

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020년 1월 9일 (09.01.2020)



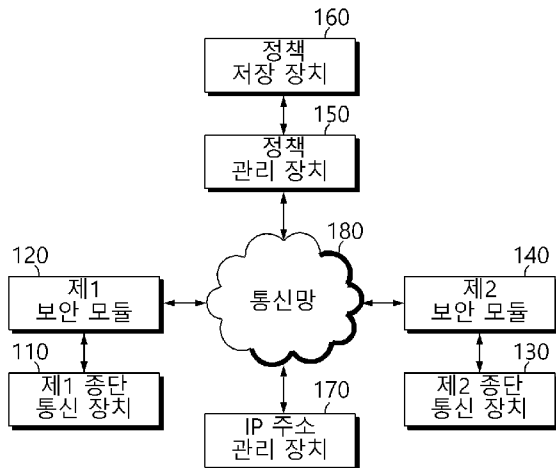
(10) 국제공개번호
WO 2020/009369 A1

- (51) 국제특허분류:
H04L 29/06 (2006.01)
- (21) 국제출원번호: PCT/KR2019/007744
- (22) 국제출원일: 2019년 6월 26일 (26.06.2019)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2018-0077305 2018년 7월 3일 (03.07.2018) KR
- (71) 출원인: 주식회사 케이티 (KT CORPORATION) [KR/KR]; 13606 경기도 성남시 분당구 불정로 90, Gyeonggi-do (KR).
- (72) 발명자: 김형주 (KIM, Hyung-Joo); 06320 서울시 강남구 개포로 303, 104동 902호, Seoul (KR). 김경남 (KIM, Kyung-Nam); 16068 경기도 의왕시 왕곡로 56, 101동 401호, Gyeonggi-do (KR). 박경원 (PARK, Kyung-Won); 04576 경기도 광주시 고불로 33, 101동 1903호, Gyeonggi-do (KR). 강혜진 (KANG, Hye-Jin); 15836 경기도 군포시 번영로 550번길 6, 125동 1002호, Gyeonggi-do (KR).

- (74) 대리인: 특허법인 필앤온지 (PHIL & ONZI INT'L PATENT & LAW FIRM); 06643 서울시 서초구 서초중앙로 36, 3층, 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 국내 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: DEVICE AND METHOD FOR PROVIDING SECURITY TO END-TO-END COMMUNICATION

(54) 발명의 명칭: 종단 간 통신에 보안을 제공하기 위한 장치 및 방법



- 110 ... First end-to-end communication device
120 ... First security module
130 ... Second end-to-end communication device
140 ... Second security module
150 ... Policy management device
160 ... Policy storage device
170 ... IP address management device
180 ... Communication network

(57) Abstract: A security device communicably connected to one end-to-end communication device so as to provide security to end-to-end communication according to an aspect: receives a packet including a destination IP address; requests and receives a first identifier corresponding to the destination IP address from an IP address management device for storing matching information between the IP address and the first identifier; identifies a second identifier of the end-to-end communication device from a table that stores matching information between the second identifier and unique information of the end-to-end communication device; transmits the first identifier, the second identifier, and a third identifier of the security device to a policy management device to inquire about a policy based on the identifiers, and receives a policy inquiry result from the policy management device; and transmits the packet to the other end-to-end communication device on the basis of the policy inquiry result.

(57) 요약서: 일 측면에 따른 종단 통신 장치에 통신 가능하게 연결되어 종단 간 통신에 보안을 제공하는 보안 장치는, 목적지 IP 주소를 포함하는 패킷을 수신하고, IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로 상기 목적지 IP 주소에 대응하는 제 1 식별자를 요청하여 수신하며, 상기 종단 통신 장치의 고유 정보와 제 2 식별자의 매칭 정보를 저장하는 테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하고, 상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를 정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책 관리 장치로부터 정책 조회 결과를 수신하며, 상기 정책 조회 결과에 기초하여 상기 패킷을 다른 종단 통신 장치로 전송한다.

(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: 종단 간 통신에 보안을 제공하기 위한 장치 및 방법 기술분야

- [1] 본 출원은 2018년 07월 03일에 출원된 한국 특허 출원번호 제10-2018-0077305호에 대한 우선권주장출원으로서, 해당 출원의 명세서 및 도면에 개시된 모든 내용은 인용에 의해 본 출원에 원용된다.
- [2] 본 발명은 IoT(Internet of Things) 기술에 관한 것으로서, 보다 구체적으로 IoT 단말과 IoT 서비스 서버 등과 같은 종단 통신 장치 간의 통신에 보안을 제공하기 위한 장치 및 방법에 관한 것이다.

배경기술

- [3] 인터넷은 인간이 정보를 생성하고 소비하는 인간 중심의 네트워크에서, 사물 등 분산된 구성 요소들 간에 정보를 주고받아 처리하는 IoT(Internet of Things, 사물인터넷) 네트워크로 진화하고 있다. IoT(Internet of Things)란, 통신 가능한 모든 사물들을 네트워크에 연결하여 상호 통신 수행이 가능한 개념을 의미한다. 시스템적으로 인지할 수 있는 모든 객체인 Things는 근거리 및 원거리 통신 기능을 탑재하고, 센서 등을 통해 데이터를 생산할 수 있다. IoT를 구현하기 위해서, 센싱 기술, 유무선 통신 및 네트워크 인프라, 서비스 인터페이스 기술 및 보안 기술과 같은 기술 요소들이 요구된다. 최근에는 사물 간의 연결을 위한 센서 네트워크(sensor network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication)등의 기술이 연구되고 있다. 이러한 IoT 서비스는 퍼블릭 네트워크(Public Network) 환경에서 제공된다. 즉 누구나 언제든지 IoT 네트워크에 접속할 수 있다. 이와 같이 IoT 서비스는 퍼블릭 네트워크 환경에서 제공되기 때문에 IoT 디바이스(IoT 단말이나 IoT 서비스 서버)는 퍼블릭 네트워크에 노출되어 보안이 취약할 수 있다.

발명의 상세한 설명

기술적 과제

- [4] 본 발명은 상술한 문제점을 해결하기 위해 제안된 것으로, IoT 단말과 IoT 서비스 서버 등과 같은 종단 통신 장치 간의 통신에서 식별자(ID : Identifier) 기반의 정책을 기초로 보안을 제공하기 위한 장치 및 방법을 제공하는 데 목적이 있다.

과제 해결 수단

- [5] 일 측면에 따른 종단 통신 장치에 통신 가능하게 연결되어 종단 간 통신에 보안을 제공하는 보안 장치는, 통신 회로; 프로세서; 및 상기 프로세서가 실행 가능한 적어도 하나의 명령어를 포함하는 메모리를 포함하고, 상기 프로세서는, 목적지 IP 주소를 포함하는 패킷을 수신하고, IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로 상기 목적지 IP 주소에 대응하는 제 1

식별자를 요청하여 수신하며, 상기 종단 통신 장치의 고유 정보와 제 2 식별자의 매칭 정보를 저장하는 테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하고, 상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를 정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책 관리 장치로부터 정책 조회 결과를 수신하며, 상기 정책 조회 결과에 기초하여 상기 패킷을 다른 종단 통신 장치로 전송한다.

- [6] 상기 프로세서는, 상기 정책 관리 장치로 토큰 시드를 요청하여 수신하고, 수신된 토큰 시드를 이용하여 토큰을 생성하며, 상기 패킷에 상기 토큰을 삽입하여 전송할 수 있다.
- [7] 상기 프로세서는, 토큰 시드를 요청시, 상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자를 전송할 수 있다.
- [8] 상기 프로세서는, nonce(Nonce), 상기 패킷의 페이로드, 타임스탬프, 상기 제 2 식별자, 상기 토큰 시드를 이용하여 토큰을 생성할 수 있다.
- [9] 상기 프로세서는, 상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자와, 상기 정책 관리 장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결 정보 간의 비교 결과에 따른 정책 조회 결과를 상기 정책 관리 장치로부터 수신할 수 있다.
- [10] 상기 제 1 식별자는, 상기 다른 종단 통신 장치에 통신 가능하게 연결된 다른 보안 장치의 식별자일 수 있다.
- [11] 상기 정책 관리 장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결 정보는, 상기 보안 장치의 식별자와, 상기 보안 장치에 통신 가능하게 연결된 통신 계층상 그 하위의 종단 통신 장치의 식별자, 그리고 그 하위의 종단 통신 장치와 종단 통신이 허용된 다른 종단 통신 장치에 통신 가능하게 연결된 통신 계층상 그 상위의 다른 보안 장치의 식별자로 이루어질 수 있다.
- [12] 상기 프로세서는, 상기 종단 통신 장치에 상기 보안 장치가 최초에 통신 가능하게 연결될 때 상기 보안 장치의 식별자와 상기 종단 통신 장치의 고유 정보를 상기 정책 관리 장치로 전송하여 식별자 기반의 정책 설정을 요청할 수 있다.
- [13] 상기 IP 주소 관리 장치에 저장되는 IP 주소 및 제 1 식별자 간의 매칭 정보는, 상기 정책 관리 장치에서 식별자 기반의 정책이 설정될 때 상기 정책 관리 장치로부터 수신되어 저장될 수 있다.
- [14] 다른 측면에 따른 종단 통신 장치에 통신 가능하게 연결되어 종단 간 통신에 보안을 제공하는 보안 장치는, 통신 회로; 프로세서; 및 상기 프로세서가 실행 가능한 적어도 하나의 명령어를 포함하는 메모리를 포함하고, 상기 프로세서는, 출발지 IP 주소를 포함하는 패킷을 수신하고, IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로 상기 출발지 IP 주소에 대응하는 제 1 식별자를 요청하여 수신하며, 상기 종단 통신 장치의 고유 정보와 제 2 식별자의

매칭 정보를 저장하는 테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하고, 상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를 정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책 관리 장치로부터 정책 조회 결과를 수신하며, 상기 정책 조회 결과에 기초하여 상기 패킷을 상기 종단 통신 장치로 전송한다.

- [15] 상기 패킷은, 상기 패킷을 전송한 측에서 삽입한 토큰을 포함하고, 상기 프로세서는, 상기 정책 관리 장치로 상기 패킷을 전송한 측에서 사용한 토큰 시드를 요청하여 수신하고, 수신된 토큰 시드를 이용하여 상기 토큰을 검증하며, 토큰 검증 성공시에 상기 패킷에 삽입된 상기 토큰을 제거할 수 있다.
- [16] 상기 프로세서는, 토큰 시드를 요청시, 상기 토큰에 평문으로 포함된 상기 패킷을 전송한 종단 통신 장치의 식별자와, 상기 제 1 식별자와, 상기 제 3 식별자를 상기 정책 관리 장치로 전송할 수 있다.
- [17] 상기 프로세서는, 상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자와, 상기 정책 관리 장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결 정보 간의 비교 결과에 따른 정책 조회 결과를 상기 정책 관리 장치로부터 수신할 수 있다.
- [18] 상기 제 1 식별자는, 상기 패킷을 전송한 종단 통신 장치에 통신 가능하게 연결된 다른 보안 장치의 식별자일 수 있다.
- [19] 또 다른 측면에 따른 종단 통신 장치에 통신 가능하게 연결된 보안 장치에서 종단 간 통신에 보안을 제공하는 방법은, 목적지 IP 주소를 포함하는 패킷을 수신하는 단계; IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로 상기 목적지 IP 주소에 대응하는 제 1 식별자를 요청하여 수신하는 단계; 상기 종단 통신 장치의 고유 정보와 제 2 식별자의 매칭 정보를 저장하는 테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하는 단계; 상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를 정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책 관리 장치로부터 정책 조회 결과를 수신하는 단계; 및 상기 정책 조회 결과에 기초하여 상기 패킷을 다른 종단 통신 장치로 전송하는 단계를 포함한다.
- [20] 또 다른 측면에 따른 종단 통신 장치에 통신 가능하게 연결된 보안 장치에서 종단 간 통신에 보안을 제공하는 방법은, 출발지 IP 주소를 포함하는 패킷을 수신하는 단계; IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로 상기 출발지 IP 주소에 대응하는 제 1 식별자를 요청하여 수신하는 단계; 상기 종단 통신 장치의 고유 정보와 제 2 식별자의 매칭 정보를 저장하는 테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하는 단계; 상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를 정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책 관리 장치로부터 정책 조회 결과를 수신하는 단계; 및 상기 정책 조회 결과에 기초하여 상기 패킷을 상기 종단 통신 장치로 전송하는 단계를 포함한다.

발명의 효과

- [21] 일 실시예에서, 네트워크 구조에 따라 변동성이 높은 IP 주소 기반의 정책을 탈피하여 식별자(ID : Identifier) 기반 정책을 이용함으로써 퍼블릭 네트워크를 통한 IoT 서비스의 보안을 높인다.
- [22] 일 실시예에서, 보안 모듈을 기준으로 한 식별자 기반의 양방향 연결 정보를 정책으로서 기록함으로써 퍼블릭 네트워크를 통한 종단 간(End-To-End) 통신에서 각 종단의 보안 모듈은 그 하위의 종단 통신 장치와 상대방 종단의 보안 모듈만 식별하면 된다. 따라서 종단 통신 장치의 퍼블릭 네트워크를 통한 노출을 최소화함으로써 보안을 강화한다.
- [23] 일 실시예에서, 종단 통신 장치에 연결되는 보안 모듈에서 송수신되는 패킷에 토큰을 삽입하고 또는 삽입된 토큰을 검증함으로써 종단 통신 장치로 악성 패킷이 수신되는 것을 차단하여 종단 통신 장치에 대한 해킹을 차단할 수 있다.
- [24] 일 실시예에서, 종단 통신 장치에 보안 모듈을 통신 가능하게 연결하면 종단 통신 장치에 식별자(ID : Identifier)를 할당하고 식별자 기반 정책을 자동으로 설정함으로써 레거시 시스템의 변화 없이 모든 IoT 서비스에 보안을 제공할 수 있다.

