



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년05월16일
 (11) 등록번호 10-1736425
 (24) 등록일자 2017년05월10일

- (51) 국제특허분류(Int. Cl.)
 H04L 12/24 (2006.01) H04L 12/26 (2006.01)
- (21) 출원번호 10-2014-7007531
- (22) 출원일자(국제) 2012년10월19일
 심사청구일자 2014년03월21일
- (85) 번역문제출일자 2014년03월21일
- (65) 공개번호 10-2014-0051447
- (43) 공개일자 2014년04월30일
- (86) 국제출원번호 PCT/US2012/061216
- (87) 국제공개번호 WO 2013/059744
 국제공개일자 2013년04월25일
- (30) 우선권주장
 13/655,399 2012년10월18일 미국(US)
 61/550,344 2011년10월21일 미국(US)
- (56) 선행기술조사문헌
 EP01750394 A2*
 US20100023604 A1*
 WO2006068548 A1*
 *는 심사관에 의하여 인용된 문헌

- (73) 특허권자
퀄컴 인코포레이티드
 미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
- (72) 발명자
둔랍, 웨인 지.
 미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)
멘차카, 벤자민 엠.
 미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)
노와코우스키, 리안 에이.
 미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)
- (74) 대리인
특허법인 남앤드남

전체 청구항 수 : 총 35 항

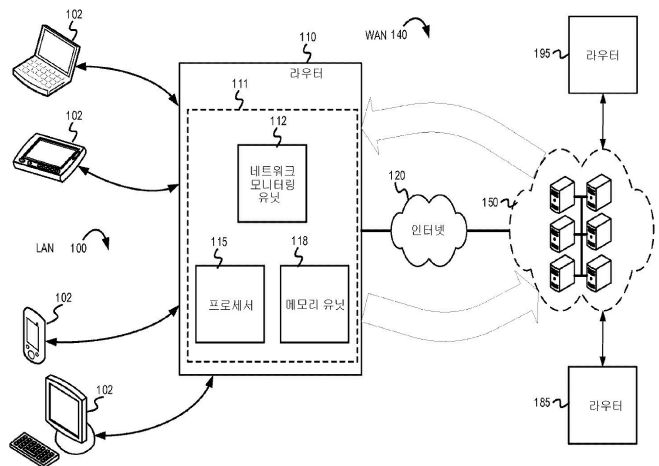
심사관 : 윤태섭

(54) 발명의 명칭 **통신 네트워크들에 대한 클라우드 컴퓨팅 강화 게이트웨이**

(57) 요약

라우터 또는 게이트웨이와 같은, 근거리 네트워크의 네트워크 트래픽 관리 노드는 근거리 네트워크의 네트워크 트래픽을 모니터링할 수 있다. 근거리 네트워크와 연관된 네트워크 이벤트는 네트워크 트래픽 관리 노드를 사용하여 검출된다. 네트워크 이벤트는 네트워크 트래픽 관리 노드로부터 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들로 보고된다. 네트워크 트래픽 관리 노드에 대한 네트워크 정책 업데이트는 클라우드-기반 컴퓨팅 네트워크로부터 수신된다. 네트워크 정책 업데이트는 클라우드-기반 컴퓨팅 네트워크에 보고되는 네트워크 이벤트의 타입에 적어도 부분적으로 기초한다. 네트워크 정책 업데이트는 네트워크 이벤트를 프로세싱하고 그리고/또는 해기 위하여 네트워크 트래픽 관리 노드에서 구현된다.

대표도



명세서

청구범위

청구항 1

제 1 네트워크의 네트워크 트래픽을 모니터링하는 단계;

상기 제 1 네트워크와 연관된 네트워크 이벤트를 검출하는 단계;

상기 네트워크 이벤트를 제 2 네트워크의 서버에 제 3 네트워크를 통해 보고하는 단계;

상기 서버로부터 상기 제 1 네트워크에 대한 네트워크 정책 업데이트(network policy update)를 수신하는 단계
 - 상기 네트워크 정책 업데이트는 상기 서버에 보고되는 상기 네트워크 이벤트의 이벤트 타입 및 제 4 네트워크로부터 상기 제 2 네트워크에서 수집되는 상기 이벤트 타입과 연관된 집합 데이터(aggregate data)의 해석에 적어도 부분적으로 기초하고, 상기 제 1 네트워크 및 상기 제 4 네트워크는 근거리 네트워크(local area network)들임 -; 및

상기 제 1 네트워크에서 상기 네트워크 정책 업데이트를 구현하는 단계를 포함하는, 방법.

청구항 2

제 1항에 있어서,

상기 모니터링 단계, 상기 검출하는 단계, 상기 보고하는 단계, 상기 수신하는 단계 및 상기 구현하는 단계는 상기 제 1 네트워크의 관리 노드에 의해 수행되는, 방법.

청구항 3

제 2항에 있어서,

상기 관리 노드는 상기 제 1 네트워크의 라우터를 포함하는, 방법.

청구항 4

제 2항에 있어서,

상기 관리 노드는 상기 제 1 네트워크의 네트워크 스위치, 케이블 모뎀, 액세스 포인트 및 라우터 중 하나 이상을 포함하는 컴퓨터 시스템을 포함하는, 방법.

청구항 5

제 1항에 있어서,

상기 네트워크 이벤트를 검출하는 단계는, 상기 제 1 네트워크에서 초과신청 이벤트(oversubscription event)를 검출하는 단계, 알려지지 않은 패킷 스트림을 상기 제 1 네트워크에서 검출하는 단계, 및 네트워크 실패 이벤트를 상기 제 1 네트워크에서 검출하는 단계 중 적어도 하나를 포함하는, 방법.

청구항 6

제 1항에 있어서,

상기 네트워크 정책 업데이트를 구현하는 단계는, 상기 네트워크 이벤트를 프로세싱하고 분석(resolve)하도록 상기 제 1 네트워크의 관리 노드를 구성한 이후에 상기 네트워크 정책 업데이트를 구현하는 단계를 포함하는, 방법.

청구항 7

제 1항에 있어서,

상기 네트워크 트래픽을 모니터링하는 단계는,

상기 제 1 네트워크의 복수의 디바이스들로부터 상기 제 3 네트워크로 송신된 네트워크 트래픽을 모니터링하는 단계; 및

상기 제 3 네트워크의 원격 노드로부터 상기 복수의 디바이스들로 송신된 네트워크 트래픽을 모니터링하는 단계를 포함하는, 방법.

청구항 8

삭제

청구항 9

제 1항에 있어서,

상기 제 1 네트워크와 연관된 네트워크 액티비티(network activity)를 검출하는 단계;

상기 서버에 상기 네트워크 액티비티를 보고하는 단계; 및

상기 제 1 네트워크에서 상기 제 2 네트워크로부터 네트워크 경고(network alert)들을 수신하는 단계를 더 포함하는, 방법.

청구항 10

제 1 네트워크의 관리 노드에서, 알려지지 않은 패킷 스트림을 검출하는 단계;

상기 알려지지 않은 패킷 스트림에 대해 디폴트(default) 분류를 선택하는 단계;

상기 관리 노드로부터 상기 알려지지 않은 패킷 스트림과 연관된 정보를 제 2 네트워크의 서버에 보고하는 단계;

상기 관리 노드에서, 상기 알려지지 않은 패킷 스트림에 대한 정책 업데이트를 상기 제 2 네트워크로부터 수신하는 단계 - 상기 정책 업데이트는 상기 알려지지 않은 패킷 스트림을 추후의 과정(instance)에서 어떻게 검출하고 분류할지를 표시하고, 상기 정책 업데이트는 상기 알려지지 않은 패킷 스트림 및 상기 알려지지 않은 패킷 스트림과 연관되는 집합 데이터의 분석에 적어도 부분적으로 기초하고, 상기 집합 데이터는 제 3 네트워크로부터 상기 서버에서 수집됨 -; 및

상기 관리 노드에서 상기 정책 업데이트를 구현하는 단계를 포함하는, 방법.

청구항 11

제 10항에 있어서,

상기 관리 노드에서 검출된 패킷 스트림과 연관된 패킷 스트림 특징을 검출하는 단계;

상기 패킷 스트림 특징에 적어도 부분적으로 기초하여, 상기 패킷 스트림과 연관된 애플리케이션을 결정하는 단계; 및

상기 애플리케이션에 적어도 부분적으로 기초하여 상기 패킷 스트림을 분류하는 단계를 포함하는, 방법.

청구항 12

제 11항에 있어서,

상기 패킷 스트림을 분류하는 단계는, 상기 애플리케이션의 애플리케이션 타입에 적어도 부분적으로 기초하는, 방법

청구항 13

제 10항에 있어서,

상기 알려지지 않은 패킷 스트림을 검출하는 단계 및 상기 디폴트 분류를 선택하는 단계는,

상기 알려지지 않은 패킷 스트림과 연관된 애플리케이션이 상기 관리 노드에 알려지지 않았다고 결정하는 단계; 및

상기 애플리케이션이 알려지지 않았다고 결정하는 것에 응답하여, 상기 알려지지 않은 패키지 스트림에 대해 상기 디폴트 분류를 선택하는 단계를 포함하는, 방법.

청구항 14

제 10항에 있어서,

상기 알려지지 않은 패키지 스트림을 검출하는 단계 및 상기 디폴트 분류를 선택하는 단계는,
 상기 알려지지 않은 패키지 스트림과 연관된 애플리케이션이 상기 관리 노드에 알려지지 않았다고 결정하는 단계;
 상기 알려지지 않은 패키지 스트림과 연관된 애플리케이션 타입을 결정하는 단계; 및
 상기 애플리케이션 타입에 적어도 부분적으로 기초하여, 상기 알려지지 않은 패키지 스트림에 대해 상기 디폴트 분류를 선택하는 단계를 포함하는, 방법.

청구항 15

제 10항에 있어서,

상기 정보를 보고하는 단계는, 상기 알려지지 않은 패키지 스트림과 연관된 패키지 스트림 특징을 보고하는 단계를 포함하는, 방법.

청구항 16

제 10항에 있어서,

상기 알려지지 않은 패키지 스트림과 연관된 애플리케이션 및 상기 알려지지 않은 패키지 스트림에 대한 분류를 표시하는 분류 정보를 수신하는 단계를 더 포함하는, 방법.

청구항 17

제 10항에 있어서,

상기 정책 업데이트를 구현하는 단계는,
 상기 관리 노드에서, 상기 정책 업데이트에 따라, 이전의 알려지지 않은 패키지 스트림과 연관된 패키지 스트림 특징을 검출하는 단계;
 상기 정책 업데이트에 따라 상기 패키지 스트림 특징과 연관된 애플리케이션을 결정하는 단계; 및
 상기 애플리케이션에 기초하여 상기 이전의 알려지지 않은 패키지 스트림에 대한 분류를 선택하는 단계를 포함하는, 방법.

청구항 18

제 1 네트워크의 서버에서, 제 2 네트워크의 제 1 라우터로부터 상기 제 1 라우터에서 검출된 제 1 네트워크 이벤트를 표시하는 보고 메시지를 수신하는 단계;

상기 제 1 네트워크 이벤트의 이벤트 타입을 결정하는 단계;

상기 이벤트 타입의 제 2 네트워크 이벤트를 검출한 제 2 라우터로부터 사전에 수신된 데이터와 함께 상기 이벤트 타입과 연관된 데이터를 집합화하는(agggregating) 단계;

상기 집합화된 데이터를 해석하는 단계;

상기 집합화된 데이터 해석의 결과에 적어도 부분적으로 기초하여 상기 이벤트 타입과 연관된 네트워크 정책 업데이트를 결정하는 단계; 및

상기 네트워크 정책 업데이트를 이용하여 상기 제 1 라우터를 구성하도록 상기 제 1 라우터에 상기 네트워크 정책 업데이트를 송신하는 단계를 포함하는, 방법.

청구항 19

제 18항에 있어서,

상기 이벤트 타입을 결정하는 단계는, 상기 이벤트 타입이 상기 제 2 네트워크에서의 초과신청 이벤트, 상기 제 1 라우터에서의 알려지지 않은 패킷 스트림의 검출, 상기 제 1 라우터로부터의 네트워크 해석 보고의 수신 및 상기 제 2 네트워크에서의 네트워크 실패 이벤트의 검출 중 적어도 하나임을 결정하는 단계를 포함하는, 방법.

청구항 20

제 18항에 있어서,

상기 집합화된 데이터 해석의 결과에 적어도 부분적으로 기초하여, 상기 제 1 라우터에 상기 이벤트 타입과 관련된 콘텐츠의 일시적 저장을 요청하는 단계를 더 포함하는, 방법.

청구항 21

제 18항에 있어서,

상기 네트워크 정책 업데이트는, 상기 제 1 라우터에서 검출된 상기 이벤트 타입의 제 3 네트워크 이벤트를 처리하고 분석하는 동작들을 표시하는, 방법.

