 모듈(531)을 갖는 글로벌 계층(501)은 학습 모듈(541, 551)을 갖는 중간 계층(511)에 연결되며, 이는 차례로 학습 모듈(561)을 갖는 데이터 계층(521)에 연결된다.

[0196] 이 세 가지 레벨에서 학습을 분해하는 이점은 상이한 시간 및 추상성 체제를 통해 인터넷 규모의 솔루션을 제공하는 것이다. 본 발명의 실시예는 하부 계층의 에이전트로부터 중간 계층 및 글로벌 계층에 있는 클라우드에 이르기까지 각각의 아키텍처 계층에서 상이한 인프라 역량의 이점을 갖는다. 따라서, 시스템이 실시간 제약 조건에 직면하는 경우, 작업 부하는 데이터 계층에서 실행될 수 있으며 반면 비 핵심 데이터의 큰 세트는 용량 문제가 적은 클라우드에서 처리된다.

[0197] 본 발명의 실시예의 다중 레벨 학습 아키텍처는 계층적 학습(Hierarchical Learning, HL)으로 지칭되며, 도 16에서 더 예시된다. 글로벌 계층(601)은 중간 계층(611)에 연결되며, 이는 차례로 데이터 계층(621)에 연결된다.

[0198] HL 아키텍처의 실시예는 각각의 레벨에서 상이한 기계 학습 기술을 사용한다. 예를 들어, 하나의 레벨은 RNN(Recursive Neural Network) 일 수 있으며, 다음 레벨은 DL(Deep Learning)을 구현할 수 있다. 각각의 레벨은 보다 낮은 레벨의 출력이 보다 높은 레벨에 대한 입력 중 하나가 된다는 점에서 다른 레벨에 접속된다. 또한, 각각의 계층에는 계층 상호 접속을 보완하는 그 자체의 데이터 세트가 있다.

[0199] 예를 들어, 데이터 계층은 입력으로서 반응 정보와 중간층으로부터의 입력(예를 들어, 정책)을 갖는다. 결과적으로, 학습 시스템의 적절한 기능을 보장하기 위해 잠재적으로 결정을 내릴 수 있으므로 각각의 레벨은 독립적이다. 예를 들어, 데이터 계층과 그 반응 학습 알고리즘이 클라우드에서 접속 해제되는 경우, 데이터 계층 내의 로컬 학습은 해당 계층이 이용 가능한 정보에 따라 최상의 CSP에 플로를 할당하도록 결정할 수 있다. 이 경우, 정보의 깊이는 클라우드와 같지 않지만, 시스템은 계속 작동할 것이다. 이후에, 계층이 접속되어 제대로 작동하는 경우, 각각의 레벨의 추상성이 상이한 시스템 비전과 함께 활용될 수 있다.

[0200] 인프라 역량은 HL에서 중요한 파라미터가 된다. 에이전트는 상이한 역량을 가진 이기종 디바이스에서 호스트되기 때문에, 각각의 디바이스에서 실행되는 학습 알고리즘은 실행 중인 플랫폼의 영향을 많이 받는다. 예를 들어, 일부 실시예에서, VM은 하이 엔드 서버에 배치되지만, 다른 경우에는 이동 전화기와 같은 리소스 제약 디바이스에서 실행되는 최적화된 에이전트가 고려된다.

[0201] 이기종 디바이스에서 실행되는 경우의 문제를 피하기 위해, 인프라 역량은 각각의 학습 레벨에서 입력으로 사용된다. 그러면, 역량은 한 레벨에서 다른 레벨로의 피드백을 통해 ML 기반 결정에 영향을 준다. 이 설계 특성은 그 다음에 기본 인프라에 따라 계층적 학습을 자율적으로 최적화하게 한다. 데이터 계층의 노드가 더 많은 계산을 수행할 수 있는 경우, 이 사실을 중간 계층에 통신한다. 그러면 중간 계층은 정책에서 더 많은 자유도를 갖게 된다. 반대의 경우, 에이전트는 제한된 리소스를 통신할 수 있으므로 정책이 보다 제한적이어서 계산 리소스

를 덜 필요로 한다.

[0202] 각각의 HL 레벨에서 사용되는 ML 기술은 보다 높은 계층으로부터의 정책에 의해 부과된 제약 사항을 기반으로 결정을 한다. 이러한 정책은 시스템을 관리하기 위해 각각의 레벨에서 이용 가능한 정보에 따라 동적으로 정의된다. 예를 들어, 이용 가능한 상이한 CSP에 대한 플로 할당을 명시한다. 각각의 정책은 자유도가 다르며, 이는 그 정책을 위반하지 않고 기계 학습 기술을 적용하기 위해 아래 레벨에서 활용된다.

[0203] 일부 실시예는 계층 사이에서 교환될 기계 학습 파라미터(예컨대 뉴런 네트워크의 가중치 또는 Bayes Nets의 확률 테이블)를 허용한다, 즉 이미 훈련된 기계 학습 엔진을 복제함으로써 얻어진 지식이 교환된다. 이 접근 방식은 각각의 계층이 자체적으로 정책과 제어 명령을 얻게 하여, 클라우드에서 접속 해제된 경우에도 계층의 자율성을 보장한다. 이 접근 방식은 또한 보다 신속한 의사 결정을 의미한다. 다시 말해, 하위 계층은 상위 계층의 가시성 및 지식을 얻고 그 반대도 마찬가지이다. 각각의 계층은 기계 학습 파라미터를 업데이트하기 위해 노력한다.

[0204] 예를 들어, 중간 계층은 10Mbps보다 큰 처리량을 가진 CSP만 사용될 수 있다고 명시하는 정책을 데이터 계층에 전송한다. 반응 정보에 따르면, 데이터 계층 ML 알고리즘은 그것이 가진 정책 및 자유도에 따라 성능을 최적화할 수 있다. 이 경우, 데이터 계층은 해당 조건을 충족하는 모든 활성 CSP 중에서 선택할 수 있다. 좀 더 제한적인 또 다른 상황은 특정 활성 CSP만을 사용하는 것일 것이다. 여기서, 정책이 이용 가능한 거동을 제한하기 때문에 데이터 계층은 거의 아무 것도 최적화할 수 없다.

[0205] 이러한 자유도는 시스템 변수(에이전트의 역량, 맥락 정보, 네트워크 구성, 트래픽 간섭 등)를 고려하여 각각의 계층 수준에서 동적으로 최적화된다. HL 구조는 NN을 통해 여러 반복을 연결하는 RNN(Recurrent Neural Networks)과 개념적으로 유사하다. 또한 NN을 항상 동일하게 하기 보다는, 상이한 ML 기술이 각각의 레벨에서의 새로운 입력과 연결되며 한편 이들 간의 피드백을 유지한다.