도면의 간단한 설명

- [25] 도 1은 본 발명의 일 실시예에 따른 종단(End-to-End) 간 통신 시스템을 나타낸 도면이다.
- [26] 도 2는 도 1의 제 1 보안 모듈의 블록도이다.
- [27] 도 3은 도 1의 제 2 보안 모듈의 블록도이다.
- [28] 도 4는 도 1의 통신 시스템에서 제 1 종단 통신 장치에서 제 2 종단 통신 장치로 패킷을 전송하는 방법의 흐름도이다.
- [29] 도 5는 도 1의 통신 시스템에서 제 1 종단 통신 장치로부터 전송된 패킷을 제 2 종단 통신 장치에서 수신하는 방법의 흐름도이다.
- [30] 도 6은 본 발명의 일 실시예에 따른 도 1의 정책 관리 장치의 블록도이다.
- [31] 도 7은 도 1의 종단(End-to-End) 간 통신 시스템에서 정책 관리 장치의 동작을 설명하는 흐름도이다.
- [32] 도 8은 도 1의 종단 간 통신 시스템의 실시예로서 IoT 단말과 IoT 서비스 서버 간 통신을 나타낸 도면이다.
- [33] 도 9는 도 8의 시스템에서 IoT 서비스 서버와 제 2 보안 모듈 간의 ID 연결 관계 정보를 생성하는 방법을 설명하는 흐름도이다.
- [34] 도 10은 도 8의 시스템에서 IoT 단말과 IoT 서비스 서버 간의 연결 정책을 설정하는 방법을 설명하는 흐름도이다.

발명의 실시를 위한 형태

- [35] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서

통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일 실시예를 상세히 설명하기로 한다.

- [36] 도 1은 본 발명의 일 실시예에 따른 종단(End-to-End) 간 통신 시스템을 나타낸 도면이다. 도 1을 참조하면, 본 실시예에 따른 종단 간 통신 시스템은, 종단 통신 장치들(110, 130), 보안 모듈들(120, 140), 정책 관리 장치(150), 정책 저장 장치(160) 및 IP 주소 관리 장치(170)를 포함하고 이들은 통신망(180)을 통해 연결된다.
- [37] 종단 통신 장치들(110, 130)은 통신 경로 상의 끝에 존재하는 통신 장치로서, 예를 들어, 가스 센서, 화재 감지 센서, 카메라, 인공지능 스피커 등의 IoT 단말이나, 이러한 IoT 단말과 통신하여 IoT 서비스를 제공하는 IoT 서비스 서버를 포함한다. IoT 단말은 메모리와 프로세서 및 통신 회로 등을 포함하여 IoT 서비스 서버와 통신할 수 있고, 또는 다른 IoT 단말과 P2P 통신을 할 수 있다. IoT 서비스 서버는 IoT 단말과 연결되어 IoT 단말로부터 주기적으로 상태 정보를 수신하고 또한 IoT 단말의 펌웨어를 업데이트하며 IoT 단말로 콘텐츠 스트리밍 등의 서비스를 제공할 수 있다.
- [38] 보안 모듈들(120, 140)은 종단 통신 장치들(110, 130)에 통신 가능하게 연결되어 종단 통신 장치(110, 130)를 통신망(180)을 통한 외부 공격으로부터 보호한다. 보안 모듈들(120, 140)은 통신 계층상 종단 통신 장치들(110, 130)의 상위 계층에 위치한다. 보안 모듈들(120, 140)은 물리적인 어댑터 형태로 제작되어 종단 통신 장치(110, 130)에 물리적으로 연결될 수 있다. 이 경우, 보안 모듈들(120, 140)은 메모리 및 프로세서 그리고 통신 회로를 포함할 수 있다. 또는 보안 모듈들(120, 140)은 소프트웨어로 제작되어 종단 통신 장치들(110, 130)의 메모리에 저장되어 실행될 수 있다. 보안 모듈들(120, 140)은 자체 저장소에 다른 보안 모듈과 구별될 수 있는 임의의 식별자(ID : Identifier, 이하에서 ID라 함)가 부여되어 저장된다.
- [39] 보안 모듈들(120, 140)은, 종단 통신 장치들(110, 130)로부터 수신된 패킷을 외부로 전송할 때, 정책 저장 장치(160)로 정책을 질의하고, 정책 조회 결과에 따라 패킷의 외부로의 전송 여부를 결정한다. 이때 정책은 식별자(ID) 기반의 정책으로서, 보안 모듈(120, 140)을 기준으로 한 양방향 연결 정보이다. 또한, 보안 모듈들(120, 140)은, 외부로부터 종단 통신 장치들(110, 130)로 향하는 패킷이 수신될 때, 마찬가지로 정책 저장 장치(160)로 정책을 질의하고, 정책 조회 결과에 따라 패킷의 내부로의 전송 여부를 결정한다. 이를 위해 보안 모듈들(120, 140)은, 종단 통신 장치들(110, 130)에 최초로 통신 가능하게 연결될 때, 자신의 ID와 종단 통신 장치들(110, 130)의 고유 정보, 예를 들어 IP 주소 또는 MAC 주소를 정책 관리 장치(150)로 전송하여 종단 통신 장치들(110, 130) 간의 연결 정책이 설정되도록 한다.

- [40] 보안 모듈(120, 140)은, 종단 통신 장치(110, 130)로부터 수신된 패킷을 외부로 전송할 때, 정책 저장 장치(160)로 토큰 시드를 요청하고 정책 저장 장치(160)로부터 수신된 토큰 시드를 이용하여 생성한 토큰을 패킷에 삽입하여 전송한다. 또한, 보안 모듈들(120, 140)은, 외부로부터 종단 통신 장치들(110, 130)로 향하는 패킷이 수신될 때, 정책 저장 장치(160)로 패킷을 전송한 측에서 사용한 토큰 시드를 요청하고, 정책 저장 장치(160)로부터 수신된 토큰 시드를 이용하여 패킷에 포함된 토큰을 검증한다. 보안 모듈들(120, 140)은, 토큰 검증에 성공시에 외부로부터 수신된 패킷에서 토큰을 제거하여 내부의 종단 통신 장치(110, 130)로 전달한다.
- [41] 정책 관리 장치(150)는, ID 기반의 종단 통신 연결 정책을 정책 저장 장치(160)에 저장한다. 여기서 ID 기반의 종단 통신 연결 정책은 보안 모듈(120, 140)을 기준으로 한 ID 기반의 양방향 연결 정보를 포함한다. 예를 들어, 상기 제 1 보안 모듈(120)을 기준으로 한 ID 기반의 양방향 연결 정보는, 제 1 종단 통신 장치(110)의 ID, 제 1 보안 모듈(120)의 ID 그리고 제 2 보안 모듈(140)의 ID로 이루어진 연결 정보이다. 그리고 제 2 보안 모듈(140)을 기준으로 한 ID 기반의 양방향 연결 정보는, 제 2 종단 통신 장치(130)의 ID, 제 2 보안 모듈(140)의 ID, 제 1 보안 모듈(120)의 ID로 이루어진 연결 정보이다. 정책 관리 장치(150)는, 관리자로부터 상기 ID 기반의 종단 통신 연결 정책을 입력받아 정책 저장 장치(160)에 저장할 수 있다.
- [42] 또는, 정책 관리 장치(150)는, 상기 ID 기반의 종단 통신 연결 정책을 스스로 설정하여 정책 저장 장치(160)에 저장할 수 있다. 정책 관리 장치(150)는, 종단 통신 장치(110, 130)에 보안 모듈(120, 140)이 통신 가능하게 연결되어 동작할 때, 보안 모듈(120, 140)로부터 자신의 ID와 보안 모듈(120, 140)에 연결된 종단 통신 장치(110, 130)의 고유 정보, 예를 들어, IP 주소나 MAC 주소를 수신한다. 정책 관리 장치(150)는, ID가 없는 종단 통신 장치(110, 130)에 ID를 부여한 후 종단 통신 장치(110, 130)와 보안 모듈(120, 140) 간의 ID 연결 관계 정보를 생성한다. 정책 관리 장치(150)는, 서로 동일한 서비스 그룹에 속하는 종단 통신 장치들(110, 130)을 확인하고, 이들의 보안 모듈(120, 140)들과의 ID 연결 관계 정보를 조합하여 종단 통신 장치들(110, 130) 간의 ID 기반의 전체 경로를 조합한다. 그리고 정책 관리 장치(150)는 전체 경로에서 보안 모듈(120, 140)을 기준으로 한 양방향 연결 정보를 생성하여 정책 저장 장치(160)에 저장한다.
- [43] 정책 관리 장치(150)는, 상기 ID 기반의 종단 통신 연결 정책을 설정하면서, 종단 통신 장치(110, 130)의 IP 주소와 보안 모듈(120, 140)의 ID 간의 매칭 정보를 IP 주소 관리 장치(170)에 전송하여 저장할 수 있다. 예를 들어, 정책 관리 장치(150)는, 제 1 종단 통신 장치(110)의 IP 주소와 제 1 보안 모듈(120)의 ID 간의 매칭 정보와, 제 2 종단 통신 장치(130)의 IP 주소와 제 2 보안 모듈(140)의 ID 간의 매칭 정보를 IP 주소 관리 장치(170)에 저장한다.
- [44] 또한, 정책 관리 장치(150)는, 상기 ID 기반의 종단 통신 연결 정책을

설정하면서, 보안 모듈(120, 140)로 그 하위의 종단 통신 장치(110, 130)에 할당한 ID를 전송하여, 보안 모듈(120, 140)이 그 하위의 종단 통신 장치(110, 130)의 ID와 고유 정보(예, MAC 주소, IP 주소)의 매칭 정보를 저장하고 관리하도록 한다. 여기서 그 매칭 정보로서 MAC 테이블을 예로 든다.

- [45] 정책 저장 장치(160)는 정책 관리 장치(150)에서 생성된 ID 기반의 종단 통신 연결 정책을 수신하여 저장한다. ID 기반의 종단 통신 연결 정책은 보안 모듈(120, 140)을 기준으로 한 ID 기반의 양방향 연결 정보를 포함한다. 정책 저장 장치(160)는 블록체인 네트워크를 구성하는 노드들을 포함한다. 블록체인 네트워크를 구성하는 노드들은 주기적으로 블록을 생성하여 트랜잭션을 기록하여 저장하는데, 본 발명의 실시예에서 트랜잭션은 상기 ID 기반의 종단 통신 연결 정책을 포함한다. 블록체인 네트워크를 구성하는 노드들에서 생성되는 블록들은 체인처럼 연결된 상태로 만들어지며, 각 노드들은 동일한 블록을 공유하고 있어, 블록에 저장된 트랜잭션을 위조하려면 노드들의 상당수를 해킹해야만 한다. 또한 블록에 트랜잭션이 일정 이상 기록되면 노드들은 서로 간의 합의 과정을 거쳐 트랜잭션들이 서로 동일하게 축적되도록 한다. 또한 정책 저장 장치(160)는 패킷을 보내는 송신자 측으로부터 수신되는 ID들의 쌍과 토큰 시드 그리고 송신자 측의 공개키를 매칭하여 저장하고, 패킷을 수신한 수신자 측으로부터 토큰 시드 요청이 수신되면 수신자 측으로부터 수신되는 ID들의 쌍과 기 저장된 ID들의 쌍을 비교하여 일치할 경우 기 저장된 ID들의 쌍에 대응하여 매칭된 토큰 시드 및 공개키를 회신한다.
- [46] IP 주소 관리 장치(170)는, 상술한 바와 같이, 종단 통신 장치(110, 130)의 IP 주소와 보안 모듈(120, 140)의 ID 간의 매칭 정보를 저장한다. 관리자로부터 입력받아 저장할 수 있고, 상술한 바와 같이, 정책 관리 장치(150)로부터 수신하여 저장할 수 있다. IP 주소 관리 장치(170)는, 정책 저장 장치(160)와 마찬가지로 블록체인 네트워크를 구성하는 노드들을 포함할 수 있다. IP 주소 관리 장치(170)는 보안 모듈(120, 140)로부터 IP 주소를 수신하면 그 수신된 IP 주소에 대응하는 ID를 회신한다.
- [47] 도 1을 참조한 실시예에서는 IP 주소 관리 장치(170)와 정책 관리 장치(150)를 구분하여 설명하였으나 여기에 제한되는 것은 아니며 IP 주소 관리 장치(170)는 정책 관리 장치(150)의 하나의 모듈로서 구현되어 통합될 수 있다.
- [48] 도 2는 도 1의 제 1 보안 모듈(120)의 블록도이다. 도 2를 참조하면, 제1 보안 모듈(120)은 수신부(210), 식별자 확인부(220), MAC 테이블(230), 정책 조회부(240), 토큰 생성부(250) 및 전송부(260)를 포함한다. 이들은 소프트웨어로 구현되어 제 1 보안 모듈(120)의 메모리에 저장되어 프로세서에 의해 실행될 수 있고, 또는 제 1 종단 통신 장치(110)의 메모리에 저장되어 제 1 종단 통신 장치(110)의 프로세서에 의해 실행될 수도 있다.
- [49] 수신부(210)는, 제 1 종단 통신 장치(110)로부터 제 2 종단 통신 장치(130)로 향하는 패킷을 수신한다. 이 패킷에는 목적지 IP 주소로서 제 2 종단 통신

장치(130)의 공인 IP 주소를 포함한다.

