(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년08월06일
(11) 등록번호 10-1885657
(24) 등록일자 2018년07월31일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 63/1425 (2013.01)
H04L 63/1466 (2013.01)
(21) 출원번호 10-2016-0120187
(22) 출원일자 2016년09월20일
심사청구일자 2016년09월20일
(65) 공개번호 10-2018-0031479
(43) 공개일자 2018년03월28일
(56) 선행기술조사문헌
KR1020160036201 A*
KR100973076 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
(72) 발명자
안명길
서울특별시 노원구 공릉로59길 28
김용현
서울특별시 송파구 양산로8길 4
(뒷면에 계속)
(74) 대리인
박장원

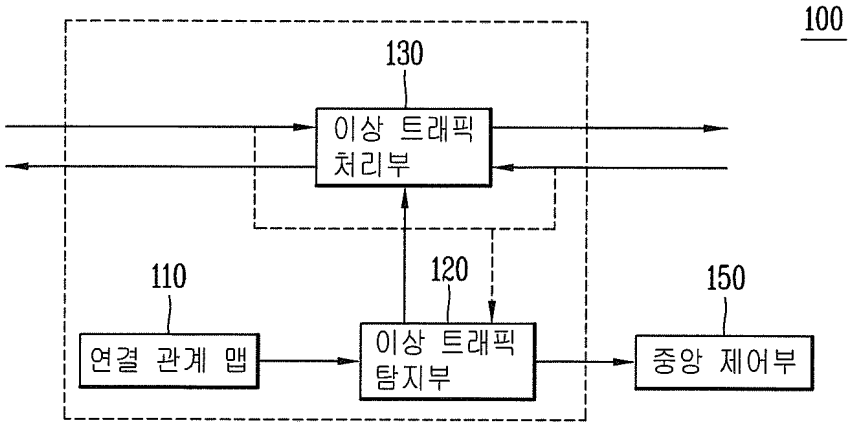
전체 청구항 수 : 총 4 항 심사관 : 문형섭

(54) 발명의 명칭 **계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치 및 그것의 탐지 방법**

(57) 요 약

계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치 및 그것의 탐지 방법이 개시된다. 본 발명에서는, 계층 구조를 갖는 정보전달망에서, 정보전달망에 포함된 노드들에 대한 기 정의된 연결 관계 정보를 포함하는 연결 관계 맵과, 정보전달망에서 발생한 트래픽의 연결 관계 여부를 연결 관계 맵으로부터 확인하여 이상 트래픽을 탐지하는 이상 트래픽 탐지부와, 이상 트래픽 탐지부의 탐지 결과에 근거하여, 정보전달망에서 발생한 트래픽의 처리를 수행하는 이상 트래픽 처리부와, 이상 트래픽의 발생을 알려주고 이상 트래픽에 대한 추가적인 처리를 수행하는 중앙 제어부를 포함하여 이루어진다.

대 표 도 - 도1



(72) 발명자
노병희
경기도 수원시 영통구 월드컵로 206
이승운
경기도 수원시 영통구 월드컵로 206

명 세 서

청구범위

청구항 1

계층 구조를 갖는 정보전달망에 있어서,

상기 정보전달망에 포함된 노드들에 대한 기 정의된 연결 관계 정보를 포함하는 연결 관계 맵;

상기 정보전달망에서 발생한 트래픽의 연결 관계 여부를 상기 연결 관계 맵으로부터 확인하여 이상 트래픽을 탐지하는 이상 트래픽 탐지부;

상기 이상 트래픽 탐지부의 탐지 결과에 근거하여, 상기 정보전달망에서 발생한 트래픽의 처리를 수행하는 이상 트래픽 처리부; 및

이상 트래픽의 발생을 알려주고 이상 트래픽에 대한 추가적인 처리를 수행하는 중앙 제어부;를 포함하며,

상기 중앙 제어부는 중앙 제어 노드와 통신가능하도록 연결되고,

상기 중앙 제어부는,

상기 중앙 제어 노드로부터 수신된 이상 트래픽에 관한 정보에 기초하여, 이상 노드에 대한 정보를 수집 및 저장하는 이상 노드 저장부, 및

상기 이상 노드 저장부로부터 수신된 이상 노드에 대한 정보를 기초로, 치료 노드에 대한 정보를 수집 및 저장하는 치료 노드 저장부를 더 포함하며,

상기 중앙 제어 노드는,

상기 치료 노드 저장부로부터 치료될 노드의 정보를 수신하여, 해당 노드로 치료 메시지를 전송하는 것을 특징으로 하는 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 정보전달망에서 발생한 트래픽에는 송신자 노드 및 수신자 노드의 식별자 정보가 포함되고,

상기 이상 트래픽 탐지부는,

상기 송신자 노드 및 수신자 노드의 식별자 정보를 이용하여 상기 연결 관계 맵에 대응되는 연결 관계 정보를 검출하고, 검출된 연결 관계 정보를 기초로 이상 트래픽을 탐지하는 것을 특징으로 하는 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치.