청구항 22

네트워크 라우터로서,

프로세서; 및

명령들을 저장하도록 구성된 메모리 유닛을 포함하고,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 네트워크 라우터로 하여금,

제 1 네트워크의 네트워크 트래픽을 모니터링하고;

상기 제 1 네트워크와 연관된 네트워크 이벤트를 검출하고;

상기 네트워크 이벤트를 제 2 네트워크의 서버에 제 3 네트워크를 통해 보고하고;

상기 서버로부터 상기 네트워크 라우터에 대한 네트워크 정책 업데이트를 수신하고 - 상기 네트워크 정책 업데이트는 상기 네트워크 이벤트의 이벤트 타입 및 제 4 네트워크로부터 상기 제 2 네트워크에서 수집되는 상기 이벤트 타입과 연관된 집합 데이터의 해석에 적어도 부분적으로 기초하고, 상기 제 1 네트워크 및 상기 제 4 네트워크는 근거리 네트워크들임 -; 그리고

상기 네트워크 라우터에서 상기 네트워크 정책 업데이트를 구현하게 하는, 네트워크 라우터.

청구항 23

제 22항에 있어서,

상기 네트워크 이벤트는 상기 제 1 네트워크에서의 초과신청 이벤트, 상기 네트워크 라우터에서 수신된 알려지지 않은 패킷 스트림 및 상기 제 1 네트워크에서의 네트워크 실패 이벤트 중 하나를 포함하는, 네트워크 라우터.

청구항 24

제 22항에 있어서,

상기 프로세서에 의해 실행되는 상기 명령들은 추가적으로 상기 네트워크 라우터로 하여금, 상기 네트워크 라우터가 구성된 이후에 상기 네트워크 정책 업데이트를 구현함으로써 상기 네트워크 이벤트를 프로세싱하고 분석하게 하는, 네트워크 라우터.

청구항 25

제 22항에 있어서,

상기 프로세서에 의해 실행되는 상기 명령들은 추가적으로 상기 네트워크 라우터로 하여금,

상기 제 1 네트워크와 연관된 네트워크 액티비티를 검출하고;
 상기 서버에 상기 네트워크 액티비티를 보고하고; 그리고
 상기 제 2 네트워크로부터 네트워크 경고들을 수신하게 하는, 네트워크 라우터.

청구항 26

네트워크 라우터로서,
 프로세서; 및
 상기 프로세서와 커플링된 네트워크 모니터링 유닛을 포함하고;
 상기 네트워크 모니터링 유닛은,

제 1 네트워크의 상기 네트워크 라우터에서 수신된 알려지지 않은 패킷 스트림을 검출하고;

상기 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하고;

상기 알려지지 않은 패킷 스트림과 연관된 정보를 제 3 네트워크를 통해 제 2 네트워크의 서버에 보고하고;

상기 알려지지 않은 패킷 스트림에 대한 정책 업데이트를 상기 제 2 네트워크로부터 수신하고 — 상기 정책 업데이트는 상기 알려지지 않은 패킷 스트림을 추후의 과정에서 어떻게 검출하고 분류할지를 표시하고, 상기 정책 업데이트는 상기 알려지지 않은 패킷 스트림 및 상기 알려지지 않은 패킷 스트림과 연관되는 집합 데이터의 분석에 적어도 부분적으로 기초하고, 상기 집합 데이터는 제 4 네트워크로부터 상기 서버에서 수집됨 —; 그리고

상기 네트워크 라우터에서 상기 정책 업데이트를 구현하도록 구성되는, 네트워크 라우터.

청구항 27

제 26항에 있어서,
 상기 네트워크 모니터링 유닛은 추가적으로,
 상기 네트워크 라우터에서 검출된 패킷 스트림과 연관된 패킷 스트림 특징을 검출하고;
 상기 패킷 스트림 특징에 적어도 부분적으로 기초하여, 상기 패킷 스트림과 연관된 애플리케이션을 결정하고;
 그리고
 상기 애플리케이션에 적어도 부분적으로 기초하여 상기 패킷 스트림을 분류하도록 구성되는, 네트워크 라우터.

청구항 28

제 27항에 있어서,
 상기 네트워크 모니터링 유닛은, 상기 애플리케이션과 연관된 애플리케이션 타입에 적어도 부분적으로 기초하여 상기 패킷 스트림을 분류하도록 구성되는, 네트워크 라우터.

청구항 29

제 26항에 있어서,
 상기 네트워크 라우터에서 상기 알려지지 않은 패킷 스트림을 검출하고 그리고 상기 디폴트 분류를 선택하도록 구성된 상기 네트워크 모니터링 유닛은,

상기 알려지지 않은 패킷 스트림과 연관된 애플리케이션이 상기 네트워크 라우터에 알려지지 않았다고 결정하고; 그리고

상기 애플리케이션이 알려지지 않았다고 결정하는 것에 응답하여 상기 알려지지 않은 패킷 스트림에 대해 상기 디폴트 분류를 선택하도록 구성되는 상기 네트워크 모니터링 유닛을 포함하는, 네트워크 라우터.

청구항 30

제 26항에 있어서,

상기 알려지지 않은 패킷 스트림을 검출하고 그리고 상기 디폴트 분류를 선택하도록 구성된 상기 네트워크 모니터링 유닛은,

상기 알려지지 않은 패킷 스트림과 연관된 애플리케이션이 상기 네트워크 라우터에 알려지지 않았다고 결정하고;

상기 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입을 결정하고; 그리고

상기 애플리케이션 타입에 기초하여 상기 알려지지 않은 패킷 스트림에 대해 상기 디폴트 분류를 선택하도록 구성되는 상기 네트워크 모니터링 유닛을 포함하는, 네트워크 라우터.

청구항 31

제 26항에 있어서,

상기 정보를 보고하도록 구성된 상기 네트워크 모니터링 유닛은, 상기 알려지지 않은 패킷 스트림과 연관된 패킷 스트림 특징을 보고하도록 구성된 상기 네트워크 모니터링 유닛을 포함하는, 네트워크 라우터.

청구항 32

제 26항에 있어서,

상기 정책 업데이트를 구현하도록 구성된 상기 네트워크 모니터링 유닛은,

상기 정책 업데이트에 따라, 이전의 알려지지 않은 패킷 스트림과 연관된 패킷 스트림 특징을 검출하고;

상기 정책 업데이트에 따라 상기 패킷 스트림 특징과 연관된 애플리케이션을 결정하고; 그리고

상기 애플리케이션에 기초하여 상기 이전의 알려지지 않은 패킷 스트림에 대한 분류를 선택하도록 구성되는 상기 네트워크 모니터링 유닛을 포함하는, 네트워크 라우터.

청구항 33

명령들을 저장한 머신-판독가능 저장 매체로서,

상기 명령들은, 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

제 1 네트워크에서, 알려지지 않은 패킷 스트림을 검출하고;

상기 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하고;

상기 알려지지 않은 패킷 스트림과 연관된 정보를 제 2 네트워크의 서버에 제 3 네트워크를 통해 보고하고;

상기 알려지지 않은 패킷 스트림에 대한 정책 업데이트를 상기 제 2 네트워크로부터 수신하고 — 상기 정책 업데이트는 상기 알려지지 않은 패킷 스트림을 추후의 과정에서 어떻게 검출하고 분류할지를 표시하고, 상기 정책 업데이트는 상기 알려지지 않은 패킷 스트림 및 상기 알려지지 않은 패킷 스트림과 연관되는 집합 데이터의 분석에 적어도 부분적으로 기초하고, 상기 집합 데이터는 제 4 네트워크로부터 상기 서버에서 수집됨 —; 그리고

상기 정책 업데이트를 구현하게 하는, 머신-판독가능 저장 매체.

청구항 34

제 33항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 추가적으로 상기 프로세서로 하여금, 상기 제 1 네트워크에서 검출된 패킷 스트림을 분류하게 하고,

상기 분류하는 것은 상기 패킷 스트림과 연관된 애플리케이션 및 상기 애플리케이션의 애플리케이션 타입 중 적어도 하나에 적어도 부분적으로 기초하는, 머신-판독가능 저장 매체.

청구항 35

제 33항에 있어서,

상기 프로세서에 의해 실행될 때, 상기 알려지지 않은 패킷 스트림을 검출하고 그리고 상기 디폴트 분류를 선택하게 하는 상기 명령들은, 추가적으로;

상기 알려지지 않은 패킷 스트림과 연관된 애플리케이션이 알려지지 않았다고 결정하고;

상기 애플리케이션이 알려지지 않았다고 결정하는 것에 응답하여 상기 알려지지 않은 패킷 스트림에 대해 상기 디폴트 분류를 선택하게 하는, 머신-판독가능 저장 매체.

청구항 36

제 33항에 있어서,

상기 프로세서에 의해 실행될 때, 상기 알려지지 않은 패킷 스트림을 검출하고 그리고 상기 디폴트 분류를 선택하게 하는 상기 명령들은, 추가적으로;

상기 제 1 네트워크에서 수신된 상기 알려지지 않은 패킷 스트림과 연관된 애플리케이션이 알려지지 않았다고 결정하고;

상기 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입을 결정하고; 그리고

상기 애플리케이션 타입에 적어도 부분적으로 기초하여, 상기 알려지지 않은 패킷 스트림에 대해 상기 디폴트 분류를 선택하게 하는, 머신-판독가능 저장 매체.

발명의 설명

기술 분야

[0001] 본 출원은, 2011년 10월 21일에 출원된 미국 가출원 일련번호 제 61/550,344호, 및 2012년 10월 18일에 출원된 미국 출원 일련번호 제13/655,399호에 대해 우선권 이익을 주장한다.

배경 기술

[0002] 본 발명의 요지의 실시예들은 일반적으로 통신 네트워크들의 분야에 관한 것이고, 더 상세하게는, 통신 네트워크들에 대한 클라우드 컴퓨팅 강화 게이트웨이에 관한 것이다.

[0003] 홈 또는 사무실 네트워크들과 같은 근거리 네트워크(LAN: local area network)들은 통상적으로, LAN을 광역 네트워크(WAN: wide area network)에 연결시키고, 2개의 네트워크들 사이에서 패킷들을 라우팅하는 라우터(또는 게이트웨이)를 포함한다. LAN의 다양한 네트워크 디바이스들은 라우터를 통해 인터넷으로부터의 정보에 액세스하고 이를 다운로드할 수 있고, 라우터는 인터넷에 액세스하는 상이한 네트워크 디바이스들로부터의 다양한 패킷 스트림들을 관리할 수 있다. LAN의 라우터는 또한, 라우터의 동작들을 구성하고 커스터마이징(customizing)하기 위한 다양한 네트워크 관리자 옵션들을 제공할 수 있다. 그러나, 네트워크 관리자들은 통상적으로 네트워크 트래픽 및 네트워크 상태들에 관한, 네트워크 관리자에게 알려진 제한된 정보에 기초하여 라우터를 수동적으로 구성해야 한다.

발명의 내용

[0004] 일부 실시예들에서, 방법은 근거리 네트워크(LAN)의 네트워크 트래픽을 모니터링하는 단계; LAN과 연관된 네트워크 이벤트를 검출하는 단계; 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 네트워크 이벤트를 보고하는 단계; 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들로부터 LAN에 대한 네트워크 정책 업데이트(network policy update)를 수신하는 단계 - 네트워크 정책 업데이트는 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 보고되는 네트워크 이벤트의 타입에 적어도 부분적으로 기초함 -; 및 LAN에서 네트워크 정책 업데이트를 구현하는 단계를 포함한다.

[0005] 일부 실시예들에서, 모니터링 단계, 검출하는 단계, 보고하는 단계, 수신하는 단계 및 구현하는 단계는 LAN의 네트워크 트래픽 관리 노드에 의해 수행된다.