- [50] 식별자 확인부(220)는, 상기 패킷에 포함된 목적지 IP 주소를 IP 주소 관리 장치(170)로 전송하여 그 목적지 IP 주소에 대응하는 제 2 보안 모듈(140)의 ID를 요청한다. IP 주소 관리 장치(170)에는 제 2 종단 통신 장치(130)의 IP 주소와 제 2 보안 모듈(140)의 ID가 매칭되어 저장되어 있으므로, 식별자 확인부(220)는 제 2 보안 모듈(140)의 ID를 수신한다. 또한, 식별자 확인부(220)는, 출발지인 제 1 종단 통신 장치(110)의 고유 정보, 예를 들어 MAC 주소에 대응하는 ID를 MAC 테이블(230)에서 확인한다. 따라서, 식별자 확인부(220)는, 출발지인 제 1 종단 통신 장치(110)의 ID와, 목적지 측인 제 2 보안 모듈(140)의 ID를 확보할 수 있다. 한편, 식별자 확인부(220)는, 제 1 보안 모듈(120)의 ID를 자체 메모리 등에서 확인할 수 있다.
- [51] 정책 조회부(240)는, 식별자 확인부(220)에서 확인된 제 1 종단 통신 장치(110)의 ID와, 제 1 보안 모듈(120)의 ID와, 제 2 보안 모듈(140)의 ID의 쌍을, 정책 관리 장치(150)로 전송하여 정책을 질의하고, 정책 관리 장치(150)로부터 정책 질의에 대한 정책 조회 결과를 수신한다. 정책 저장 장치(160)에는 보안 모듈(120, 140)을 기준으로 한 양방향 연결 정보가 저장되어 있다. 본 실시예에서, 제 1 보안 모듈(120)을 기준으로 한 양방향 연결 정보는, 제 1 종단 통신 장치(110)의 ID와, 제 1 보안 모듈(120)의 ID와, 제 2 보안 모듈(140)의 ID의 쌍이므로, 정책 조회부(240)는 통신 연결 가능한 정책 조회 결과를 수신한다.
- [52] 토큰 생성부(250)는, 패킷에 삽입할 토큰을 생성한다. 먼저, 토큰 생성부(250)는, 정책 관리 장치(150)로 상기 정책 조회부(240)에서 정책 질의를 할 때 사용한 ID의 쌍과 동일한 ID의 쌍을 정책 관리 장치(150)로 전송하여 토큰 시드를 요청하고, 정책 관리 장치(150)로부터 토큰 시드를 수신한다. 토큰 생성부(250)는, 토큰의 재사용 방지를 위한 랜덤 값인 넌스(Nonce)와 타임스탬프(Timestamp)를 생성한 후, 다음과 같이 토큰을 생성한다. 토큰은, 일정 주기 내에서, 또는 일정 사용 횟수 범위 내에서만 유효하도록 설정될 수 있다.
- [53] $\text{토큰(Token)} = \text{sign}(\text{hmac}(\text{seed xor Nonce, Payload}) \parallel \text{Nonce} \parallel \text{Timestamp} \parallel \text{ID})$
- [54] 여기서 $\text{hmac}(\text{seed xor Nonce, Payload})$ 는 패킷의 페이로드를 해시한 값을 토큰 시드(seed)와 Nonce를 xor한 값으로 암호화한 것을 의미하며, $\parallel$ 는 평문으로 이어붙이기를 의미한다. 그리고 ID는 제 1 종단 통신 장치(110)의 ID이고, sign은 제 1 보안 모듈(120)의 개인키로 서명하는 것을 의미한다.
- [55] 전송부(260)는 상기 토큰 생성부(250)에서 생성된 토큰을 패킷에 삽입하여 통신망(180)을 통해 제 2 종단 통신 장치(130) 측으로 전송한다.
- [56] 도 3은 도 1의 제 2 보안 모듈(140)의 블록도이다. 도 3을 참조하면, 제2 보안 모듈(140)은 수신부(310), 식별자 확인부(320), MAC 테이블(330), 토큰 검증부(340), 정책 조회부(350) 및 전송부(360)를 포함한다. 이들은 소프트웨어로 구현되어 제 2 보안 모듈(140)의 메모리에 저장되어 프로세서에 의해 실행될 수 있고, 또는 제 2 종단 통신 장치(130)의 메모리에 저장되어 제 2 종단 통신

장치(130)의 프로세서에 의해 실행될 수도 있다.

- [57] 수신부(310)는, 제 1 종단 통신 장치(110) 측의 제 1 보안 모듈(120)로부터 토큰이 삽입된 패킷을 수신한다. 패킷에는 출발지 IP 주소로서 제 1 종단 통신 장치(110)의 IP 주소와 목적지 IP 주소로서 제 2 종단 통신 장치(130)의 IP 주소가 포함된다.
- [58] 식별자 확인부(320)는, 상기 패킷에 포함된 출발지 IP 주소를 IP 주소 관리 장치(170)로 전송하여 그 출발지 IP 주소에 대응하는 제 1 보안 모듈(120)의 ID를 요청한다. IP 주소 관리 장치(170)에는 제 1 종단 통신 장치(110)의 IP 주소와 제 1 보안 모듈(120)의 ID가 매칭되어 저장되어 있으므로, 식별자 확인부(320)는 제 1 보안 모듈(120)의 ID를 수신한다.
- [59] 또한, 식별자 확인부(320)는, 목적지인 제 2 종단 통신 장치(130)의 고유 정보, 예를 들어 MAC 주소에 대응하는 ID를 MAC 테이블(330)에서 확인한다. 따라서, 식별자 확인부(320)는, 목적지인 제 2 종단 통신 장치(130)의 ID와, 출발지 측인 제 1 보안 모듈(120)의 ID를 확보할 수 있다. 한편, 식별자 확인부(320)는, 제 2 보안 모듈(140)의 ID는 자체 메모리 등에서 확인할 수 있다.
- [60] 토큰 검증부(340)는, 상기 수신부(310)에서 수신한 패킷에 삽입되어 있는 토큰을 검증한다. 먼저 토큰 검증부(340)는, 정책 관리 장치(150)로 송신 측에서 사용한 토큰 시드를 요청한다. 토큰 검증부(340)는 상기 수신된 패킷에 삽입되어 있는 토큰에서 평문으로 삽입되어 있는 제 1 종단 통신 장치(110)의 ID를 추출하고, 그 제 1 종단 통신 장치(110)의 ID, 상기 식별자 확인부(320)에서 확인한 제 1 보안 모듈(120)의 ID, 그리고 제 2 보안 모듈(140)의 ID의 쌍을 정책 관리 장치(150)로 전송하여 토큰 시드를 요청한다. 송신측에서 사용한 ID의 쌍으로 토큰 시드를 요청하므로, 토큰 검증부(340)는 정책 관리 장치(150)로부터 송신측에서 사용한 동일한 토큰 시드를 수신한다. 동시에 토큰 검증부(340)는 정책 관리 장치(150)로부터 제 1 보안 모듈(120)의 공개키를 함께 수신한다. 토큰 검증부(340)는 토큰에 평문으로 삽입되어 있는 넌스(Nonce), 타임스탬프(Timestamp) 그리고 제 1 종단 통신 장치(110)의 ID와, 수신된 토큰 시드를 이용하여 토큰을 생성하여 상기 패킷에 삽입되어 있는 토큰과 동일한지 확인한다. 또한 토큰 검증부(340)는 상기 수신된 제 1 보안 모듈(120)의 공개키로 토큰의 서명을 검증한다. 토큰 검증부(340)는 토큰 검증 실패시에 패킷을 폐기한다.
- [61] 정책 조회부(350)는, 상기 토큰 검증부(340)에서 토큰 검증에 성공시에, 상기 식별자 확인부(320)에서 확인한 제 1 보안 모듈(120)의 ID, 제 2 보안 모듈(140)의 ID, 그리고 제 2 종단 통신 장치(130)의 ID의 쌍을 정책 관리 장치(150)로 전송하여 정책을 질의하고, 정책 관리 장치(150)로부터 정책 질의에 대한 정책 조회 결과를 수신한다. 정책 저장 장치(160)에는 보안 모듈(120, 140)을 기준으로 한 양방향 연결 정보가 저장되어 있다. 본 실시예에서, 제 2 보안 모듈(140)을 기준으로 한 양방향 연결 정보는, 제 1 보안 모듈(120)의 ID와, 제 2 보안

모듈(140)의 ID와, 제 2 종단 통신 장치(130)의 ID의 쌍이므로, 정책 조회부(350)는 통신 연결 가능의 정책 조회 결과를 수신한다.

[62] 전송부(360)는 상기 정책 조회부(350)에서 통신 연결 가능의 정책 조회 결과가 수신되면, 패킷에 삽입되어 있는 토큰을 제거하여 제 2 종단 통신 장치(130)로 전송한다.

[63] 이상의 도 2 및 도 3에서 제 1, 2 보안 모듈(120, 140)을 구분하여 설명하였으나, 도 2 및 도 3에서 설명한 기능들은 하나의 보안 모듈에 모두 포함되는 것을 이해하여야 한다.

[64] 도 4는 도 1의 통신 시스템에서 제 1 종단 통신 장치(110)에서 제 2 종단 통신 장치(130)로 패킷을 전송하는 방법의 흐름도이다.

[65] 도 4를 참조하면, 단계 S401에서, 제 1 보안 모듈(120)은, 제 1 종단 통신 장치(110)로부터 제 2 종단 통신 장치(130)로 향하는 패킷을 수신한다. 이 패킷에는 목적지 IP 주소로서 제 2 종단 통신 장치(130)의 공인 IP 주소를 포함한다.

[66] 단계 S402에서, 제 1 보안 모듈(120)은, 상기 패킷에 포함된 목적지 IP 주소를 IP 주소 관리 장치(170)로 전송하여 그 목적지 IP 주소에 대응하는 제 2 보안 모듈(140)의 ID를 요청한다.

[67] 단계 S403에서, IP 주소 관리 장치(170)에는 제 2 종단 통신 장치(130)의 IP 주소와 제 2 보안 모듈(140)의 ID가 매칭되어 저장되어 있으므로, 제 1 보안 모듈(120)은, 제 2 보안 모듈(140)의 ID를 수신한다.

[68] 단계 S404에서, 또한, 제 1 보안 모듈(120)은, 출발지인 제 1 종단 통신 장치(110)의 고유 정보, 예를 들어 MAC 주소에 대응하는 ID를 MAC 테이블(230)에서 확인한다. 따라서, 제 1 보안 모듈(120)은, 출발지인 제 1 종단 통신 장치(110)의 ID와, 목적지 측인 제 2 보안 모듈(140)의 ID를 확보할 수 있다. 한편, 제 1 보안 모듈(120)은, 자신의 ID는 자체 메모리 등에서 확인할 수 있다.

[69] 단계 S405에서, 제 1 보안 모듈(120)은, 확인된 제 1 종단 통신 장치(110)의 ID와, 제 1 보안 모듈(120)의 ID와, 제 2 보안 모듈(140)의 ID의 쌍을, 정책 관리 장치(150)로 전송하여 정책을 질의한다.

[70] 단계 S406에서, 제 1 보안 모듈(120)은 정책 관리 장치(150)로부터 정책 질의에 대한 정책 조회 결과를 수신한다. 정책 저장 장치(160)에는 보안 모듈(120, 140)을 기준으로 한 양방향 연결 정보가 저장되어 있다. 본 실시예에서, 제 1 보안 모듈(120)을 기준으로 한 양방향 연결 정보는, 제 1 종단 통신 장치(110)의 ID와, 제 1 보안 모듈(120)의 ID와, 제 2 보안 모듈(140)의 ID의 쌍이므로, 제 1 보안 모듈(120)은 통신 연결 가능의 정책 조회 결과를 수신한다.

[71] 단계 S407에서, 제 1 보안 모듈(120)은, 패킷에 삽입할 토큰을 생성하기 위해 정책 관리 장치(150)로 정책 질의를 할 때 사용한 ID의 쌍과 동일한 ID의 쌍을 정책 관리 장치(150)로 전송하여 토큰 시드를 요청한다. 단계 S408에서, 제 1 보안 모듈(120)은 정책 관리 장치(150)로부터 토큰 시드를 수신한다.

- [72] 단계 S409에서, 제 1 보안 모듈(120)은, 토큰의 재사용 방지를 위한 랜덤 값인 넌스(Nonce)와 타임스탬프(Timestamp)를 생성한 후, 다음과 같이 토큰을 생성한다.
- [73] $\text{Token} = \text{sign}(\text{hmac}(\text{seed} \text{ xor } \text{Nonce}, \text{Payload}) \parallel \text{Nonce} \parallel \text{Timestamp} \parallel \text{ID})$
- [74] 여기서 $\text{hmac}(\text{seed} \text{ xor } \text{Nonce}, \text{Payload})$ 는 패킷의 페이로드를 해시한 값을 토큰 시드(seed)와 Nonce를 xor한 값으로 암호화한 것을 의미하며, $\parallel$ 는 평문으로 이어붙이기를 의미한다. 그리고 ID는 제 1 종단 통신 장치(110)의 ID이고, sign은 제 1 보안 모듈(120)의 개인키로 서명하는 것을 의미한다.
- [75] 단계 S410에서, 제 1 보안 모듈(120)은, 상기 생성된 토큰을 패킷에 삽입하여 통신망(180)을 통해 제 2 종단 통신 장치(130) 측으로 전송한다.
- [76] 도 5는 도 1의 통신 시스템에서 제 1 종단 통신 장치(110)로부터 전송된 패킷을 제 2 종단 통신 장치(130)에서 수신하는 방법의 흐름도이다.
- [77] 단계 S501에서, 제 2 보안 모듈(140)은, 토큰이 삽입된 패킷을 수신한다. 패킷에는 출발지 IP 주소로서 제 1 종단 통신 장치(110)의 IP 주소와 목적지 IP 주소로서 제 2 종단 통신 장치(130)의 IP 주소가 포함된다.
- [78] 단계 S502에서, 제 2 보안 모듈(140)은 상기 패킷에 포함된 출발지 IP 주소를 IP 주소 관리 장치(170)로 전송하여 그 출발지 IP 주소에 대응하는 제 1 보안 모듈(120)의 ID를 요청한다. IP 주소 관리 장치(170)에는 제 1 종단 통신 장치(110)의 IP 주소와 제 1 보안 모듈(120)의 ID가 매칭되어 저장되어 있으므로, 제 2 보안 모듈(140)은 제 1 보안 모듈(120)의 ID를 수신한다.
- [79] 단계 S504에서, 제 2 보안 모듈(140)은, 목적지인 제 2 종단 통신 장치(130)의 고유 정보, 예를 들어 MAC 주소에 대응하는 ID를 MAC 테이블(330)에서 확인한다. 따라서, 제 2 보안 모듈(140)은, 목적지인 제 2 종단 통신 장치(130)의 ID와, 출발지 측인 제 1 보안 모듈(120)의 ID를 확보할 수 있다. 한편, 제 2 보안 모듈(140)은, 제 2 보안 모듈(140)의 ID는 자체 메모리 등에서 확인할 수 있다.
- [80] 단계 S505에서, 제 2 보안 모듈(140)은 패킷에 삽입되어 있는 토큰을 검증하기 위해 정책 관리 장치(150)로 송신 측에서 사용한 토큰 시드를 요청한다. 구체적으로 제 2 보안 모듈(140)은 상기 수신된 패킷에 삽입되어 있는 토큰에서 평문으로 삽입되어 있는 제 1 종단 통신 장치(110)의 ID를 추출하고, 그 제 1 종단 통신 장치(110)의 ID, 상기 제 1 보안 모듈(120)의 ID, 그리고 제 2 보안 모듈(140)의 ID의 쌍을 정책 관리 장치(150)로 전송하여 토큰 시드를 요청한다.
- [81] 단계 S506에서, 송신측에서 사용한 ID의 쌍으로 토큰 시드를 요청하므로, 제 2 보안 모듈(140)은 정책 관리 장치(150)로부터 송신측에서 사용한 동일한 토큰 시드를 수신한다. 동시에 토큰 검증부(340)는 정책 관리 장치(150)로부터 제 1 보안 모듈(120)의 공개키를 함께 수신한다.
- [82] 단계 S507에서, 제 2 보안 모듈(140)은 토큰에 평문으로 삽입되어 있는 넌스(Nonce), 타임스탬프(Timestamp) 그리고 제 1 종단 통신 장치(110)의 ID와, 수신된 토큰 시드를 이용하여 토큰을 생성하여 상기 패킷에 삽입되어 있는