[0206] 본 발명의 실시예에서, 기계 학습은 상이한 영역에 적용된다. HL 내부의 알고리즘은 다음과 같은 광범위한 영역들에 적용될 수 있다: 1. 터널 발견(IP 주소, 발견 시간 등을 기준으로 통과된 네트워크 노드가 있는 경로 정보); 2. CSP 승격 및 강등; 3. CSP 상태 전환; 4. 애플리케이션 유형, SLA, QoE 등에 따라 CSP 분류; 5. 플로 및 트래픽 분류; 6. CSP에 대한 플로 할당(맥락 정보, 인프라 역량, 네트워크 상태 등에 기초하여 플로 분할(몇 개의 서브 플로로 분할되는지)); 7. 과거 이력, 사건 등에 따라 네트워크 상태를 예상; 및 8. (중간 계층 및 글로벌 계층에서) 정책 생성. 이러한 영역은 보다 높은 레벨로부터의 정책에 의해 부과된 각각의 아키텍처 레벨의 자유도에 따라 조건이 지정된다.

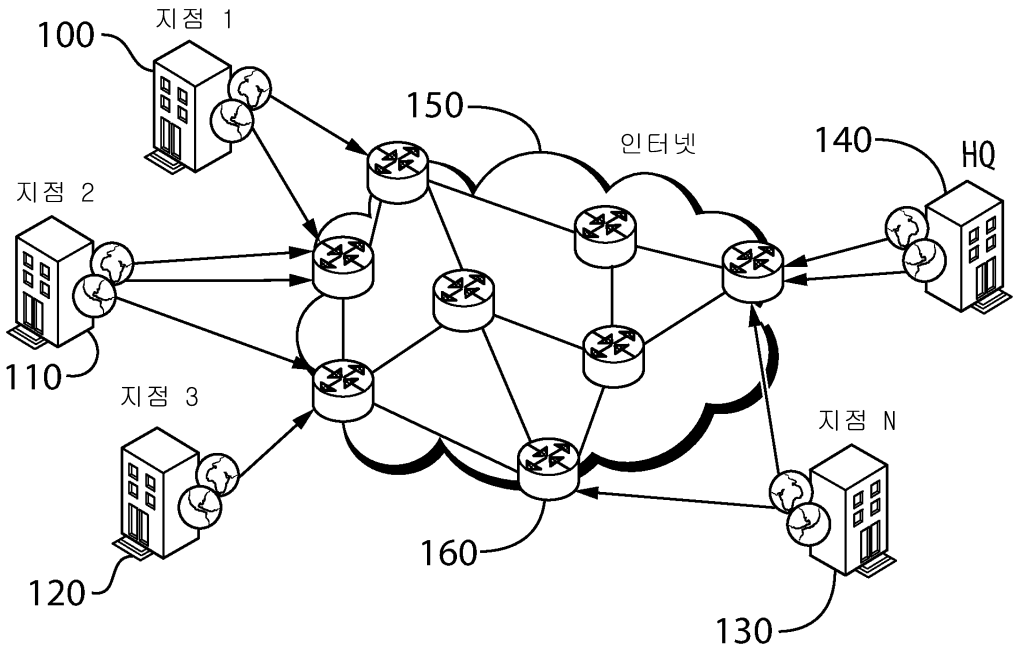
[0207] ML 기술이 적용되는 주요 영역은 이용 가능한 CSP에 대한 플로 할당이다. 효율적인 솔루션을 제공하기 위해, 이 할당은 동적이어야 하고 네트워크 변동에 적응해야 한다. 고려해야 할 데이터의 양은 많으며 시간이 지남에 따라 크게 달라지며, 이는 아키텍처에 심각한 문제가 된다. 이것은 더 정적인 CSP/터널 발견과는 대조적이다.

[0208] CSP 할당에 최적화된 플로를 제공하기 위해, 상이한 ML 기술이 HL 아키텍처에서 실행되는 것으로 간주된다. 데이터 계층의 일부 실시예에서, 실시간 반응 정보를 다루는 RNN(Recurrent Neural Network)이 사용된다. 중간 및 글로벌 계층에서는, Deep Learning 기술의 이점을 활용하여 각각 로컬 및 글로벌 맥락 정보를 커버한다.

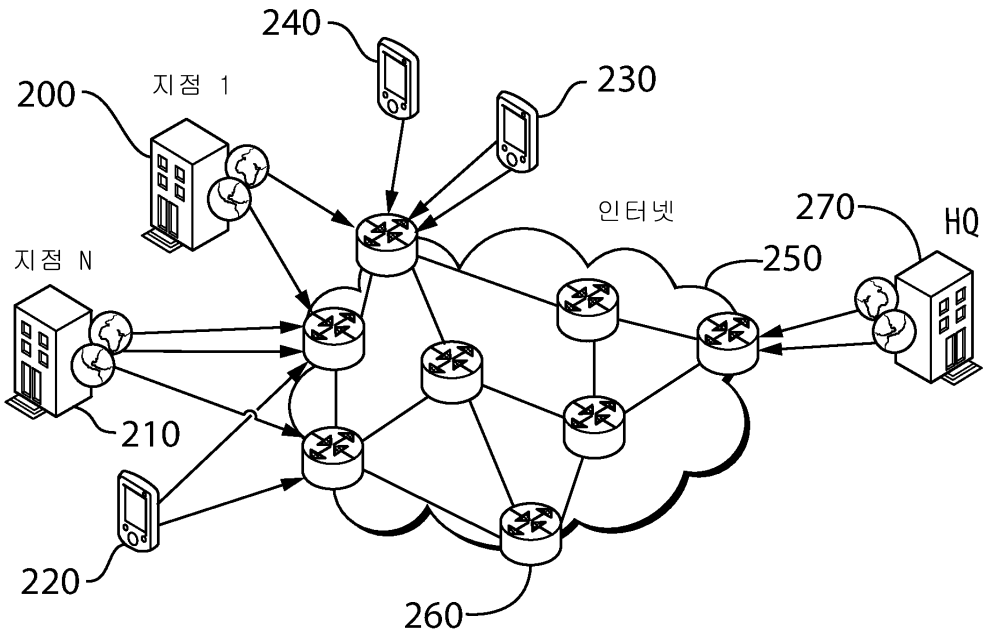
[0209] 본 발명은 여러 가지 바람직한 실시예와 관련하여 전술되었다. 이는 설명의 목적으로만 행해졌으며, 본 발명의 변형은 본 기술분야의 통상의 기술자에게는 쉽게 자명하며 또한 본 발명의 범위 내에 있다.