- [0006] 일부 실시예들에서, 네트워크 트래픽 관리 노드는 LAN의 라우터를 포함한다.
- [0007] 일부 실시예들에서, 네트워크 트래픽 관리 노드는 LAN의 네트워크 스위치, 케이블 모뎀, 액세스 포인트 및 라우터 중 하나 이상을 포함하는 컴퓨터 시스템을 포함한다.
- [0008] 일부 실시예들에서, LAN과 연관된 네트워크 이벤트를 검출하는 단계는 LAN에서 초과신청 이벤트(oversubscription event)를 검출하는 단계, LAN에서, 알려지지 않은 패킷 스트림을 검출하는 단계, 및 LAN에서 네트워크 실패 이벤트를 검출하는 단계 중 적어도 하나를 포함한다.
- [0009] 일부 실시예들에서, 네트워크 정책 업데이트를 구현하는 단계는 네트워크 이벤트를 프로세싱하고 분석(resolve)하기 위하여 LAN의 네트워크 트래픽 관리 노드의 구성 이후에 네트워크 정책 업데이트를 구현하는 단계를 포함한다.
- [0010] 일부 실시예들에서, LAN의 네트워크 트래픽을 모니터링하는 단계는 LAN의 복수의 네트워크 디바이스들 중 하나 이상으로부터 광역 네트워크로 송신된 네트워크 트래픽을 모니터링하는 단계 및 광역 네트워크의 원격 네트워크 노드로부터 LAN의 복수의 네트워크 디바이스들 중 하나 이상으로 송신된 네트워크 트래픽을 모니터링하는 단계를 포함한다.
- [0011] 일부 실시예들에서, 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들로부터 수신되는 네트워크 정책 업데이트는 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 보고되는 네트워크 이벤트의 타입에 기초하며 그리고 복수의 추가 근거리 네트워크들로부터 클라우드-기반 컴퓨팅 네트워크에서 수집되는 네트워크 이벤트의 타입과 연관된 집합 데이터(aggregate data)의 해석(analysis)에 기초한다.
- [0012] 일부 실시예들에서, 방법은 LAN과 연관된 네트워크 액티비티(network activity)를 검출하는 단계; 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 LAN과 연관된 네트워크 액티비티를 보고하는 단계; 및 클라우드-기반 컴퓨팅 네트워크로부터의 네트워크 경고(network alert)들을 LAN에서 수신하는 단계를 더 포함한다.
- [0013] 일부 실시예들에서, 방법은 근거리 네트워크(LAN)의 네트워크 트래픽 관리 노드에서 검출되는 복수의 패킷 스트림들을 분류(classify)하는 단계; 네트워크 트래픽 관리 노드에서, 알려지지 않은 패킷 스트림을 검출하는 단계; 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 단계; 알려지지 않은 패킷 스트림과 연관된 정보를 네트워크 트래픽 관리 노드로부터 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 보고하는 단계; 클라우드-기반 컴퓨팅 네트워크로부터의 알려지지 않은 패킷 스트림에 대한 패킷 스트림 검출 정책 업데이트를 네트워크 트래픽 관리 노드에서 수신하는 단계; 및 알려지지 않은 패킷 스트림을 추후에 검출하여 분류하기 위하여, 네트워크 트래픽 관리 노드에서 패킷 스트림 검출 정책 업데이트를 구현하는 단계를 포함한다.
- [0014] 일부 실시예들에서, 네트워크 트래픽 관리 노드에서 검출되는 복수의 패킷 스트림들을 분류하는 단계는 복수의 패킷 스트림들과 연관된 패킷 스트림 특징들을 검출하는 단계; 대응하는 패킷 스트림 특징들에 적어도 부분적으로 기초하여, 복수의 패킷 스트림들 각각과 연관된 애플리케이션을 결정하는 단계; 및 패킷 스트림들 각각과 연관된 애플리케이션에 적어도 부분적으로 기초하여 복수의 패킷 스트림들 각각을 분류하는 단계를 포함한다.
- [0015] 일부 실시예들에서, 네트워크 트래픽 관리 노드에서 검출되는 복수의 패킷 스트림들을 분류하는 단계는 복수의 패킷 스트림들 각각과 연관된 애플리케이션 및 복수의 패킷 스트림들 각각과 연관된 애플리케이션 타입 중 적어도 하나에 기초하여 복수의 패킷 스트림들을 분류하는 단계를 포함한다.
- [0016] 일부 실시예들에서, 네트워크 트래픽 관리 노드에서, 알려지지 않은 패킷 스트림을 검출하는 단계 및 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 단계는 네트워크 트래픽 관리 노드에서 수신된 패킷 스트림과 연관된 애플리케이션이 알려지지 않음을 결정하는 단계; 및 애플리케이션이 알려지지 않음을 결정하는 것에 응답하여, 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 단계를 포함한다.
- [0017] 일부 실시예들에서, 네트워크 트래픽 관리 노드에서, 알려지지 않은 패킷 스트림을 검출하는 단계 및 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 단계는 네트워크 트래픽 관리 노드에서 수신되는 패킷 스트림과 연관된 애플리케이션이 알려지지 않음을 결정하는 단계; 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입을 결정하는 단계; 및 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입에 기초하여, 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 단계를 포함한다.
- [0018] 일부 실시예들에서, 알려지지 않은 패킷 스트림과 연관된 정보를 네트워크 트래픽 관리 노드로부터 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들로 보고하는 단계는 알려지지 않은 패킷 스트림과 연관된 패킷 스트림

특징들을 보고하는 단계를 포함한다.

- [0019] 일부 실시예들에서, 방법은 패킷 스트림 검출 정책 업데이트를 수신하는 단계에 부가하여, 알려지지 않은 패킷 스트림과 연관된 애플리케이션 및 알려지지 않은 패킷 스트림에 대한 분류를 표시하는 정보를 수신하는 단계를 더 포함한다.
- [0020] 일부 실시예들에서, 알려지지 않은 패킷 스트림을 추후에 검출하고 분류하기 위하여 네트워크 트래픽 관리 노드에서 패킷 스트림 검출 정책 업데이트를 구현하는 단계는 패킷 스트림 검출 정책 업데이트에 따라, 이전의 알려지지 않은 패킷 스트림과 연관된 패킷 스트림 특징을 네트워크 트래픽 관리 노드에서 검출하는 단계; 패킷 스트림 검출 정책 업데이트에 따라 패킷 스트림 특징들과 연관된 애플리케이션을 결정하는 단계; 및 패킷 스트림 특징들과 연관된 애플리케이션에 기초하여 이전의 알려지지 않은 패킷 스트림에 대한 분류를 선택하는 단계를 포함한다.
- [0021] 일부 실시예들에서, 방법은 근거리 네트워크(LAN)의 라우터에서 검출되었던 네트워크 이벤트를 표시하는, 라우터로부터의 보고 메시지를 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에서 수신하는 단계; LAN의 라우터에 의해 검출되었던 네트워크 이벤트의 타입을 결정하는 단계; 네트워크 이벤트의 타입을 또한 검출했던 다른 라우터들로부터 사전에 수신된 데이터와 함께 라우터에 의해 보고된 네트워크 이벤트의 타입과 연관된 데이터를 집합화하는 단계(aggregating); 네트워크 이벤트의 타입과 연관된 집합 데이터를 해석하는 단계; 네트워크 이벤트의 타입과 연관된 집합 데이터의 해석의 결과에 기초하여 네트워크 이벤트의 타입과 연관된 네트워크 정책 업데이트들을 결정하는 단계; 및 네트워크 이벤트의 타입과 연관된 네트워크 정책 업데이트들로 라우터를 구성하도록 LAN의 라우터에 네트워크 정책 업데이트들을 송신하는 단계를 포함한다.
- [0022] 일부 실시예들에서, LAN의 라우터에 의해 검출되었던 네트워크 이벤트의 타입을 결정하는 단계는 네트워크 이벤트의 타입이 LAN에서의 초과신청 이벤트, 라우터에서의 알려지지 않은 패킷 스트림의 검출, 라우터로부터의 네트워크 해석 보고의 수신 및 LAN에서의 네트워크 실패 이벤트의 검출 중 하나임을 결정하는 단계를 포함한다.
- [0023] 일부 실시예들에서, 방법은 라우터에의 콘텐츠의 일시적 저장을 요청하기 위한 커맨드들을 네트워크 이벤트의 타입과 연관된 집합 데이터의 해석의 결과들에 기초하여 LAN의 라우터에 송신하는 단계를 더 포함한다.
- [0024] 일부 실시예들에서, 네트워크 이벤트의 타입과 연관된 집합 데이터의 해석의 결과들에 기초하여 네트워크 이벤트의 타입과 연관된 네트워크 정책 업데이트들을 결정하는 단계는 라우터에서 검출된 네트워크 이벤트의 타입을 프로세싱하고 분석하기 위한 네트워크 정책 업데이트들을 결정하는 단계를 포함한다.
- [0025] 일부 실시예들에서, 네트워크 라우터는 하나 이상의 프로세서들; 및 하나 이상의 명령들을 저장하도록 구성된 하나 이상의 메모리 유닛들을 포함하며; 하나 이상의 명령들은, 하나 이상의 프로세서들에 의해 실행될 때, 네트워크 라우터로 하여금, 근거리 네트워크(LAN)의 네트워크 트래픽을 모니터링하는 동작; LAN과 연관된 네트워크 이벤트를 검출하는 동작; 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 네트워크 이벤트를 보고하는 동작; 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들로부터 네트워크 라우터에 대한 네트워크 정책 업데이트를 수신하는 동작 - 네트워크 정책 업데이트는 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 보고되는 네트워크 이벤트의 타입에 적어도 부분적으로 기초함 -; 및 네트워크 라우터에서 네트워크 정책 업데이트를 구현하는 동작을 포함하는 동작들을 수행하도록 한다.
- [0026] 일부 실시예들에서, LAN과 연관된 네트워크 이벤트는 LAN에서의 초과신청 이벤트, 네트워크 라우터에서 수신되는 알려지지 않은 패킷 스트림 및 LAN에서의 네트워크 실패 이벤트 중 하나를 포함한다.
- [0027] 일부 실시예들에서, 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 명령들은, 네트워크 라우터로 하여금, 네트워크 라우터의 구성 이후에 네트워크 정책 업데이트를 구현함으로써 네트워크 이벤트를 프로세싱하고 분석하는 동작을 더 포함하는 동작들을 수행하도록 한다.
- [0028] 일부 실시예들에서, 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 명령들은, 네트워크 라우터로 하여금, LAN과 연관된 네트워크 액티비티를 검출하는 동작; 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 LAN과 연관된 네트워크 액티비티를 보고하는 동작; 및 클라우드-기반 컴퓨팅 네트워크로부터의 네트워크 경고들을 네트워크 라우터에서 수신하는 동작을 더 포함하는 동작들을 수행하도록 한다.
- [0029] 일부 실시예들에서, 네트워크 라우터는 프로세서; 및 프로세서와 커플링된 네트워크 모니터링 유닛을 포함하며; 네트워크 모니터링 유닛은 근거리 네트워크(LAN)의 네트워크 라우터에서 검출되는 복수의 패킷 스트림들을 분류하며; 네트워크 라우터에서 수신되는 알려지지 않은 패킷 스트림을 검출하며; 알려지지 않은 패킷 스트림에 대

해 디폴트 분류를 선택하며; 알려지지 않은 패킷 스트림과 연관된 정보를 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 보고하며; 알려지지 않은 패킷 스트림에 대한 패킷 스트림 검출 정책 업데이트를 클라우드-기반 컴퓨팅 네트워크로부터 수신하며; 그리고 알려지지 않은 패킷 스트림을 추후에 검출하고 분류하기 위하여, 네트워크 라우터에서 패킷 스트림 검출 정책 업데이트를 구현하도록 구성된다.

- [0030] 일부 실시예들에서, 네트워크 라우터에서 검출되는 복수의 패킷 스트림들을 분류하도록 구성된 네트워크 모니터링 유닛은, 복수의 패킷 스트림들과 연관된 패킷 스트림 특징들을 검출하며; 대응하는 패킷 스트림 특징들에 적어도 부분적으로 기초하여, 복수의 패킷 스트림들 각각과 연관된 애플리케이션을 결정하며; 그리고 패킷 스트림들 각각과 연관된 애플리케이션에 적어도 부분적으로 기초하여 복수의 패킷 스트림들 각각을 분류하도록 구성된 네트워크 모니터링 유닛을 포함한다.
- [0031] 일부 실시예들에서, 네트워크 라우터에서 검출되는 복수의 패킷 스트림들을 분류하도록 구성된 네트워크 모니터링 유닛은 복수의 패킷 스트림들 각각과 연관된 애플리케이션 및 복수의 패킷 스트림들 각각과 연관된 애플리케이션 타입 중 적어도 하나에 기초하여 복수의 패킷 스트림들을 분류하도록 구성된 네트워크 모니터링 유닛을 포함한다.
- [0032] 일부 실시예들에서, 네트워크 트래픽 관리 노드에서, 알려지지 않은 패킷 스트림을 검출하고 그리고 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하도록 구성된 네트워크 모니터링 유닛은, 네트워크 라우터에서 검출된 패킷 스트림과 연관된 애플리케이션이 알려지지 않음을 결정하며; 그리고 애플리케이션이 알려지지 않음을 결정하는 것에 응답하여 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하도록 구성되는 네트워크 모니터링 유닛을 포함한다.
- [0033] 일부 실시예들에서, 네트워크 라우터에서, 알려지지 않은 패킷 스트림을 검출하고 그리고 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하도록 구성된 네트워크 모니터링 유닛은, 네트워크 라우터에서 수신되는 패킷 스트림과 연관된 애플리케이션이 알려지지 않음을 결정하며; 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입을 결정하며; 그리고 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입에 기초하여 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하도록 구성되는 네트워크 모니터링 유닛을 포함한다.
- [0034] 일부 실시예들에서, 알려지지 않은 패킷 스트림과 연관된 정보를 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 보고하도록 구성된 네트워크 모니터링 유닛은 알려지지 않은 패킷 스트림과 연관된 패킷 스트림 특징들을 보고하도록 구성된 네트워크 모니터링 유닛을 포함한다.
- [0035] 일부 실시예들에서, 알려지지 않은 패킷 스트림의 추후에 검출 및 분류를 위하여 네트워크 라우터에서 패킷 스트림 검출 정책 업데이트를 구현하도록 구성된 네트워크 모니터링 유닛은 패킷 스트림 검출 정책 업데이트에 따라, 이전의 알려지지 않은 패킷 스트림과 연관된 패킷 스트림 특징을 검출하며; 패킷 스트림 검출 정책 업데이트에 따라 패킷 스트림 특징들과 연관된 애플리케이션을 결정하며; 그리고 패킷 스트림 특징들과 연관된 애플리케이션에 기초하여 이전의 알려지지 않은 패킷 스트림에 대한 분류를 선택하도록 구성되는 네트워크 모니터링 유닛을 포함한다.
- [0036] 일부 실시예들에서, 하나 이상의 머신-판독가능 저장 매체에는 명령들이 저장되며, 명령들은, 하나 이상의 프로세서들에 의해 실행될 때, 하나 이상의 프로세서들로 하여금, 근거리 네트워크(LAN)에서 검출되는 복수의 패킷 스트림들을 분류하는 동작; LAN에서, 알려지지 않은 패킷 스트림을 검출하는 동작; 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 동작; 알려지지 않은 패킷 스트림과 연관된 정보를 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 보고하는 동작; 클라우드-기반 컴퓨팅 네트워크로부터의 알려지지 않은 패킷 스트림에 대한 패킷 스트림 검출 정책 업데이트를 수신하는 동작; 및 알려지지 않은 패킷 스트림을 추후에 검출하여 분류하기 위하여, 패킷 스트림 검출 정책 업데이트를 구현하는 동작을 포함하는 동작들을 수행하도록 한다.
- [0037] 일부 실시예들에서, LAN에서 검출된 복수의 패킷 스트림들을 분류하는 상기 동작은 복수의 패킷 스트림들 각각과 연관된 애플리케이션 및 복수의 패킷 스트림들 각각과 연관된 애플리케이션 타입 중 적어도 하나에 기초하여 복수의 패킷 스트림들을 분류하는 동작을 포함한다.
- [0038] 일부 실시예들에서, 알려지지 않은 패킷 스트림을 검출하고 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 상기 동작들은 LAN에서 수신된 패킷 스트림과 연관된 애플리케이션이 알려지지 않음을 결정하는 동작; 및 애플리케이션이 알려지지 않음을 결정하는 것에 응답하여 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 동작을 포함한다.
- [0039] 일부 실시예들에서, 알려지지 않은 패킷 스트림을 검출하고 그리고 알려지지 않은 패킷 스트림에 대해 디폴트

분류를 선택하는 상기 동작들은 LAN에서 수신되는 패킷 스트림과 연관된 애플리케이션이 알려지지 않음을 결정하는 동작; 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입을 결정하는 동작; 및 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입에 기초하여, 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택하는 동작을 포함한다.

