(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2019 년 8 월 15 일 (15.08.2019)

WIPO | PCT

(10) 국제공개번호
WO 2019/156278 A1

(51) 국제특허분류:
H04L 12/26 (2006.01)

(21) 국제출원번호: PCT/KR2018/002348

(22) 국제출원일: 2018 년 2 월 27 일 (27.02.2018)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2018-0016579 2018 년 2 월 9 일 (09.02.2018) KR

(71) 출원인: **경희대학교 산학협력단 (UNIVERSITY-INDUSTRY COOPERATION GROUP OF KYUNG HEE UNIVERSITY)** [KR/KR]; 17104 경기도 용인시 기흥구 덕영대로 1732, Gyeonggi-do (KR).

(72) 발명자: **홍충선 (HONG, Choong Seon)**; 16941 경기도 용인시 수지구 상현로 30-10 233동 101호, Gyeonggi-do (KR). **수하일사바 (SUHAIL, Sabah)**; 17104 경기도 용인시 기흥구 덕영대로 1732 경희대학교 국제캠퍼스 전자정보대학 352호, Gyeonggi-do (KR). **김영기 (KIM, Young Ki)**; 16705 경기도 수원시 영통구 청명로 59번길 45-14, 203호, Gyeonggi-do (KR). **판데이라즈샤시 (PANDEY RAJ, Shashi)**; 17104 경기도 용인시 기흥구 덕영대로 1732 경희대학교 국제캠퍼스 전자정보대학 352호, Gyeonggi-do (KR).

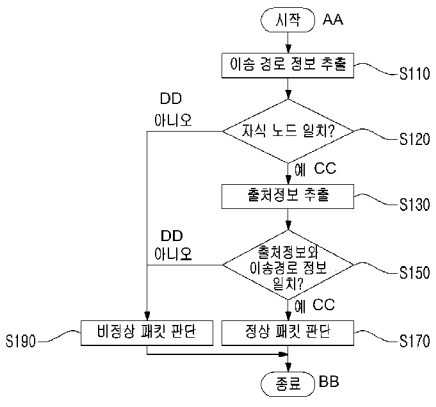
(74) 대리인: **김홍석 (KIM, Hong Suk)**; 08390 서울시 구로구 디지털로26길 111, 414호 동진국제특허법률사무소 (구로동, 제이엔케이디지털타워), Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI

(54) **Title:** METHOD FOR DETERMINING INTEGRITY OF PACKET

(54) **발명의 명칭:** 패킷의 무결성을 판단하는 방법



S110 ... Extract transfer path information
S120 ... Coincide with child node?
S130 ... Extract source information
S150 ... Does source information coincide with transfer path information?
S170 ... Determination of normal packet
S190 ... Determination of abnormal packet
AA ... Start
BB ... End
CC ... Yes
DD ... No

(57) **Abstract:** The present invention relates to a method for determining integrity of a packet in a sensor network, and relates to a method for determining integrity of a packet, wherein the method: can dually determine integrity of a packet by determining whether all sub-nodes, which exist in a transfer path from an origination node to a root node in a sensor network, are child nodes of the root node, or by comparing a transfer path provided in a packet with a transfer path of encrypted source information so as to determine the integrity of the relevant packet; and can easily recognize a revoked node of a third party which is not allowed in the sensor network by counting the number of abnormal packets, the integrity of which is not admitted in the sensor network, and determining whether the counted number of the abnormal packets exceeds a threshold number.

(57) **요약서:** 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 이송경로와 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.

WO 2019/156278 A1

[다음 쪽 계속]

(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 패킷의 무결성을 판단하는 방법

기술분야

[1] 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.

[2] 본 발명은 과학기술정보통신부의 국가연구개발사업인 '정보통신·방송 연구개발사업'의 일환으로 수행한 연구로부터 도출된 것이다 [과제고유번호: 2015-0-00557, 연구과제명: IoT기기의 물리적 속성, 관계, 역할 기반 Resilient/Fault-Tolerant 자율 네트워킹 기술연구, 연구기간: 2017.06.01 ~ 2018. 03.31, 주관기관 : 한국과학기술원].