도면

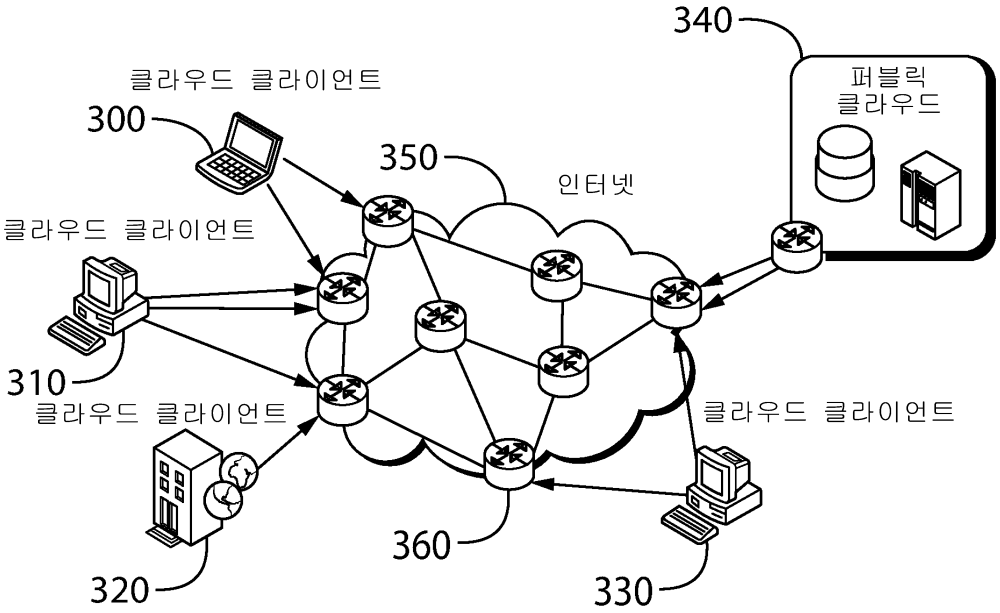
도면1


100
지점 1
150
인터넷
140
HQ
지점 2
110
지점 3
지점 N
120
160
130

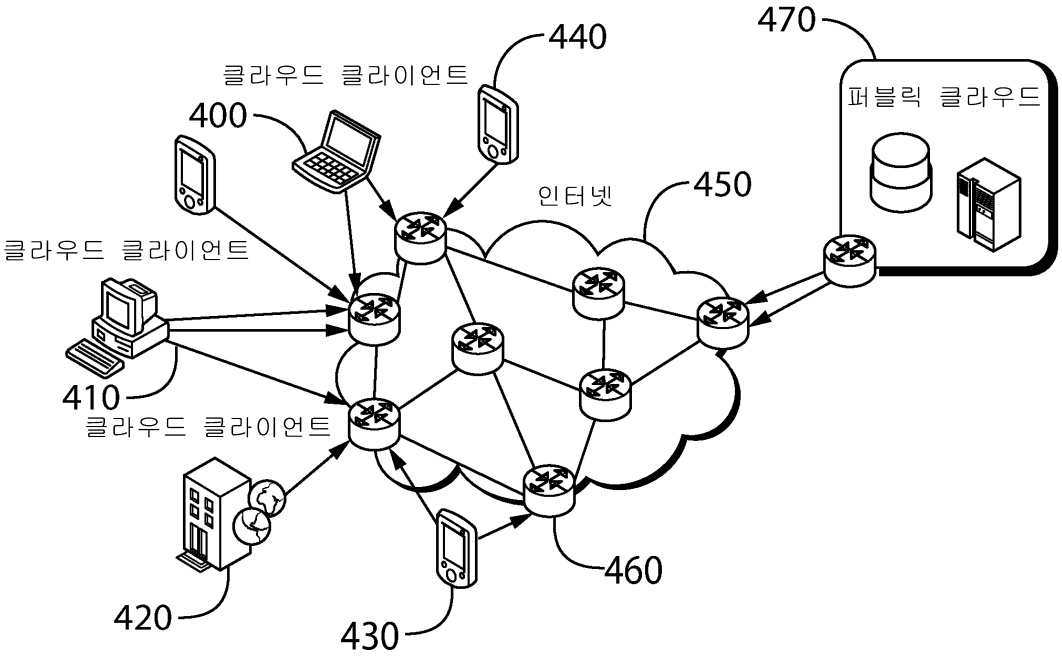
도면2


240
200
지점 1
230
인터넷
270
HQ
지점 N
250
210
220
260

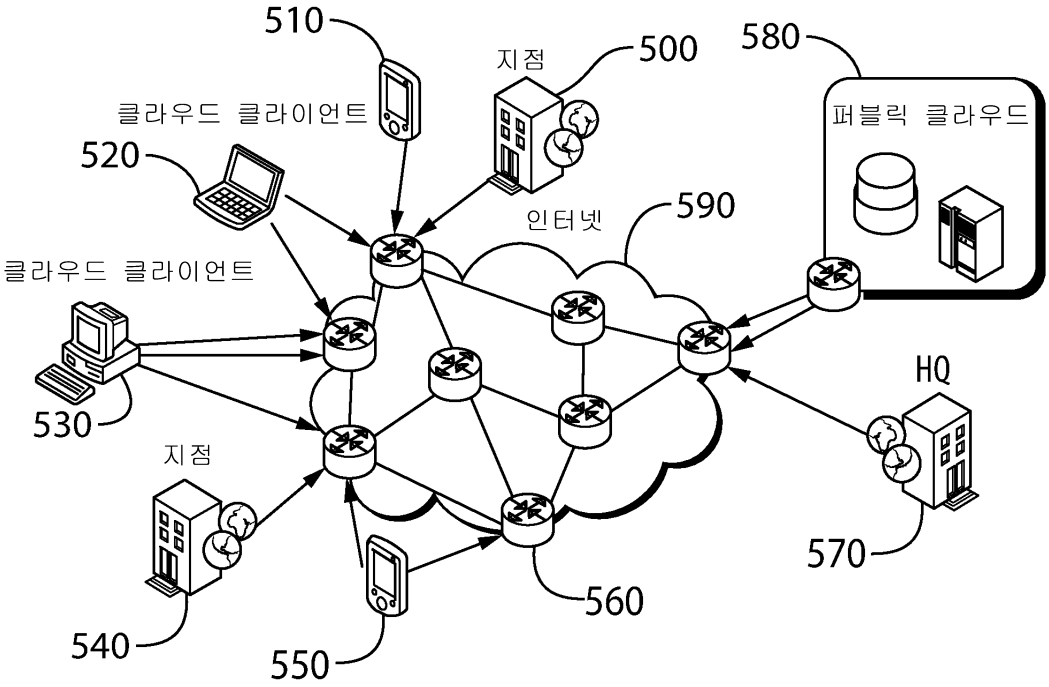
도면3


340
퍼블릭
클라우드
클라우드 클라이언트
300
350
인터넷
클라우드 클라이언트
310
클라우드 클라이언트
클라우드 클라이언트
360
320
330