청구항 5

제1항에 있어서,

상기 이상 트래픽 처리부는,

상기 이상 트래픽 탐지부로부터 수신된 트래픽이 이상 트래픽으로 탐지된 경우이면 해당 트래픽 전송을 차단하고, 상기 이상 트래픽 탐지부로부터 수신된 트래픽이 이상 트래픽으로 탐지되지 않은 경우이면 해당 트래픽을 통과시키는 것을 특징으로 하는 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치.

청구항 6

계층 구조를 갖는 정보전달망에서의 이상 트래픽 탐지 방법으로서,

상기 정보전달망으로부터 트래픽을 수신하는 단계;

기정의된 연결 관계 정보를 포함하는 연결 관계 맵을 이용하여, 상기 수신된 트래픽의 연결 관계를 검색하는 단계;

검색 결과, 상기 수신된 트래픽의 연결 관계가 존재하는지를 판단하는 단계;

상기 판단에 기초하여, 해당 트래픽의 전송 여부를 결정하는 단계;를 포함하며,

상기 해당 트래픽의 전송 여부를 결정하는 단계는,

상기 수신된 트래픽의 연결 관계가 존재하면 해당 트래픽을 통과시키고, 상기 수신된 트래픽의 연결 관계가 존재하지 않으면 해당 트래픽을 차단하는 단계를 포함하며,

상기 수신된 트래픽의 연결 관계가 존재하지 않으면, 이상 트래픽으로 판단하고, 이상 트래픽을 발생하는 이상 노드를 수집하여 해당 노드로 치료 메시지를 전송하는 단계를 더 포함하는 것을 특징으로 하는 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 방법.

청구항 7

삭제

청구항 8

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 전장 모의 실험에서, 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치 및 그것의 탐지 방법에 관한 것이다.

배 경 기 술

[0002] 정보전달망(data transport network)은 양 지점 간의 정보를 전달하는 기능적인 측면의 네트워크 자원을 의미한다. 계층적이고 정형화된 정보전달망은, 군 전술 통신망, SCADA와 같이 감시 제어 및 데이터 취득을 목적으로 하는 네트워크(예를 들어, 산업 제어 시스템 네트워크)에서 사용되는 통신망을 의미한다.

[0003] 일반적인 통신망 환경에서는, 통신망에 연결되어 있는 모든 노드들 간의 제약이 없는 풀 메쉬 형태를 형성한다. 반면, 계층적이고 정형화된 정보통신망은 노드들이 그룹을 이루어 계층을 이루고, 각 계층에는 분리된 그룹이 존재할 수 있다. 이러한 경우, 동일 계층에 속하더라도 다른 그룹에 속한 노드들 간에는 직접적인 통신이 제한되며, 대신 이들의 상위 계층에 속한 그룹(들)을 경유해야만 통신이 가능하다.

[0004] 또한, 계층적이고 정형화된 정보전달망에서의 정보 전달은 모든 노드들 간에서 수행되지 않고, 그룹 내의 특정 노드 간, 특정 그룹 간, 또는 특정 계층 간에서와 같이 노드들 간에 논리적 관계가 미리 정의되어 있고, 이와 같이 정의된 관계의 노드들 간에만 정보 교환이 허용된다. 즉, 네트워크 노드가 단대단(end-to-end)으로 연결되어 있더라도, 구조적 또는 정책적인 특징에 따라 모든 노드들 간의 통신이 제한될 수 있다.

[0005] 한편, 최근 인터넷환경에는 이상 트래픽을 유발하여 네트워크에 피해를 주는 서비스 거부, 웜(computer worm) 등의 공격 등이 존재한다. 이러한 공격들로 인한 피해가 증가하고 있으며, 이에 대한 탐지 및 방지 기술들이 도입되고 있다. 예를 들어, 패턴 매칭, 프로토콜 스펙 위반 등과 같은 패킷 검사 등의 기존 기술들은 일반 인터넷망의 환경을 고려한 것으로서 계층적인 정보전달망이 갖는 특성을 반영하지 않는다.