[0040] 첨부된 도면들을 참조함으로써, 본 실시예들은 더 양호하게 이해될 수 있고, 다수의 목적들, 특징들 및 이점들은 이 분야의 당업자들에게 명백해질 수 있다.

도면의 간단한 설명

[0041] 도 1은 일부 실시예들에 따른, 통신 네트워크에 대한 클라우드 컴퓨팅 강화 라우터를 예시하는 예시적인 블록도이다.

도 2는 일부 실시예들에 따른, 도 1에 도시된 근거리 네트워크에 대한 클라우드 컴퓨팅 강화 라우터를 구현하기 위한 예시적인 동작들을 예시하는 흐름도이다.

도 3은 일부 실시예들에 따른, 도 1에 도시된 클라우드 컴퓨팅 강화 라우터 시스템을 구현하기 위한 예시적인 동작들을 예시하는 흐름도이다.

도 4는 일부 실시예들에 따른, 도 1-3에 설명된 클라우드 컴퓨팅 강화 라우터에서 패킷 스트림 검출을 구현하기 위한 예시적인 동작들을 예시하는 흐름도이다.

도 5는 일 실시예들에 따른, 근거리 네트워크 라우팅, 모니터링 및 클라우드-기반 지원을 위한 메커니즘을 포함하는 네트워크 디바이스의 일 실시예의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0042] 후속하는 설명은, 본 발명 요지의 기술들을 구현하는 예시적인 시스템들, 방법들, 기술들, 명령 시퀀스들 및/또는 컴퓨터 프로그램 물건들을 포함한다. 그러나, 설명된 실시예들은 이 특정 세부사항들 없이도 실시될 수 있음이 이해된다. 예를 들어, 예들이 홈 근거리 네트워크(LAN)들에서 클라우드 컴퓨팅 강화 라우터들을 활용하는 것에 관한 것일지라도, 다른 예들에서, 클라우드 컴퓨팅 강화 라우터들은 사무실 네트워크, 멀티-주거 네트워크(multi-dwelling network), 대학 네트워크 등과 같은 임의의 적절한 타입의 네트워크에서 사용될 수 있다. 다른 사례들에서, 설명을 모호하지 않게 하기 위해, 주지의 명령 인스턴스들, 프로토콜들, 구조들 및 기술들은 상세히 도시되지 않았다.

[0043] 통신 네트워크들에 대한 라우터들(또는 게이트웨이들)은 점점더 복잡해지고 있다. 동시에, 경쟁은 라우터들의 비용의 인하를 촉진시키고 있다. 결과적으로, 오늘날 홈 LAN 라우터들의 프로세싱 전력은 성능 관점 및 사양 관점 둘다에서, 라우터들의 전력을 강화할 정교한 알고리즘들을 레버리지(leverage)하는데 충분치 않다. 게다가, 모든 라우터들은 본래 프로세싱 전력, 스토리지(storage), 소프트웨어 및 다른 특징들과 같은 제한된 양의 이용가능한 자원들을 가진다.

[0044] 도 1은 일부 실시예들에 따른, 통신 네트워크에 대한 클라우드 컴퓨팅 강화 라우터를 예시하는 예시적인 블록도이다. LAN(100)은 복수의 네트워크 디바이스들(102) 및 라우터(110)를 포함한다. 복수의 네트워크 디바이스들(102)은, 다양한 타입의 유선 및 무선 네트워킹 디바이스들, 예를 들어, 노트북 컴퓨터들, 태블릿 컴퓨터들, 모바일 폰들, 데스크탑 컴퓨터들, 디지털 카메라들, 텔레비전들, 게이밍 콘솔들, 스마트 기기들 및 다른 적절한 디바이스들을 포함할 수 있다. 라우터(110)(또는 게이트웨이)는, 통신 네트워크로부터 패킷들을 수신하고 통신 네트워크에 패킷들을 라우팅하는, 통신 네트워크의 노드이다. 라우터(110)는, 네트워크들과 연관된 패킷들을 수신, 프로세싱 및 라우팅하는, 2개 이상의 네트워크들 사이의 네트워크 트래픽 관리 노드이다. 그러나, 다른 실시예들에서, LAN(100)은, 다른 타입들의 네트워크 트래픽 관리 노드들 및/또는 네트워크(들)에 대한 다양한 기능들을 수행하도록 구성되는 네트워크 트래픽 관리 노드들, 예를 들어, 케이블 모뎀, 게이트웨이/라우터, 무선 액세스 포인트, 브리지, 스위치 및/또는 스토리지 중 하나 이상을 통합하는 서버 컴퓨터 시스템을 포함할 수 있고, 서버 컴퓨터 시스템은 또한 도 1 내지 도 5를 참조하여 여기에서 설명되는 기능을 구현할 수 있음을 주목한다. 도 1에 도시된 바와 같이, 라우터(110)는, LAN(100)의 네트워크 디바이스들(102)이 WAN(140)에 액세스하고 WAN(140)으로부터 콘텐츠를 수신하도록 허용한다. LAN(100)은, 일반적으로 인터넷(120)으로 지칭될 수 있는 WAN(140)을 형성하는 다수의 LAN들 중 하나이다. 예시된 바와 같이, WAN(140)은 또한 서버들의 다양한 네트워크들(및 다른 네트워크 디바이스들 및 소프트웨어)을 포함할 수 있다. 일례에서, 서버들의 네트워크는, 인터넷

(120)상에서 클라우드 컴퓨팅을 구현할 수 있으며, 클라우드 컴퓨팅은 여기에서 클라우드 컴퓨팅 네트워크(150)(또는 클라우드(150))로 참조될 것이다. 라우터(110)는 LAN(100)이 인터넷(120)을 통해 클라우드(150)에 의해 제공되는 다양한 서비스들의 장점을 획득하도록 허용할 수 있다. 다른 LAN들을 서비스하는 다양한 다른 라우터들(예를 들어, 라우터들(185 및 195))은 또한 클라우드(150)에 연결될 수 있다. 모든 라우터들이 인터넷에 연결되기 때문에, 라우터들을 증대시키기 위하여 클라우드(150)에서 이용가능한 클라우드 컴퓨팅 자원들을 사용하면, 더 정교한 라우터들이 초래되며 또한 라우터들의 비용이 감소될 수 있다.

[0045] 클라우드(150)는 인터넷(120)에 연결된 다양한 라우터들로부터 통계를 수집하고 라우터들에서 실행되는 네트워크 관리 알고리즘들을 개량(refine)하기 위하여 크라우드소싱(crowd sourcing)의 개념을 사용하도록 구성될 수 있으며, 이는 클라우드(150)에 연결된 모든 다른 라우터들의 경험을 레버리지하는 더 스마트한 "학습" 라우터들을 초래할 수 있다. 일부 실시예들에서, 라우터(110)(및 또한 라우터들(185 및 195)과 같은 다양한 라우터들)는 다양한 타입들의 네트워크 이벤트들, 통계 정보 및 다른 네트워크 액티비티를 클라우드(150)에 보고할 수 있다. 예를 들어, 이하에서 추가로 설명되는 바와같이, 라우터(110)는 알려지지 않은 라우터에서 수신되는 패킷 스트림들 및 라우터에 의해 검출되는, LAN(100)의 초과신청 이벤트들과 연관된 정보를 보고할 수 있다. 클라우드(150)는 다양한 라우터들에 의해 보고되는 네트워크 이벤트들과 연관된 정보를 집합화할 수 있으며, 라우터 정책들 및 절차들을 개선하고 업데이트하기 위하여(예를 들어, 라우터들에 저장되는 네트워크 관리 알고리즘들을 업데이트하기 위하여) 데이터를 해석할 수 있다. 라우터(110)는 또한 클라우드(150)가 LAN(100)에 대하여 네트워크 해석을 수행하도록 클라우드(150)에 네트워크 액티비티 보고들을 송신하고 라우터에 네트워크 경고들을 송신할 수 있다. 라우터(110)가 네트워크 액티비티를 보고하는 것에 부가하여, 라우터(110)는 클라우드(150)의 스토리지를 활용할 수 있다. 클라우드(150)는 서비스들을 개인화하여 LAN(100) 및 LAN(100)의 사용자들에게 제안(suggestion)들을 제공하기 위하여(예를 들어, 한산한 야간 시간들 동안 공통 파일 및 소프트웨어 다운로드들을 수행하기 위하여) 네트워크 액티비티 및 스토리지 활용을 모니터링할 수 있다.

[0046] 일부 구현들에서, 라우터(110)는 라우터(110)를 통해 WAN(140)으로/으로부터 패킷 스트림들을 생성하고 프로세싱하는 애플리케이션들을 지능적으로 검출하도록 구성될 수 있다. 예를 들어, 라우터(110)는(예를 들어, 제 1 네트워크 디바이스(102)에서 구현되는) Netflix[®] 비디오 스트리밍 애플리케이션으로부터 패킷 스트림을 그리고 라우터(110)를 통해 패킷들을 활성적으로 송신하는 파일 다운로드 애플리케이션(예를 들어, 제 2 네트워크 디바이스(102)에서 구현되는 비트 토렌트(bit torrent))으로부터 패킷 스트림을 검출할 수 있다. 일부 예들에서, 비디오 스트리밍 서비스(또는 다른 콘텐츠)를 제공한 서버들은 네트워크 디바이스들(102) 중 하나에서 실행되는 클라이언트 애플리케이션에 그리고 라우터(110)를 통해 LAN(100)에 비디오 콘텐츠를 스트리밍할 수 있다. 그러나, 일부 경우들에서, 라우터(110)는 알려지지 않은 패킷 스트림을 검출하거나 또는 패킷 스트림이 인지할 수 없음을 결정할 수 있다. 다른 경우들에서, 알려진 스트림 "지문들" 또는 스트림 특징들을 가진 알려진 애플리케이션은 자신이 생성하는 패킷 스트림들을 변경할 수 있으며(즉, 스트림 특징들을 변경할 수 있으며), 이는 이전의 검출가능한 패킷 스트림을 검출가능하지 않게 만들 수 있다. 일 구현에서, 라우터(110)는 클라우드 컴퓨팅 네트워크(150)의 하나 이상의 서버들에 모든 알려지지 않은 패킷 스트림들에 대한 정보(예를 들어, 스트림 특징들)를 송신하도록 구성될 수 있다. 클라우드(150)는 알려지지 않은 패킷 스트림들에 관하여 다양한 다른 라우터들로부터 수집된 관련 집합 데이터(aggregate data)에 액세스할 수 있다. 관련 집합 데이터에 대한 통계 해석 및/또는 패킷 검사를 수행하는 것에 기초하여, 그리고 또한 인터넷(120)상의 다양한 서비스 제공자로부터의 패킷 스트림들을 연속적으로 모니터링하는 것에 기초하여, 클라우드(150)는 알려지지 않은 패킷 스트림들을 지능적으로 식별할 수 있다. 이후, 클라우드(150)는 라우터(110)(그리고 또한 라우터(185 및 195)와 같은 다른 라우터들)에 대한 새로운 검출 규칙들을 다운로드할 수 있다.