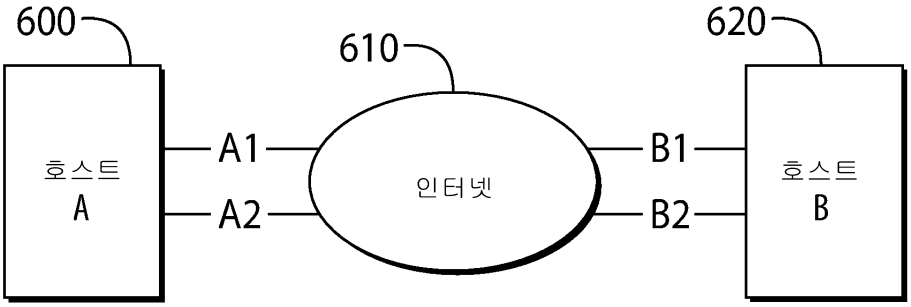
도면4


470
440
퍼블릭 클라우드
클라우드 클라이언트
400
인터넷
450
클라우드 클라이언트
410
클라우드 클라이언트
460
420
430

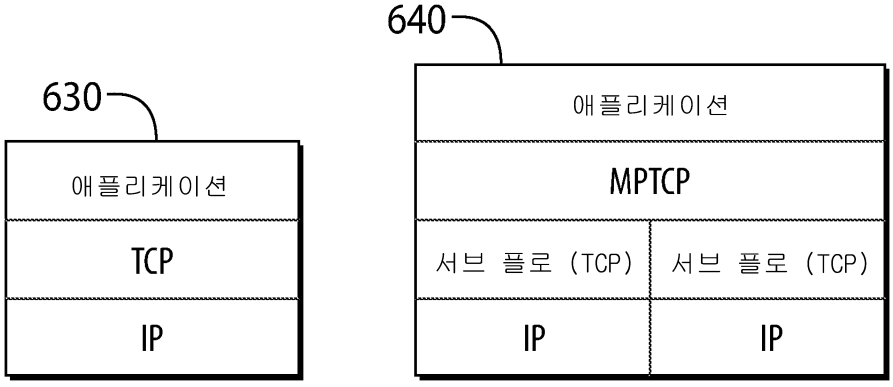
도면5



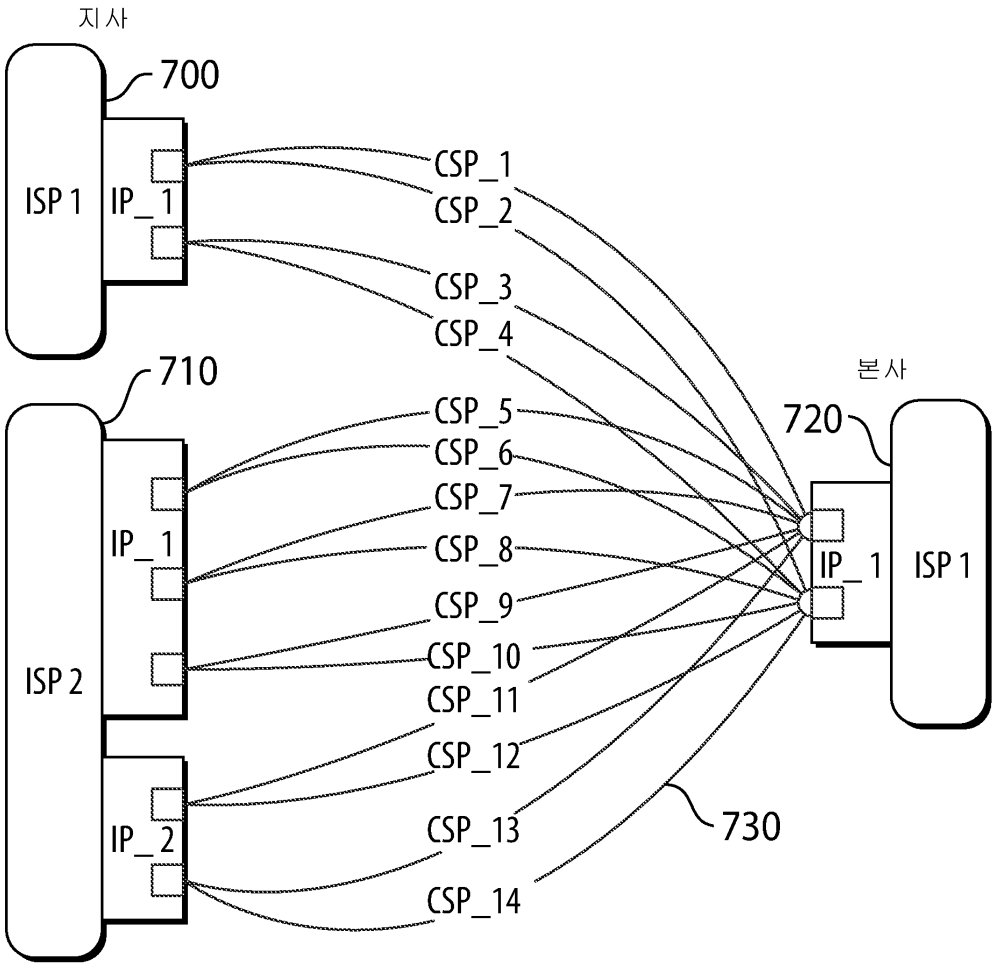
도면6a



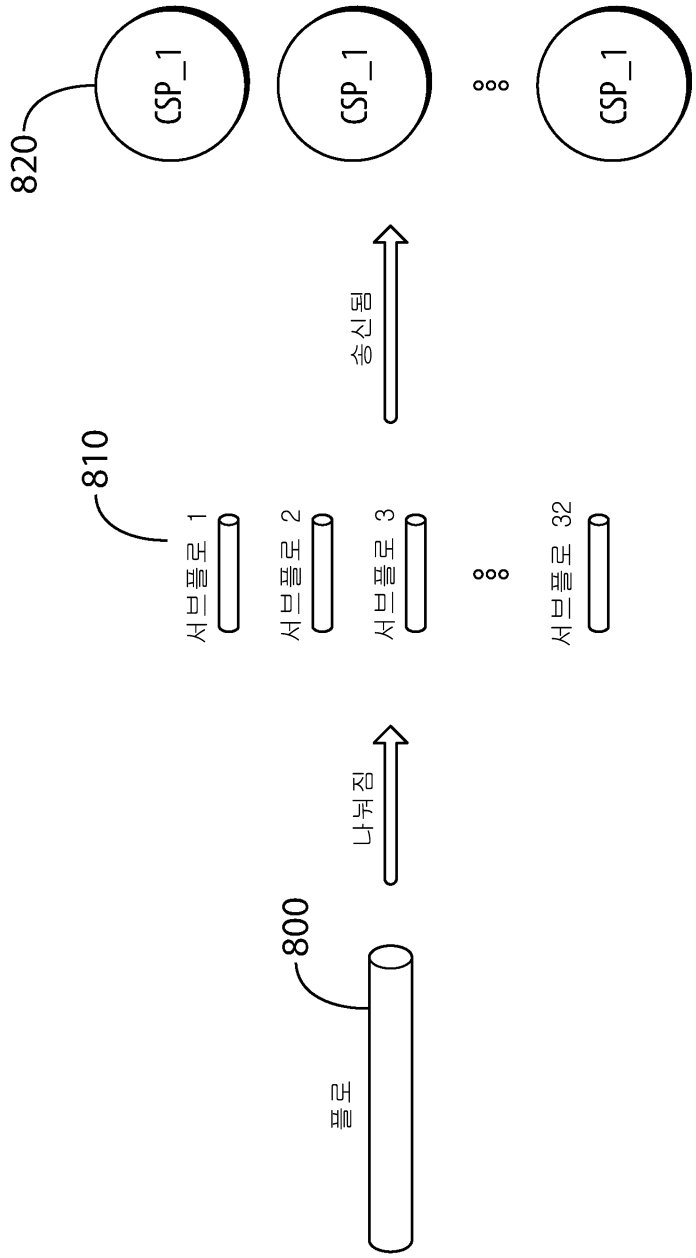
도면6b



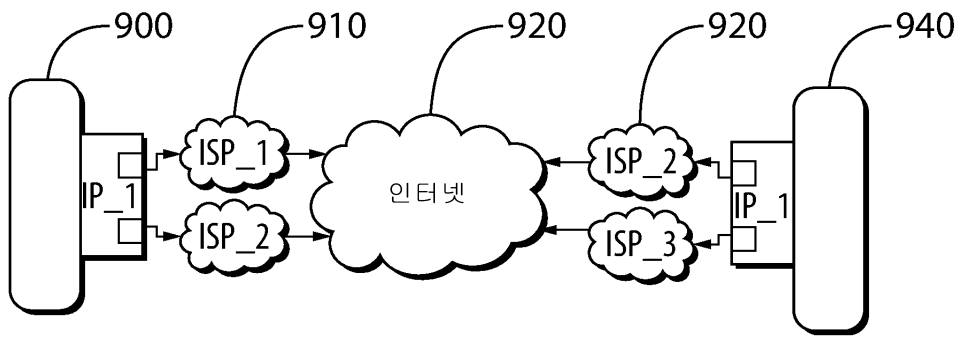
도면7


지사
700
ISP 1
IP_1
710
ISP 2
IP_1
IP_2
CSP_1
CSP_2
CSP_3
CSP_4
CSP_5
CSP_6
CSP_7
CSP_8
CSP_9
CSP_10
CSP_11
CSP_12
CSP_13
CSP_14
730
본사
720
IP_1
ISP 1