배경기술

[3] 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.

[4] 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, 센서노드들에 IP를 할당하여 IP 네트워크 상에서 가능한 여러 기술들의 이점을 얻을 수 있다.

[5] 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.

[6] 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.

[7] 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 상세한 설명

기술적 과제

[8] 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.

[9] 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.

[10] 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.

과제 해결 수단

[11] 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(b단계)와, 패킷으로부터 출처 정보를 추출하고 출처 정보에서 패킷의 순차적인 이송경로와 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.

[12] 본 발명의 일 실시예에서 패킷의 무결성 판단 방법의 (a) 단계 내지 (d) 단계는

루트 노드에서 수행되는 것을 특징으로 한다.

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

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

[15] 바람직하게, 본 발명의 일 실시예에서 출처 정보는 발신 노드로부터 루트 노드까지의 이송 경로 중 이전 하위 노드로부터 수신한 해쉬값과 현재 하위노드의 식별값에 기초하여 현재 하위 노드의 해쉬값을 계산하는 단계와, 현재 하위노드로부터 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.

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

[17] 여기서 발신 노드로부터 루트 노드까지 패킷의 이송 경로에 위치하는 노드는 자신의 자식 노드 리스트를 구비하고 있는 것을 특징으로 한다.

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

[19] [수학식 1]

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

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

[22] 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.

[23] 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 출처정보를 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.

[24] 여기서 이송 경로 정보는 패킷의 발신 노드부터 루트 노드까지 패킷의

순차적인 이송 경로에 존재하는 하위 노드의 식별자가 포함되어 있는 것을 특징으로 한다.

[25] 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.

[26] 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.

[27] 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.

[28] 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

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

[30] 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.

[31] 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

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

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

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

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

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

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

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

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

발명의 실시를 위한 형태

[40] 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.

[41] 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.

[42] 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.

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

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

[45] 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.

[46] 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.

[47] 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.

[48] 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 응용서버(70)는 제1 센서 네트워크(SN1)에 사용되는 응용 서버와 제2 센서 네트워크(SN2)에 사용되는 응용 서버가 다수 존재할 수 있다.

[49] 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.

[50] 여기서 제1 센서 네트워크(SN1)의 루트 노드(R1)에는 네트워크(30)의 제1 경계 라우터(미도시)가 접속되어 있으며, 제2 센서 네트워크(SN2)의 루트 노드(R2)에는 네트워크의 제2 경계 라우터(미도시)가 접속되어 있다.

[51] 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.

[52] 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 제2경계 라우터로 송신하며 제2 경계 라우터는 제2 센서 네트워크(SN2)에서 송수신되는 패킷의 무결성을 판단할 수 있다.

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

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

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

[56] 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.

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

[58] 하위 노드 판단부(150)는 추출한 패킷의 이송 경로 정보에서 발신로드로부터 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.

[59] 무결성 판단부(180)는 추출한 출처 정보에서 패킷의 순차적인 이송경로와 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.

[60] 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.

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

[62] 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.

[63] 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.

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

[65] 도 4를 참고로 보다 구체적으로 살펴보면, 루트 노드는 하위 노드로부터 패킷을 수신하는 경우 수신한 패킷에서 이송 경로 정보를 추출한다(S110).

[66] 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.

[67] 추출한 이송 경로 정보에서 패킷의 이송 경로에 위치하는 모든 하위노드의 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.

[68] 수신한 패킷의 이송 경로에 위치하는 모든 하위 노드가 루트 노드의 자식 노드인 경우, 수신한 패킷에서 출처 정보를 추출한다(S130). 여기서 출처정보는 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.

[69] 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).

[70] 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.

[71] 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.

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

[73] [수학식 1]

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

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

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

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

[84] 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.

[85] 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.

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

[87] 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).