토큰과 동일한지 확인한다. 또한 토큰 검증부(340)는 상기 수신된 제 1 보안 모듈(120)의 공개키로 토큰의 서명을 검증한다. 토큰 검증부(340)는 토큰 검증 실패시에 패킷을 폐기한다.

- [83] 단계 S508에서, 제 2 보안 모듈(140)은, 토큰 검증에 성공시에, 제 1 보안 모듈(120)의 ID, 제 2 보안 모듈(140)의 ID, 그리고 제 2 종단 통신 장치(130)의 ID의 쌍을 정책 관리 장치(150)로 전송하여 정책을 질의한다.
- [84] 단계 S509에서, 제 2 보안 모듈(140)은 정책 관리 장치(150)로부터 정책 질의에 대한 정책 조회 결과를 수신한다. 정책 저장 장치(160)에는 보안 모듈(120, 140)을 기준으로 한 양방향 연결 정보가 저장되어 있다. 본 실시예에서, 제 2 보안 모듈(140)을 기준으로 한 양방향 연결 정보는, 제 1 보안 모듈(120)의 ID와, 제 2 보안 모듈(140)의 ID와, 제 2 종단 통신 장치(130)의 ID의 쌍이므로, 제 2 보안 모듈(140)은 통신 연결 가능의 정책 조회 결과를 수신한다.
- [85] 단계 S510에서, 제 2 보안 모듈(140)은 통신 연결 가능의 정책 조회 결과가 수신되면, 패킷에 삽입되어 있는 토큰을 제거한다. 그리고 단계 S511에서, 제 2 보안 모듈(140)은 제 2 종단 통신 장치(130)로 토큰이 제거된 패킷을 전송한다.
- [86] 도 6은 본 발명의 일 실시예에 따른 도 1의 정책 관리 장치의 블록도이다. 정책 관리 장치(150)는 메모리, 메모리 제어기, 하나 이상의 프로세서(CPU), 주변 인터페이스, 입출력(I/O) 서브시스템, 디스플레이 장치, 입력 장치 및 통신 회로를 포함할 수 있다. 이러한 구성요소는 하나 이상의 통신 버스 또는 신호선을 통하여 통신한다. 이러한 여러 구성요소는 하나 이상의 신호 처리 및/또는 애플리케이션 전용 집적 회로(application specific integrated circuit)를 포함하여, 하드웨어, 소프트웨어 또는 하드웨어와 소프트웨어 둘의 조합으로 구현될 수 있다.
- [87] 메모리는 고속 랜덤 액세스 메모리를 포함할 수 있고, 또한 하나 이상의 자기 디스크 저장 장치, 플래시 메모리 장치와 같은 불휘발성 메모리, 또는 다른 불휘발성 반도체 메모리 장치를 포함할 수 있다. 일부 실시예에서, 메모리는 하나 이상의 프로세서로부터 멀리 떨어져 위치하는 저장 장치, 예를 들어 RF 회로와, 인터넷, 인트라넷, LAN(Local Area Network), WLAN(Wide LAN), SAN(Storage Area Network) 등, 또는 이들의 적절한 조합과 같은 통신 네트워크(도시하지 않음)를 통하여 액세스되는 네트워크 부착형(attached) 저장 장치를 더 포함할 수 있다. 프로세서 및 주변 인터페이스와 같은 장치의 다른 구성요소에 의한 메모리로의 액세스는 메모리 제어기에 의하여 제어될 수 있다.
- [88] 주변 인터페이스는 장치의 입출력 주변 장치를 프로세서 및 메모리와 연결한다. 하나 이상의 프로세서는 다양한 소프트웨어 프로그램 및/또는 메모리에 저장되어 있는 명령어 세트를 실행하여 시스템을 위한 여러 기능을 수행하고 데이터를 처리한다. 일부 실시예에서, 주변 인터페이스, 프로세서 및 메모리 제어기는 칩과 같은 단일 칩 상에서 구현될 수 있다. 일부 다른 실시예에서, 이들은 별개의 칩으로 구현될 수 있다.

- [89] I/O 서브시스템은 디스플레이 장치, 입력 장치와 같은 장치의 입출력 주변장치와 주변 인터페이스 사이에 인터페이스를 제공한다. 디스플레이 장치는 LCD(liquid crystal display) 기술 또는 LPD(light emitting polymer display) 기술을 사용할 수 있고, 이러한 디스플레이 장치는 용량형, 저항형, 적외선형 등의 터치 디스플레이일 수 있다.
- [90] 프로세서는 시스템에 연관된 동작을 수행하고 명령어들을 수행하도록 구성된 프로세서로서, 예를 들어, 메모리로부터 검색된 명령어들을 이용하여, 시스템의 컴포넌트 간의 입력 및 출력 데이터의 수신과 조작을 제어할 수 있다. 일부 실시예에서, 소프트웨어 구성요소는 운영 체제, 그래픽 모듈(명령어 세트), 본 발명을 위한 동작을 수행하기 위한 프로그램이 탑재(설치)될 수 있다. 운영 체제는, 예를 들어, 다윈(Darwin), RTXC, LINUX, UNIX, OSX, WINDOWS 또는 VxWorks, 안드로이드, iOS 등과 같은 내장 운영체제일 수 있고, 일반적인 시스템 태스크(task)(예를 들어, 메모리 관리, 저장 장치 제어, 전력 관리 등)를 제어 및 관리하는 다양한 소프트웨어 구성요소 및/또는 장치를 포함하고, 다양한 하드웨어와 소프트웨어 구성요소 사이의 통신을 촉진시킨다.
- [91] 통신 회로는 이더넷 통신 회로 및 RF 회로를 포함할 수 있다. 이더넷 통신 회로는 유선 통신을 수행하고, RF 회로는 전자파를 송수신한다. RF 회로는 전기 신호를 전자파로 또는 그 반대로 변환하며 이 전자파를 통하여 통신 네트워크, 다른 이동형 게이트웨이 및 통신 장치와 통신한다. RF 회로는 예를 들어 안테나 시스템, RF 트랜시버, 하나 이상의 증폭기, 튜너, 하나 이상의 오실레이터, 디지털 신호 처리기, CODEC 칩셋, 메모리 등을 포함하지만 이에 한정되지 않는 이러한 기능을 수행하기 위한 주지의 회로를 포함할 수 있다. RF 회로는 셀룰러 전화 네트워크, 무선 LAN 및/또는 MAN(metropolitan area network)와 같은 무선 네트워크, 그리고 근거리 무선 통신에 의하여 다른 장치와 통신할 수 있다.
- [92] 도 6에 도시된 바와 같이, 수신부(610), 식별자 관리부(620), 연결 관계 정보 DB(630), 서비스 그룹 식별부(640), 서비스 그룹 정보 DB(650), 중단 장치 관리부(660), 정책 관리부(670)를 포함한다. 수신부(610), 식별자 관리부(620), 서비스 그룹 식별부(640), 중단 장치 관리부(660) 및 정책 관리부(670)는 프로그램으로 구현되어 메모리에 저장된 후 프로세서에 의해 실행될 수 있고, 또는 하드웨어와 소프트웨어의 조합으로 구현될 수도 있다.
- [93] 수신부(610)는, 중단 통신 장치(110, 130)에 보안 모듈(120, 140)이 통신 가능하게 연결되어 동작할 때, 보안 모듈(120, 140)로부터 자신의 ID와 보안 모듈(120, 140)에 연결된 중단 통신 장치(110, 130)의 고유 정보, 예를 들어, IP 주소나 MAC 주소를 수신한다. 예를 들어, 제 1 보안 모듈(120)로부터 그의 ID와 제 1 중단 통신 장치(110)의 MAC 주소를 수신한다. 제 2 보안 모듈(140)로부터는 그의 ID와 제 2 중단 통신 장치(130)의 IP 주소를 수신한다.
- [94] 식별자 관리부(620)는, ID가 없는 중단 통신 장치(110, 130)에 ID를 부여한 후 중단 통신 장치(110, 130)와 보안 모듈(120, 140) 간의 ID 연결 관계 정보를

생성하여 연결 관계 정보 DB(630)에 저장한다. 예를 들어, 상기 수신부(610)에 제 1 보안 모듈(120)로부터 그의 ID와 제 1 종단 통신 장치(110)의 MAC 주소가 수신되었을 때, 식별자 관리부(620)는, 제 1 종단 통신 장치(110)에 임시적인 ID를 부여하고, 제 1 보안 모듈(120)의 ID와 제 1 종단 통신 장치(110)의 ID를 매칭한, 연결 관계 정보를 연결 관계 정보 DB(630)에 저장한다. 또한, 상기 수신부(610)에 제 2 보안 모듈(140)로부터 그의 ID와 제 2 종단 통신 장치(130)의 IP 주소가 수신되었을 때, 식별자 관리부(620)는, 제 2 종단 통신 장치(130)에 임시적인 ID를 부여하고, 제 2 보안 모듈(140)의 ID와 제 2 종단 통신 장치(130)의 ID를 매칭한, 연결 관계 정보를 연결 관계 정보 DB(630)에 저장한다.

- [95] 또한, 식별자 관리부(620)는 종단 통신 장치(110, 130)의 ID와 해당 종단 통신 장치(110, 130)의 고유 정보(MAC 주소, 또는 IP 주소 등)의 쌍을 해당 종단 통신 장치(110, 130)에 연결된 보안 모듈(120, 140)로 전송한다. 따라서, 제 1 보안 모듈(120)에는 제 1 종단 통신 장치(110)의 ID 및 고유 정보의 쌍이 저장되고, 제 2 보안 모듈(140)에는 제 2 종단 통신 장치(130)의 ID 및 고유 정보의 쌍이 저장된다.
- [96] 또한, 식별자 관리부(620)는 종단 통신 장치(110, 130)의 고유 정보인 IP 주소와 보안 모듈(120, 140)의 ID의 쌍을 IP 주소 관리 장치(170)로 전송한다. 즉, 제 1 종단 통신 장치(110)의 IP 주소와 제 1 보안 모듈(120)의 ID의 쌍, 그리고 제 2 종단 통신 장치(130)의 IP 주소와 제 2 보안 모듈(140)의 ID의 쌍이 IP 주소 관리 장치(170)에 전송되어 저장된다.
- [97] 서비스 그룹 식별부(640)는, 서비스 그룹 정보 DB(650)에 저장된 정보를 참조하여 보안 모듈들(120, 140)에 연결된 종단 통신 장치들(110, 130)의 서비스 그룹을 확인한다. 서비스 그룹 식별부(640)는, 수신부(610)로부터 종단 통신 장치(110, 130)의 고유 정보, 예를 들어, IP 주소나 MAC 주소를 수신하고, 그 수신된 고유 정보를 이용하여 서비스 그룹 정보 DB(650)에서 해당하는 서비스 그룹 정보를 확인한다. 서비스 그룹 정보 DB(650)에는 서비스 그룹별로 해당 서비스 그룹명, 해당 서비스 그룹에 속하는 종단 통신 장치들(110, 130)의 MAC 주소 또는 IP 주소의 목록이 저장된다. 예를 들어, 삼성전자에서 IoT 서비스를 제공한다면, IoT 서비스를 제공하는 플랫폼 서버의 IP 주소와 그 IoT 서비스를 제공하는 삼성전자에서 제조하여 판매하는 IoT 단말들의 MAC 주소가 서비스 그룹 정보 DB(650)에 저장된다.
- [98] 종단 장치 관리부(660)는, 상기 서비스 그룹 식별부(640)에서 확인한 종단 통신 장치들(110, 130)의 서비스 그룹 정보를 이용하여 종단 통신 장치들(110, 130)의 대응 관계를 확인한다. 종단 장치 관리부(660)는, 대응 관계가 확인된 종단 통신 장치들(110, 130)의 ID들을 식별자 관리부(620)로부터 수신하고 그 수신된 ID들을 매칭한 연결 관계 정보를 생성한다. 종단 장치 관리부(660)는 그 생성한 종단 통신 장치들(110, 130)의 ID 연결 관계 정보를 연결 관계 정보 DB(630)에 저장할 수 있다.