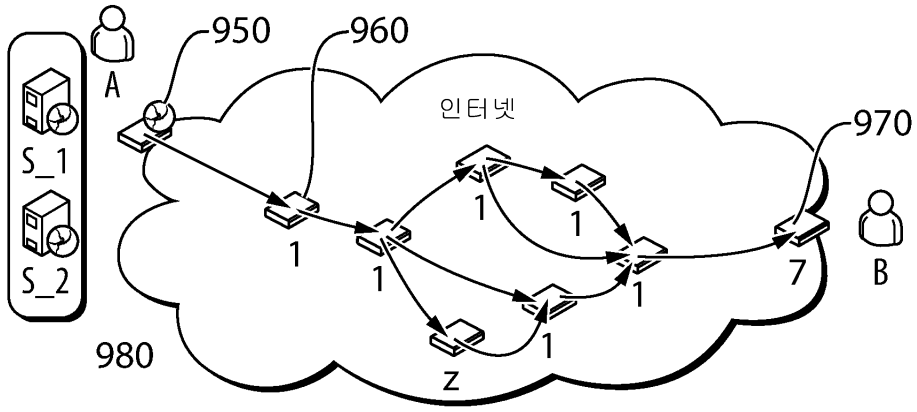
도면8


820
CSP_1
CSP_1
CSP_1
송신됨
810
서브플로 1
서브플로 2
서브플로 3
서브플로 32
나눠짐
800
플로

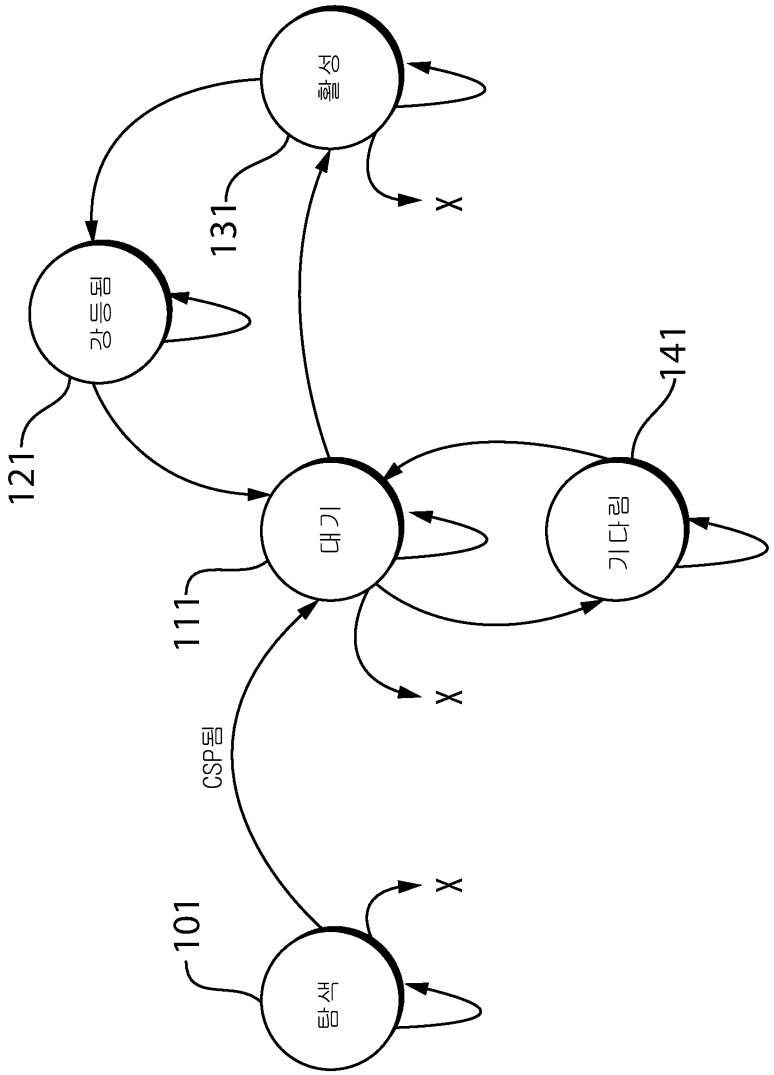
도면9a


900
910
920
920
940
IP_1
ISP_1
ISP_2
인터넷
ISP_2
ISP_3
IP_1

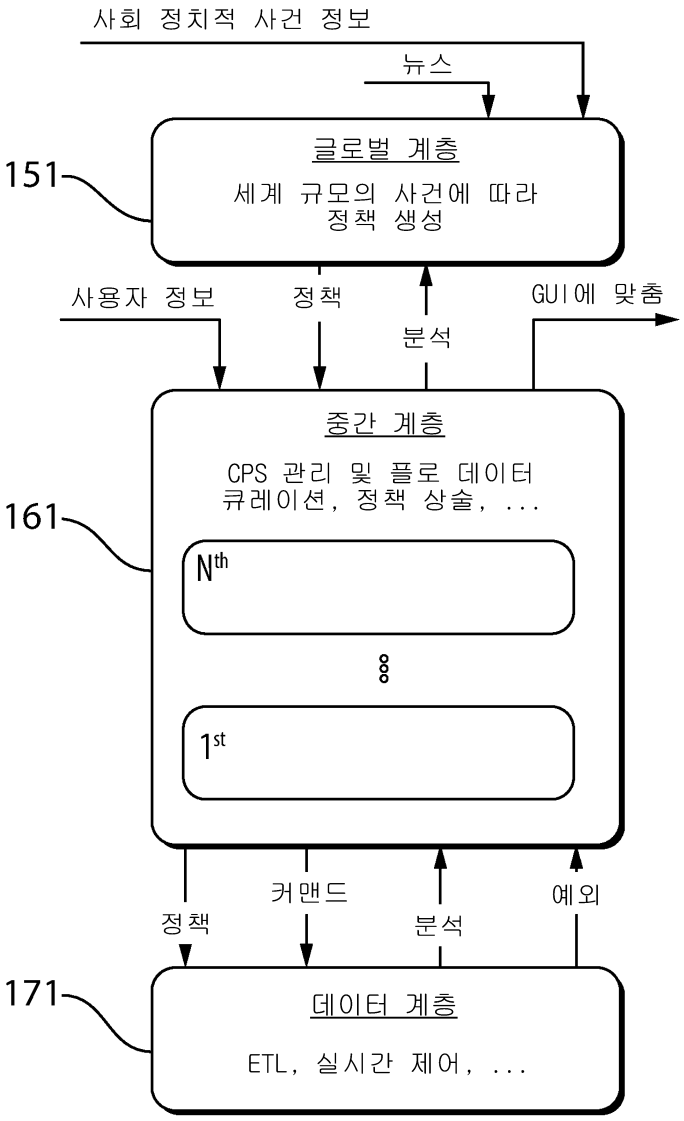
도면9b


A
950
960
인터넷
970
S_1
S_2
1
1
1
1
1
1
7
B
980
