(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년02월14일
(11) 등록번호 10-1948214
(24) 등록일자 2019년02월08일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01)
(52) CPC특허분류
H04L 43/10 (2013.01)
H04L 43/16 (2013.01)
(21) 출원번호 10-2018-0016579
(22) 출원일자 2018년02월09일
심사청구일자 2018년02월09일
(56) 선행기술조사문헌
KR101081433 B1
(뒷면에 계속)

(73) 특허권자
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
홍충선
경기도 용인시 수지구 상현로 30-10, 233동 101호(상현동,상현마을성원상떼빌아파트)
사바 수하일
경기도 용인시 기흥구 덕영대로 1732 경희대학교 국제캠퍼스 전자정보대학 352호(서천동)
(뒷면에 계속)
(74) 대리인
서재승

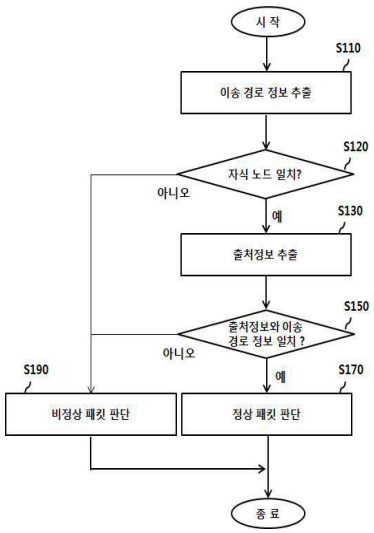
전체 청구항 수 : 총 16 항 심사관 : 전용해

(54) 발명의 명칭 **패킷의 무결성을 판단하는 방법**

(57) 요 약

본 발명은 센서 네트워크에서 패킷의 무결성을 판단하는 방법에 관한 것으로, 센서 네트워크에서 발신 노드로부터 루트 노드까지의 이송 경로에 존재하는 모든 하위 노드가 루트 노드의 자식 노드인지를 판단하거나 패킷에 구비된 이송 경로와 암호화된 출처 정보의 이송 경로를 비교하여 해당 패킷의 무결성을 판단함으로써 패킷의 무결성을 이중으로 판단할 수 있으며, 센서 네트워크에서 무결성이 인정되지 않는 비정상 패킷의 수를 카운트함으로써 카운트한 비정상 패킷의 수가 임계수를 초과하는지 여부에 따라 센서 네트워크에 허락받지 않은 제3자의 불법 노드를 용이하게 인식할 수 있는 패킷의 무결성 판단 방법에 관한 것이다.

대 표 도 - 도4



(72) 발명자

김영기

경기도 수원시 영통구 청명로59번길 45-14, 203호 (영통동)

샤시 라즈 판데이

경기도 용인시 기흥구 덕영대로 1732 경희대학교 국제캠퍼스 전자정보대학 352호(서천동)

(56) 선행기술조사문헌

KR1020090052638 A

KR1020090125754 A

US20140022997 A1

US20160080416 A1

이 발명을 지원한 국가연구개발사업

과제고유번호 2015-0-00557

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신·방송 연구개발 사업

연구과제명 IoT 기기의 물리적 속성, 관계, 역할 기반 Resilient/Fault-Tolerant 자율 네트워킹 기술 연구

기 여 율 1/1

주관기관 한국과학기술원

연구기간 2017.06.01 ~ 2018.03.31

명 세 서

청구범위

청구항 1

(a) 하위 노드로부터 수신한 패킷에서 상기 패킷의 발신 노드로부터 루트 노드까지의 이송 경로 정보를 추출하는 단계;

(b) 상기 이송 경로 정보에 기초하여 상기 이송 경로에 존재하는 하위 노드들이 상기 루트 노드의 자식 노드들인지 확인하는 단계;

(c) 상기 패킷으로부터 출처 정보를 추출하고, 상기 출처 정보에서 상기 패킷의 순차적인 이송 경로와 상기 이송 경로 정보에서 상기 패킷의 순차적인 이송 경로가 서로 일치하는지 판단하는 단계; 및

(d) 상기 출처 정보에서 상기 패킷의 순차적인 이송 경로와 상기 이송 경로 정보에서 상기 패킷의 순차적인 이송 경로가 서로 일치하는지 여부에 기초하여 상기 패킷의 무결성을 판단하는 단계를 포함하는 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 2

제 1 항에 있어서, 상기 패킷의 무결성 판단 방법의 (a) 단계 내지 (d) 단계는 상기 루트 노드에서 수행되는 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 3

제 1 항에 있어서, 상기 패킷의 무결성 판단 방법의 (a) 단계 내지 (d) 단계는 상기 루트 노드와 연결된 경계 라우터에서 수행되는 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 4

제 2 항 또는 제 3 항에 있어서, 상기 이송 경로 정보는

상기 패킷의 발신 노드부터 상기 루트 노드까지 상기 패킷의 순차적인 이송 경로에 존재하는 하위 노드의 식별자를 포함하는 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 5

제 4 항에 있어서, 상기 출처 정보는

상기 발신 노드로부터 상기 루트 노드까지의 이송 경로 중 이전 하위 노드로부터 수신한 해쉬값과 현재 하위 노드의 식별값에 기초하여 상기 현재 하위 노드의 해쉬값을 계산하는 단계; 및

상기 현재 하위 노드로부터 상기 루트 노드까지의 순차적 이송 경로에 위치하는 모든 하위 노드에서 각 하위 노드의 이전 하위 노드로부터 수신한 해쉬값과 각 하위 노드의 식별값에 기초하여 각 하위 노드의 해쉬값을 생성하여 상기 발신 노드로부터 상기 루트 노드까지의 출처 정보를 생성하는 단계를 통해 생성되는 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 6

제 5 항에 있어서, 상기 패킷의 발신 노드는

상기 발신 노드의 식별자와 랜덤하게 생성되는 초기화 값으로부터 상기 발신 노드의 해쉬값을 계산하는 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 7

제 5 항에 있어서, 상기 발신 노드로부터 상기 루트 노드까지 상기 패킷의 이송 경로에 위치하는 노드는 자신의 자식 노드 리스트를 구비하고 있는 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 8

제 5 항에 있어서, 상기 발신 노드에서 상기 루트 노드까지 상기 패킷의 이송 경로에 위치하는 각 노드(i)의 해쉬값(H(i))은 아래의 수학식 (1)에 의해 계산되는데,

[수학식 1]

$H(i)=H(H(i-1)+ID_i)$

여기서 H(i-1)는 이전 노드(i-1)의 해쉬값이며 ID_i는 노드(i)의 식별자인 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 9

제 5 항에 있어서, 상기 패킷의 무결성 판단 방법은

상기 출처 정보에서 상기 패킷의 순차적인 이송 경로와 상기 이송 경로 정보에서 상기 패킷의 순차적인 이송 경로가 서로 일치하지 않은 비정상 패킷을 식별하여 카운트하는 단계;

카운트한 상기 비정상 패킷의 수와 임계수를 비교하는 단계; 및

상기 비정상 패킷의 수가 상기 임계수를 초과하는 경우, 경고 메시지를 생성하여 센서 네트워크의 관리자 단말기로 송신하는 단계를 더 포함하는 것을 특징으로 하는 패킷의 무결성 판단 방법.