[0006] 구체적으로, 계층 구조를 갖는 정보전달망의 경우, 기존 기술을 이용한 이상 트래픽 탐지 및 방지 기술을 사용할 경우, 이상 트래픽 탐지 및 방어 시 불필요한 패킷 검사를 수행해야 하기 때문에 비효율적인 탐지가 이루어진다. 이에, 계층 구조를 갖는 정보전달망의 특성을 반영한 효율적인 이상 트래픽 탐지 기술이 필요하다.

발명의 내용

해결하려는 과제

[0007] 따라서, 본 발명의 일 목적은, 노드들이 단대단으로 연결된 계층적이고 정형화된 정보전달망의 특성을 반영하여 이상 트래픽을 탐지할 수 있는, 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치 및 그것의 탐지 방법을 제공하는 데 있다.

[0008] 또한, 본 발명의 또 다른 목적은, 계층구조를 갖는 정보전달망에서, 이상 트래픽이 발생한 노드를 회복할 수 있는, 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치 및 그것의 탐지 방법을 제공하는 데 있다.

과제의 해결 수단

[0009] 이를 위해, 본 발명에 따른 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치는, 상기 정보전달망에 포함된 노드들에 대한 기 정의된 연결 관계 정보를 포함하는 연결 관계 맵; 상기 정보전달망에서 발생한 트래픽의 연결 관계 여부를 상기 연결 관계 맵으로부터 확인하여 이상 트래픽을 탐지하는 이상 트래픽 탐지부; 상기 이상 트래픽 탐지부의 탐지 결과에 근거하여, 상기 정보전달망에서 발생한 트래픽의 처리를 수행하는 이상 트래픽 처리부; 및 이상 트래픽의 발생을 알려주고 이상 트래픽에 대한 추가적인 처리를 수행하는 중앙 제어부를 포함하여 이루어진다.

[0010] 일 실시 예에서, 상기 중앙 제어부는 중앙 제어 노드와 통신가능하도록 연결되고, 상기 중앙 제어부는, 상기 중앙 제어 노드로부터 수신된 이상 트래픽에 관한 정보에 기초하여, 이상 노드에 대한 정보를 수집 및 저장하는 이상 노드 저장부, 및 상기 이상 노드 저장부로부터 수신된 이상 노드에 대한 정보를 기초로, 치료 노드에 대한 정보를 수집 및 저장하는 치료 노드 저장부를 더 포함할 수 있다.

[0011] 일 실시 예에서, 상기 중앙 제어 노드는, 상기 치료 노드 저장부로부터 치료될 노드의 정보를 수신하여, 해당 노드로 치료 메시지를 전송할 수 있다.

[0012] 일 실시 예에서, 상기 정보전달망에서 발생한 트래픽에는 송신자 노드 및 수신자 노드의 식별자 정보가 포함되고, 상기 이상 트래픽 탐지부는, 상기 송신자 노드 및 수신자 노드의 식별자 정보를 이용하여 상기 연결 관계 맵에 대응되는 연결 관계 정보를 검출하고, 검출된 연결 관계 정보를 기초로 이상 트래픽을 탐지할 수 있다.

[0013] 일 실시 예에서, 상기 이상 트래픽 탐지부로부터 수신된 트래픽이 이상 트래픽으로 탐지된 경우이면 해당 트래픽 전송을 차단하고, 상기 이상 트래픽 탐지부로부터 수신된 트래픽이 이상 트래픽으로 탐지되지 않은 경우이면 해당 트래픽을 통과시킬 수 있다.

[0014] 또한, 본 발명의 일 실시 예에 따른 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 방법은, 정보전달망으로부터 트래픽을 수신하는 단계; 기정의된 연결 관계 정보를 포함하는 연결 관계 맵을 이용하여, 상기 수신된 트래픽의 연결 관계를 검색하는 단계; 검색 결과, 상기 수신된 트래픽의 연결 관계가 존재하는지를 판단하는 단계; 및 상기 판단에 기초하여, 해당 트래픽의 전송 여부를 결정하는 단계를 포함하여 이루어진다.

[0015] 일 실시 예에서, 상기 해당 트래픽의 전송 여부를 결정하는 단계는, 상기 수신된 트래픽의 연결 관계가 존재하면 해당 트래픽을 통과시키고, 상기 수신된 트래픽의 연결 관계가 존재하지 않으면 해당 트래픽을 차단하는 단계를 포함할 수 있다.

[0016] 일 실시 예에서, 상기 탐지 방법은, 상기 수신된 트래픽의 연결 관계가 존재하지 않으면, 이상 트래픽으로 판단하고, 이상 트래픽을 발생하는 이상 노드를 수집하여 해당 노드로 치료 메시지를 전송하는 단계를 더 포함할 수 있다.