[0047] 일부 구현들에서, 라우터(110)는 인터넷을 통해 송신되는 가장 공통적인 애플리케이션 패킷 스트림들(예를 들어, 탑 100 애플리케이션들)을 검출하기 위한 알고리즘들로 구성될 수 있다. 라우터(100)를 통과하는 임의의 다른 알려지지 않은 패킷 스트림들은 검출 및 식별하기 위하여 클라우드(150)에 송신될 수 있다. 일례에서, 알려지지 않은 패킷 정보가 추가 해석을 위하여 클라우드(150)에 송신된 이후에, 라우터(110)는 알려지지 않은 패킷 스트림에 디폴트 분류를 일시적으로 할당할 수 있다. 예를 들어, 비록 라우터(110)가 패킷 스트림과 연관된 특정 애플리케이션을 검출할 수 없을 수 있을지라도, 라우터(110)는 패킷 스트림이 스트리밍 비디오임을 결정할 수 있으며, 비디오 트래픽에 대해 디폴트 분류를 일시적으로 할당할 수 있다. 다시 말해서, 비록 라우터(110)가 특정 애플리케이션을 검출할 수 없을 수 있을지라도, 라우터(110)는 애플리케이션 타입(예를 들어, 비디오 트래픽)을 검출하고, 애플리케이션 타입에 기초하여, 알려지지 않은 패킷 스트림에 대해 디폴트 분류를 선택할 수 있다. 클라우드(150)가 새로운 검출 규칙들을 결정한 이후에, 결과들은 라우터(110)에 다시 송신될 수 있으

며, 라우터(110)는 패킷 스트림을 적절하게 식별하여 프로세싱하기 위하여 새로운 검출 규칙들을 구현할 수 있다. 이는 라우터(110)가 검출 알고리즘들을 실행하며, 클라우드(150)에 송신되는 통계를 수집하며, 다양한 라우터들로부터의 통계가 클라우드(150)에서 집합화되어 해석되며, 새로운 검출 알고리즘들이 추후에 결정되어 모든 라우터들에 송신되는 셀프-피드백 루프(self-feedback loop)를 생성한다.

[0048] 일부 구현들에서, 라우터(110)는 또한 LAN(100)에서 초과신청 이벤트들을 보고할 수 있다. 라우터(110)는 라우터가 LAN(100)에서 상이한 타입들의 초과신청 이벤트들을 어떻게 조절하였는지를 보고할 수 있다. 일례에서, LAN(100)의 일부 사용자들은 WAN(140)으로부터 라우터(110)를 통해 LAN의 상이한 네트워크 디바이스들(102)로 5개의 영화들을 동시에 스트리밍하기 위하여 5개의 상이한 비디오 스트리밍 애플리케이션들을 개시할 수 있다. 이러한 상황에서, 네트워크는 5개의 상이한 비디오 스트리밍 애플리케이션들에 대해 5개의 상이한 패킷 스트림들을 지원하기에 충분한 대역폭을 갖지 않을 가능성이 있을 것이며, 따라서 라우터는 초과신청 이벤트를 검출할 것이다. 라우터(110)는 초과신청 이벤트를 분석할 하나의 기술을 구현할 수 있으며, 사용되었던 기술 및 그 결과들을 클라우드(150)에 보고할 수 있다. 예를 들어, 라우터(110)는 특정 백분율(예를 들어, 10-20%) 만큼 모든 비디오 스트림들의 대역폭을 감소시키는 것을 결정할 수 있다. 클라우드(150)의 서버들은 유사한 시나리오에 대하여 다른 라우터들로부터 수집되는 집합 데이터를 사용하고, 해석을 수행하며, 라우터(110)가 마주치는 초과신청 이벤트를 조절하기 위한 양호한 기술이 존재함을 결정할 수 있다. 이후, 클라우드(150)의 서버들은 새로운 초과신청 분석 기술에 관한 세부사항들을 라우터(110)에 제공할 수 있으며, 즉 클라우드(150)의 하나 이상의 서버들은 그 타입의 초과신청 이벤트를 분석하기 위한 새로운 알고리즘으로 라우터(110)를 프로그래밍할 수 있다. 예를 들어, 클라우드(150)는 15% 만큼 모든 5개의 비디오 스트림들의 대역폭을 감소시키는 대신에 라우터(110)가 비디오 스트림들 중 4개의 비디오 스트림에 대해 최적 대역폭을 유지해야 함을 결정할 수 있으며, 비디오 스트림들 중 하나의 비디오 스트림의 대역폭을 최소 허용가능 레벨로 감소시킬 수 있다.

[0049] 일부 구현들에서, 라우터(110)는 또한 네트워크 액티비티의 일부 또는 모두를 클라우드(150)에 보고하고 클라우드(150)에 데이터의 대부분 또는 모두를 저장할 수 있다. 보고들을 검출하고 라우터(110)로부터 데이터를 수집하는 것에 응답하여, 클라우드(150)는 LAN(100)에 대하여 네트워크 해석을 수행하고 또한 네트워크 경고들을 송신할 수 있다. 클라우드(150)는 로컬 네트워크 라우터 또는 다른 디바이스가 고유하게 가질 제한 없이, 예를 들어 제한된 자원들 및 스토리지 없이, 수 주 동안, 수 달 동안 및 수 년 동안 네트워크 해석을 수행할 수 있다. 일례에서, 네트워크 액티비티 보고들에 기초하여, 클라우드(150)는 디바이스가 활성화될 때(예를 들어, 디바이스가 계속해서 전송할 때) 특정 디바이스 또는 특정 클래스의 디바이스들이 불균형 양의 대역폭을 사용함을 결정할 수 있다. 클라우드(150)는 LAN(100)을 모니터링할 수 있으며, 디바이스가 활성화되고 이러한 행동을 보임을 자신이 검출할 때 네트워크 경고를 송신할 수 있다. 또 다른 예에서, 클라우드(150)는 업스트림 트래픽이 오버로드됨을 검출하고, 라우터(110)가 업스트림 트래픽을 감소시키고 잠재적으로 양호한 성능을 획득하기 위하여, 통지된 이용가능한 대역폭을 절반으로(예를 들어, 10Mbps로부터 5Mbps로) 감소시킴을 제안하는 네트워크 경고를 라우터(110)에 송신할 수 있다. 라우터(110)가 다른 타입들의 네트워크 이벤트들을 보고할 수 있다는 것에 유의해야 한다. 일부 경우들에서, 라우터(110)는 네트워크 실패들을 클라우드(150)에 보고할 수 있으며, 클라우드(150)는 집합 데이터에 기초하여 분석 절차들을 결정할 수 있으며, 라우터(110)에 솔루션(예를 들어, 구성 업데이트들 또는 새로운 분석 절차 단계들)을 보고할 수 있다. 일부 구현들에서, 클라우드(150)가 LAN(100)과 연관된 네트워크 액티비티 및 네트워크 이벤트들의 대부분 또는 모두를 라우터(110)로부터 수신하기 때문에, 클라우드(150)는 또한 LAN(100)에 대한 다른 개인화된 서비스들을 제공할 수 있다. 예를 들어, 클라우드(150)는 네트워크 디바이스들(102) 중 하나 이상의 디바이스의 소프트웨어 프로그램(예를 들어, Adobe® Acrobat®)이 자동 업데이트들로 (또는 사용자가 정기적으로 업데이트들을 검사하도록) 구성됨을 검출할 수 있다. 사용자가 업데이트를 다운로드중이라는 정보를 또 다른 라우터로부터 클라우드(150)가 수신할 때, 클라우드는 업데이트가 이용가능한 과거에 애플리케이션을 업데이트하였음을 그리고 트래픽이 많지 않을 때 (예를 들어, 오프-피크 시간에) 라우터가 업데이트를 다운로드해야 함을 (예를 들어, 캐시에 업데이트를 일시적으로 저장해야 함을) 다른 라우터들에 알릴 수 있다. 또 다른 예에서, 클라우드(150)는 전자책들이 발표될 때 사용자들 중 하나가 특정 작가의 전자책들을 다운로드함을 검출할 수 있다. 이러한 액티비티에 기초하여, 클라우드(150)는 작가가 새로운 전자책을 발표할 때 라우터(110)의 로컬 스토리지에 전자책을 자동적으로 다운로드할 수 있으며, 따라서 사용자는 WAN 링크를 사용하지 않고 전자책에 액세스하여 전자책을 국부적으로 다운로드할 수 있다.

[0050] 도 1에 도시된 바와같이, 일부 실시예들에서, 라우터(110)는 네트워크 모니터링 유닛(112), 하나 이상의 프로세서들(115), 및 메모리 유닛(118)을 포함할 수 있다. 라우터(110)의 네트워크 모니터링 유닛(112), 하나 이상의 프로세서들(115) 및 메모리 유닛(118)은 클라우드 컴퓨팅 네트워크(150)와 함께 동작하는, 여기에 설명된 네트

워크 이벤트 모니터링 및 보고 동작들을 구현하도록 구성될 수 있다. 일부 실시예들에서, 라우터(110)의 하나 이상의 프로세서들(115)은 여기에서 설명된 네트워크 이벤트 모니터링 및 보고 기술들, 예를 들어 알려지지 않은 패킷 스트림들 및 초과신청 이벤트들을 클라우드(150)에 보고하는 것 및 클라우드(150)로부터 획득되는 정보에 기초하여 새로운 검출 및 분석 정책들을 구현하도록 네트워크 모니터링 유닛(112)과 연관된 (예를 들어, 메모리 유닛(118)에 저장된) 프로그램 명령들을 실행할 수 있다. 일부 구현들에서, 라우터(110)는 네트워크 인터페이스 카드(또는 모듈)(111)를 포함할 수 있다. 네트워크 인터페이스 카드(111)는 네트워크 모니터링 유닛(112), 하나 이상의 프로세서들(115) 및 메모리 유닛(118)을 (예를 들어, 하나 이상의 집적회로들로) 구현할 수 있다. 다른 구현들에서, 라우터(110)는 복수의 네트워크 인터페이스 카드들 및 회로 보드들(네트워크 인터페이스 카드(111)를 포함함)을 포함할 수 있으며, 복수의 네트워크 인터페이스 카드들은 네트워크 모니터링 유닛(112), 하나 이상의 프로세서들(115) 및 메모리 유닛(118)을 구현할 수 있다. 비록 도 1에 도시되지 않을지라도, 일부 구현들에서, 라우터(110)는 프로세서(들)(115) 및 메모리 유닛(118) 외에 하나 이상의 추가 프로세서들 및 메모리 유닛들(및 다른 컴포넌트들)을 포함할 수 있다. 예를 들어, 라우터(110)는 하나 이상의 추가 회로 보드들에서 하나 이상의 프로세서들 및 하나 이상의 메모리 유닛들을 포함할 수 있다.

[0051] 도 2는 일부 실시예들에 따른, 도 1에 도시된 근거리 네트워크에 대한 클라우드 컴퓨팅 강화 라우터를 구현하기 위한 예시적인 동작들을 예시하는 흐름도("흐름")(200)이다. 흐름은 도 2의 블록(202)에 시작한다.

[0052] 블록(202)에서, 근거리 네트워크의 네트워크 트래픽은 라우터를 사용하여 모니터링된다. 예를 들어, 라우터(110)의 네트워크 모니터링 유닛(112)(도 1에 도시됨)은 하나 이상의 네트워크 디바이스들(102)로부터 WAN(140)에 송신되는 네트워크 트래픽(예를 들어, 파일 업로드들) 및 WAN으로부터 LAN(100)에서 수신되는 네트워크 트래픽(예를 들어, 비디오 스트리밍)을 모니터링한다. 더욱이, 네트워크 모니터링 유닛(112)은 LAN(100)의 네트워크 디바이스들(102) 사이에서 송신되는 네트워크 트래픽을 모니터링할 수 있다. 블록(202) 이후에, 흐름은 블록(204)에서 계속된다.

[0053] 블록(204)에서, 근거리 네트워크와 연관된 하나 이상의 네트워크 이벤트들은 라우터를 사용하여 검출된다. 일부 구현들에서, 네트워크 모니터링 유닛(112)은 LAN(100)의 네트워크 트래픽에 기초하여 하나 이상의 네트워크 이벤트들을 검출한다. 앞서 설명된 바와같이, 일부 예들에서, 네트워크 모니터링 유닛(112)은 라우터(110)를 통해 라우팅되는 알려지지 않은 패킷 스트림을 검출하고 그리고/또는 LAN(100)에서 초과신청 이벤트를 검출할 수 있다. 네트워크 모니터링 유닛(112)은 또한 네트워크 실패들 또는 네트워크 대역폭의 불균형 사용과 같은 다른 네트워크 이벤트들을 검출할 수 있다. 블록(204) 이후에, 흐름은 블록(206)으로 계속된다.

[0054] 블록(206)에서, 하나 이상의 네트워크 이벤트들은 라우터로부터 클라우드 컴퓨팅 네트워크로 보고된다. 일부 구현들에서, 네트워크 모니터링 유닛(112)은 라우터(110)로부터 클라우드 컴퓨팅 네트워크(150)의 하나 이상의 서버들에 하나 이상의 네트워크 이벤트들을 보고할 수 있다. 일부 구현들에서, 모든 네트워크 이벤트들 또는 네트워크 액티비티들을 클라우드 컴퓨팅 네트워크(150)에 보고하는 대신에, 라우터(110)는 특정 네트워크 이벤트들("미리 정해진 네트워크 이벤트들")을 보고하도록 구성될 수 있다. 예를 들어, 라우터(110)는 클라우드(150)에 단지 초과신청 이벤트들 및 알려지지 않은 패킷 스트림들만을 보고하도록 구성될 수 있다. 블록(206) 이후에, 흐름은 블록(208)에서 계속된다.