청구항 10

하위 노드로부터 수신한 패킷에서 상기 패킷의 발신 노드로부터 루트 노드까지의 이송 경로 정보를 추출하는 이송 경로 추출부;

상기 패킷에서 상기 패킷의 발신 노드로부터 상기 루트 노드까지의 출처 정보를 추출하는 출처 정보 추출부;

상기 이송 경로 정보에 기초하여 상기 이송 경로에 존재하는 하위 노드들이 상기 루트 노드의 자식 노드들인지 판단하는 하위 노드 판단부; 및

상기 출처 정보에서 상기 패킷의 순차적인 이송 경로와 상기 이송 경로 정보에서 상기 패킷의 순차적인 이송 경로가 서로 일치하는지 판단하여 상기 패킷의 무결성을 판단하는 무결성 판단부를 포함하는 것을 특징으로 하는 패킷의 무결성 판단 장치.

청구항 11

제 10 항에 있어서, 상기 이송 경로 정보는

상기 패킷의 발신 노드부터 상기 루트 노드까지 상기 패킷의 순차적인 이송 경로에 존재하는 하위 노드의 식별자가 포함되어 있는 것을 특징으로 하는 패킷의 무결성 판단 장치.

청구항 12

제 11 항에 있어서, 상기 패킷의 무결성 판단 장치는

상기 발신 노드로부터 상기 루트 노드까지 상기 패킷의 이송 경로에 위치하는 자신의 자식 노드 리스트를 저장하고 있는 노드 데이터베이스를 더 포함하고 있는 것을 특징으로 하는 패킷의 무결성 판단 장치.

청구항 13

제 12 항에 있어서, 상기 출처 정보는

상기 발신 노드로부터 상기 루트 노드까지의 이송 경로 중 상기 루트 노드까지의 순차적 이송 경로에 위치하는 모든 하위 노드에서 각 하위 노드의 이전 하위 노드로부터 수신한 해쉬값과 각 하위 노드의 식별값으로부터 각 하위 노드의 해쉬값을 계산하여 생성되는 것을 특징으로 하는 패킷의 무결성 판단 장치.

청구항 14

제 13 항에 있어서,

상기 발신 노드에서 상기 루트 노드까지 상기 패킷의 이송 경로에 위치하는 각 노드(i)의 해쉬값(H(i))은 아래의 수학식 (2)에 의해 계산되는데,

[수학식 2]

$H(i)=H(H(i-1)+ID_i)$

여기서 H(i-1)는 이전 노드(i-1)의 해쉬값이며 ID_i는 노드(i)의 식별자인 것을 특징으로 하는 패킷의 무결성 판단 장치.

청구항 15

제 13 항에 있어서, 상기 패킷의 무결성 판단 장치는

상기 출처 정보에서 상기 패킷의 순차적인 이송 경로와 상기 이송 경로 정보에서 상기 패킷의 순차적인 이송 경로가 서로 일치하는지 여부에 기초하여 상기 패킷의 이송 경로에 대한 정상 여부를 판단하는 정상 판단부를 더 포함하는 것을 특징으로 하는 패킷의 무결성 판단 장치.

청구항 16

제 15 항에 있어서, 상기 정상 판단부는

상기 출처 정보에서 상기 패킷의 순차적인 이송 경로와 상기 이송 경로 정보에서 상기 패킷의 순차적인 이송 경로가 서로 일치하지 않은 비정상 패킷을 식별하여 카운트하는 카운트부;

카운트한 상기 비정상 패킷의 수와 임계수를 비교하는 비교부; 및

상기 비정상 패킷의 수가 상기 임계수를 초과하는 경우, 경고 메시지를 생성하여 센서 네트워크의 관리자 단말기로 송신하는 경고 제어부를 더 포함하는 것을 특징으로 하는 패킷의 무결성 판단 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 센서 네트워크에서 패킷의 무결성을 판단하는 방법에 관한 것으로, 센서 네트워크에서 패킷의 발신 노드로부터 루트 노드까지의 이송 경로에 존재하는 모든 하위 노드가 루트 노드의 자식 노드인지를 판단하거나 패킷에 구비된 패킷의 순차적인 이송 경로와 암호화된 출처 정보의 순차적인 패킷의 이송 경로를 비교하여 해당 패킷의 무결성을 판단함으로써 패킷의 무결성을 이중으로 판단할 수 있으며, 센서 네트워크에서 무결성이 인정되지 않는 비정상 패킷의 수를 카운트함으로써 카운트한 비정상 패킷의 수가 임계수를 초과하는지 여부에 따라 센서 네트워크에 허락받지 않은 제3자의 불법 노드를 용이하게 인식할 수 있는 패킷의 무결성 판단 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷은 우리의 삶에서 매우 중요한 부분이 되었다. IP 계층을 사용하는 인터넷은 IP를 이용하여 서로 다른 링크인 무선과 유선이 서로 통신 할 수 있도록 한다. 개발자들은 매일 같이 새로운 인터넷 엑세스 기술을 개발하고 있기 때문에 인터넷을 기반으로 한 네트워크의 크기는 점차 증대되고 있다.

[0003] IP 기반 센서 네트워크는(IP-USN, IP-based Ubiquitous Sensor Network)은 센서 네트워크를 구성하는 센서 노드들에 IP를 할당하고, 센서 네트워크를 인터넷에 연결하여 외부 단말기와 통신할 수 있는 네트워크이다. IP 기반 센서 네트워크는 군사분야, 민간분야의 환경과 거주지 모니터링, 실시간 건강 관리, 지뢰 탐지, 지능적 운송 시스템 등 여러 곳에서 다양하게 사용되고 있으며, 센서 노드들에 IP를 할당하여 IP 네트워크 상에서 가능한 여러 기술들의 이점을 얻을 수 있다.

[0004] 그러나 IP 기반 센서 네트워크에서 장소와 시간에 구분없이 센서 네트워크를 통해 다양한 정보를 획득하는 등 IP 기반 센서 네트워크의 순기능과 함께 분산 시스템들의 증가와 인터넷의 확산으로 인해 IP 기반 센서 네트워크를 통한 시스템의 해킹, 정보 유출, 불법 침입, 악성 바이러스 유포 등 역기능도 점차 확대되고 있다.

[0005] 특히 신뢰할 수 없는 인터넷 영역과 6LoWPAN 기반의 센서 네트워크 사이의 상호 연결성은 센서 노드의 자원 제약 조건으로 인해 심각한 보안 문제를 야기한다. 센서 네트워크에서 공격자는 센서 네트워크에 악성 노드를 삽입하거나 일반 노드를 손상시킴으로써 노드가 생성한 데이터를 탈취하는 방식으로 공격을 수행한다. 데이터의 위조 또는 변조는 중요한 의사 결정 프로세스(decision-making process), 위험 평가(risk assessment) 및 성능 평가(performance evaluation)를 위해 사물 데이터에 의존하는 응용 프로그램에 특히 치명적인 결과를 초래한다.