발명의 효과

[0017] 이와 같은, 본 발명의 실시 예에 따른 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치 및 그것의 탐지 방법에 의하면, 특수한 계층적 정보전달망의 상황에서도 추가적인 탐지 방법 없이 효율적인 이상 트래픽 탐지 및 방어가 이루어질 수 있다. 그에 따라, 정보전달의 연결 관계를 확인할 수 있는 연결 관계 맵을 이용하여 이상 트래픽 탐지를 용이하게 확인할 수 있다.

[0018] 또한, 본 발명의 실시 예에 따른 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치 및 그것의 탐지 방법에 의하면, 이상 트래픽의 탐지 이후에 회복 장치를 추가적으로 구성할 수 있으므로, 이상 트래픽의 발견시 신속한 대응을 제공할 수 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 일 실시예에 따른 계층구조를 갖는 정보전달망에서, 연결 관계 맵을 이용한 이상 트래픽 탐지 장치에 대한 예시 블록도이다.

도 2는 본 발명의 일 실시예에 따른 계층 구조를 갖는 정보 전달망에서, 이상 트래픽이 발생한 노드의 회복하는 방법과 연관된 예시 블록도이다.

도 3은 본 발명의 일 실시예에 따른 계층 구조를 갖는 정보 전달망에서, 연결 관계를 이용한 이상 트래픽 탐지 방법을 보여주는 대표 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 먼저, 본 발명의 실시예는 노드들이 연결된 통신망에서 이상 트래픽의 탐지가 가능한 모든 환경에 적용될 수 있음을 미리 밝혀둔다

[0021] 또한, 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시 예를 가질 수 있는 바, 특정 실시 예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0022] 여기서 설명되는 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 즉, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항복들 중의 어느 항목을 포함한다.

[0023] 또한, 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0024] 또한, 본 출원에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0025] 또한, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 갖는다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0026] 이하, 첨부한 도면들을 참조하여 본 발명에 바람직한 실시 예들을 상세히 설명하기로 하며, 첨부 도면을 참조하여 설명함에 있어 도면 부호에 상관없이 동일하거나 대응하는 구성요소는 동일한 참조번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0027] 이하, 본 발명의 실시예에 따른 계층 구조를 갖는 정보전달망에서, 노드들의 연결 관계 맵을 이용한 이상 트래픽 탐지 방법 및 장치(이하, 이상 트래픽 탐지 방법 및 장치)에 대하여 구체적으로 설명하겠다. 군 전술 통신망 및 SCADA와 같은 정보전달망의 경우, 노드들 간의 논리적 관계가 미리 정의되고, 정의된 관계의 노드들 간에만 정보 공유가 이루어지는 특수한 구조를 갖는다. 따라서, 정의된 관계 이외의 이상 트래픽이 특정량 이상으로 발생할 경우에, 이상 트래픽으로 감지할 수 있다. 이에 따라, 본 발명의 일 실시예에 따른 이상 트래픽 탐지 방법

및 장치는 정의된 관계의 노드들에 대한 트래픽 정보를 고려하여 이상 트래픽 탐지를 수행하는 것을 특징으로 한다.

[0028] 먼저, 도 1은 본 발명의 일 실시예에 따른 계층구조를 갖는 정보전달망에서, 연결 관계 맵을 이용한 이상 트래픽 탐지 장치(100)에 대한 예시 블록도이다.

[0029] 이상 트래픽 탐지 장치(100)는 연결 관계 맵(110), 이상 트래픽 탐지부(120), 이상 트래픽 처리부(130), 및 중앙 제어부(150)를 포함하여 이루어질 수 있다. 여기서, 상기 연결 관계 맵(110), 이상 트래픽 탐지부(120), 이상 트래픽 처리부(130), 및 중앙 제어부(150)의 각 구성들은 본 발명의 이해를 돕기 위해 기능별로 구분된 것이라는 점이 이해되어야 한다. 즉, 본 발명의 일 실시 예에 따른 이상 트래픽 탐지 장치(100)는 하나의 노드에 포함된 구성이거나 또는 CPU, MPU 및 GPU와 같은 하나의 처리부로 구성될 수 있다. 이하, 도 1을 참조하여, 본 발명의 일 실시예에 따른 이상 트래픽 탐지 장치(100)의 각 구성에 대하여 보다 구체적으로 설명하겠다.