[88] 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 제3노드가 센서 네트워크의 패킷 이송 경로에 개입한 것으로 판단할 수 있다.

[89] 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.

[90] 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.

[91] 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.

[92] 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.

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 이송경로에 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 이송경로에 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.

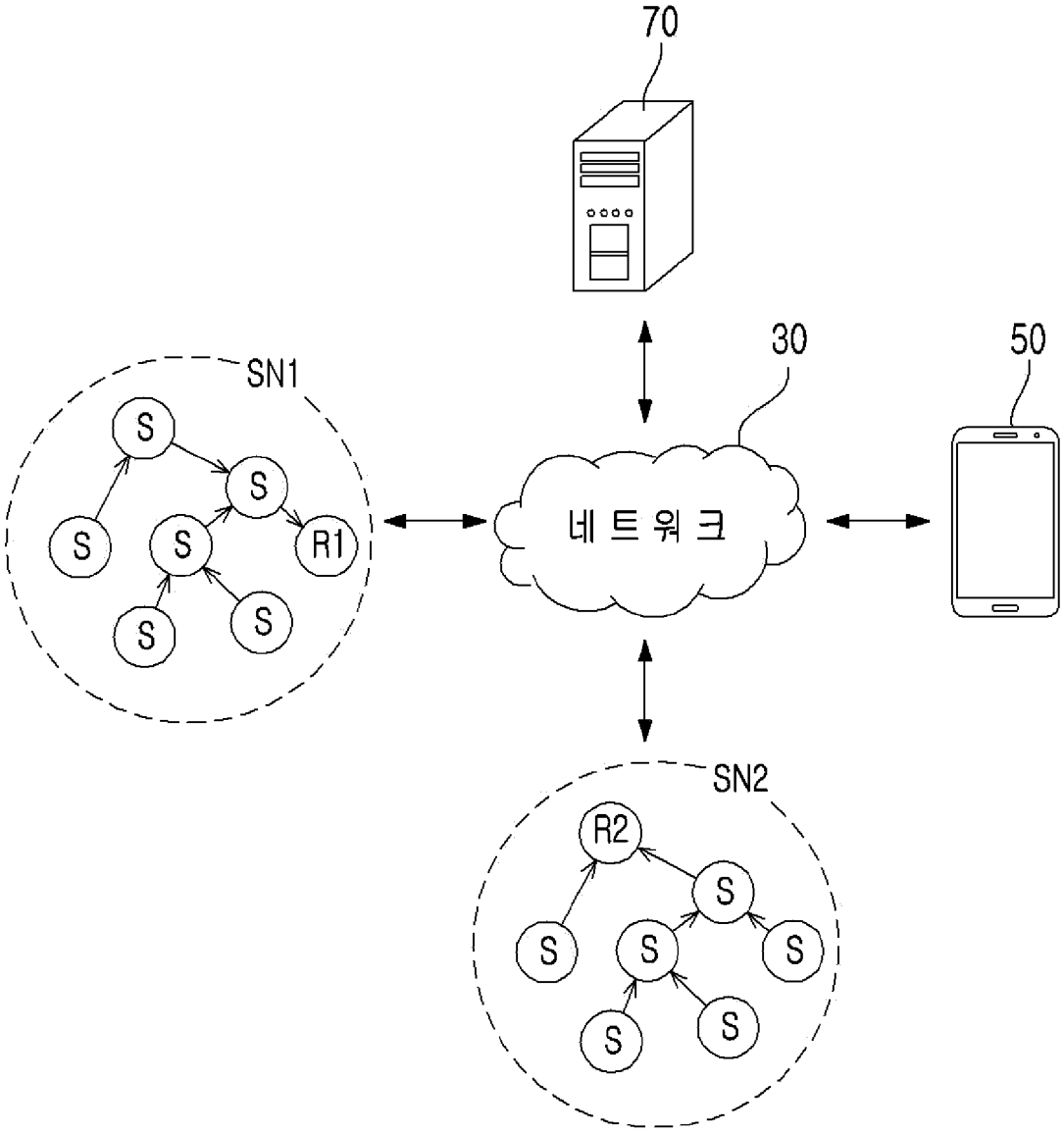
[청구항 13] 제 12 항에 있어서,
상기 출처 정보는 상기 발신 노드로부터 상기 루트 노드까지의 이송 경로 중 상기 루트 노드까지의 순차적 이송 경로에 위치하는 모든 하위 노드에서 각 하위 노드의 이전 하위노드로부터 수신한 해쉬값과 각 하위 노드의 식별값으로부터 각 하위 노드의 해쉬값을 계산하여 생성되는 것을 특징으로 하는 패킷의 무결성 판단 장치.