[0006] 예를 들어, 이란 핵 발전소의 스턱스넷 웜(Stuxnet worm)에 의한 파괴, 메드트로닉(Medtronic)에 의한 당뇨병 환자에게 치명적인 인슐린 양을 투여하기 위한 인슐린 펌프 해킹 및 차량을 제어하는 공격 등이 있다. 따라서 데이터 디버깅, 조정, 복제, 의사 결정, 성능 조정, 감사, 포렌식 분석 등 센서 데이터의 무결성을 보장할 수 있는 무결성 판단 방법이 필요하다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 위에서 언급한 종래 센서 네트워크가 가지는 문제점을 해결하기 위한 것으로 본 발명이 이루고자 하는 목적은 센서 네트워크에서 송수신되는 패킷의 무결성을 판단하는 방법을 제공하는 것이다.

[0008] 본 발명이 이루고자 하는 다른 목적은 센서 네트워크에서 패킷의 발신 노드로부터 루트 노드까지의 이송 경로에 위치하는 모든 하위 노드가 루트 노드의 자식 노드인지를 판단하거나 패킷에 구비된 패킷의 순차적인 이송 경로와 암호화된 출처 정보의 패킷의 순차적인 이송 경로를 비교하여 해당 패킷의 무결성을 이중으로 판단할 수 있는 패킷의 무결성 판단 방법을 제공하는 것이다.

[0009] 본 발명이 이루고자 하는 또 다른 목적은 센서 네트워크에서 무결성이 인정되지 않는 비정상 패킷의 수를 카운트하여 센서 네트워크에 허락받지 않은 제3자의 불법 노드를 인식할 수 있는 패킷의 무결성 판단 방법을 제공하는 것이다.

과제의 해결 수단

[0010] 본 발명의 목적을 달성하기 위하여, 본 발명에 따른 패킷의 무결성 판단 방법은 하위 노드로부터 수신한 패킷에서 패킷의 발신 노드로부터 루트 노드까지의 이송 경로 정보를 추출하는 단계(a 단계)와, 이송 경로 정보에 기초하여 이송 경로에 존재하는 하위 노드들이 루트 노드의 자식 노드들인지 확인하는 단계(b 단계)와, 패킷으로부터 출처 정보를 추출하고 출처 정보에서 패킷의 순차적인 이송 경로와 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하는지 판단하는 단계(c 단계)와, 출처 정보에서 패킷의 순차적인 이송 경로와 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하는지 여부에 기초하여 패킷의 무결성을 판단하는 단계(d 단계)를 포함하는 것을 특징으로 한다.

[0011] 본 발명의 일 실시예에서 패킷의 무결성 판단 방법의 (a) 단계 내지 (d) 단계는 루트 노드에서 수행되는 것을 특징으로 한다.

[0012] 본 발명의 다른 실시예에서 패킷의 무결성 판단 방법의 (a) 단계 내지 (d) 단계는 루트 노드와 연결된 경계 라우터에서 수행되는 것을 특징으로 한다.

[0013] 바람직하게, 이송 경로 정보는 패킷의 발신 노드부터 루트 노드까지 패킷의 순차적인 이송 경로에 존재하는 하위 노드의 식별자를 포함하는 것을 특징으로 한다.

[0014] 바람직하게, 본 발명의 일 실시예에서 출처 정보는 발신 노드로부터 루트 노드까지의 이송 경로 중 이전 하위 노드로부터 수신한 해쉬값과 현재 하위 노드의 식별값에 기초하여 현재 하위 노드의 해쉬값을 계산하는 단계와, 현재 하위 노드로부터 루트 노드까지의 순차적 이송 경로에 위치하는 모든 하위 노드에서 각 하위 노드의 이전 하위 노드로부터 수신한 해쉬값과 각 하위 노드의 식별값에 기초하여 각 하위 노드의 해쉬값을 생성하여 발신 노드로부터 루트 노드까지의 출처 정보를 생성하는 단계를 통해 생성되는 것을 특징으로 한다.

[0015] 여기서 패킷의 발신 노드는 발신 노드의 식별자와 랜덤하게 생성되는 초기화 값으로부터 발신 노드의 해쉬값을 계산하는 것을 특징으로 한다.

[0016] 여기서 발신 노드로부터 루트 노드까지 패킷의 이송 경로에 위치하는 노드는 자신의 자식 노드 리스트를 구비하

고 있는 것을 특징으로 한다.

[0017] 바람직하게, 발신 노드에서 루트 노드까지 패킷의 이송 경로에 위치하는 각 노드(i)의 해쉬값(H(i))은 아래의 수학식 (1)에 의해 계산되는데,

[0018] [수학식 1]

[0019] $H(i)=H(H(i-1)+ID_i)$

[0020] 여기서 H(i-1)는 이전 노드(i-1)의 해쉬값이며 ID_i는 노드(i)의 식별자인 것을 특징으로 한다.

[0021] 바람직하게, 본 발명의 일 실시예에 따른 패킷의 무결성 판단 방법은 출처 정보에서 패킷의 순차적인 이송 경로와 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하지 않은 비정상 패킷을 식별하여 카운트하는 단계와, 카운트한 비정상 패킷의 수와 임계수를 비교하는 단계와, 비정상 패킷의 수가 임계수를 초과하는 경우 경고 메시지를 생성하여 센서 네트워크의 관리자 단말기로 송신하는 단계를 더 포함하는 것을 특징으로 한다.

[0022] 한편, 본 발명에 따른 패킷의 무결성 판단 장치는 하위 노드로부터 수신한 패킷에서 패킷의 발신 노드로부터 루트 노드까지의 이송 경로 정보를 추출하는 이송 경로 추출부와, 패킷에서 패킷의 발신 노드로부터 루트 노드까지의 출처 정보를 추출하는 출처 정보 추출부와, 이송 경로 정보에 기초하여 이송 경로에 존재하는 하위 노드들이 루트 노드의 자식 노드들인지 판단하는 하위 노드 판단부와, 출처 정보에서 패킷의 순차적인 이송 경로와 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하는지 판단하여 패킷의 무결성을 판단하는 무결성 판단부를 포함하는 것을 특징으로 한다.

[0023] 여기서 이송 경로 정보는 패킷의 발신 노드부터 루트 노드까지 패킷의 순차적인 이송 경로에 존재하는 하위 노드의 식별자가 포함되어 있는 것을 특징으로 한다.

[0024] 바람직하게, 본 발명의 일 실시예에 따른 패킷의 무결성 판단 장치는 발신 노드로부터 루트 노드까지 패킷의 이송 경로에 위치하는 자신의 하위 노드 리스트를 저장하고 있는 노드 데이터베이스를 더 포함하고 있는 것을 특징으로 한다.

[0025] 본 발명에 따른 패킷의 무결성 판단 장치에서 출처 정보는 발신 노드로부터 루트 노드까지의 이송 경로 중 루트 노드까지의 순차적 이송 경로에 위치하는 모든 하위 노드에서 각 하위 노드의 이전 하위 노드로부터 수신한 해쉬값과 각 하위 노드의 식별값으로부터 각 하위 노드의 해쉬값을 계산하여 생성되는 것을 특징으로 한다.

[0026] 바람직하게, 본 발명에 따른 패킷의 무결성 판단 장치는 출처 정보에서 패킷의 순차적인 이송 경로와 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하는지 여부에 기초하여 패킷의 이송 경로에 대한 정상 여부를 판단하는 정상 판단부를 더 포함하는 것을 특징으로 한다.