- [99] 실시예에 따라, 종단 장치 관리부(660)는, 종단 통신 장치(110, 130) 중 어느 한 종단 통신 장치(예, 110)의 서비스 그룹 정보가 서비스 그룹 식별부(640)로부터 수신되면, 식별자 관리부(620)로부터 수신된 해당 종단 통신 장치(110)의 ID를 서비스 그룹 정보 DB(650)의 해당 서비스 그룹에 매칭하여 저장한다. 그리고 종단 장치 관리부(660)는, 다른 종단 통신 장치(130)의 서비스 그룹 정보가 서비스 그룹 식별부(640)로부터 수신되면, 그 수신된 서비스 그룹 정보를 이용하여 서비스 그룹 정보 DB(650)에 종단 통신 장치(110)의 ID를 질의하여 수신한 후, 수신된 종단 통신 장치(110)의 ID와 식별자 관리부(620)로부터 수신되는 종단 통신 장치(130)의 ID와 매칭하여 종단 통신 장치(110, 130) 간의 ID 연결 관계 정보를 획득할 수 있다.
- [100] 정책 관리부(670)는, 연결 관계 정보 DB(630)에 저장된 종단 통신 장치들(110, 130)과 보안 모듈들(120, 140) 간의 ID 연결 관계 정보와, 상기 종단 장치 관리부(660)에서 확인된 종단 통신 장치들(110, 130)의 대응 관계, 구체적으로는 종단 통신 장치들(110, 130) 간의 ID 연결 관계 정보를 이용하여, 보안 모듈(120, 140)을 기준으로 한 ID 기반의 양방향 연결 정보를 생성하고 이를 정책 저장 장치(160)로 전송하여 저장한다. 구체적으로, 정책 관리부(670)는, 종단 통신 장치들(110, 130) 간의 ID 연결 관계 정보를 이용하여, 연결 관계 정보 DB(630)에서 종단 통신 장치들(110, 130)과 보안 모듈들(120, 140) 간의 ID 연결 관계 정보를 조회하고, 조회된 종단 통신 장치들(110, 130)과 보안 모듈들(120, 140) 간의 ID 연결 관계 정보를 이용하여 ID 기반의 종단 통신 장치(110, 130) 간의 전체 경로를 조합한다. 그리고 정책 관리부(670)는 상기 전체 경로에서 예를 들어, 제 1 보안 모듈(120)을 기준으로 한 양방향 연결 정보와 제 2 보안 모듈(140)을 기준으로 한 양방향 연결 정보를 각각 정책 저장 장치(160)에 전송하여 저장한다. 예를 들어, 상기 제 1 보안 모듈(120)을 기준으로 한 ID 기반의 양방향 연결 정보는, 제 1 종단 통신 장치(110)의 ID, 제 1 보안 모듈(120)의 ID 그리고 제 2 보안 모듈(140)의 ID로 이루어진 연결 정보이다. 그리고 제 2 보안 모듈(140)을 기준으로 한 ID 기반의 양방향 연결 정보는, 제 2 종단 통신 장치(130)의 ID, 제 2 보안 모듈(140)의 ID, 제 1 보안 모듈(120)의 ID로 이루어진 연결 정보이다.
- [101] 도 7은 도 1의 종단(End-to-End) 간 통신 시스템에서 정책 관리 장치(150)의 동작을 설명하는 흐름도이다.
- [102] 단계 701에서, 정책 관리 장치(150)는, 제 1 종단 통신 장치(110)의 ID와 제 1 보안 모듈(120)의 ID를 매칭한 연결 관계 정보를 생성한다. 정책 관리 장치(150)는, 제 1 보안 모듈(120)로부터 그의 ID와 제 1 종단 통신 장치(110)의 IP 주소 또는 MAC 주소가 수신되었을 때, 제 1 종단 통신 장치(110)에 임시적인 ID를 부여하고, 제 1 보안 모듈(120)의 ID와 제 1 종단 통신 장치(110)의 ID를 매칭한, 연결 관계 정보를 연결 관계 정보 DB(630)에 저장한다.
- [103] 단계 702에서, 정책 관리 장치(150)는, 제 2 종단 통신 장치(130)의 ID와 제 2

보안 모듈(140)의 ID를 매칭한 연결 관계 정보를 생성한다. 정책 관리 장치(150)는, 제 2 보안 모듈(140)로부터 그의 ID와 제 2 종단 통신 장치(130)의 IP 주소 또는 MAC 주소가 수신되었을 때, 제 2 종단 통신 장치(130)에 임시적인 ID를 부여하고, 제 2 보안 모듈(140)의 ID와 제 2 종단 통신 장치(130)의 ID를 매칭한, 연결 관계 정보를 연결 관계 정보 DB(630)에 저장한다.

- [104] 단계 S703에서, 정책 관리 장치(150)는, 제 1, 2 종단 통신 장치들(110, 130)을 포함하는 종단 통신 장치들의 서비스 그룹 정보와 제 1, 2 종단 통신 장치들(110, 130)의 고유 정보, 예를 들어 IP 주소 또는 MAC 주소에 기초하여 제 1 종단 통신 장치(110)와 상기 제 2 종단 통신 장치(130)의 대응 관계를 확인한다. 정책 관리 장치(150)는, 보안 모듈들(120, 140)로부터 수신된 종단 통신 장치(110, 130)의 고유 정보, 예를 들어, IP 주소나 MAC 주소를 이용하여 서비스 그룹 정보 DB(650)에서 해당하는 서비스 그룹 정보를 확인하여 동일한지 확인한다. 정책 관리 장치(150)는, 대응 관계가 확인된 종단 통신 장치들(110, 130) 간의 ID 연결 관계 정보를 생성한다. 실시예에 따라, 정책 관리 장치(150)는, 제 1 종단 통신 장치(110)의 IP 주소나 MAC 주소를 이용하여 서비스 그룹 정보를 확인한 후 그 서비스 그룹 정보에 제 1 종단 통신 장치(110)의 ID를 매칭하여 저장한다. 그리고 정책 관리 장치(150)는 제 2 종단 통신 장치(130)의 IP 주소나 MAC 주소를 이용하여 서비스 그룹 정보에 매칭된 제 1 종단 통신 장치(110)의 ID를 조회한 후, 종단 통신 장치들(110, 130) 간의 ID 연결 관계 정보를 생성한다.

- [105] 단계 S704에서, 정책 관리 장치(150)는, 단계 S701 및 단계 S702에서 저장한 종단 통신 장치들(110, 130)과 보안 모듈(120, 140) 간의 ID 연결 관계 정보와, 단계 S703에서 확인된 종단 통신 장치들(110, 130) 간의 대응 관계를 이용하여, 각 보안 모듈(120, 140)을 기준으로 한 ID 기반의 양방향 연결 정보를 생성하여 정책 저장 장치(160), 예를 들어 블록체인에 저장한다. 정책 관리 장치(150)는, 종단 통신 장치(110, 130) 간의 전체 경로를 조합한 후, 전체 경로에서 제 1 보안 모듈(120)을 기준으로 한 양방향 연결 정보와 제 2 보안 모듈(140)을 기준으로 한 양방향 연결 정보를 각각 정책 저장 장치(160)에 전송하여 저장한다. 예를 들어, 상기 제 1 보안 모듈(120)을 기준으로 한 ID 기반의 양방향 연결 정보는, 제 1 종단 통신 장치(110)의 ID, 제 1 보안 모듈(120)의 ID 그리고 제 2 보안 모듈(140)의 ID로 이루어진 연결 정보이다. 그리고 제 2 보안 모듈(140)을 기준으로 한 ID 기반의 양방향 연결 정보는, 제 2 종단 통신 장치(130)의 ID, 제 2 보안 모듈(140)의 ID, 제 1 보안 모듈(120)의 ID로 이루어진 연결 정보이다.

- [106] 도 8은 도 1의 종단 간 통신 시스템의 실시예로서 IoT 단말과 IoT 서비스 서버 간 통신을 나타낸 도면이다. 예를 들어, IoT 단말은, 마이크로폰과 스피커를 구비하여, 사용자로부터 음성 요청을 수신하고 이를 IoT 서비스 서버로 전송하고, IoT 서비스 서버로부터 수신되는 응답을 수신하여 출력하는, 소위 인공지능 스피커이다. IoT 서비스 서버는 인공지능 음성 어시스턴트(Voice Assistant) 서비스를 제공하는 장치로서 음성을 인식하고 분석하여 이에 대한

서비스를 제공한다. 도 8을 참조한 실시예에서 IoT 단말(810)은 도 1을 참조한 실시예에서의 제 1 종단 통신 장치(110)일 수 있고, IoT 서비스 서버(830)는, 도 1을 참조한 실시예에서의 제 2 종단 통신 장치(130)일 수 있다. 제 1 보안 모듈(120)은 IoT 단말(810)에 물리적인 어댑터 형태로 연결될 수 있고, 또는 소프트웨어로 구현되어 IoT 단말(810)에 설치되어 동작할 수 있다. 도 8에서 게이트웨이(820)는 예를 들어 공유기일 수 있다. 제 1 보안 모듈(120)에 복수의 IoT 단말(810)이 연결될 때 게이트웨이(820)는 공인 IP 주소를 할당받고 상기 복수의 IoT 단말(810)에는 사설 IP 주소를 할당한다. IoT 단말(810)은 게이트웨이(820) 및 인터넷(840)을 통해 IoT 서비스 서버(830)와 통신한다.

- [107] 도 8을 참조한 실시예에서, IoT 서비스 서버(830)에 제 2 보안 모듈(140)이 연결되면, 정책 관리 장치(150)는 IoT 서비스 서버(830)에 임시적인 ID를 부여하여 제 2 보안 모듈(140)의 ID와의 연결 관계를 설정한다. 이후 IoT 단말(810)에 제 1 보안 모듈(120)이 연결되면, 정책 관리 장치(150)는 IoT 단말(810)에 임시적인 ID를 부여하여 제 1 보안 모듈(120)의 ID와의 연결 관계를 설정한다. 정책 관리 장치(150)는 IoT 단말(810)의 MAC 주소, IoT 서비스 서버(830)의 IP 주소를 이용하여 이들이 동일한 서비스 그룹에 속한 것을 확인한 후, IoT 서비스 서버(830)와 제 2 보안 모듈(140) 간의 ID 연결 관계 정보, 및 IoT 단말(810)과 제 1 보안 모듈(120) 간의 ID 연결 관계 정보를 이용하여, 보안 모듈(120, 140)을 기준으로 한 양방향 연결 정보를 생성하여 정책 저장 장치(160)에 저장한다.
- [108] 도 9는 도 8의 시스템에서 IoT 서비스 서버와 제 2 보안 모듈 간의 ID 연결 관계 정보를 생성하는 방법을 설명하는 흐름도이다.
- [109] 도 9를 참조하면, 단계 S901에서, IoT 서비스 서버(830)에 제 2 보안 모듈(140)이 통신 가능하게 연결된다. 여기서 통신 가능한 연결이란, 물리적 연결 또는 소프트웨어적 연결을 포함한다. 단계 S902에서, 제 2 보안 모듈(140)은 IoT 서비스 서버(830)의 공인 IP 주소를 수집하고 그 수집된 공인 IP 주소와 자신의 ID₁를 정책 관리 장치(150)로 전송한다.
- [110] 단계 S903에서, 정책 관리 장치(150)는, IoT 서비스 서버(830)에 임시적인 ID₂를 부여한다. 단계 S904에서, 정책 관리 장치(150)는 제 2 보안 모듈(140)과 IoT 서비스 서버(830) 간의 ID 연결 관계, 즉 (ID₁, ID₂)를 저장한다. 단계 S905에서, 정책 관리 장치(150)는, IoT 서비스 서버(830)의 공인 IP 주소를 이용하여 서비스 그룹을 확인한다. 예를 들어, 삼성전자의 IoT 서비스임을 확인한다. 단계 S906에서, 정책 관리 장치(150)는, 해당 서비스 그룹에 IoT 서비스 서버(830)의 ID₂를 매칭하여 저장한다.
- [111] 도 10은 도 8의 시스템에서 IoT 단말과 IoT 서비스 서버 간의 연결 정책을 설정하는 방법을 설명하는 흐름도로서, 도 9를 참조하여 설명한 절차 이후에 동작하는 흐름도이다.
- [112] 도 10을 참조하면, 단계 S1001에서, IoT 단말(810)에 제 1 보안 모듈(120)이 통신

가능하게 연결된다. 여기서 통신 가능한 연결이란, 물리적 연결 또는 소프트웨어적 연결을 포함한다. 단계 S1002에서, 제 1 보안 모듈(120)은 IoT 단말(810)의 MAC 주소를 수집하고 그 수집된 MAC 주소와 자신의 ID₃을 정책 관리 장치(150)로 전송한다.