[0030] 연결 관계 맵(110)은 정보전달망에 포함된 노드들 간의 트래픽 정보를 담고 있는 기능을 수행한다. 연결 관계 맵(110)에 저장된 트래픽 정보는 이후 이상 트래픽 탐지부에 전달되어 정의되지 않은 이상, 트래픽이 존재하는지 여부를 판단하는데 사용될 수 있다. 트래픽 정보는 노드들 간의 현재 네트워크의 상태에 관한 정보를 포함한다.

[0031] 또, 연결 관계 맵(110)은 정형화된 정보전달의 송수신 관계를 근거로 연결 관계 정보를 포함한다. 여기서, 연결 관계 정보는 다음의 수학식 1과 같이 표현될 수 있다.

수학식 1

$$i \xrightarrow{p_{ij}} j, \quad 0 \le p_{ij} \le 1$$

[0032]

[0033] 수학식 1에서 p_{ij}는 이하에 기술된 연결 관계 맵에 포함된 연결 관계 맵 원소 즉, 연결 관계 정보를 나타낸다. 그리고, i 및 j는 정보전달망에 포함된 노드의 식별자 정보로, i는 송신자 노드의 식별자 정보를 나타내고, j는 수신자 노드의 식별자 정보를 나타낸다.

[0034] 또, p_{ij}는 0과 1사이의 값으로 표현될 수 있는데, 0일 경우 연결 관계가 없음을 나타내고, 1일 경우 연결 관계가 있음을 나타낸다. 따라서, 0과 1 사이의 값일 경우 p_{ij}의 확률만큼의 연결성을 가질 수 있다.

[0035] 이와 같이 수학식 1을 이용하여 산출된 연결 관계 정보(pij)에 기초하여 송신자 노드와 수신자 노드 간의 인접 행렬을 생성할 수 있다. 이와 같이 생성된 인접 행렬은 아래의 수학식 2와 같이 표현될 수 있다.

수학식 2

$$C_G = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix}_{N \times N}$$

[0036]

[0037] 여기서, n은 정보전달망에 포함된 노드들의 개수를 나타낸다.

[0038] 이와 같이 수학식 2로 표현된 인접 행렬은 전술한 연결 관계 맵(110)으로 정의될 수 있다. 즉, 연결 관계 맵(110)은 수학식 1 및 수학식 2를 참조하여 설명한 바와 같이, 송신자 노드와 수신자 노드 간의 인접 행렬 즉, 2차원 배열 형태를 가질 수 있다. 이때, 2차원 배열에서 행과 열의 개수는 노드의 개수로 정의될 수 있다.

[0039] 계속해서 도 1에서 이상 트래픽 탐지부(120)는 정보전달망에서 발생하는 트래픽 정보를 통해 이상 트래픽을 탐지한다. 여기서, 트래픽 정보는 정보전달망 내에서의 송신자 노드 및 수신자 노드에 관한 정보를 포함할 수 있

다. 또한, 이상 트래픽 탐지부(120)는 트래픽 정보에 연결 관계가 정의되었는지를 확인하는 작업을 수행한다. 구체적으로, 이상 트래픽 탐지부(120)는 트래픽 정보에 포함된 송신자 노드 및 수신자 노드의 식별자 정보를 이용하여, 연결 관계 맵에 해당하는 연결 관계 정보를 검출할 수 있다. 연결 관계 맵에 트래픽 정보와 동일한 정보가 존재하지 않을 경우, 이상 트래픽 탐지부(120)는 이를 이상 트래픽으로 인식한 다음, 이후 기술할 이상 트래픽 처리부(130)와 중앙 제어부(150)에 이상 트래픽이 발견되었음을 알려주는 정보를 전달한다.

[0040] 다음, 이상 트래픽 처리부(130)는 이상 트래픽 탐지부(120)의 결과를 수집하여 트래픽에 대한 처리를 수행한다. 여기서, 이상 트래픽 탐지부(120)의 결과는 이상 트래픽 탐지의 결과를 불리언 값(boolean value), 즉 0 또는 1로 표현할 수 있다. 이에 따라, 이상 트래픽 처리부(130)는 수신된 트래픽이 이상 트래픽으로 탐지되지 않았을 경우, 트래픽을 통과시킨다. 또한, 이상 트래픽 처리부(130)는 수신된 트래픽이 이상트래픽으로 탐지되었을 경우, 트래픽 전송을 차단한다.

[0041] 중앙 제어부(150)는 탐지된 이상 트래픽 정보를 통해 정보전달망의 중앙 제어 노드가 특정 작업을 수행하게끔 한다. 여기서, 중앙 제어부(150)는 정보전달망의 중앙 제어 노드에 포함된 기능 또는 이러한 기능을 실행하는 장치일 수 있다. 또한, 상기 중앙 제어부(150)는 정보전달망 전체 또는 정보전달망에 포함된 적어도 일부의 노드들에게 이상 트래픽의 발생을 알려준다.