[0027] 바람직하게, 본 발명의 일 실시예에 따른 정상 판단부는 출처 정보에서 패킷의 순차적인 이송 경로와 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하지 않은 비정상 패킷을 식별하여 카운트하는 카운트부와, 카운트한 비정상 패킷의 수와 임계수를 비교하는 비교부와, 비정상 패킷의 수가 임계수를 초과하는 경우 경고 메시지를 생성하여 센서 네트워크의 관리자 단말기로 송신하는 경고 제어부를 더 포함하는 것을 특징으로 한다.

발명의 효과

[0028] 본 발명에 따른 센서 네트워크에서 패킷의 무결성을 판단하는 방법은 다음과 같은 효과를 가진다.

[0029] 본 발명에 따른 패킷의 무결성 판단 방법은 센서 네트워크에서 발신 노드로부터 루트 노드까지의 이송 경로에 존재하는 모든 하위 노드가 루트 노드의 자식 노드인지를 판단하거나 패킷에 구비된 패킷의 순차적인 이송 경로와 암호화된 출처 정보에서 패킷의 순차적인 이송 경로를 비교하여 해당 패킷의 무결성을 판단함으로써, 패킷의 무결성을 이중으로 판단할 수 있다.

[0030] 또한, 본 발명에 따른 패킷의 무결성 판단 방법은 센서 네트워크에서 무결성이 인정되지 않는 비정상 패킷의 수를 카운트함으로써, 카운트한 비정상 패킷의 수가 임계수를 초과하는지 여부에 따라 센서 네트워크에 허락받지 않은 제3자의 불법 노드를 용이하게 인식할 수 있다.

도면의 간단한 설명

[0031] 도 1은 본 발명에 따른 패킷의 무결성 판단 시스템을 설명하기 위한 도면이다.

도 2는 본 발명에 따른 패킷의 무결성 판단 장치를 설명하기 위한 기능 블록도이다.

도 3은 본 발명의 일 실시예에 따른 정상 판단부(190)를 설명하기 위한 기능 블록도이다.

도 4는 본 발명의 일 실시예에 따른 패킷의 무결성 판단 방법을 설명하기 위한 흐름도이다.

도 5는 패킷의 이송 경로에서 생성되는 출처 정보의 일 예를 설명하기 위한 도면이다.

도 6은 패킷의 이송 경로에서 생성되는 출처 정보의 다른 예를 설명하기 위한 도면이다.

도 7은 본 발명에 따른 패킷의 무결성 판단 방법에서 비정상 패킷을 판단하는 일 예를 설명하기 위한 흐름도이다.

도 8은 본 발명에서 관리자 단말기로 송신되는 경고 메시지의 일 예를 도시하고 있다.

발명을 실시하기 위한 구체적인 내용

[0032] 본 발명에서 사용되는 기술적 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아님을 유의해야 한다. 또한, 본 발명에서 사용되는 기술적 용어는 본 발명에서 특별히 다른 의미로 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 의미로 해석되어야 하며, 과도하게 포괄적인 의미로 해석되거나, 과도하게 축소된 의미로 해석되지 않아야 한다. 또한, 본 발명에서 사용되는 기술적인 용어가 본 발명의 사상을 정확하게 표현하지 못하는 잘못된 기술적 용어일 때에는, 당업자가 올바르게 이해할 수 있는 기술적 용어로 대체되어 이해되어야 할 것이다.

[0033] 또한, 본 발명에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함한다. 본 발명에서, "구성된다" 또는 "포함한다" 등의 용어는 발명에 기재된 여러 구성 요소들, 또는 여러 단계를 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성 요소들 또는 일부 단계들은 포함되지 않을 수도 있고, 또는 추가적인 구성 요소 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다.

[0034] 또한, 첨부된 도면은 본 발명의 사상을 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 발명의 사상이 제한되는 것으로 해석되어서는 아니 됨을 유의해야 한다.

[0035] 이하 첨부한 도면을 참고로 본 발명에 따른 센서 네트워크에서 패킷의 무결성을 판단하는 방법 및 그 장치에 대해 보다 구체적으로 살펴본다.

[0036] 도 1은 본 발명에 따른 패킷의 무결성 판단 시스템을 설명하기 위한 도면이다.

[0037] 도 1을 참고로 보다 구체적으로 살펴보면, 네트워크(30)에는 제1 센서 네트워크(SN1)과 제2 센서 네트워크(SN2)가 접속되어 있으며, 네트워크(30)에는 제1 센서 네트워크(SN1) 또는 제2 센서 네트워크(SN2)를 관리하는 관리자가 사용하는 관리자 단말기(50) 및 응용 서버(70)가 접속되어 있다.

[0038] 여기서 제1 센서 네트워크(SN1) 또는 제2 센서 네트워크(SN2)는 6LoWPAN 기반으로 패킷을 송수신하는 단위 센서 네트워크로 본 발명이 적용되는 분야에 따라 다양한 수의 센서 네트워크가 네트워크(30)에 접속될 수 있다.

[0039] 제1 센서 네트워크(SN1) 또는 제2 센서 네트워크(SN2)의 각 단위 센서 네트워크는 단위 센서 네트워크에 구비되어 있는 센서 노드들에서 감지하거나 측정한 센서 정보를 순차적 이동 경로를 통해 각 단위 센서 네트워크의 루트 노드(R1 또는 R2)로 송신한다.

[0040] 제1 센서 네트워크(SN1)의 루트 노드(R1)는 하위 노드들로부터 수신한 패킷을 네트워크(30)를 통해 해당 패킷을 이용하는 응용 서버(70)로 송신하거나 제2 센서 네트워크(SN2)의 루트 노드(R2)는 하위 노드들로부터 수신한 패킷을 네트워크(30)를 통해 해당 패킷을 이용하는 응용 서버(70)로 송신한다. 여기서 응용 서버(70)는 제1 센서 네트워크(SN1)에 사용되는 응용 서버와 제2 센서 네트워크(SN2)에 사용되는 응용 서버가 다수 존재할 수 있다.

[0041] 제1 센서 네트워크(SN1)와 제2 센서 네트워크(SN2)에 대해 보다 구체적으로 살펴보면, 제1 센서 네트워크(SN1)에는 다수의 센서 노드들이 분포 배치되어 있는데 제1 센서 네트워크(SN1)의 각 센서 노드들은 배치되어 있는 장소에서 측정하거나 센싱한 센서 정보를 생성하고 생성한 센서 정보를 인접한 주변 노드를 통해 루트 노드(R1)로 송신한다. 한편, 제2 센서 네트워크(SN2)에는 다수의 센서 노드들이 분포 배치되어 있는데 제2 센서 네트워크(SN2)의 각 센서 노드들은 배치되어 있는 장소에서 측정하거나 센싱한 센서 정보를 생성하고 생성한 센서 정보를 인접한 주변 노드를 통해 루트 노드(R2)로 송신한다.

[0042] 여기서 제1 센서 네트워크(SN1)의 루트 노드(R1)에는 네트워크(30)의 제1 경계 라우터(미도시)가 접속되어 있으

며, 제2 센서 네트워크(SN2)의 루트 노드(R2)에는 네트워크의 제2 경계 라우터(미도시)가 접속되어 있다.