- [113] 단계 S1003에서, 정책 관리 장치(150)는, IoT 단말(810)에 임시적인 ID₄를 부여한다. 단계 S1004에서, 정책 관리 장치(150)는 제 1 보안 모듈(120)과 IoT 단말(810) 간의 ID 연결 관계, 즉 (ID₃, ID₄)를 저장한다. 단계 S1005에서, 정책 관리 장치(150)는, IoT 단말(810)의 MAC 주소를 이용하여 서비스 그룹을 확인한다. 예를 들어, 삼성전자의 IoT 단말임을 확인한다.
- [114] 도 9를 참조한 실시예에서 IoT 서비스 서버(830)의 ID₂가 서비스 그룹에 매칭되어 있으므로, 단계 S1006에서, 정책 관리 장치(150)는, IoT 단말(810)과 IoT 서비스 서버(830) 간의 ID 연결 관계 정보(ID₂: ID₄)를 생성한다. 단계 S1007에서, 정책 관리 장치(150)는, IoT 단말(810)과 IoT 서비스 서버(830) 간의 ID 연결 관계 정보(ID₂: ID₄)를 이용하여, IoT 서비스 서버(830)와 제 2 보안 모듈(140) 간의 ID 연결 관계 정보, 및 IoT 단말(810)과 제 1 보안 모듈(120) 간의 ID 연결 관계 정보를 확인하고, 이를 이용하여 IoT 단말(810)과 IoT 서비스 서버(830) 간의 ID 기반 전체 경로를 조합한다. ID 기반 전체 경로는 (ID₂: ID₁: ID₃: ID₄)이다.
- [115] 단계 S1008에서, 정책 관리 장치(150)는 ID 기반 전체 경로를 기초로, 보안 모듈(120, 140)을 기준으로 한 양방향 연결 정보를 생성하여 정책 저장 장치(160)에 저장한다. 제 1 보안 모듈(120)을 기준으로 한 ID 기반의 양방향 연결 정보는, (ID₄, ID₃, ID₁)이다. 제 2 보안 모듈(140)을 기준으로 한 ID 기반의 양방향 연결 정보는, (ID₃, ID₁, ID₂)이다.
- [116] 본 명세서는 많은 특징을 포함하는 반면, 그러한 특징은 본 발명의 범위 또는 특허청구범위를 제한하는 것으로 해석되어서는 안 된다. 또한, 본 명세서에서 개별적인 실시예에서 설명된 특징들은 단일 실시예에서 결합되어 구현될 수 있다. 반대로, 본 명세서에서 단일 실시예에서 설명된 다양한 특징들은 개별적으로 다양한 실시예에서 구현되거나, 적절히 결합되어 구현될 수 있다.
- [117] 도면에서 동작들이 특정한 순서로 설명되었으나, 그러한 동작들이 도시된 바와 같은 특정한 순서로 수행되는 것으로, 또는 일련의 연속된 순서, 또는 원하는 결과를 얻기 위해 모든 설명된 동작이 수행되는 것으로 이해되어서는 안 된다. 특정 환경에서 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다. 아울러, 상술한 실시예에서 다양한 시스템 구성요소의 구분은 모든 실시예에서 그러한 구분을 요구하지 않는 것으로 이해되어야 한다. 상술한 프로그램 구성요소 및 시스템은 일반적으로 단일 소프트웨어 제품 또는 멀티플 소프트웨어 제품에 패키지로 구현될 수 있다.
- [118] 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(시디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기

디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

- [119] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

청구범위

- [청구항 1] 종단 통신 장치에 통신 가능하게 연결되어 종단 간 통신에 보안을 제공하는 보안 장치에 있어서,
통신 회로;
프로세서; 및
상기 프로세서가 실행 가능한 적어도 하나의 명령어를 포함하는 메모리를 포함하고,
상기 프로세서는,
목적지 IP 주소를 포함하는 패킷을 수신하고,
IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로 상기 목적지 IP 주소에 대응하는 제 1 식별자를 요청하여 수신하며,
상기 종단 통신 장치의 고유 정보와 제 2 식별자의 매칭 정보를 저장하는 테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하고,
상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를 정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책 관리 장치로부터 정책 조회 결과를 수신하며,
상기 정책 조회 결과에 기초하여 상기 패킷을 다른 종단 통신 장치로 전송하는 것을 특징으로 하는 보안 장치.
- [청구항 2] 제 1 항에 있어서,
상기 프로세서는,
상기 정책 관리 장치로 토큰 시드를 요청하여 수신하고, 수신된 토큰 시드를 이용하여 토큰을 생성하며,
상기 패킷에 상기 토큰을 삽입하여 전송하는 것을 특징으로 하는 보안 장치.
- [청구항 3] 제 2 항에 있어서,
상기 프로세서는,
토큰 시드를 요청시, 상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자를 전송하는 것을 특징으로 하는 보안 장치.
- [청구항 4] 제 2 항에 있어서,
상기 프로세서는,
nonce(Nonce), 상기 패킷의 페이로드, 타임스탬프, 상기 제 2 식별자, 상기 토큰 시드를 이용하여 토큰을 생성하는 것을 특징으로 하는 보안 장치.
- [청구항 5] 제 1 항에 있어서,
상기 프로세서는,
상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자와, 상기 정책 관리 장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결 정보 간의 비교 결과에 따른 정책 조회 결과를 상기 정책 관리 장치로부터

- 수신하는 것을 특징으로 하는 보안 장치.
- [청구항 6] 제 5 항에 있어서,
상기 제 1 식별자는, 상기 다른 종단 통신 장치에 통신 가능하게 연결된 다른 보안 장치의 식별자인 것을 특징으로 하는 보안 장치.
- [청구항 7] 제 5 항에 있어서,
상기 정책 관리 장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결 정보는,
상기 보안 장치의 식별자와, 상기 보안 장치에 통신 가능하게 연결된 통신 계층상 그 하위의 종단 통신 장치의 식별자, 그리고 그 하위의 종단 통신 장치와 종단 통신이 허용된 다른 종단 통신 장치에 통신 가능하게 연결된 통신 계층상 그 상위의 다른 보안 장치의 식별자로 이루어진 것을 특징으로 하는 보안 장치.
- [청구항 8] 제 7 항에 있어서,
상기 프로세서는,
상기 종단 통신 장치에 상기 보안 장치가 최초에 통신 가능하게 연결될 때 상기 보안 장치의 식별자와 상기 종단 통신 장치의 고유 정보를 상기 정책 관리 장치로 전송하여 식별자 기반의 정책 설정을 요청하는 것을 특징으로 하는 보안 장치.
- [청구항 9] 제 8 항에 있어서,
상기 IP 주소 관리 장치에 저장되는 IP 주소 및 제 1 식별자 간의 매칭 정보는, 상기 정책 관리 장치에서 식별자 기반의 정책이 설정될 때 상기 정책 관리 장치로부터 수신되어 저장되는 것을 특징으로 하는 보안 장치.
- [청구항 10] 종단 통신 장치에 통신 가능하게 연결되어 종단 간 통신에 보안을 제공하는 보안 장치에 있어서,
통신 회로;
프로세서; 및
상기 프로세서가 실행 가능한 적어도 하나의 명령어를 포함하는 메모리를 포함하고,
상기 프로세서는,
출발지 IP 주소를 포함하는 패킷을 수신하고,
IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로 상기 출발지 IP 주소에 대응하는 제 1 식별자를 요청하여 수신하며,
상기 종단 통신 장치의 고유 정보와 제 2 식별자의 매칭 정보를 저장하는 테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하고,
상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를 정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책 관리 장치로부터 정책 조회 결과를 수신하며,
상기 정책 조회 결과에 기초하여 상기 패킷을 상기 종단 통신 장치로

- 전송하는 것을 특징으로 하는 보안 장치.
- [청구항 11] 제 10 항에 있어서,
상기 패킷은, 상기 패킷을 전송한 측에서 삽입한 토큰을 포함하고,
상기 프로세서는,
상기 정책 관리 장치로 상기 패킷을 전송한 측에서 사용한 토큰 시드를
요청하여 수신하고, 수신된 토큰 시드를 이용하여 상기 토큰을 검증하며,
토큰 검증 성공시에 상기 패킷에 삽입된 상기 토큰을 제거하는 것을
특징으로 하는 보안 장치.
- [청구항 12] 제 11 항에 있어서,
상기 프로세서는,
토큰 시드를 요청시, 상기 토큰에 평문으로 포함된 상기 패킷을 전송한
종단 통신 장치의 식별자와, 상기 제 1 식별자와, 상기 제 3 식별자를 상기
정책 관리 장치로 전송하는 것을 특징으로 하는 보안 장치.
- [청구항 13] 제 10 항에 있어서,
상기 프로세서는,
상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자와, 상기 정책 관리
장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결
정보 간의 비교 결과에 따른 정책 조회 결과를 상기 정책 관리 장치로부터
수신하는 것을 특징으로 하는 보안 장치.
- [청구항 14] 제 13 항에 있어서,
상기 제 1 식별자는, 상기 패킷을 전송한 종단 통신 장치에 통신 가능하게
연결된 다른 보안 장치의 식별자인 것을 특징으로 하는 보안 장치.
- [청구항 15] 종단 통신 장치에 통신 가능하게 연결된 보안 장치에서 종단 간 통신에
보안을 제공하는 방법에 있어서,
목적지 IP 주소를 포함하는 패킷을 수신하는 단계;
IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로
상기 목적지 IP 주소에 대응하는 제 1 식별자를 요청하여 수신하는 단계;
상기 종단 통신 장치의 고유 정보와 제 2 식별자의 매칭 정보를 저장하는
테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하는 단계;
상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를
정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책
관리 장치로부터 정책 조회 결과를 수신하는 단계; 및
상기 정책 조회 결과에 기초하여 상기 패킷을 다른 종단 통신 장치로
전송하는 단계를 포함하는 방법.
- [청구항 16] 제 15 항에 있어서,
상기 정책 관리 장치로 토큰 시드를 요청하여 수신하고, 수신된 토큰
시드를 이용하여 토큰을 생성하는 단계; 및
상기 패킷에 상기 토큰을 삽입하는 단계를 더 포함하는 것을 특징으로

- 하는 방법.
- [청구항 17] 제 16 항에 있어서,
상기 토큰을 생성하는 단계는,
토큰 시드를 요청시, 상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자를 전송하는 것을 특징으로 하는 방법.
- [청구항 18] 제 16 항에 있어서,
상기 토큰을 생성하는 단계는,
nonce(Nonce), 상기 패킷의 페이로드, 타임스탬프, 상기 제 2 식별자, 상기 토큰 시드를 이용하여 토큰을 생성하는 것을 특징으로 하는 방법.
- [청구항 19] 제 15 항에 있어서,
상기 정책 조회 결과를 수신하는 단계는,
상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자와, 상기 정책 관리 장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결 정보 간의 비교 결과에 따른 정책 조회 결과를 상기 정책 관리 장치로부터 수신하는 것을 특징으로 하는 방법.
- [청구항 20] 제 19 항에 있어서,
상기 제 1 식별자는, 상기 다른 종단 통신 장치에 통신 가능하게 연결된 다른 보안 장치의 식별자인 것을 특징으로 하는 방법.
- [청구항 21] 제 19 항에 있어서,
상기 정책 관리 장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결 정보는,
상기 보안 장치의 식별자와, 상기 보안 장치에 통신 가능하게 연결된 통신 계층상 그 하위의 종단 통신 장치의 식별자, 그리고 그 하위의 종단 통신 장치와 종단 통신이 허용된 다른 종단 통신 장치에 통신 가능하게 연결된 통신 계층상 그 상위의 다른 보안 장치의 식별자로 이루어진 것을 특징으로 하는 방법.
- [청구항 22] 제 21 항에 있어서,
상기 종단 통신 장치에 상기 보안 장치가 최초에 통신 가능하게 연결될 때 상기 보안 장치의 식별자와 상기 종단 통신 장치의 고유 정보를 상기 정책 관리 장치로 전송하여 식별자 기반의 정책 설정을 요청하는 단계를 더 포함하는 것을 특징으로 하는 방법.
- [청구항 23] 종단 통신 장치에 통신 가능하게 연결된 보안 장치에서 종단 간 통신에 보안을 제공하는 방법에 있어서,
출발지 IP 주소를 포함하는 패킷을 수신하는 단계;
IP 주소와 제 1 식별자 간의 매칭 정보를 저장하는 IP 주소 관리 장치로 상기 출발지 IP 주소에 대응하는 제 1 식별자를 요청하여 수신하는 단계;
상기 종단 통신 장치의 고유 정보와 제 2 식별자의 매칭 정보를 저장하는 테이블에서, 상기 종단 통신 장치의 제 2 식별자를 확인하는 단계;

상기 제 1 식별자, 상기 제 2 식별자 및 상기 보안 장치의 제 3 식별자를 정책 관리 장치로 전송하여 식별자 기반의 정책을 질의하고 상기 정책 관리 장치로부터 정책 조회 결과를 수신하는 단계; 및
상기 정책 조회 결과에 기초하여 상기 패킷을 상기 종단 통신 장치로 전송하는 단계를 포함하는 방법.

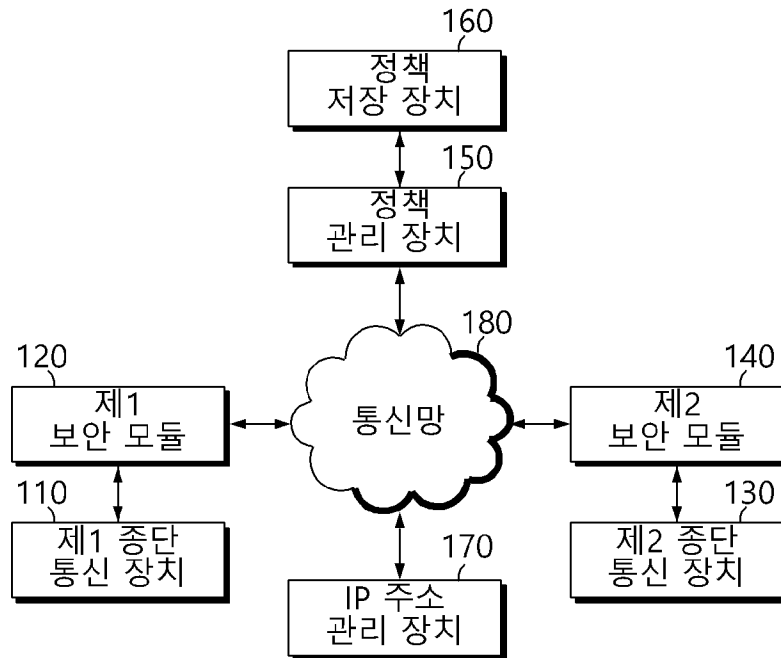
[청구항 24] 제 23 항에 있어서,
상기 패킷은, 상기 패킷을 전송한 측에서 삽입한 토큰을 포함하고,
상기 방법은,
상기 정책 관리 장치로 상기 패킷을 전송한 측에서 사용한 토큰 시드를 요청하여 수신하고, 수신된 토큰 시드를 이용하여 상기 토큰을 검증하는 단계; 및
토큰 검증 성공시에 상기 패킷에 삽입된 상기 토큰을 제거하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[청구항 25] 제 24 항에 있어서,
상기 토큰을 검증하는 단계는,
토큰 시드를 요청시, 상기 토큰에 평문으로 포함된 상기 패킷을 전송한 종단 통신 장치의 식별자와, 상기 제 1 식별자와, 상기 제 3 식별자를 상기 정책 관리 장치로 전송하는 것을 특징으로 하는 방법.