[0042] 또한, 중앙 제어부(150)는 중앙 처리를 통해 이상 트래픽을 발생하는 노드에 대한 치료나 차단 등의 기능을 수행하는 어떠한 모듈, 장치, 알고리즘이라도 될 수 있다. 따라서, 이에 대한 사항은 특정한 방식의 제한 없이, 사용자 설정에 의해 가변될 수 있음을 밝혀둔다.

[0043] 이상에서 살펴본 바와 같이, 본 발명의 일 실시예에 따른 이상 트래픽 탐지 장치에 따르면, 계층적이고 정형화된 정보 전달망의 특성을 고려하여서, 연결 관계 맵을 통해 사전에 정의된 연결 관계를 갖는 노드들을 확인할 수 있다. 또한, 이를 기초로 하여 관계가 정의되지 않은 노드간에 발생하는 트래픽을 이상 트래픽이라고 판단하여서 사전에 차단할 수 있다. 이에 따르면, 특수한 계층적 정보 전달망에서도 효율적인 이상 트래픽 탐지 및 방어가 이루어질 수 있다.

[0044] 한편, 이와 같이 정보전달망에서 이상 트래픽이 탐지되었을 경우, 이상 트래픽을 발생하는 이상 노드가 존재할 수 있다. 본 발명에서는 이러한 노드를 대상으로 중앙 제어부를 이용하여 회복/치료 기능을 수행하는 것이 가능하다.

[0045] 이에, 이하에서는 도 2를 참조하여 본 발명에 실시 예에 따른 계층구조를 갖는 정보전달망에서 이상 트래픽을 발생하는 노드를 회복하는 방법에 대하여 구체적으로 설명하겠다.

[0046] 도 2에서, 이상 트래픽을 발생하는 노드를 회복하는 기능을 수행하기 위해, 중앙제어 노드(260)와 중앙 제어부(250)가 서로 통신가능하게 연결된다. 또한, 중앙 제어부(250)는 이상 노드 저장부(251) 및 치료 노드 저장부(252)를 더 포함할 수 있다.

[0047] 중앙 제어 노드(260)는 도 1의 이상 트래픽 탐지부(120)로부터 수집한 이상 노드에 관한 정보에 기초하여, 중앙 제어부(250)에 이상 트래픽에 관한 정보를 전달한다. 또한, 중앙 제어 노드(260) 치료될 노드의 정보를 중앙 제어부(250)로부터 수신하여 해당 노드로 치료 메시지를 보내는 기능을 수행한다.

[0048] 중앙 제어부(250)는 이상 노드의 정보를 저장하기 위해 이상 노드 저장부(251)를 포함한다. 또, 중앙 제어부(250)는 이상 노드의 치료를 위해, 치료 노드 저장부(252)를 포함한다.

[0049] 이상 노드 저장부(251)는 이상 트래픽 탐지부(120)로부터 수신된 이상 트래픽의 정보, 예를 들어 이상 노드에 대한 정보를 수집하여 저장하는 기능을 수행한다. 이때, 이상 노드 저장부(251)는 중앙 제어부(250) 내에 별도의 장치로 구현되거나 중앙 제어부(250)의 하나의 기능이거나, 또는 중앙 제어부(250)와 독립된 별도의 장치로 구현될 수 있다. 또한, 이상 노드에 대한 정보는 이상 노드의 식별자 정보이거나 또는 이상 노드의 IP 주소일 수 있다.

[0050] 치료 노드 저장부(252)는 이상 노드 저장부(251)로부터 전달된 이상 노드에 대한 정보를 수집하고 저장하는 기능을 수행한다. 또한, 치료 노드 저장부(252)도 중앙 제어부(250) 내에 별도의 장치로 구현되거나 중앙 제어부(250)의 하나의 기능이거나, 또는 중앙 제어부(250)와 독립된 별도의 장치로 구현될 수 있다. 또한, 여기서 치료 노드에 대한 정보는 이상 노드의 식별자 정보이거나 또는 이상 노드의 IP 주소일 수 있다.

[0051] 다음, 도 3은 본 발명의 일 실시예에 따른 계층 구조를 갖는 정보 전달망에서, 연결 관계를 이용한 이상 트래픽

탐지 방법을 보여주는 대표 흐름도이다.