[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.

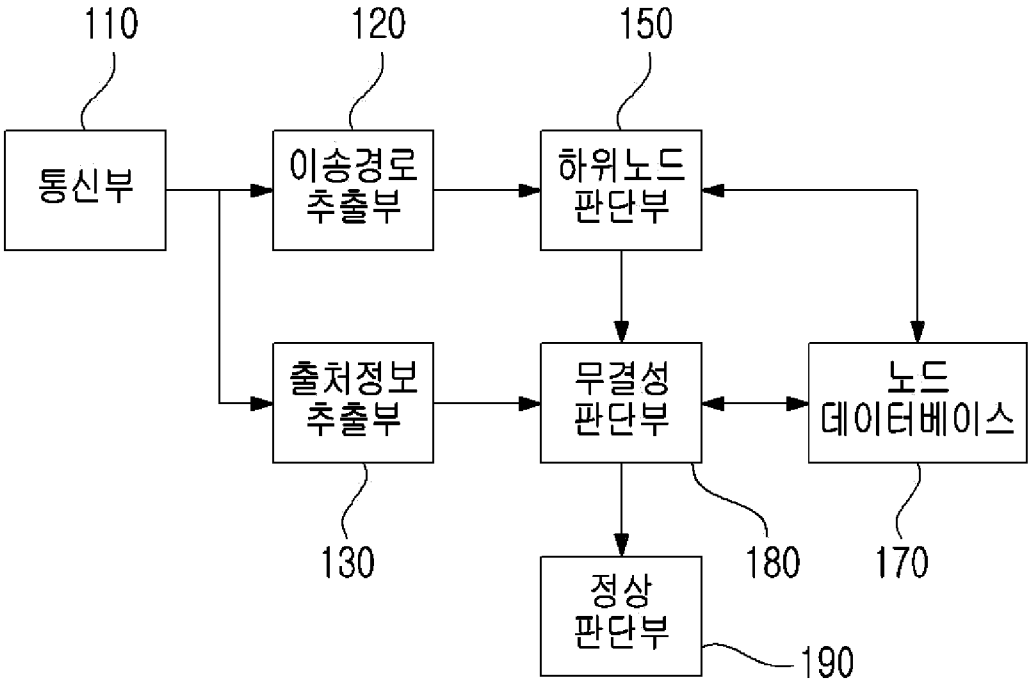
[청구항 15] 제 13 항에 있어서,
상기 패킷의 무결성 판단 장치는 상기 출처 정보에서 상기 패킷의 순차적인 이송 경로와 상기 이송 경로 정보에서 상기 패킷의 순차적인 이송 경로가 서로 일치하는지 여부에 기초하여 상기 패킷의 이송 경로에 대한 정상 여부를 판단하는 정상 판단부를 더 포함하는 것을 특징으로 하는 패킷의 무결성 판단 장치.

[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.