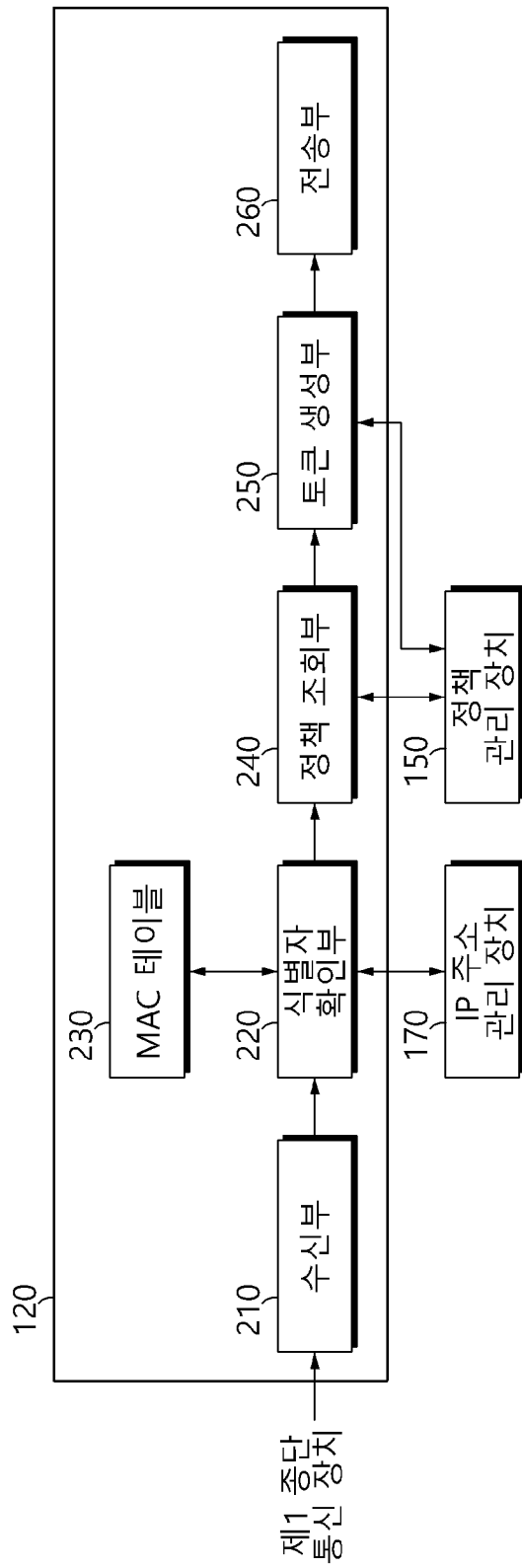
[청구항 26] 제 23 항에 있어서,
상기 정책 조회 결과를 수신하는 단계는,
상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자와, 상기 정책 관리 장치에 저장된 상기 보안 장치를 기준으로 한 식별자 기반의 양방향 연결 정보 간의 비교 결과에 따른 정책 조회 결과를 상기 정책 관리 장치로부터 수신하는 것을 특징으로 하는 방법.

[청구항 27] 제 26 항에 있어서,
상기 제 1 식별자는, 상기 패킷을 전송한 종단 통신 장치에 통신 가능하게 연결된 다른 보안 장치의 식별자인 것을 특징으로 하는 방법.

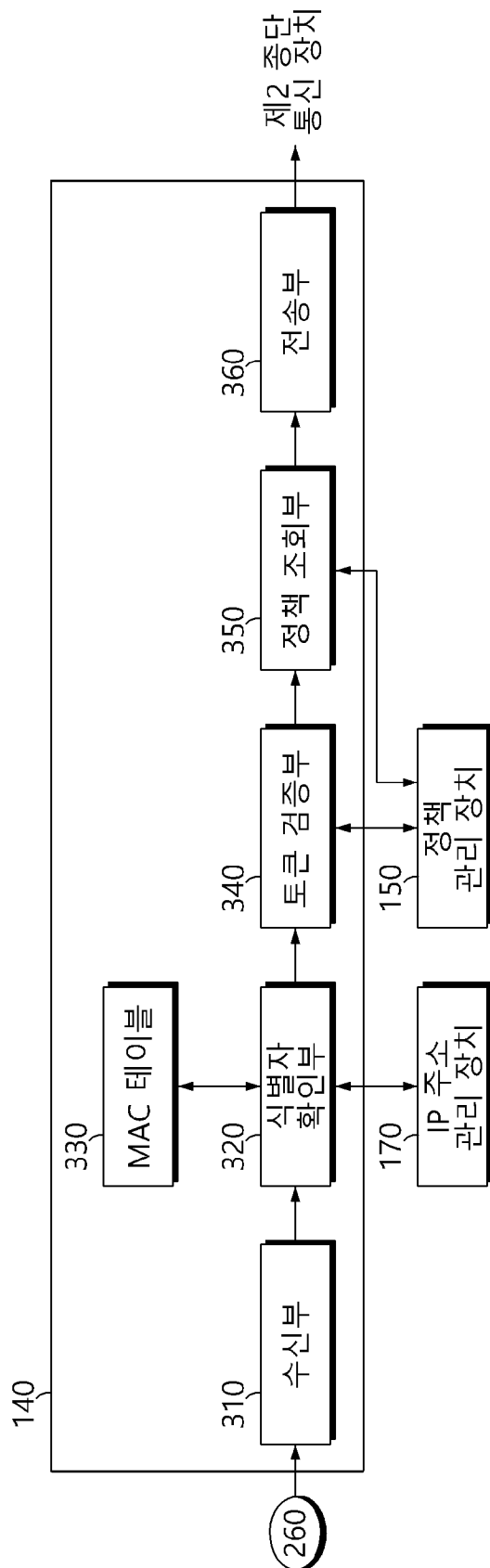
[도1]



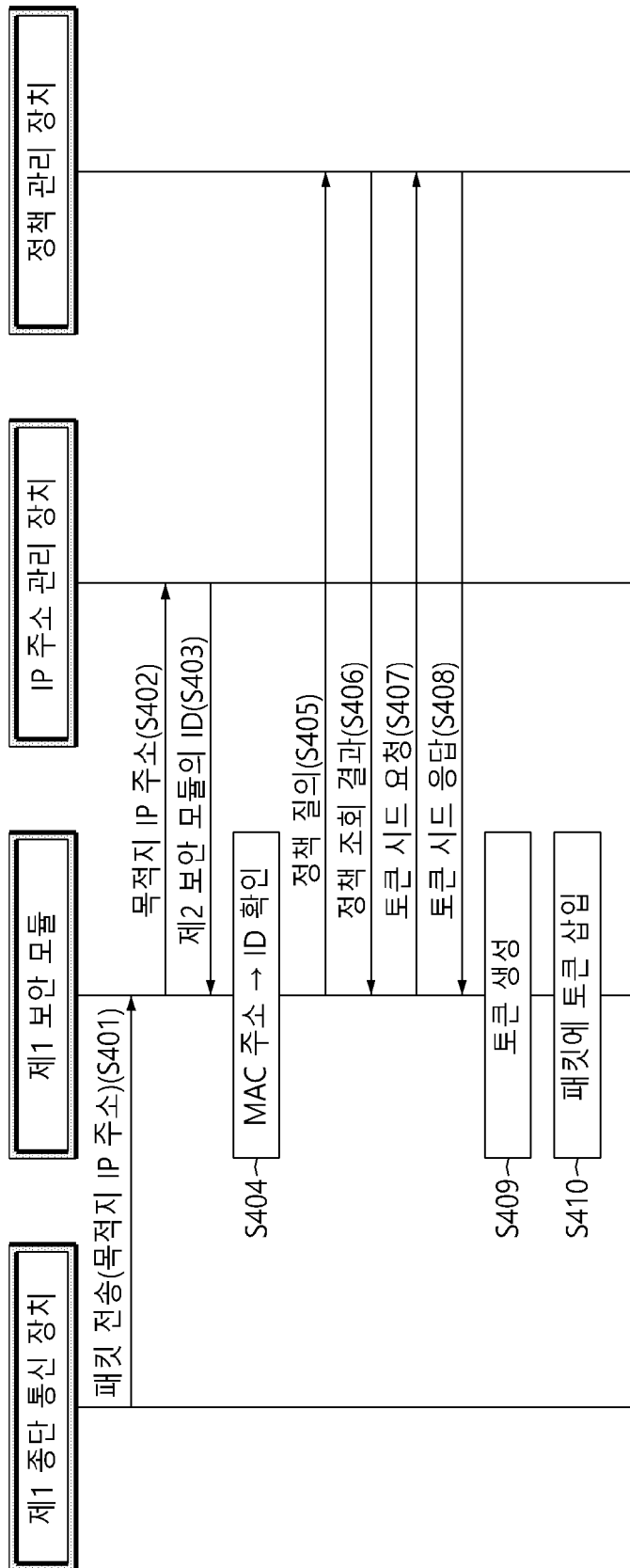
[도2]



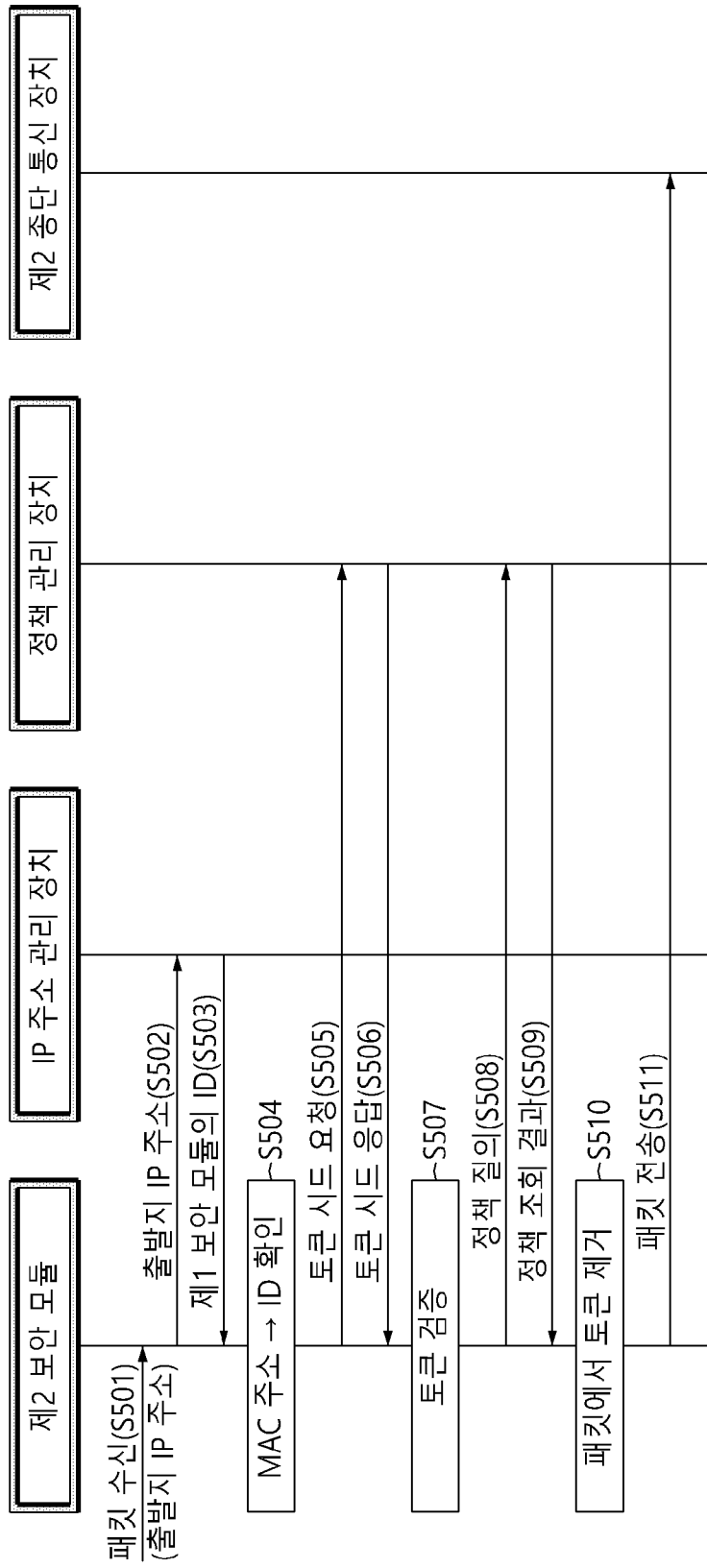
[도3]

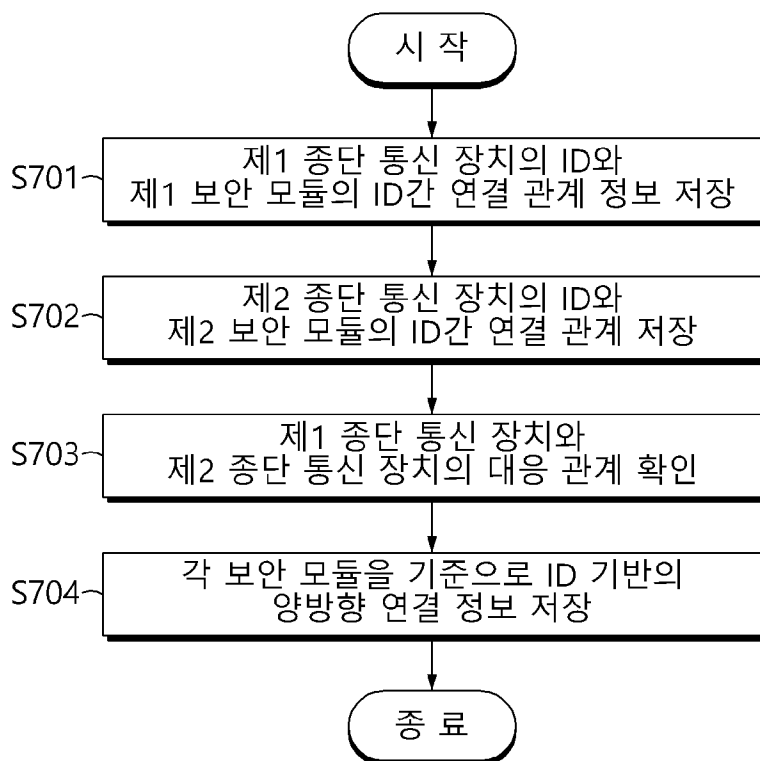


[도4]