[0052] 이하, 도 3을 참조로 본 발명의 일 실시예에 따른 계층 구조를 갖는 정보 전달망에서 연결 관계를 이용한 이상 트래픽 탐지 방법에 대한 설명이 이루어진다. 아래의 설명에서는 위에서 설명한 부분과 중복되는 사항은 생략하여 설명이 이루어진다.

[0053] 먼저 이상 트래픽을 판단하기 위한 초기 단계로, 트래픽 정보를 수신하여 이상 트래픽 탐지부(120, 도 1)로 전달하는 단계(S310)가 수행된다. 위에서 설명한 것처럼, 트래픽 정보는 트래픽의 송신자 노드 및 수신자 노드를 포함할 수 있다.

[0054] 다음, 트래픽 탐지부(120)에 수신된 트래픽의 연결 관계 정보를 연결 관계 맵으로부터 검색하는 단계(S320)가 수행된다.

[0055] 이때, 계층 구조를 갖는 정보전달망은 기 정의된 관계 노드간에서만 데이터 전달이 이루어진다. 따라서 연결 관계 맵을 검색하는 S320 단계는 이러한 정보 전달의 특성을 고려하여, 데이터 연결 정보를 갖는 연결 관계 맵을 호출하여 연결 관계의 여부를 판단하는 과정을 포함한다.

[0056] 다음, S320의 검색 결과, 수신된 트래픽 정보의 연결 관계가 존재하는지 여부를 판단하는 단계(S330)를 수행한다. 단계 S330의 판단 결과, 연결관계가 있을 경우, 이상 트래픽이 아닌 것으로 판단하여 S340의 단계로 넘어가서 트래픽을 전송한다. 그렇지 않은 경우, 즉 연결 관계가 없을 경우, 이상 트래픽으로 판단하여 S350의 단계로 넘어가서 트래픽을 무시하고(S350), 전송을 차단한다. 이때, 차단된 트래픽에 대한 보고가 수행될 수 있다.

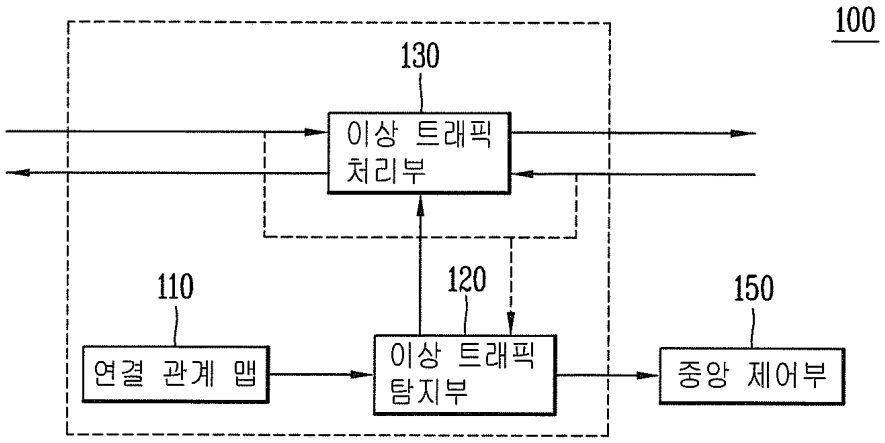
[0057] 한편, S330의 판단 결과 이상 트래픽으로 판단된 경우, 이상 트래픽을 발생하는 이상 노드를 수집하여 해당 노드로 치료 메시지를 전송할 수 있다.

[0058] 이상에서 설명한 바와 같이, 이와 같은, 본 발명의 실시 예에 따른 계층 구조를 갖는 정보전달망에서 연결 관계를 이용한 이상 트래픽 탐지 장치 및 그것의 탐지 방법에 의하면, 특수한 계층적 정보전달망의 상황에서도 추가적인 탐지 방법 없이 효율적인 이상 트래픽 탐지 및 방어가 이루어질 수 있다. 그에 따라, 정보전달의 연결 관계를 확인할 수 있는 연결 관계 맵을 이용하여 이상 트래픽 탐지를 용이하게 확인할 수 있다. 또한, 이상 트래픽의 탐지 이후에 회복 장치를 추가적으로 구성할 수 있으므로, 이상 트래픽의 발견시 신속한 대응을 제공할 수 있다.