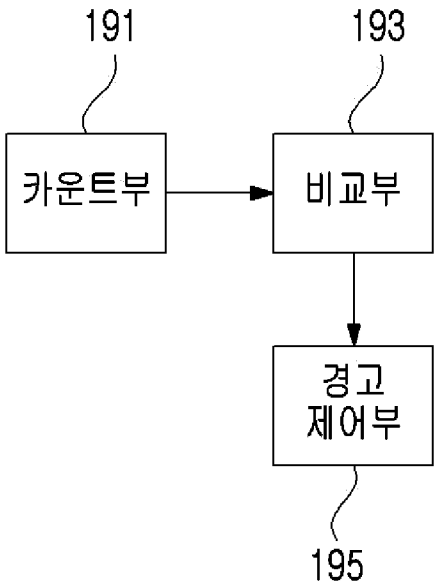
[도1]



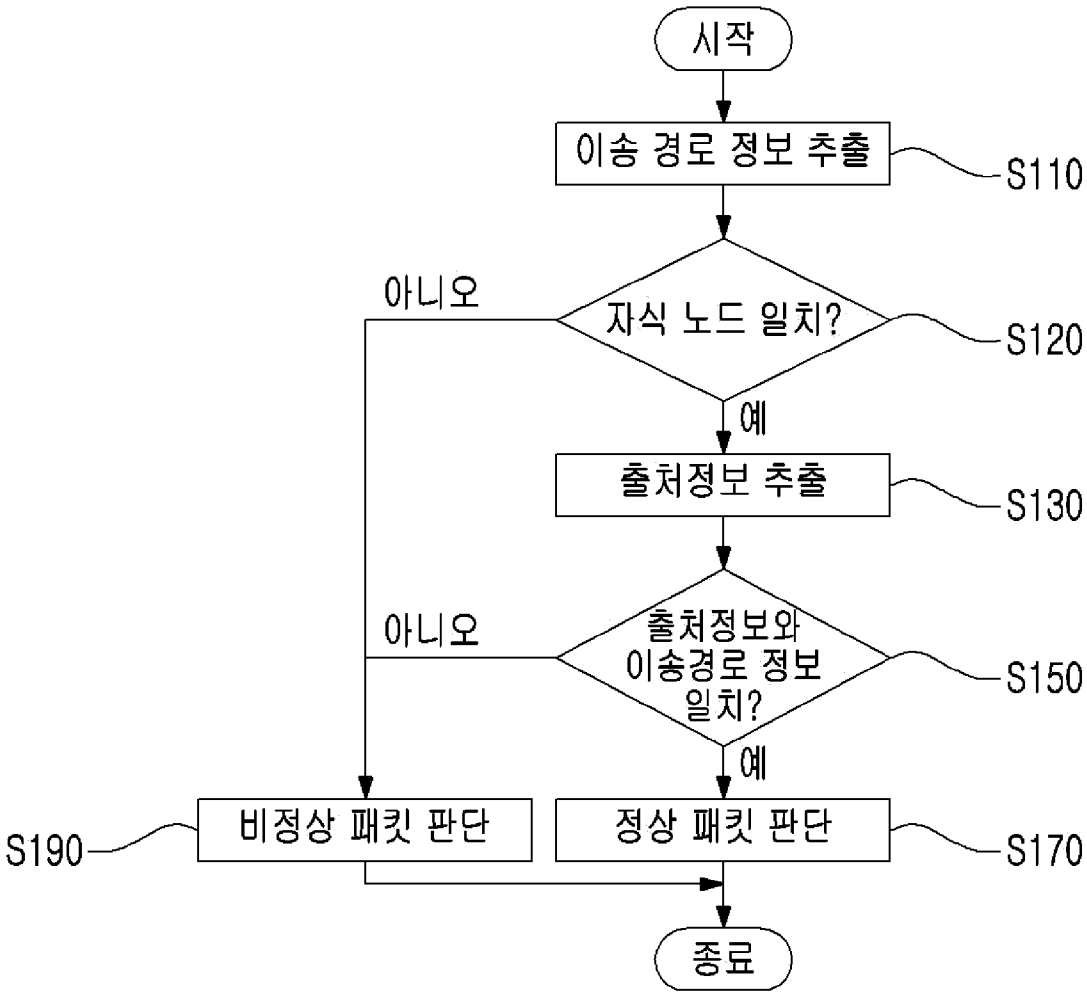
[도2]