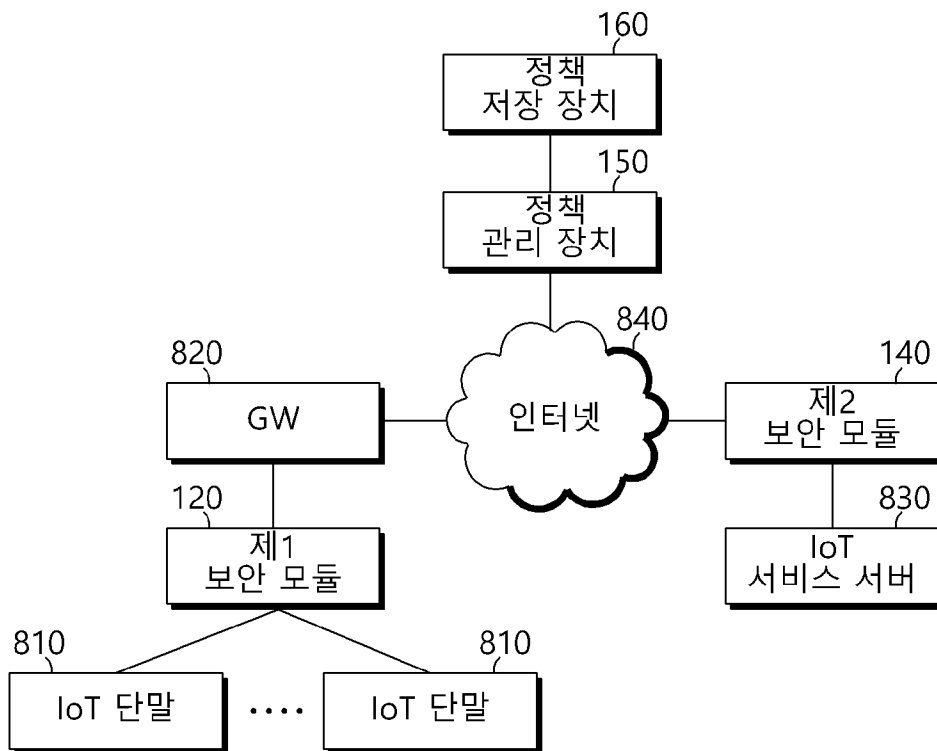


[도5]

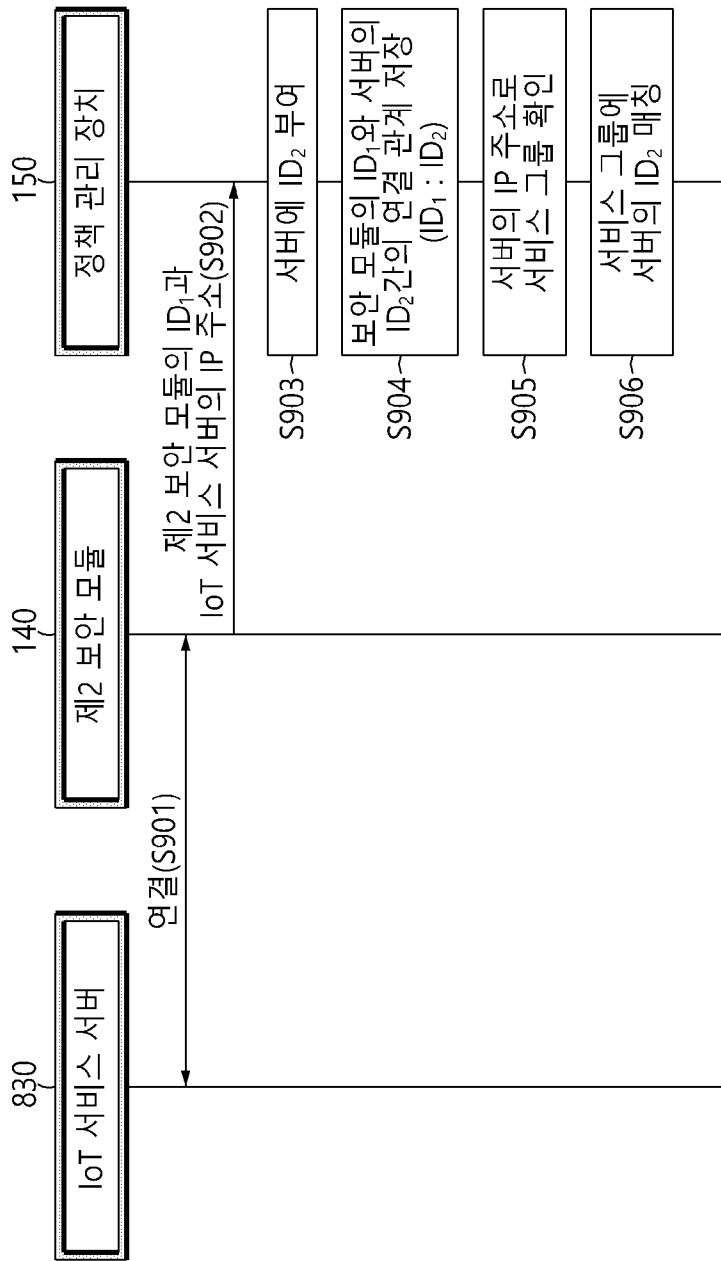




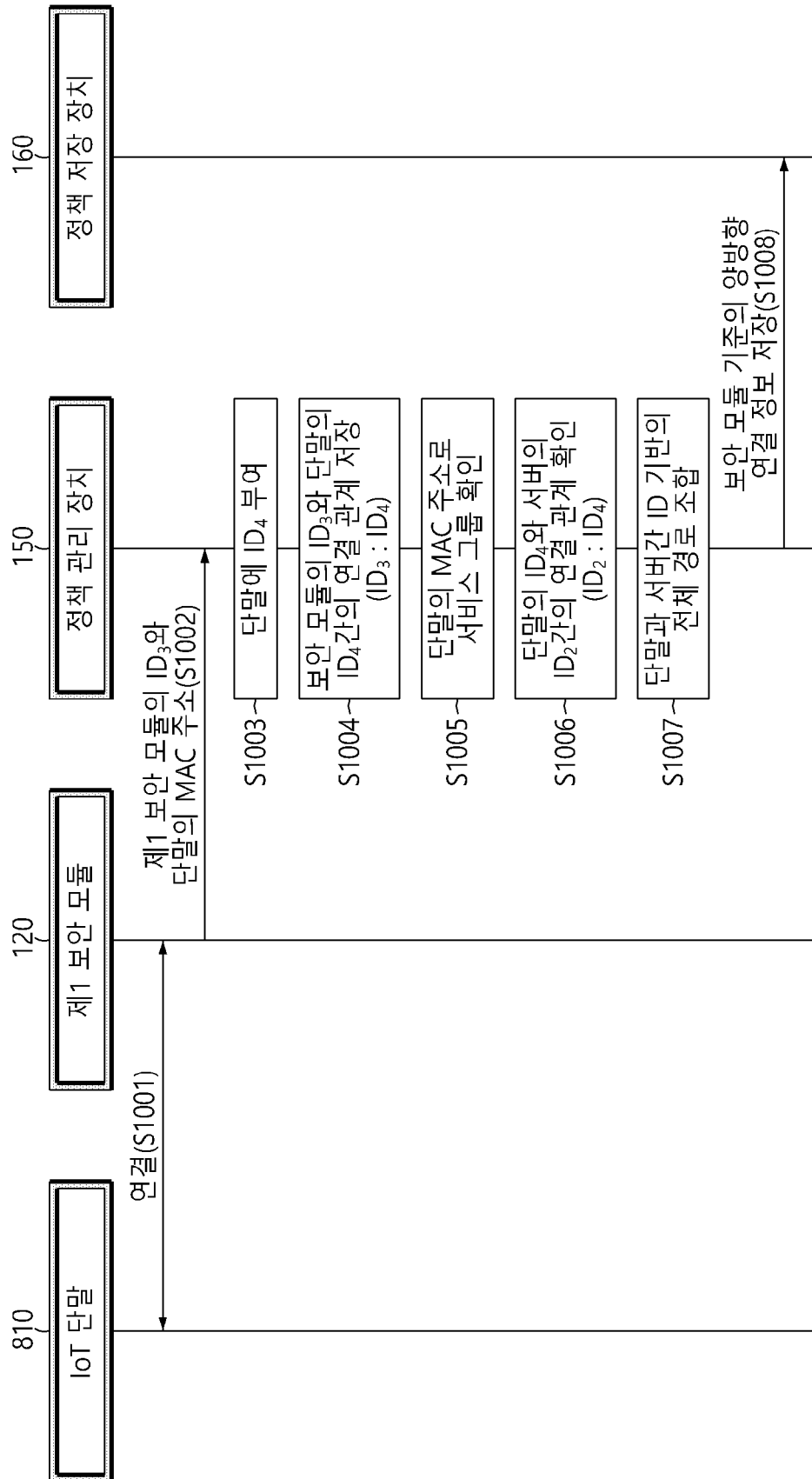
[도8]



[도9]



[도10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2019/007744**A. CLASSIFICATION OF SUBJECT MATTER****H04L 29/06(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 29/06; H04L 12/26; H04L 12/46; H04L 12/741; H04L 12/851; H04L 29/12; H04W 12/04; H04W 76/02

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: IP address, identifier, communication device, security, IoT(internet of things)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2017-0075588 A (KT CORPORATION) 03 July 2017 See paragraphs [0027]-[0031], [0060]-[0061], claim 1 and figures 1, 3.	1-27
A	KR 10-2018-0007898 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 24 January 2018 See paragraphs [0013]-[0030] and figures 1-2.	1-27
A	KR 10-2010-0034933 A (KT CORPORATION) 02 April 2010 See paragraphs [0020]-[0032] and figure 1.	1-27
A	KR 10-1619371 B1 (SECUI CORPORATION) 10 May 2016 See paragraphs [0020]-[0025] and figure 2.	1-27
A	US 2017-0006643 A1 (AFERO, INC.) 05 January 2017 See paragraphs [0035]-[0039], [0131]-[0136] and figures 1A, 17.	1-27



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

23 OCTOBER 2019 (23.10.2019)

Date of mailing of the international search report

23 OCTOBER 2019 (23.10.2019)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsu-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/KR2019/007744

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2017-0075588 A	03/07/2017	KR 10-1821794 B1 KR 10-1893209 B1 KR 10-2017-0078482 A WO 2017-111404 A1	08/03/2018 29/08/2018 07/07/2017 29/06/2017
KR 10-2018-0007898 A	24/01/2018	None	
KR 10-2010-0034933 A	02/04/2010	KR 10-1456699 B1	12/11/2014
KR 10-1619371 B1	10/05/2016	None	
US 2017-0006643 A1	05/01/2017	CN 107710216 A JP 2018-525891 A KR 10-2018-0025903 A US 2017-0006003 A1 US 2017-0339120 A1 US 9699814 B2 US 9729528 B2 WO 2017-007725 A1	16/02/2018 06/09/2018 09/03/2018 05/01/2017 23/11/2017 04/07/2017 08/08/2017 12/01/2017

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 29/06; H04L 12/26; H04L 12/46; H04L 12/741; H04L 12/851; H04L 29/12; H04W 12/04; H04W 76/02

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: IP 주소(IP address), 식별자(identifier), 통신 장치(communication device), 보안(privacy), IoT(internet of things)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2017-0075588 A (주식회사 케이티) 2017.07.03 단락 [0027]-[0031], [0060]-[0061], 청구항 1 및 도면 1, 3 참조.	1-27
A	KR 10-2018-0007898 A (한국전자통신연구원) 2018.01.24 단락 [0013]-[0030] 및 도면 1-2 참조.	1-27
A	KR 10-2010-0034933 A (주식회사 케이티) 2010.04.02 단락 [0020]-[0032] 및 도면 1 참조.	1-27
A	KR 10-1619371 B1 (주식회사 시큐아이) 2016.05.10 단락 [0020]-[0025] 및 도면 2 참조.	1-27
A	US 2017-0006643 A1 (AFERO, INC.) 2017.01.05 단락 [0035]-[0039], [0131]-[0136] 및 도면 1A, 17 참조.	1-27

☐ 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

“D” 본 국제출원에서 출원인이 인용한 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후 “X”에 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

2019년 10월 23일 (23.10.2019)

국제조사보고서 발송일

2019년 10월 23일 (23.10.2019)

ISA/KR의 명칭 및 우편주소



대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

진상범

전화번호 +82-42-481-8398



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2017-0075588 A	2017/07/03	KR 10-1821794 B1 KR 10-1893209 B1 KR 10-2017-0078482 A WO 2017-111404 A1	2018/03/08 2018/08/29 2017/07/07 2017/06/29
KR 10-2018-0007898 A	2018/01/24	없음	
KR 10-2010-0034933 A	2010/04/02	KR 10-1456699 B1	2014/11/12
KR 10-1619371 B1	2016/05/10	없음	
US 2017-0006643 A1	2017/01/05	CN 107710216 A JP 2018-525891 A KR 10-2018-0025903 A US 2017-0006003 A1 US 2017-0339120 A1 US 9699814 B2 US 9729528 B2 WO 2017-007725 A1	2018/02/16 2018/09/06 2018/03/09 2017/01/05 2017/11/23 2017/07/04 2017/08/08 2017/01/12