[0055] 블록(208)에서, 라우터에 대한 네트워크 정책 업데이트는 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들로부터 수신된다. 네트워크 정책 업데이트는 클라우드-기반 컴퓨팅 네트워크의 하나 이상의 서버들에 보고되는 네트워크 이벤트의 타입에 적어도 부분적으로 기초한다. 일부 구현들에서, 라우터(110)는 클라우드(150)로부터 네트워크 정책 업데이트를 수신한다. 수신되는 네트워크 정책 업데이트는 클라우드(150)에 보고되었던 네트워크 이벤트의 타입에 적어도 부분적으로 기초한다. 예를 들어, 도 3을 참조로 하여 이하에서 추가로 설명되는 바와같이, 클라우드(150)는 보고되었던 네트워크 이벤트의 타입에 기초하여 그리고 WAN(140)의 다수의 근거리 네트워크들로부터 수집되는 동일한 타입의 네트워크 이벤트와 연관된 집합 데이터에 대하여 수행되는 해석의 결과들에 기초하여 네트워크 정책 업데이트를 결정할 수 있다. 예를 들어, 만일 라우터(110)에 의해 보고되는 네트워크 이벤트가 라우터(110)에서 검출되는 알려지지 않은 패킷 스트림이면, 클라우드(150)는 알려지지 않은 패킷 스트림에서 동일한 패킷 스트림 특징들 중 일부를 또한 검출하였던, WAN(140)의 다른 근거리 네트워크들로부터 그리고 LAN(100)으로부터 수집되었던 집합 데이터에 대한 해석을 수행한다. 집합 데이터로부터, 클라우드(150)는 알려지지 않은 패킷 스트림의 미래의 검출 및 식별을 위하여, 알려지지 않은 패킷 스트림의 특징들에 기초하여 새로운 패킷 스트림 검출 정책들을 결정할 수 있다. 이후, 클라우드(150)는 라우터(110)에서 구현되는 스트림 검출 정책들을 업데이트하기 위하여 새로운 패킷 스트림 검출 정책들을 라우터(110)에 송신할 수 있다.

다. 블록(208) 이후에, 흐름은 블록(210)에서 계속된다.

- [0056] 블록(210)에서, 네트워크 정책 업데이트는 구성 이후에 네트워크 트래픽 관리 노드에서 구현된다. 일부 구현들에서, 네트워크 모니터링 유닛(112)은 네트워크 정책 업데이트로 구성되며, 이후 LAN(100)의 네트워크 이벤트들을 검출하고 프로세싱할 때 라우터(110)에서 네트워크 정책 업데이트를 구현한다. 예를 들어, 알려지지 않은 패킷 스트림 예에서, 네트워크 모니터링 유닛(112)은 패킷 스트림 검출 및 식별을 위해 클라우드(150)로부터 수신되는 새로운 패킷 스트림 검출 정책들을 구현하도록 업데이트될 수 있다. 블록(210) 이후에, 흐름은 종료된다.
- [0057] 도 3은 일부 실시예들에 따른, 도 1에 도시된 클라우드 컴퓨팅 강화 라우터 시스템을 구현하기 위한 예시적인 동작들을 예시하는 흐름도("흐름")(300)이다. 흐름은 도 3의 블록(302)에서 시작한다.
- [0058] 블록(302)에서, 클라우드 컴퓨팅 네트워크(150)의 하나 이상의 서버들은 LAN(100)에서 검출되었던 네트워크 이벤트들을 표시하는 보고 메시지들을 라우터(110)로부터 수신한다. 예를 들어, 앞서 사전에 설명된 바와같이, 라우터(110)는 라우팅된 패킷 스트림들 중 하나가 알려지지 않음을 결정할 수 있으며, 알려지지 않은 패킷 스트림과 연관된 정보를 클라우드(150)에 송신할 수 있다. 또 다른 예로서, 라우터(110)는 LAN(100)에서 초과신청 이벤트를 검출할 수 있으며, 초과신청 이벤트를 분석하는 것을 시도하도록 구현되었던 기술을 표시하는 보고를 클라우드(150)에 송신할 수 있다. 보고에서, 라우터(110)는 또한 초과신청 이벤트 및 기술의 특정 결과들을 분석할 때 특정 기술이 성공적이었는지의 여부를 표시할 수 있다. 블록(302) 이후에, 흐름은 블록(304)에서 계속된다.
- [0059] 블록(304)에서, 클라우드 컴퓨팅 네트워크(150)는 라우터(110)로부터 수신되는 보고 메시지들과 연관된 네트워크 이벤트의 타입을 결정한다. 예를 들어, 클라우드(150)는 보고 메시지가 라우터(110)에서 수신되었던 알려지지 않은 패킷 스트림과 연관됨을 또는 보고 메시지가 LAN(100)에서 검출된 초과신청 이벤트와 연관됨을 결정한다. 그러나, 도 1를 참조로 하여 앞서 설명된 바와같이, 보고 메시지가 다양한 다른 네트워크 이벤트들(예를 들어, 네트워크 실패 보고)을 표시할 수 있다는 것에 유의해야 한다. 블록(304) 이후에, 흐름은 블록(306)에서 계속된다.
- [0060] 블록(306)에서, 클라우드 컴퓨팅 네트워크(150)는 동일한 또는 유사한 타입의 검출된 네트워크 이벤트들에 대해 다른 근거리 네트워크들의 다른 라우터들로부터 사전에 수신된 데이터와 보고된 네트워크 이벤트들과 연관된 데이터를 집합화한다. 예를 들어, 클라우드(150)는 다양한 라우터들에 의해 보고되었던 알려지지 않은 패킷 스트림들과 연관된 모든 정보(예를 들어, 패킷 스트림 특징들)를 집합화한다. 또 다른 예로서, 클라우드(150)는 다양한 라우터들에 의해 보고되는 동일한 또는 유사한 타입의 초과신청 이벤트들과 연관된 모든 데이터(예를 들어, 사용된 분석 기술들 및 결과들)를 집합화한다. 블록(306) 이후에, 흐름은 블록(308)에서 계속된다.
- [0061] 블록(308)에서, 클라우드 컴퓨팅 네트워크(150)는 동일한 또는 유사한 타입의 보고된 네트워크 이벤트들과 연관된 집합화된 데이터를 해석한다. 예를 들어, 클라우드(150)는 다른 근거리 네트워크들의 다양한 라우터들에 의해 보고되었던 알려지지 않은 패킷 스트림들과 연관된 집합화된 데이터를 해석한다. 일례에서, 클라우드(150)는 알려지지 않은 패킷 스트림들과 연관된 집합화된 데이터에 대해 깊은(deep) 패킷 검사 및 통계 해석을 수행할 수 있으며, 알려지지 않은 패킷 스트림들과 연관된 상이한 스트림 특징들을 해석할 수 있다. 동시에, 클라우드(150)는 인터넷(120)상의 다양한 서비스 제공자들로부터의 패킷 스트림들을 연속적으로 모니터링할 수 있으며, 알려지지 않은 패킷 스트림들을 식별하는 것을 돕기 위하여 대응하는 패킷 스트림들의 임의의 변화들을 식별할 수 있다. 또 다른 예에서, 클라우드(150)는 다양한 라우터들에 의해 보고되었던 다양한 초과신청 이벤트들과 연관된 집합화된 데이터를 해석할 수 있다. 클라우드(150)는 초과신청 이벤트를 분석하기 위하여 사용되는 다양한 기술들을 조사할 수 있으며, 상이한 기술들을 구현하는 결과들을 비교한다. 블록(308) 이후에, 흐름은 블록(310)에서 계속된다.
- [0062] 블록(310)에서, 클라우드 컴퓨팅 네트워크(150)는 검출된 네트워크 이벤트들을 조절하기 위한 개선된 네트워크 정책들 또는 절차들을 결정하며, 라우터 구성들을 업데이트하기 위하여 LAN(100)의 라우터(110)에 업데이트된 네트워크 정책들 또는 절차들을 송신한다. 예를 들어, 앞의 블록(308)에서 수행되는 해석에 기초하여, 클라우드(150)는 패킷 스트림들을 검출하기 위한 개선된 패킷 스트림 검출 정책들(예를 들어, 업데이트된 스트림 특징 기준)을 결정할 수 있거나 또는 초과신청 이벤트를 조절하기 위한 개선된 분석 정책들을 결정할 수 있다. 블록(310) 이후에, 흐름은 종료된다.
- [0063] 일부 구현들에서, 클라우드 컴퓨팅 네트워크(150)는 실시간으로 네트워크 정책 업데이트들을 결정하여 라우터

(110)에 송신한다. 예를 들어, 만일 클라우드 컴퓨팅 네트워크(150)가 WAN(140)의 다양한 라우터들로부터 충분한 데이터를 집합화하였고 집합적인 데이터의 해석을 수행하였다면, 클라우드 컴퓨팅 네트워크(150)는 라우터(110)가 네트워크 이벤트를 보고할 때 실시간으로 라우터(110)에 네트워크 정책 업데이트들을 송신할 수 있다. 결과로서, 라우터(110)는 보고된 네트워크 이벤트를 실시간으로 프로세싱하고 그리고/또는 분석하기 위하여 실시간으로 네트워크 정책 업데이트들을 구현할 수 있다. 일부 구현들에서, 라우터(110)로부터의 네트워크 이벤트와 연관된 보고 메시지(들)를 수신한 이후에, 클라우드 컴퓨팅 네트워크(150)는 WAN(140)의 다른 라우터들로부터의 네트워크 이벤트와 연관된 추가 데이터를 집합화하는 것을 계속하고 그리고/또는 집합화된 데이터에 대하여 추가 해석을 수행할 수 있다. 예를 들어, 클라우드 컴퓨팅 네트워크(150)는 네트워크 이벤트에 대한 개선된 네트워크 정책을 결정하기 위하여 자신이 추가 데이터를 클라우드 소싱하고 그리고/또는 추가 해석을 수행할 필요가 있음을 결정할 수 있다. 이러한 예에서, 클라우드 컴퓨팅 네트워크(150)는 라우터(110)에 네트워크 정책 업데이트를 실시간으로 송신할 것이다. 대신에, 클라우드 컴퓨팅 네트워크(150)는 나중 시간에 네트워크 정책 업데이트를 송신할 것이며, 라우터(110)는 네트워크 이벤트의 추후 발생을 프로세싱하고 및/또는 분석하기 위하여 네트워크 정책 업데이트를 구현할 것이다.

[0064] 도 4는 일부 실시예들에 따라, 도 1-3에 설명된 클라우드 컴퓨팅 강화 라우터에서 패킷 스트림 검출을 구현하기 위한 예시적인 동작들을 예시하는 흐름도("흐름")(400)이다. 흐름은 도 4의 블록(402)에서 시작한다.

[0065] 블록(402)에서, 근거리 네트워크의 라우터에서 검출되는 복수의 패킷 스트림들이 분류된다. 일부 구현들에서, 라우터(110)의 네트워크 모니터링 유닛(112)(도 1에 도시됨)은 네트워크 트래픽을 모니터링하고, 복수의 패킷 스트림들을 검출하며 패킷 스트림들을 분류한다. 예를 들어, (예를 들어, 깊은 패킷 검사를 사용하여) 패킷 스트림의 특징 및 통계를 검출한 이후에, 네트워크 모니터링 유닛(112)은 패킷 스트림과 연관된 애플리케이션을 결정하고, 연관된 애플리케이션에 기초하여 패킷 스트림을 분류할 수 있다. 일례에서, 만일 패킷 스트림이 Netflix[®] 비디오 스트리밍 서비스로부터 분배됨을 패킷 스트림 특징들 및 통계가 표시하면, 네트워크 모니터링 유닛(112)은 Netflix[®] 애플리케이션 패킷 스트림으로서 패킷 스트림을 분류한다. 블록(402) 이후에, 흐름은 블록(404)에서 계속된다.

[0066] 블록(404)에서, 알려지지 않은 패킷 스트림이 라우터에서 검출된다. 일부 구현들에서, 네트워크 모니터링 유닛(112)은 패킷 스트림 특징들 및 통계를 검출하고, 패킷 스트림 특징들 및 통계를 알려진 패킷 스트림들과 비교하며, 패킷 스트림이 알려지지 않은 패킷 스트림 특징들 및 통계를 가진 알려지지 않은 패킷 스트림임을 결정한다. 블록(404) 이후에, 흐름은 블록(406)에서 계속된다.

[0067] 블록(406)에서, 알려지지 않은 패킷 스트림에 대해 디폴트 분류가 선택된다. 일부 구현들에서, 비록 네트워크 모니터링 유닛(112)이 알려지지 않은 패킷 스트림과 연관된 특정 애플리케이션을 결정할 수 없을지라도, 네트워크 모니터링 유닛(112)은 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입(예를 들어, 스트리밍 비디오 또는 오디오)에 기초하여 디폴트 분류를 선택할 수 있다. 예를 들어, 알려지지 않은 패킷 스트림의 애플리케이션 타입은 스트리밍 비디오 또는 스트리밍 오디오로서 결정될 수 있으며, 디폴트 분류는 애플리케이션 타입에 기초하여, 알려지지 않은 패킷 스트림에 할당될 수 있다. 일부 구현들에서, 네트워크 모니터링 유닛(112)은 알려지지 않은 패킷 스트림과 연관된 애플리케이션 타입 및 특정 애플리케이션 모두를 결정할 수 없을 수도 있으며, 따라서 알려지지 않은 애플리케이션 및 애플리케이션 타입을 가진 패킷 스트림들에 대해 디폴트 분류를 일시적으로 선택할 수 있다. 디폴트 분류는 특정 애플리케이션이 결정될 수 있을 때까지 알려지지 않은 패킷 스트림이 라우터(110)에 의해 프로세싱되도록 일시적으로 할당될 수 있다. 예를 들어, 디폴트 분류는 알려지지 않은 패킷 스트림에 최소 및 최대 대역폭 요건들 및 일부 경우들에서 우선순위 값을 할당할 수 있다. 일례에서, 만일 애플리케이션 타입으로서 비디오 스트리밍에 기초하여 알려지지 않은 패킷 스트림에 대하여 디폴트 분류가 선택되면, 디폴트 분류는 비디오 스트리밍 애플리케이션들에 대하여 통상적인 최소 및 최대 대역폭 요건들(예를 들어, 비디오 스트리밍 애플리케이션들에 대한 평균 대역폭 수들)을 할당한다. 블록(406) 이후에, 흐름은 블록(408)에서 계속된다.