z

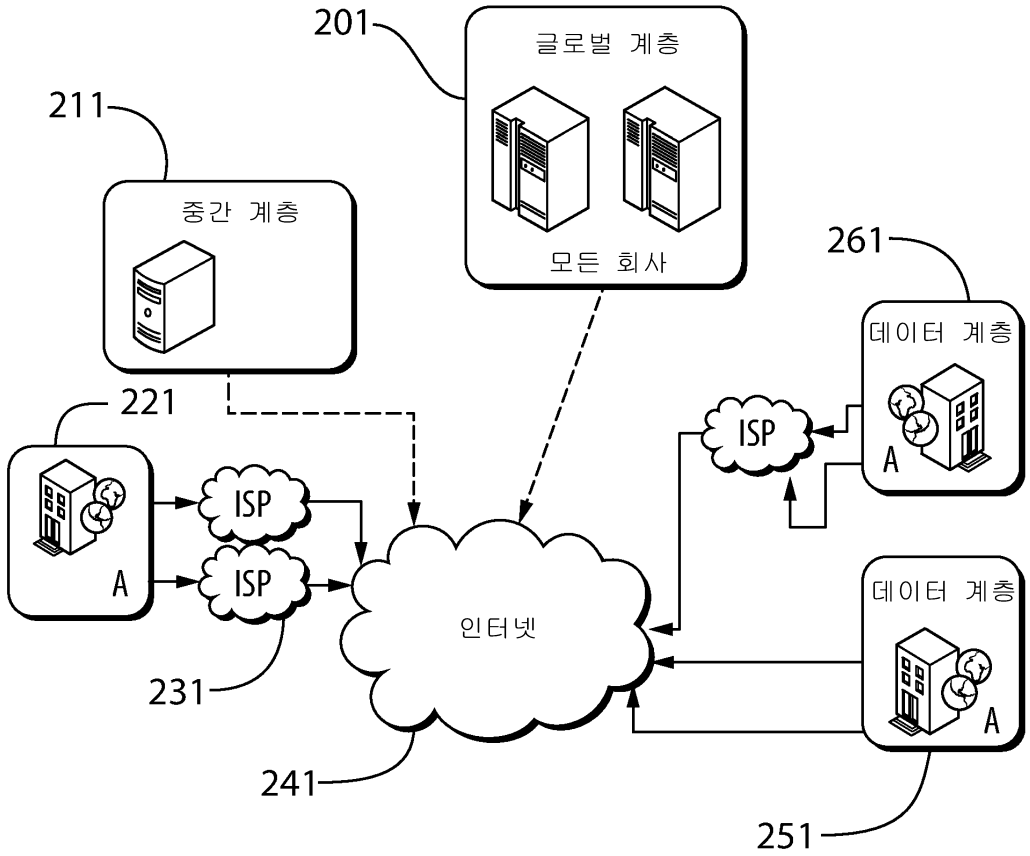
도면10


활성
131
X
강등됨
121
141
대기
기다림
111
X
CSP됨
101
X
탐색

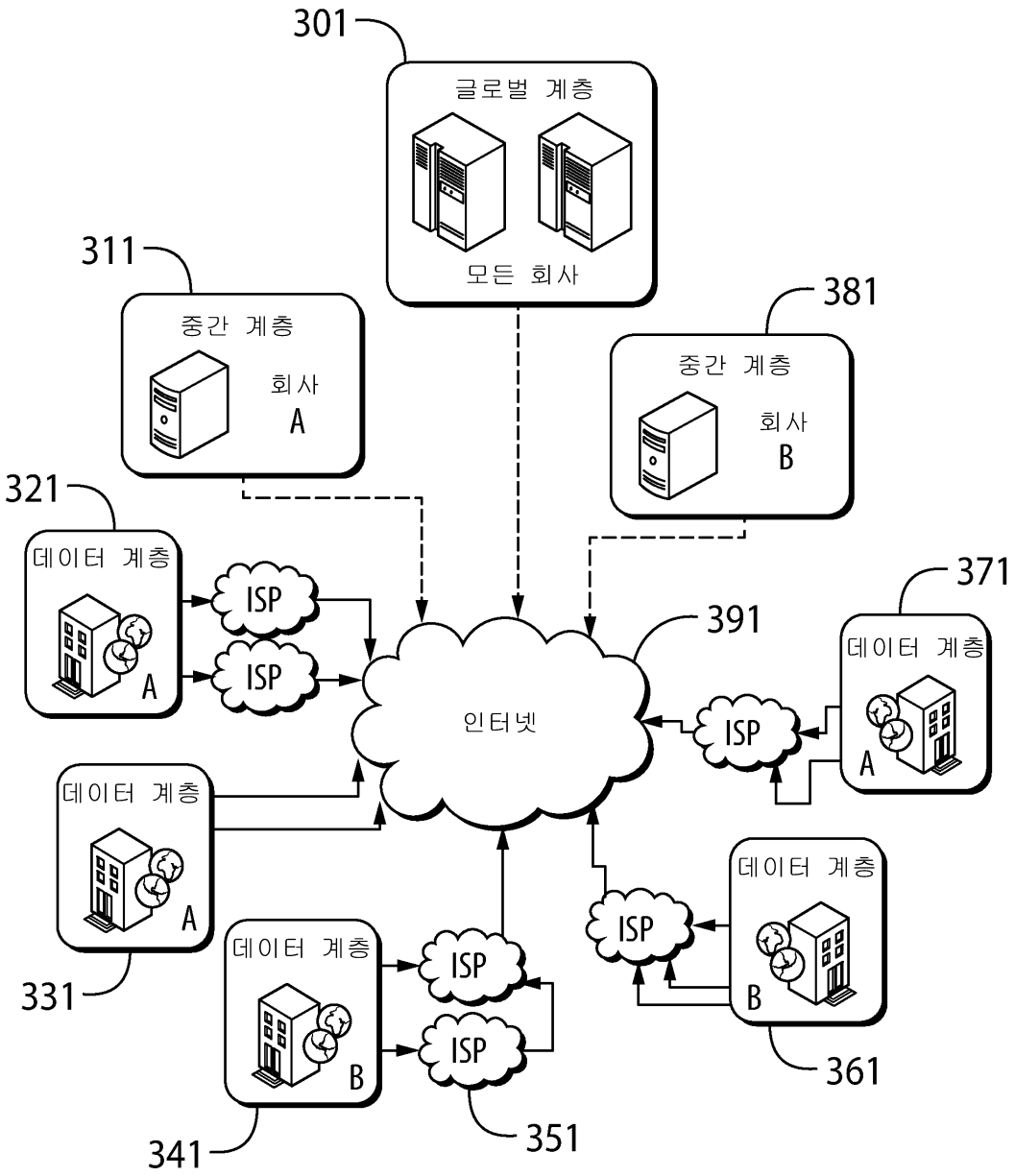
도면11


사회 정치적 사건 정보
뉴스
151
글로벌 계층
세계 규모의 사건에 따라
정책 생성
사용자 정보
정책
분석
GUI에 맞춤
161
중간 계층
CPS 관리 및 플로 데이터
큐레이션, 정책 상술, ...
Nth
1st
정책
커맨드
분석
예외
171
데이터 계층
ETL, 실시간 제어, ...