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

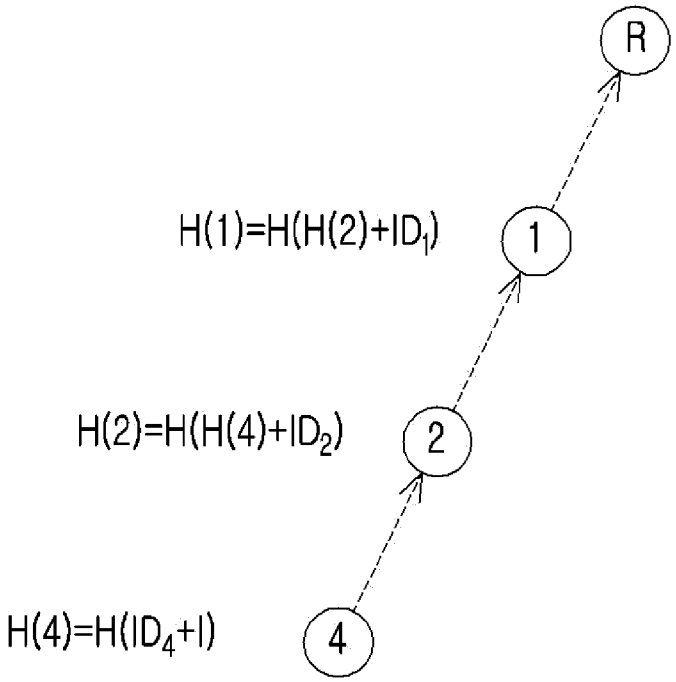
[도3]


191
193
카운트부
비교부
경고 제어부
195

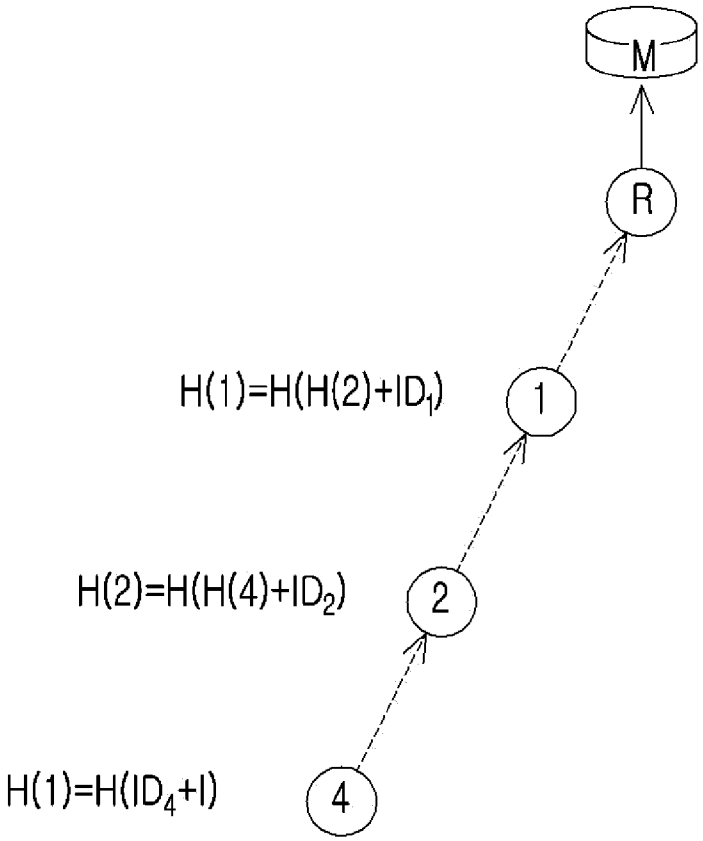
[도4]


시작
이송 경로 정보 추출
S110
자식 노드 일치?
아니오
S120
예
출처정보 추출
S130
출처정보와 이송경로 정보 일치?
아니오
S150
예
비정상 패킷 판단
S190
정상 패킷 판단
S170
종료