[0068] 블록(408)에서, 알려지지 않은 패킷 스트림과 연관된 정보는 클라우드 컴퓨팅 네트워크의 하나 이상의 서버들에 보고된다. 일부 구현들에서, 네트워크 모니터링 유닛(112)은 라우터(110)로부터 인터넷을 통해 클라우드(150)로 알려지지 않은 패킷 스트림과 연관된 패킷 스트림 특징들 및 통계를 표시하는 보고 메시지를 송신할 수 있다. 블록(408) 이후에, 흐름은 블록(410)에서 계속된다.

[0069] 블록(410)에서, 업데이트된 패킷 스트림 검출 정책은 클라우드 컴퓨팅 네트워크로부터 수신된다. 일부 구현들에서, 네트워크 모니터링 유닛(112)은 이전의 알려지지 않은 패킷 스트림을 검출하고 분류하기 위하여 사용될

수 있는 업데이트된 패킷 스트림 검출 정책을 클라우드(150)로부터 수신할 수 있다. 일례에서, 클라우드(150)는 알려지지 않은 패킷 스트림에서 동일한 패킷 스트림 특징들 및 통계의 일부를 또한 검출했던, WAN(140)의 다른 근거리 네트워크들로부터 그리고 라우터(110)로부터 수집되었던 집합 데이터에 대하여 해석을 수행한다. 클라우드는 또한 인터넷의 애플리케이션들 및 서비스 제공자들로부터의 패킷 스트림 특징들 및 통계를 수집하는 것을 계속한다. 집합 데이터로부터, 클라우드(150)는 알려지지 않은 패킷 스트림의 미래의 식별 및 분류를 위하여, 알려지지 않은 패킷 스트림의 특징들 및 통계에 기초하여 새로운 패킷 스트림 검출 정책들을 결정할 수 있다. 예를 들어, 클라우드(150)는 클라우드(150)에 의해 집합화된 패킷 스트림 특징들 및 통계와 최근에 온라인에서 팔린 새로운 오디오 스트리밍 서비스로부터의 패킷 스트림 특징들 및 통계를 비교한 이후에, 알려지지 않은 패킷 스트림이 그 새로운 오디오 스트리밍 서비스로부터 유래함을 결정할 수 있다. 또 다른 예에서, 클라우드(150)는 기존의 비디오 스트리밍 서비스가 클라우드(150)의 서비스 및 애플리케이션들과 연관된 패킷 스트림 특징들 통계를 변경하였음을 결정할 수 있다. 블록(410) 이후에, 흐름은 블록(412)에서 계속된다.

[0070] 블록(412)에서, 업데이트된 패킷 스트림 검출 정책은 라우터에서 구현된다. 일부 구현들에서, 네트워크 모니터링 유닛(112)은 라우터(110)가 새로운 정책으로 구성된 이후에 업데이트된 패킷 스트림 검출 정책을 구현한다. 업데이트된 패킷 스트림 검출 정책은 이전의 알려지지 않은 패킷 스트림의 추후 검출 및 분류를 위하여 사용될 수 있다. 흐름(412) 이후에, 흐름은 종료된다.

[0071] 도 1-5 및 여기에서 설명된 동작들이 실시예들을 이해할 때 도움이 되도록 의도된 예들이고, 청구항들의 범위를 제한하거나 실시예들을 제한하도록 사용되지 않아야 함을 이해해야 한다. 실시예들은, 추가적인 동작들을 수행하고, 더 적은 동작들을 수행하고, 동작들을 상이한 순서로 수행하고, 동작들을 병렬적으로 수행하고 그리고 일부 동작들을 상이하게 수행할 수 있다.

[0072] 이 분야의 당업자에 의해 인식될 바와 같이, 본 발명의 요지의 양상들은 시스템, 방법 또는 컴퓨터 프로그램 물건으로 구현될 수 있다. 따라서, 본 발명의 요지의 양상들은, 전체적으로 하드웨어 실시예, 소프트웨어 실시예(펌웨어, 상주 소프트웨어, 마이크로-코드 등을 포함함), 또는 소프트웨어와 하드웨어 양상들을 결합한 실시예의 형태를 취할 수 있고, 이들 모두는 일반적으로 여기에서 "회로", "모듈" 또는 "시스템"으로 지칭될 수 있다. 게다가, 본 발명의 요지의 양상들은, 컴퓨터 판독가능 프로그램 코드가 구현된 하나 이상의 컴퓨터 판독가능 매체(들)로 구현되는 컴퓨터 프로그램 물건의 형태를 취할 수 있다.

[0073] 하나 이상의 컴퓨터 판독가능 매체(들)의 임의의 조합이 활용될 수 있다. 컴퓨터 판독가능 매체는 컴퓨터 판독가능 신호 매체 또는 컴퓨터 판독가능 저장 매체일 수 있다. 컴퓨터 판독가능 저장 매체는, 예를 들어, 전자, 자기, 광학, 전자기, 적외선 또는 반도체 시스템, 장치 또는 디바이스 또는 상기한 것들의 임의의 적절한 조합일 수 있지만 이에 제한되는 것은 아니다. 컴퓨터 판독가능 저장 매체의 더 특정한 예들(비포괄적 리스트)은 다음의 것들, 즉, 휴대용 컴퓨터 디스켓, 하드 디스크, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 소거 가능한 프로그래머블 판독 전용 메모리(EPROM 또는 플래쉬 메모리), 휴대용 콤팩트 디스크 판독 전용 메모리(CD-ROM), 광학 저장 디바이스, 자기 저장 디바이스 또는 상기한 것들의 임의의 적절한 조합을 포함할 것이다. 본 문헌의 문맥에서, 컴퓨터 판독가능 저장 매체는, 명령 실행 시스템, 장치 또는 디바이스에 의해 또는 이와 관련하여 사용하기 위한 프로그램을 포함 또는 저장할 수 있는 임의의 유형의(tangible) 매체일 수 있다. 컴퓨터 판독가능 신호 매체는, 예를 들어, 반송파의 일부로서 또는 기저대역에서, 컴퓨터 판독가능 프로그램 코드가 구현된 전파된 데이터 신호를 포함할 수 있다. 이러한 전파된 신호는, 전자기, 광학, 또는 이들의 임의의 적절한 조합을 포함하는(그러나, 이들에 제한되지 않음) 다양한 형태들 중 임의의 형태를 취할 수 있다. 컴퓨터 판독가능 신호 매체는, 컴퓨터 판독가능 저장 매체가 아니며, 명령 실행 시스템, 장치 또는 디바이스에 의해 또는 이와 관련하여 사용하기 위한 프로그램을 통신, 전파 또는 전송할 수 있는 임의의 컴퓨터 판독가능 매체일 수 있다. 컴퓨터 판독가능 매체 상에 구현되는 프로그램 코드는, 무선, 유선, 광 섬유 케이블, RF 등, 또는 상기한 것들의 임의의 적절한 조합을 포함하는(그러나, 이들에 제한되지 않음) 임의의 적절한 매체를 사용하여 전송될 수 있다.

[0074] 본 발명의 요지의 양상들에 대한 동작들을 수행하기 위한 컴퓨터 프로그램 코드는, Java, Smalltalk, C++ 등과 같은 객체 지향적 프로그래밍 언어, 및 "C" 프로그래밍 언어 또는 유사한 프로그래밍 언어들과 같은 종래의 절차 지향적 프로그래밍 언어들을 포함하는 하나 이상의 언어들 임의의 조합으로 기록될 수 있다. 프로그램 코드는, 전체적으로 사용자의 컴퓨터 상에서, 부분적으로 사용자의 컴퓨터 상에서, 독립형 소프트웨어 패키지로써, 부분적으로는 사용자의 컴퓨터 상에서 그리고 부분적으로는 원격 컴퓨터 상에서, 또는 전체적으로 원격 컴퓨터 또는 서버 상에서 실행될 수 있다. 후자의 시나리오에서, 원격 컴퓨터는, 근거리 네트워크(LAN) 또는 광역 네트워크(WAN)를 포함하는 임의의 타입의 네트워크를 통해 사용자의 컴퓨터에 연결될 수 있거나, 또

는 외부 컴퓨터에 대해 (예를 들어, 인터넷 서비스 제공자를 사용한 인터넷을 통해) 연결이 행해질 수 있다.

[0075] 본 발명의 요지의 양상들은, 본 발명의 요지의 실시예들에 따른 방법들, 장치(시스템들) 및 컴퓨터 프로그램 물건들의 흐름도 예시들 및/또는 블록도들을 참조하여 설명된다. 흐름도 예시들 및/또는 블록도들의 각각의 블록, 및 흐름도 예시들 및/또는 블록도들의 블록들의 조합들은 컴퓨터 프로그램 명령들에 의해 구현될 수 있음이 이해될 것이다. 이 컴퓨터 프로그램 명령들은, 머신을 생성하기 위한 범용 컴퓨터, 특수 목적 컴퓨터, 또는 다른 프로그래머블 데이터 프로세싱 장치의 프로세서에 제공될 수 있어서, 컴퓨터 또는 다른 프로그래머블 데이터 프로세싱 장치의 프로세서를 통해 실행되는 명령들은, 흐름도 및/또는 블록도의 블록 또는 블록들에서 특정되는 기능들/동작들을 구현하기 위한 수단을 생성한다.

[0076] 이러한 컴퓨터 프로그램 명령들은 또한, 컴퓨터, 다른 프로그래머블 데이터 프로세싱 장치 또는 다른 디바이스들이 특정한 방식으로 기능하도록 지시할 수 있는 컴퓨터 판독가능 매체에 저장될 수 있어서, 컴퓨터 판독가능 매체에 저장된 명령들은, 흐름도 및/또는 블록도의 블록 또는 블록들에서 특정된 기능/동작을 구현하는 명령들을 포함하는 제조 물품을 생성한다.

[0077] 컴퓨터 프로그램 명령들은 또한, 컴퓨터, 다른 프로그래머블 데이터 프로세싱 장치, 또는 다른 디바이스들 상으로 로딩되어, 컴퓨터 구현된 프로세스를 생성하도록 일련의 동작 단계들이 컴퓨터, 다른 프로그래머블 장치 또는 다른 디바이스들 상에서 수행되게 할 수 있어서, 컴퓨터 또는 다른 프로그래머블 장치 상에서 실행되는 명령들은 흐름도 및/또는 블록도의 블록 또는 블록들에서 특정된 기능들/동작들을 구현하기 위한 프로세스들을 제공한다.

[0078] 도 5는, 일부 실시예들에 따라 광역 네트워크에서 근거리 네트워크 모니터링 및 클라우드-기반 지원을 위한 메커니즘을 포함하는 네트워크 디바이스(500)의 일 실시예의 블록도이다. 일부 구현들에서, 네트워크 디바이스(500)는, 네트워크들과 연관된 패킷들을 수신, 프로세싱 및 라우팅하는, 2개 이상의 네트워크들(예를 들어, LAN 및 WAN) 사이의 네트워크 트래픽 관리 노드인데, 예를 들어, 네트워크 트래픽 관리 노드는 LAN(예를 들어, 도 1에 도시된 LAN(100))의 라우터/게이트웨이일 수 있다. 그러나, 다른 구현들에서, 네트워크 디바이스(500)는, 케이블 모뎀, 무선 액세스 포인트, 네트워크 브리지, 네트워크 스위치, 데스크탑 컴퓨터, 게이밍 콘솔, 모바일 컴퓨팅 디바이스 등과 같은, 도 1 내지 도 4를 참조하여 앞서 설명된 기능을 구현하도록 구성될 수 있는 다른 적절한 타입들의 네트워크 디바이스들일 수 있음을 주목한다. 네트워크 디바이스(500)는 (가능하게는, 다수의 프로세서들, 다수의 코어들, 다수의 노드들을 포함하고 그리고/또는 멀티-스레딩을 구현하는 등의) 프로세서 유닛(502)을 포함한다. 네트워크 디바이스(500)는 메모리 유닛(506)을 포함한다. 메모리 유닛(506)은 시스템 메모리(예를 들어, 캐시, SRAM, DRAM, 제로 커패시터 RAM, 트윈 트랜지스터 RAM, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM 등 중 하나 이상), 또는 머신-판독가능 저장 매체의 앞서 이미 설명된 가능한 실현들 중 임의의 하나 이상일 수 있다. 네트워크 디바이스(500)는 또한 버스(510)(예를 들어, PCI, ISA, PCI-Express, HyperTransport®, InfiniBand®, NuBus, AHB, AXI 등), 및 무선 네트워크 인터페이스(예를 들어, 블루투스 인터페이스, WLAN 802.11 인터페이스, WiMAX 인터페이스, Zigbee® 인터페이스, 무선 USB 인터페이스 등) 및 유선 네트워크 인터페이스(예를 들어, 이더넷 인터페이스, 전력선 통신 인터페이스 등) 중 적어도 하나를 포함하는 네트워크 인터페이스(들)(508)를 포함한다. 예시된 바와 같이, 네트워크 인터페이스(들)(508)는 또한 네트워크 모니터링 유닛(512)을 포함한다. 예를 들어, 네트워크 모니터링 유닛(512)은 네트워크 인터페이스(들)(508)의 네트워크 인터페이스 모듈 또는 네트워크 인터페이스 카드 내에 구현될 수 있다. 네트워크 모니터링 유닛(512)은 도 1 내지 도 4를 참조하여 앞서 설명된 바와 같이, 네트워크 디바이스(500)에 대한 (다른 특징들 중에서) 네트워크 트래픽 모니터링, 네트워크 이벤트 검출 및 클라우드-기반 액세스 및 지원을 위한 메커니즘을 구현하도록 동작가능하다.