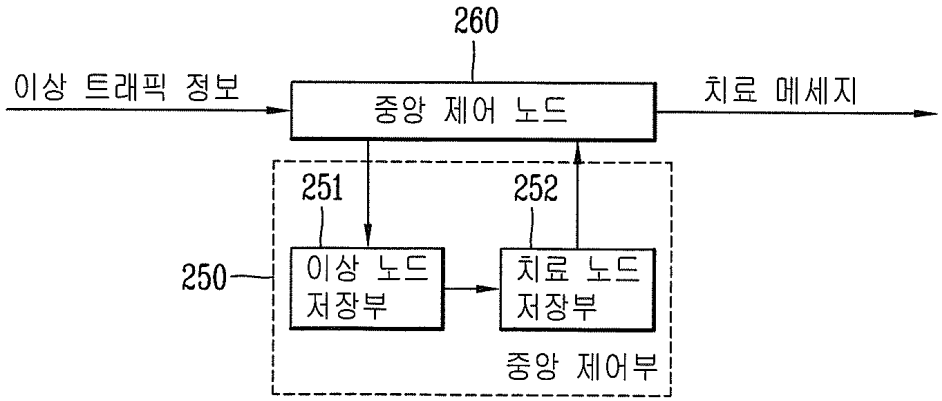
[0059] 이상에서는 본 발명의 바람직한 실시 예를 예시적으로 설명하였으나, 본 발명의 범위는 이와 같은 특정 실시 예에만 한정되는 것은 아니므로, 본 발명은 본 발명의 사상 및 특허청구범위에 기재된 범주 내에서 다양한 형태로 수정, 변경, 또는 개선될 수 있다. 또한, 여기에서 기술된 본 발명에 따른 방법은 소프트웨어, 하드웨어, 또는 이들의 조합으로 구현될 수 있다. 예를 들어, 본 발명에 따른 방법은 저장매체(예, 단말내부 메모리, 플래쉬 메모리, 하드디스크, 등)에 저장될 수 있고, 프로세서(예, 단말 내부 마이크로 프로세서)에 의해 실행될 수 있는 소프트웨어 프로그램 내에 포함되는 코드들 또는 명령어들로 구현될 수 있다.

도면

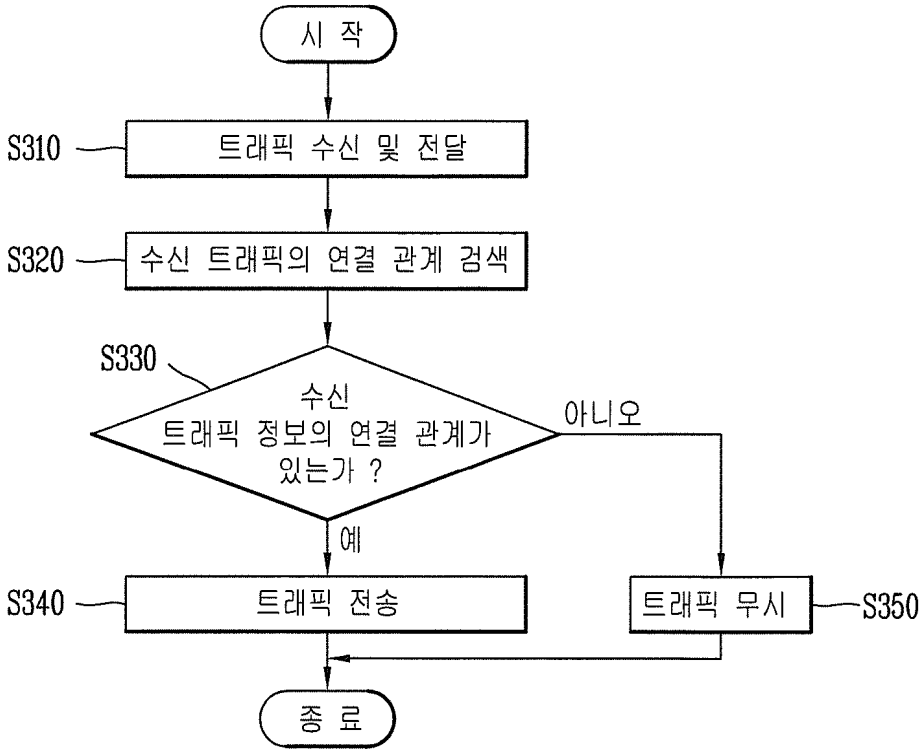
도면1


100
130
이상 트래픽
처리부
110
120
150
연결 관계 맵
이상 트래픽
탐지부
중앙 제어부

도면2


260
이상 트래픽 정보
중앙 제어 노드
치료 메세지
251
252
250
이상 노드
저장부
치료 노드
저장부
중앙 제어부

도면3


시 작
S310
트래픽 수신 및 전달
S320
수신 트래픽의 연결 관계 검색
S330
수신
트래픽 정보의 연결 관계가
있는가 ?
아니오
예
S340
트래픽 전송
트래픽 무시
S350
종 료