[0043] 본 발명의 일 실시예에서 제1 센서 네트워크(SN1)의 루트 노드(R1)는 제1 센서 네트워크(SN1)의 하위 노드들로부터 수신한 패킷의 무결성을 판단하며 제2 센서 네트워크(SN2)의 루트 노드(R2)는 제2 센서 네트워크(SN2)의 하위 노드들로부터 수신한 패킷의 무결성을 판단한다.

[0044] 본 발명이 적용되는 분야에 따라 본 발명의 다른 실시예에서 제1 센서 네트워크(SN1)의 루트 노드(R1)는 제1 센서 네트워크(SN1)의 하위 노드들로부터 수신한 패킷을 제1 경계 라우터로 송신하며 제1 경계 라우터는 제1 센서 네트워크(SN1)에서 송수신되는 패킷의 무결성을 판단할 수 있고, 제2 센서 네트워크(SN2)의 루트 노드(R2)는 제2 센서 네트워크(SN2)의 하위 노드들로부터 수신한 패킷을 제2 경계 라우터로 송신하며 제2 경계 라우터는 제2 센서 네트워크(SN2)에서 송수신되는 패킷의 무결성을 판단할 수 있다.

[0045] 도 2는 본 발명에 따른 패킷의 무결성 판단 장치를 설명하기 위한 기능 블록도이다.

[0046] 도 2를 참고로 보다 구체적으로 살펴보면, 통신부(110)는 주변 센서 노드로부터 패킷을 수신하거나 접속되어 있는 루트 노드로부터 패킷을 수신한다.

[0047] 이송 경로 추출부(120)는 수신한 패킷에서 이송 경로 정보를 추출하고, 출처 정보 추출부(130)는 수신한 패킷에서 출처 정보를 추출한다.

[0048] 여기서 이송 경로 정보는 센서 정보를 생성한 발신 노드로부터 루트 노드까지의 패킷의 이송 경로에 위치하는 하위 노드의 식별자이며, 발신 노드로부터 루트 노드까지의 이송 경로에 위치하는 하위 노드는 자신의 식별자를 패킷에 포함하여 다음 이송 경로의 노드로 패킷을 송신한다.

[0049] 한편, 출처 정보는 발신 노드로부터 루트 노드까지의 이송 경로에 위치하는 각 하위 노드들이 순차적으로 자신의 식별자와 이전 하위 노드로부터 수신한 해쉬값을 계산하여 생성된다.

[0050] 하위 노드 판단부(150)는 추출한 패킷의 이송 경로 정보에서 발신 로드로부터 루트 노드까지의 이송 경로에 위치하는 하위 노드의 식별자에 기초하여 이송 경로에 위치하는 모든 하위 노드들이 해당 센서 네트워크의 자식 노드인지 판단한다. 노드 데이터베이스(170)에는 센서 네트워크에 배치되어 있는 모든 자식 노드들의 리스트가 저장되어 있는데, 하위 노드 판단부(150)는 패킷으로부터 추출한 이송 경로 정보와 노드 데이터베이스(170)에 저장되어 있는 자식 노드들의 리스트를 비교하여 패킷의 이송 경로에 위치하는 하위 노드들이 해당 센서 네트워크의 자식 노드인지 여부를 판단할 수 있다.

[0051] 무결성 판단부(180)는 추출한 출처 정보에서 패킷의 순차적인 이송 경로와 추출한 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하는지 여부에 기초하여 해당 패킷의 무결성을 판단한다. 여기서 무결성이란 해당 패킷이 센서 네트워크에 배치되어 있는 노드를 통해 정상적인 이송 경로로 루트 노드까지 이송되었는지를 의미하는 것이다.

[0052] 정상 판단부(190)는 출처 정보에서 패킷의 순차적인 이송 경로와 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하는지 여부에 기초하여 해당 센서 네트워크에서 패킷의 이송 경로에 대한 정상 여부를 판단한다.

[0053] 도 3은 본 발명의 일 실시예에 따른 정상 판단부(190)를 설명하기 위한 기능 블록도이다.

[0054] 도 3을 참고로 보다 구체적으로 살펴보면, 카운트부(191)는 비정상 패킷의 수를 카운트하는데, 하위 노드 판단부에서 패킷의 이송 경로에 위치하는 모든 하위 노드들이 해당 센서 네트워크의 자식 노드가 아닌 경우 수신한 패킷을 비정상 패킷으로 수를 카운트하거나 또는 무결성 판단부에서 출처 정보에 기초하여 패킷의 순차적인 이송 경로와 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 불일치한 패킷의 수를 카운트한다.

[0055] 비교부(193)는 카운트한 비정상 패킷의 수를 기설정한 임계수와 비교하며, 경고 제어부(195)는 카운트한 비정상 패킷의 수가 임계수를 초과하는 경우 해당 센서 네트워크에서 허락받지 않은 제3 노드가 존재함을 경고하기 위한 경고 메시지를 생성하고 생성한 경고 메시지를 해당 센서 네트워크를 관리하는 관리자 단말기로 송신 제어한다.

[0056] 도 4는 본 발명의 일 실시예에 따른 패킷의 무결성 판단 방법을 설명하기 위한 흐름도이다.

[0057] 도 4를 참고로 보다 구체적으로 살펴보면, 루트 노드는 하위 노드로부터 패킷을 수신하는 경우 수신한 패킷에서 이송 경로 정보를 추출한다(S110). 수신한 패킷은 헤더, 데이터 및 출처 정보를 구비하는데, 패킷의 이송 경로

중 해당 패킷을 수신한 노드는 이전 하위 노드의 식별자와 해당 패킷을 송신할 다음 하위 노드의 식별자를 헤더에 포함하여 생성한다. 따라서 루트 노드에서 수신한 패킷의 헤더에는 발신 노드로부터 루트 노드까지 해당 패킷의 이송 경로에 위치하는 모든 하위 노드의 식별자가 구비되어 있다.

[0058] 추출한 이송 경로 정보에서 패킷의 이송 경로에 위치하는 모든 하위 노드의 식별자가 해당 센서 네트워크에 구비되어 있는 자식 노드인지 판단한다(S120). 즉 루트 노드에는 해당 루트 노드의 자식 노드들의 리스트가 등록 저장되어 있는데, 수신한 패킷의 이송 경로에 위치하는 모든 하위 노드의 식별자와 자식 노드의 리스트를 비교하여 모든 하위 노드가 자식 노드 리스트의 식별자와 일치하는지 여부를 판단한다.

[0059] 수신한 패킷의 이송 경로에 위치하는 모든 하위 노드가 루트 노드의 자식 노드인 경우, 수신한 패킷에서 출처 정보를 추출한다(S130). 여기서 출처 정보는 발신 노드로부터 루트 노드까지의 이송 경로 중 루트 노드까지의 순차적 이송 경로에 위치하는 모든 하위 노드에서 각 하위 노드의 이전 하위 노드로부터 수신한 해쉬값과 각 하위 노드의 식별값으로부터 각 하위 노드의 해쉬값을 계산하여 생성되는데, 루트 노드는 수신한 패킷의 출처 정보에 구비되어 있는 해쉬값을 역변환하여 출처 정보에서 패킷의 순차적인 이동 경로를 추출한다.

[0060] 출처 정보에서 패킷의 순차적인 이송 경로와 추출한 패킷의 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하는지 여부를 판단하며(S150), 출처 정보에서 패킷의 순차적인 이송 경로와 추출한 패킷의 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하는 경우 해당 패킷은 정상적인 패킷으로 판단한다(S170).