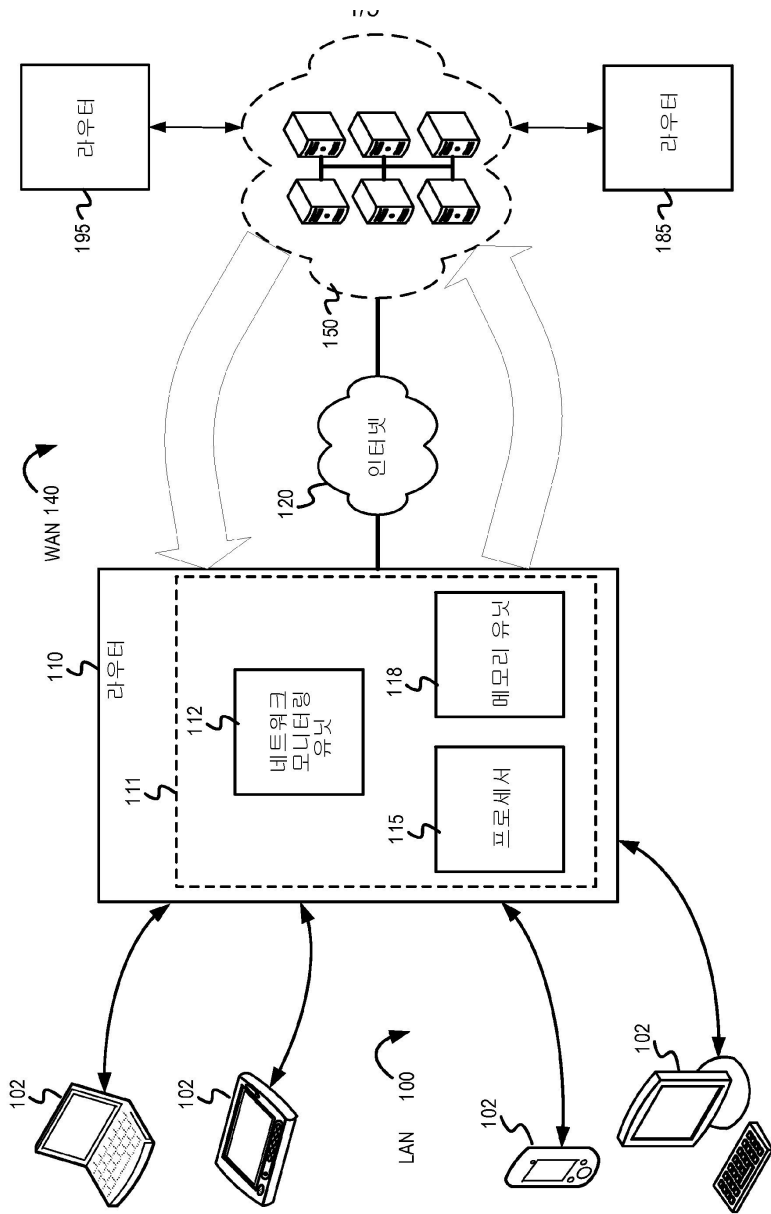
[0079] 이 기능들 중 임의의 기능은 하드웨어로 그리고/또는 프로세서 유닛(502) 상에서 부분적으로(또는 전체적으로) 구현될 수 있다. 예를 들어, 기능은, 하나 이상의 주문형 집적 회로들, 하나 이상의 시스템-온-어-칩(SoC: system-on-a-chip) 또는 다른 타입의 집적 회로(들)로, 프로세서 유닛(502)에서 구현된 로직에서, 주변 디바이스 또는 카드 상의 코-프로세서에서, 네트워크 인터페이스(508) 내에서 구현되는 별개의 프로세서 및/또는 메모리에서 등으로 구현될 수 있다. 추가로, 실현들은, 더 적은 컴포넌트들 또는 도 5에 예시되지 않은 추가적인 컴포넌트들(예를 들어, 비디오 카드들, 오디오 카드들, 추가적인 네트워크 인터페이스들, 주변 디바이스들 등)을 포함할 수 있다. 프로세서 유닛(502), 메모리 유닛(506) 및 네트워크 인터페이스들(508)은 버스(510)에 커플링된다. 버스(510)에 커플링되는 것으로 도시되지만, 메모리 유닛(506)은 프로세서 유닛(502)에 커플링될 수 있다.

[0080] 실시예들은 다양한 구현들 및 이용들을 참조하여 설명되지만, 이 실시예들은 예시적이고, 본 발명의 요지의 범위는 이들에 제한되지 않음을 이해할 것이다. 일반적으로, 여기에서 설명되는 바와 같이 통신 네트워크들에 대한 클라우드 컴퓨팅 강화 라우터들을 구현하기 위한 기술들은 임의의 하드웨어 시스템 또는 하드웨어 시스템들과 일치하는 펌웨어들로 구현될 수 있다. 많은 변화들, 변형들, 추가들 및 개선들이 가능하다.

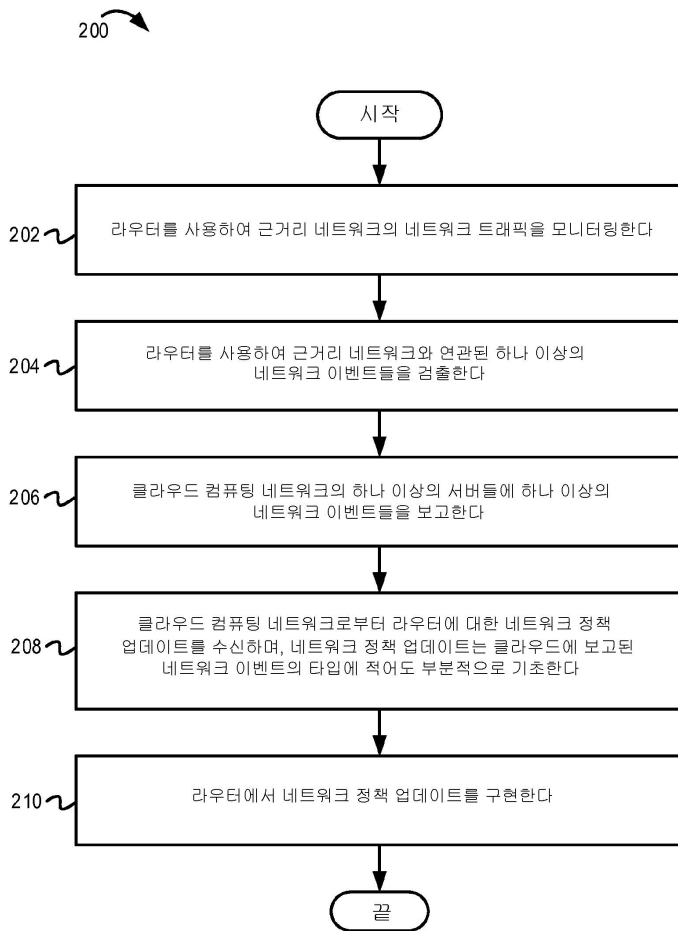
[0081] 여기에서 단일의 예로 설명되는 컴포넌트들, 동작들 또는 구조들에 대해 복수의 예들이 제공될 수 있다. 마지막으로, 다양한 컴포넌트들, 동작들 및 데이터 스토어들 사이의 경계들은 다소 임의적이고, 특정한 동작들은 특정한 예시적인 구성들의 상황에서 예시된다. 기능의 다른 할당들이 고려되고, 이는 본 발명의 요지의 범위 내에 속할 수 있다. 일반적으로, 예시적인 구성들에서 별개의 컴포넌트들로서 제시된 구조들 및 기능은 결합된 구조 또는 컴포넌트로서 구현될 수 있다. 유사하게, 단일 컴포넌트로서 제시된 구조들 및 기능은 별개의 컴포넌트들로서 구현될 수 있다. 이러한 변화들, 변형들, 추가들 및 개선들 및 다른 변화들, 변형들, 추가들 및 개선들은 본 발명의 요지의 범위 내에 속할 수 있다.

도면

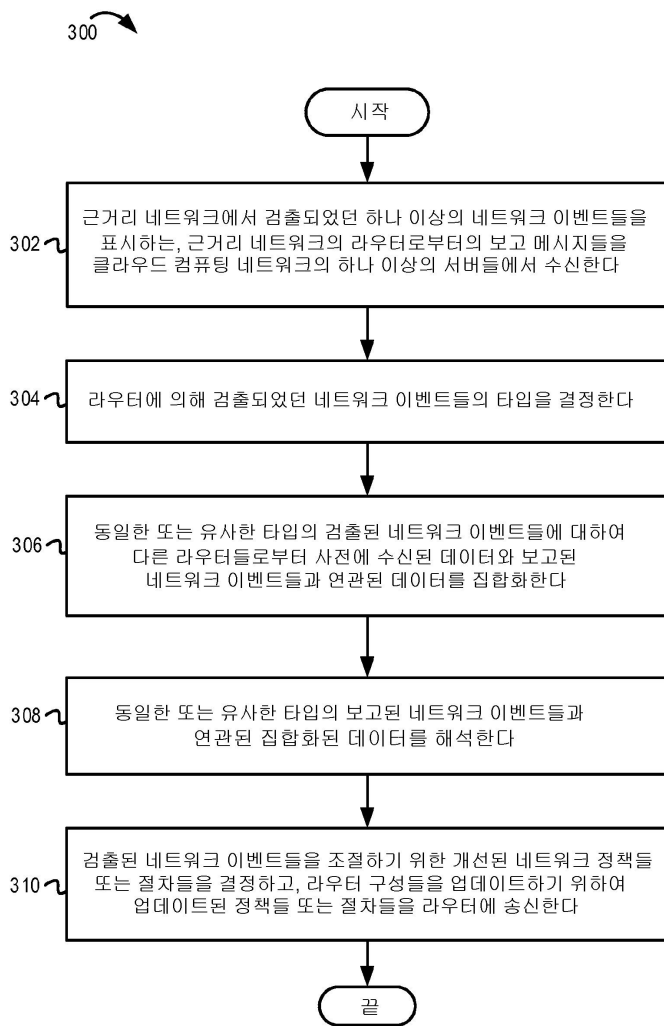
도면1



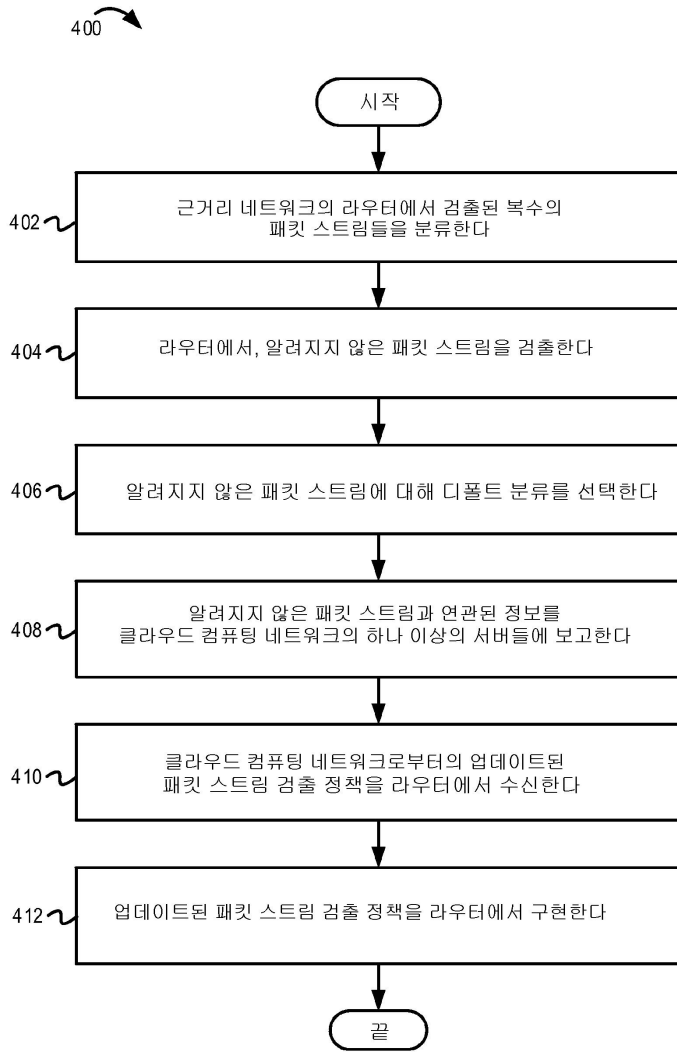
도면2



도면3



도면4



도면5