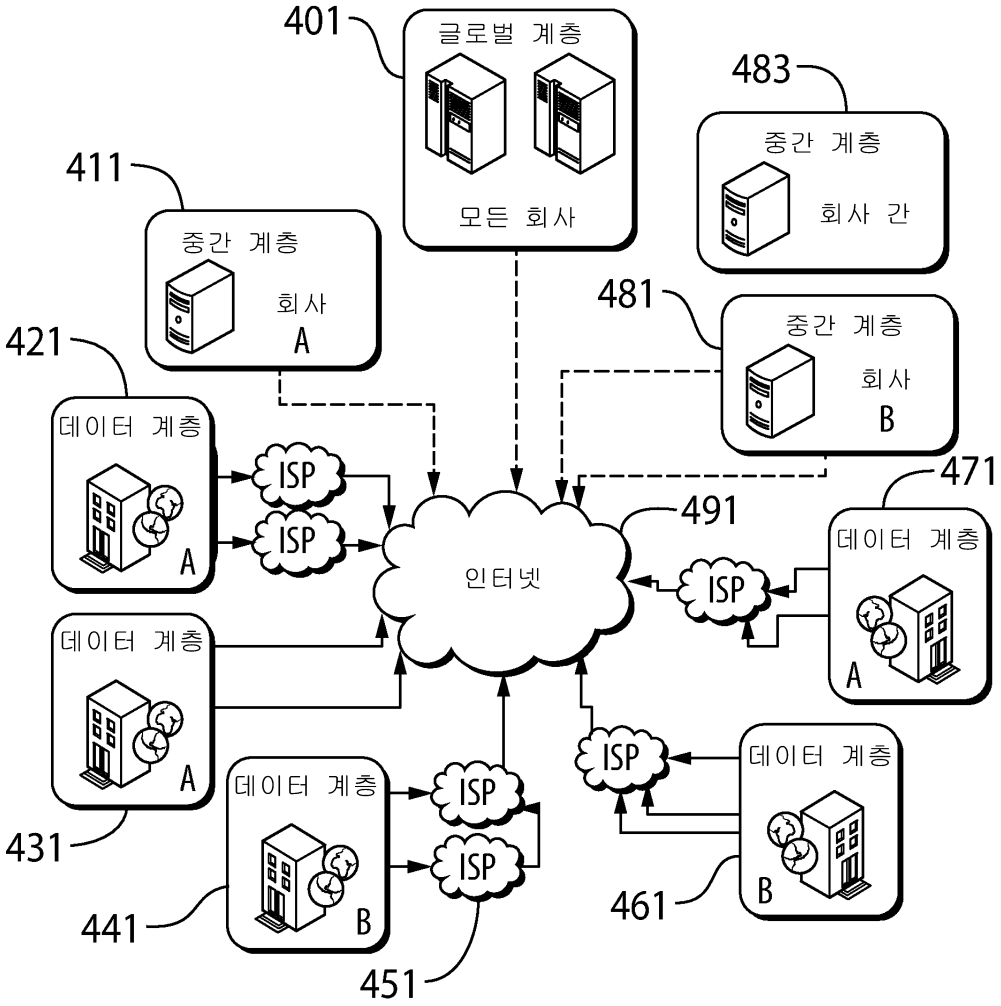
도면12


201
글로벌 계층
모든 회사
211
중간 계층
261
데이터 계층
A
ISP
221
A
ISP
ISP
인터넷
231
241
데이터 계층
A
251

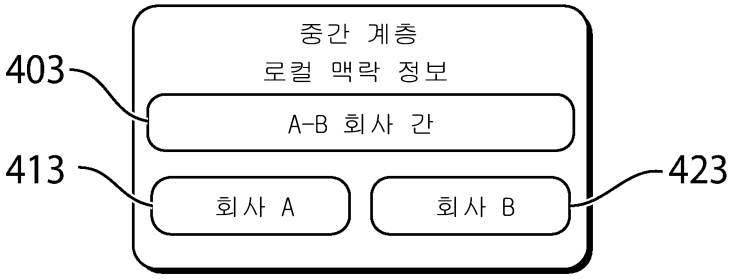
도면13


301
글로벌 계층
모든 회사
311
중간 계층
회사
A
381
중간 계층
회사
B
321
데이터 계층
A
ISP
ISP
391
인터넷
371
데이터 계층
A
ISP
데이터 계층
A
331
데이터 계층
B
341
ISP
ISP
351
ISP
데이터 계층
B
361