[0061] 그러나 출처 정보에서 패킷의 순차적인 이송 경로와 추출한 패킷의 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 불일치하는 경우, 해당 패킷은 비정상적인 패킷, 즉 허락받지 않은 제3 노드를 통해 경유되어 이송되었거나 허락받지 않은 제3 노드에 의해 변조되었거나, 허락받지 않은 제3 노드에 의해 생성된 패킷으로 판단한다.

[0062] 여기서 출처 정보의 생성 과정에 대해 보다 구체적으로 살펴보면, 발신 노드로부터 루트 노드까지의 이송 경로 중 이전 하위 노드로부터 수신한 해쉬값과 현재 하위 노드의 식별값에 기초하여 현재 하위 노드의 해쉬값을 계산하는 단계와, 현재 하위 노드로부터 루트 노드까지의 순차적 이송 경로에 위치하는 모든 하위 노드에서 각 하위 노드의 이전 하위 노드로부터 수신한 해쉬값과 각 하위 노드의 식별값에 기초하여 각 하위 노드의 해쉬값을 생성하여 발신 노드로부터 루트 노드까지의 출처 정보를 생성하는 단계를 통해 출처 정보가 생성된다.

[0063] 바람직하게, 발신 노드에서 루트 노드까지 패킷의 이송 경로에 위치하는 각 노드(i)의 해쉬값(H(i))은 아래의 수학식 (1)에 의해 계산되는데,

[0064] [수학식 1]

[0065] $H(i)=H(H(i-1)+ID_i)$

[0066] 여기서 $H(i-1)$는 이전 노드(i-1)의 해쉬값이며 ID_i는 노드(i)의 식별자인 것을 특징으로 한다.

[0067] 도 5는 패킷의 이송 경로에서 생성되는 출처 정보의 일 예를 설명하기 위한 도면이다.

[0068] 도 5를 참고로 보다 구체적으로 살펴보면, 발신 노드(4)는 패킷을 생성시 발신 노드(4)의 식별자(ID_4)와 랜덤하게 생성되는 초기화 값(I)을 해쉬함수(H)에 적용하여 발신 노드(4)의 해쉬값(H(4))을 계산하고 계산한 해쉬값(H(4))을 구비하는 패킷을 이송 경로의 상위 노드(2)로 송신한다.

[0069] 상위 노드(2)는 발신 노드(4)로부터 수신한 패킷에서 발신 노드(4)의 해쉬값(H(4))를 추출하고 추출한 발신 노드(4)의 해쉬값(H(4))과 상위 노드(2)의 식별자(ID_2)를 해쉬함수(H)에 적용하여 상위 노드(2)의 해쉬값(H(2))을 계산하며, 계산한 해쉬값(H(2))을 구비하는 패킷을 이송 경로의 상위 노드(1)로 송신한다.

[0070] 상위 노드(1)는 상위 노드(1)로부터 수신한 패킷에서 상위 노드(2)의 해쉬값(H(2))를 추출하고 추출한 상위 노드(2)의 해쉬값(H(2))과 상위 노드(1)의 식별자(ID_1)를 해쉬함수(H)에 적용하여 상위 노드(1)의 해쉬값(H(1))을 계산하며, 계산한 해쉬값(H(1))을 구비하는 패킷을 이송 경로의 루트 노드(R)로 송신한다.

[0071] 루트 노드는 수신한 패킷에서 출처 정보를 추출하고 추출한 출처 정보의 해쉬값을 이송 경로의 하위 노드 수만큼 순차적으로 역변환하여 발신노드로부터 루트 노드까지의 순차적인 패킷의 이송 경로를 추출한다.

[0072] 본 발명이 적용되는 분야에서 패킷의 무결성은 루트 노드가 접속되어 있는 경계 라우터에서 판단될 수 있는데, 도 6은 패킷의 이송 경로에서 생성되는 출처 정보의 다른 예를 설명하기 위한 도면이다.

[0073] 도 6을 참고로 보다 구체적으로 살펴보면, 발신 노드(4)는 패킷을 생성시 발신 노드(4)의 식별자(ID_4)와 랜덤하게 생성되는 초기화 값(I)을 해쉬함수(H)에 적용하여 발신 노드(4)의 해쉬값(H(4))을 계산하고 계산한 해쉬값(H(4))을 구비하는 패킷을 이송 경로의 상위 노드(2)로 송신한다.

[0074] 상위 노드(2)는 발신 노드(4)로부터 수신한 패킷에서 발신 노드(4)의 해쉬값(H(4))를 추출하고 추출한 발신 노드(4)의 해쉬값(H(4))과 상위 노드(2)의 식별자(ID_2)를 해쉬함수(H)에 적용하여 상위 노드(2)의 해쉬값(H(2))을 계산하며, 계산한 해쉬값(H(2))을 구비하는 패킷을 이송 경로의 상위 노드(1)로 송신한다.

[0075] 상위 노드(1)는 상위 노드(1)로부터 수신한 패킷에서 상위 노드(2)의 해쉬값(H(2))를 추출하고 추출한 상위 노드(2)의 해쉬값(H(2))과 상위 노드(1)의 식별자(ID_1)를 해쉬함수(H)에 적용하여 상위 노드(1)의 해쉬값(H(1))을 계산하며, 계산한 해쉬값(H(1))을 구비하는 패킷을 이송 경로의 루트 노드(R)로 송신한다.

[0076] 루트 노드는 수신한 패킷을 루트 노드가 접속한 경계 라우터(M)로 송신하며, 경계 라우터(M)는 출처 정보를 추출하고 추출한 출처 정보의 해쉬값을 이송 경로의 하위 노드 수만큼 순차적으로 역변환하여 발신노드로부터 루트 노드까지의 순차적인 패킷의 이송 경로를 추출한다.

[0077] 도 7은 본 발명에 따른 패킷의 무결성 판단 방법에서 비정상 패킷을 판단하는 일 예를 설명하기 위한 흐름도이다.

[0078] 도 7을 참고로 보다 구체적으로 살펴보면, 수신한 패킷으로부터 추출한 출처 정보에서 패킷의 순차적인 이송 경로와 수신한 패킷으로부터 추출한 이송 경로 정보에서 패킷의 순차적인 이송 경로가 서로 일치하지 않은 비정상 패킷을 식별하여 카운트한다(S210).

[0079] 카운트한 비정상 패킷의 수와 임계수를 비교하여(S230), 비정상 패킷의 수가 임계수를 초과하는 경우, 경고 메시지를 생성하여 센서 네트워크의 관리자 단말기로 송신한다(S250). 센서 네트워크에서 센서 노드의 오동작 또는 노이즈로 인하여 자연적인 비정상 패킷이 발생할 수 있는데, 카운트한 비정상 패킷의 수가 임계수를 초과하는 경우에는 자연적인 비정상 패킷을 벗어나 허락받지 못한 제3 노드가 센서 네트워크의 패킷 이송 경로에 개입한 것으로 판단할 수 있다.