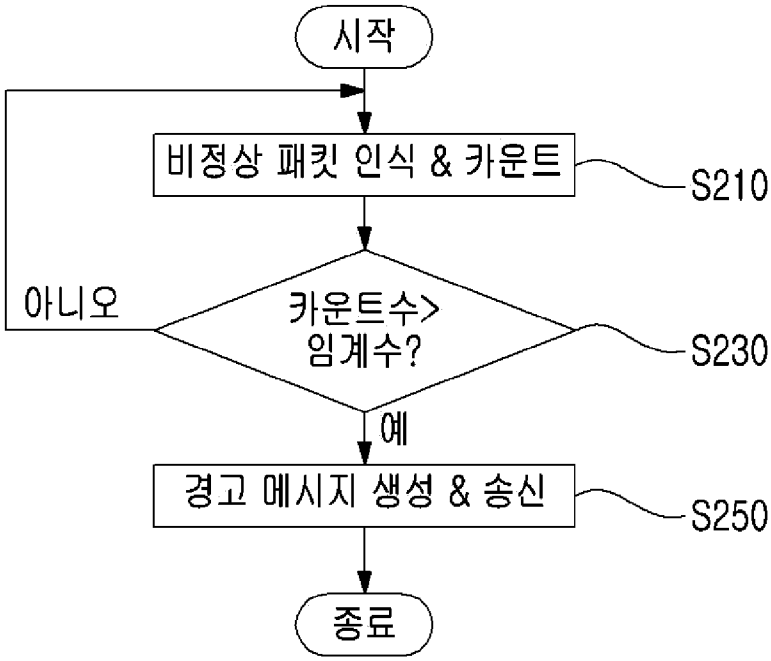
[도5]



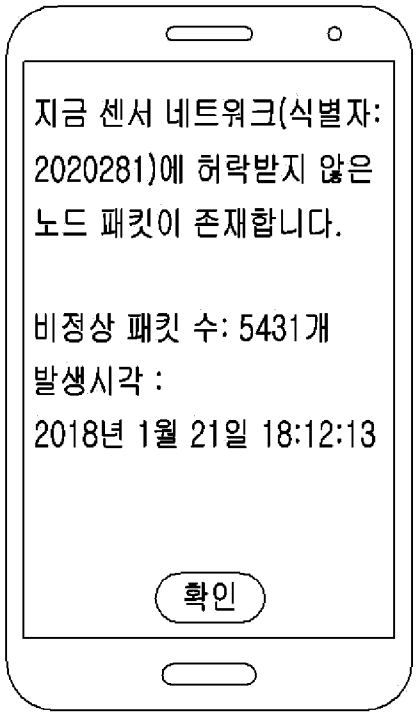
[도6]


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

[도7]


시작
비정상 패킷 인식 & 카운트
S210
아니오
카운트수>
임계수?
S230
예
경고 메시지 생성 & 송신
S250
종료

[도8]


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

(a)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2018/002348

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/26(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/26; H04L 12/18; H04L 12/22; H04L 12/28; H04L 29/06; H04W 24/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: packet integrity verification, pathway, child node, sensor network, hash

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2009-0125754 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 07 December 2009 See paragraphs [0030]-[0041], [0069], claims 1, 6 and figure 1.	1-16
A	US 2016-0080416 A1 (PUROHIT, Sibasis) 17 March 2016 See paragraphs [0036]-[0038] and figure 1.	1-16
A	KR 10-1081433 B1 (THE INDUSTRY & ACADEMIC COOPERATION IN CHUNGNAM NATIONAL UNIVERSITY) 09 November 2011 See paragraphs [0062]-[0064] and figure 5b.	1-16
A	KR 10-2009-0052638 A (SAMSUNG ELECTRONICS CO., LTD.) 26 May 2009 See paragraphs [0040]-[0046] and figure 9b.	1-16
A	US 2014-0022997 A1 (XUE, Tao et al.) 23 January 2014 See claims 5-6 and figure 3.	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 OCTOBER 2018 (17.10.2018)	**18 OCTOBER 2018 (18.10.2018)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2018/002348