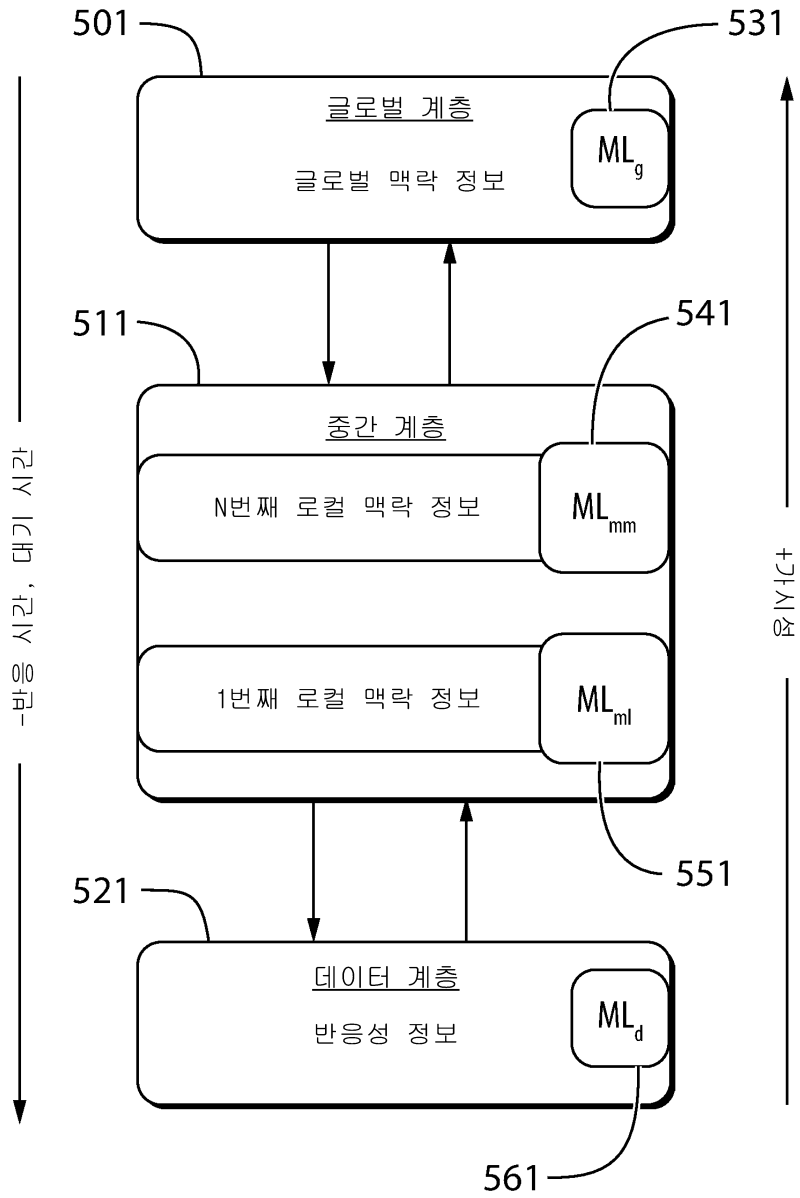
도면14a


401
글로벌 계층
모든 회사
483
중간 계층
회사 간
411
중간 계층
회사
A
481
중간 계층
회사
B
421
데이터 계층
A
ISP
ISP
인터넷
491
471
데이터 계층
A
ISP
데이터 계층
A
431
데이터 계층
B
441
ISP
ISP
451
ISP
데이터 계층
B
461

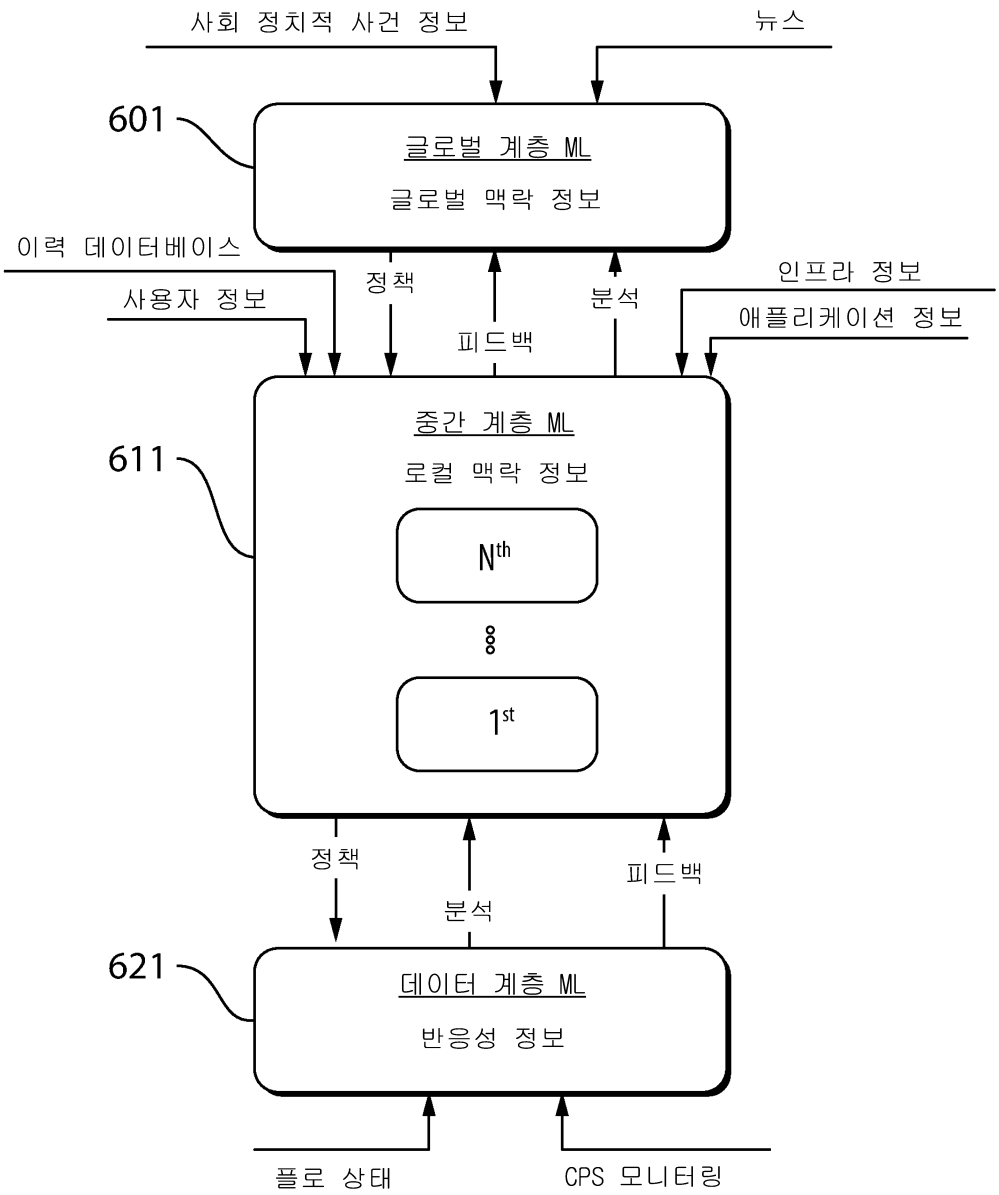
도면14b


중간 계층
로컬 맥락 정보
403
A-B 회사 간
413
회사 A
회사 B
423

도면15


501
531
글로벌 계층
글로벌 맥락 정보
ML_g
511
541
중간 계층
N번째 로컬 맥락 정보
ML_{mm}
1번째 로컬 맥락 정보
ML_{ml}
551
521
데이터 계층
반응성 정보
ML_d
561
-반응 시간, 대기 시간
+대기 시간

도면16


사회 정치적 사건 정보
뉴스
601
글로벌 계층 ML
글로벌 맥락 정보
이력 데이터베이스
사용자 정보
정책
분석
피드백
인프라 정보
애플리케이션 정보
611
중간 계층 ML
로컬 맥락 정보
Nth
1st
정책
분석
피드백
621
데이터 계층 ML
반응성 정보
플로 상태
CPS 모니터링