[0080] 도 8은 본 발명에서 관리자 단말기로 송신되는 경고 메시지의 일 예를 도시하고 있는데, 경고 메시지에는 단위 시간(예를 들어, 1시간, 1일 등) 동안 발생한 비정상 패킷의 수와 단위 시간 동안 비정상 패킷의 수가 임계수를 초과한 시각에 대한 정보가 포함될 수 있다.

[0081] 한편, 상술한 본 발명의 실시 예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0082] 상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장 매체(예를 들어, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

[0083] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

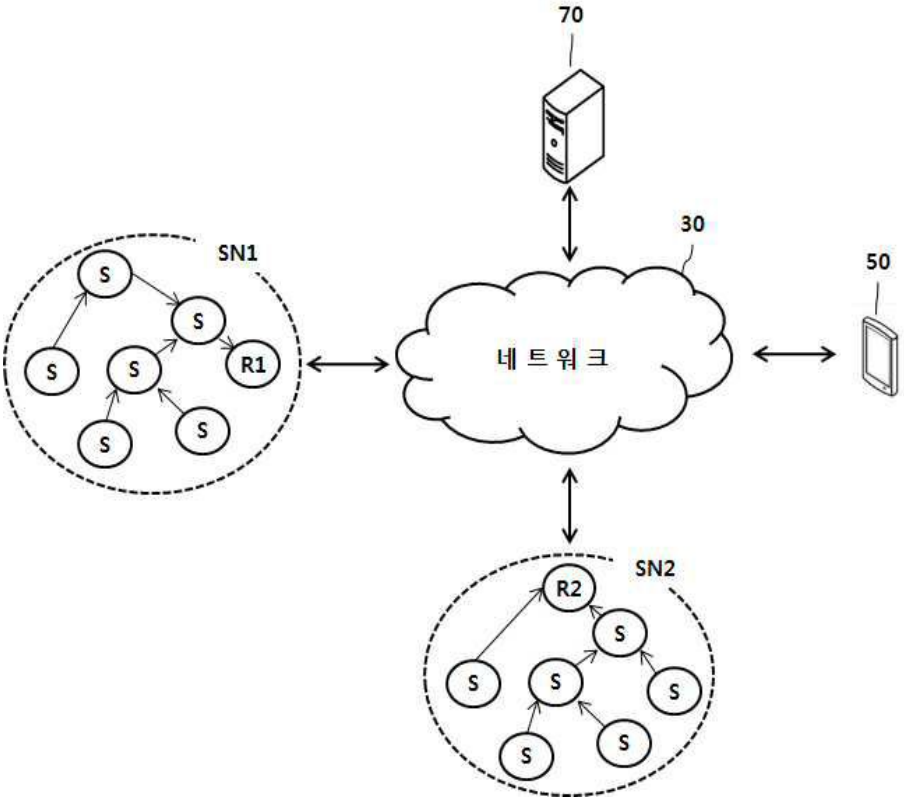
부호의 설명

[0084]

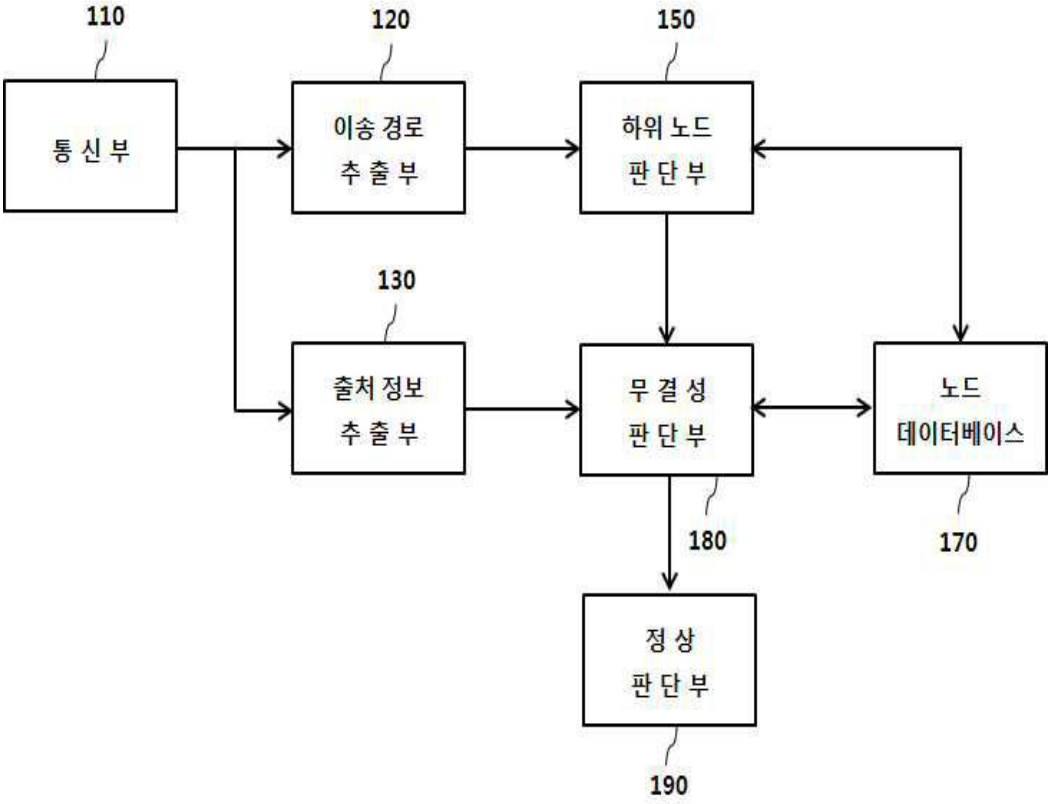
30: 네트워크	50: 관리자 단말기
70: 응용 서버	110: 통신부
120: 이송 경로 추출부	130: 출처 정보 추출부
150: 하위 노드 판단부	170: 노드 데이터베이스
180: 무결성 판단부	190: 정상 판단부
191: 카운트부	193: 비교부
195: 경고 제어부	