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0125754 A	07/12/2009	AT 511295 T	15/06/2011
		BR PI0808619 A2	12/08/2014
		CA 2672696 A1	09/10/2008
		EP 2140650 A2	06/01/2010
		EP 2140650 B1	25/05/2011
		JP 2010-528496 A	19/08/2010
		JP 4683383 B2	18/05/2011
		TW 200849888 A	16/12/2008
		US 2008-0244739 A1	02/10/2008
		US 8695089 B2	08/04/2014
		WO 2008-119672 A2	09/10/2008
		WO 2008-119672 A3	22/01/2009
		WO 2008-119672 A4	26/03/2009
US 2016-0080416 A1	17/03/2016	US 9491196 B2	08/11/2016
KR 10-1081433 B1	09/11/2011	None	
KR 10-2009-0052638 A	26/05/2009	KR 10-1445188 B1	01/10/2014
		US 2009-0133122 A1	21/05/2009
		US 8136159 B2	13/03/2012
US 2014-0022997 A1	23/01/2014	CN 102196481 A	21/09/2011
		EP 2680636 A1	01/01/2014
		EP 2680636 A4	15/04/2015
		EP 2680636 B1	17/01/2018
		US 9161255 B2	13/10/2015
		WO 2012-167644 A1	13/12/2012

국 제 조 사 보 고 서

국제출원번호
PCT/KR2018/002348

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 12/26(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 12/26; H04L 12/18; H04L 12/22; H04L 12/28; H04L 29/06; H04W 24/10

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 패킷 무결성 검증, 경로, 자식 노드, 센서 네트워크, 해시(hash)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2009-0125754 A (인터내셔널 비지네스 머신즈 코포레이션) 2009.12.07 단락 [0030]-[0041], [0069], 청구항 1, 6 및 도면 1 참조.	1-16
A	US 2016-0080416 A1 (SIBASIS PUROHIT) 2016.03.17 단락 [0036]-[0038] 및 도면 1 참조.	1-16
A	KR 10-1081433 B1 (충남대학교산학협력단) 2011.11.09 단락 [0062]-[0064] 및 도면 5b 참조.	1-16
A	KR 10-2009-0052638 A (삼성전자주식회사) 2009.05.26 단락 [0040]-[0046] 및 도면 9b 참조.	1-16
A	US 2014-0022997 A1 (TAO XUE 등) 2014.01.23 청구항 5-6 및 도면 3 참조.	1-16

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2018년 10월 17일 (17.10.2018)	2018년 10월 18일 (18.10.2018)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
김성우
전화번호 +82-42-481-3348

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2018/002348

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0125754 A	2009/12/07	AT 511295 T	2011/06/15
		BR PI0808619 A2	2014/08/12
		CA 2672696 A1	2008/10/09
		EP 2140650 A2	2010/01/06
		EP 2140650 B1	2011/05/25
		JP 2010-528496 A	2010/08/19
		JP 4683383 B2	2011/05/18
		TW 200849888 A	2008/12/16
		US 2008-0244739 A1	2008/10/02
		US 8695089 B2	2014/04/08
		WO 2008-119672 A2	2008/10/09
		WO 2008-119672 A3	2009/01/22
		WO 2008-119672 A4	2009/03/26
US 2016-0080416 A1	2016/03/17	US 9491196 B2	2016/11/08
KR 10-1081433 B1	2011/11/09	없음	
KR 10-2009-0052638 A	2009/05/26	KR 10-1445188 B1	2014/10/01
		US 2009-0133122 A1	2009/05/21
		US 8136159 B2	2012/03/13
US 2014-0022997 A1	2014/01/23	CN 102196481 A	2011/09/21
		EP 2680636 A1	2014/01/01
		EP 2680636 A4	2015/04/15
		EP 2680636 B1	2018/01/17
		US 9161255 B2	2015/10/13
		WO 2012-167644 A1	2012/12/13