도면

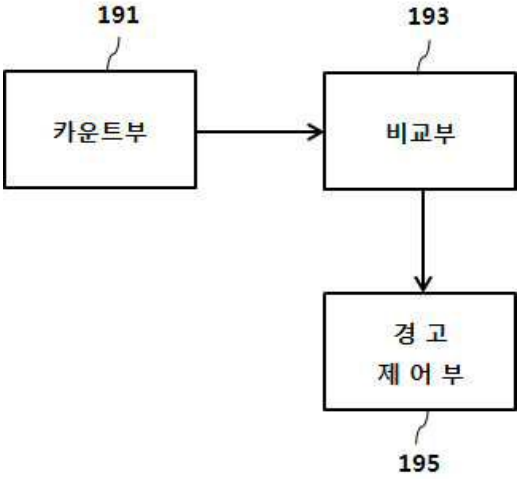
도면1


70
30
50
SN1
S
R1
네트워크
SN2
R2

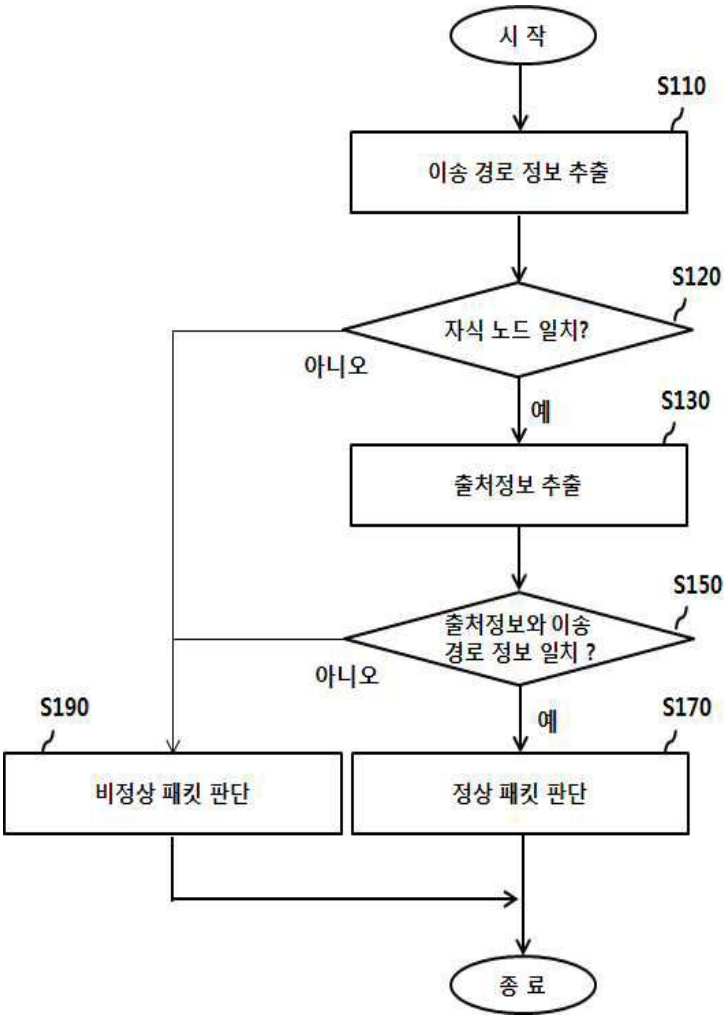
도면2


110
통신부
120
이송경로
추출부
150
하위노드
판단부
130
출처정보
추출부
무결성
판단부
노드
데이터베이스
180
170
정상
판단부
190

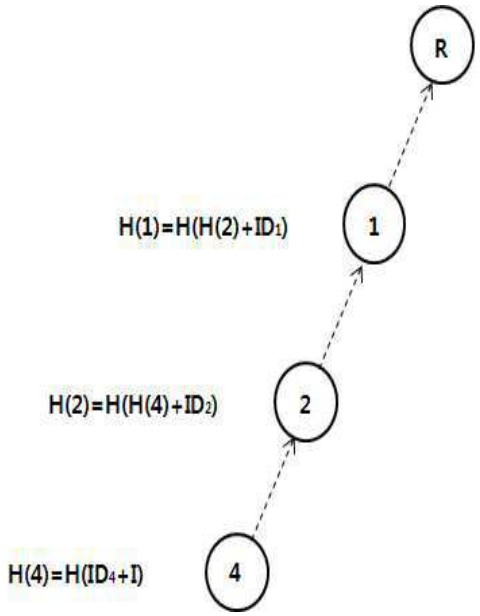
도면3


191
193
카운트부
비교부
경 고
제 어 부
195

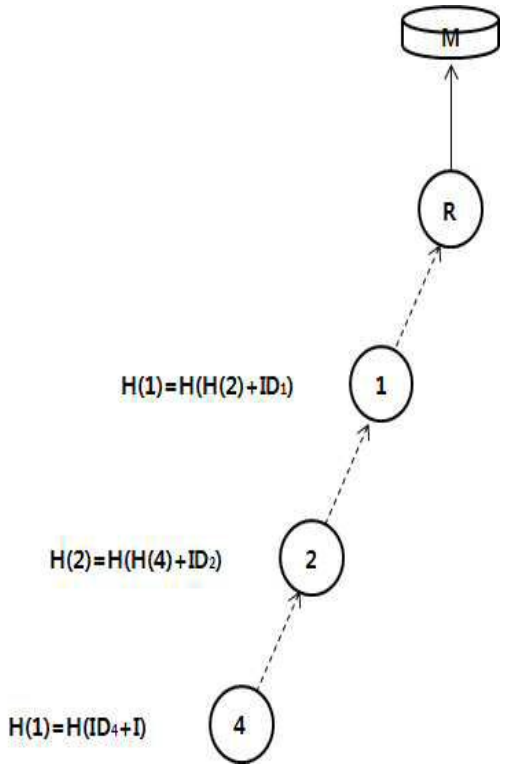
도면4


시 작
S110
이송 경로 정보 추출
S120
자식 노드 일치?
아니오
예
S130
출처정보 추출
S150
출처정보와 이송
경로 정보 일치 ?
아니오
예
S190
S170
비정상 패킷 판단
정상 패킷 판단
종 료

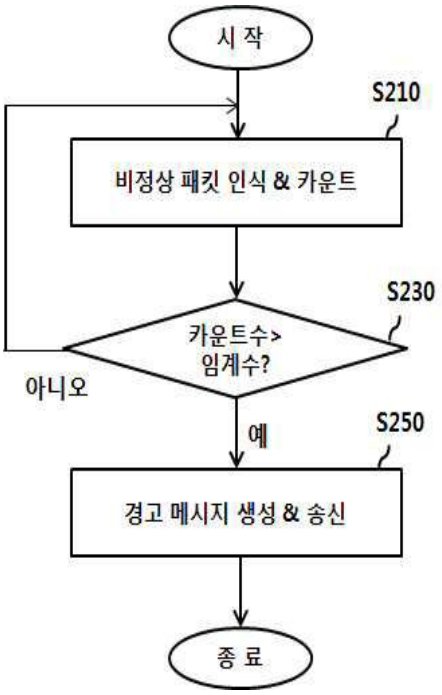
도면5


R
H(1)=H(H(2)+ID1)
1
H(2)=H(H(4)+ID2)
2
H(4)=H(ID4+I)
4

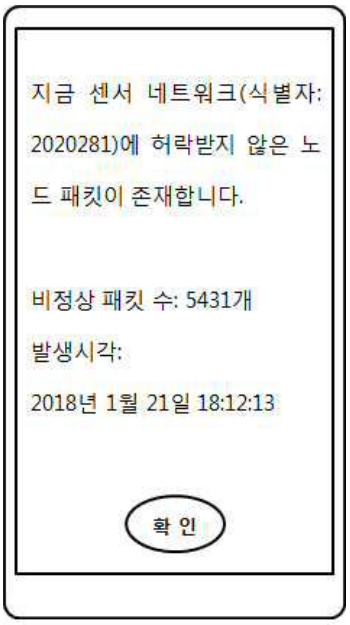
도면6


M
R
H(1)=H(H(2)+ID1)
1
H(2)=H(H(4)+ID2)
2
H(1)=H(ID4+I)
4

도면7


시 작
S210
비정상 패킷 인식 & 카운트
S230
카운트수>
임계수?
아니오
예
S250
경고 메시지 생성 & 송신
종 료

도면8


지금 센서 네트워크(식별자: 2020281)에 허락받지 않은 노드 패킷이 존재합니다.
비정상 패킷 수: 5431개
발생시각:
2018년 1월 21일 18:12:13
확 인

(a)