(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0091274
(43) 공개일자 2018년08월16일

(51) 국제특허분류(Int. Cl.)
*H04L 9/32* (2006.01) *H04L 9/08* (2006.01)
*H04L 9/30* (2006.01)
(52) CPC특허분류
*H04L 9/3242* (2013.01)
*H04L 9/0866* (2013.01)
(21) 출원번호 10-2017-0016224
(22) 출원일자 2017년02월06일
심사청구일자 2018년02월07일

(71) 출원인
**한국전자통신연구원**
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
**김태환**
대전광역시 서구 도안동로 183
(74) 대리인
**특허법인 무한**

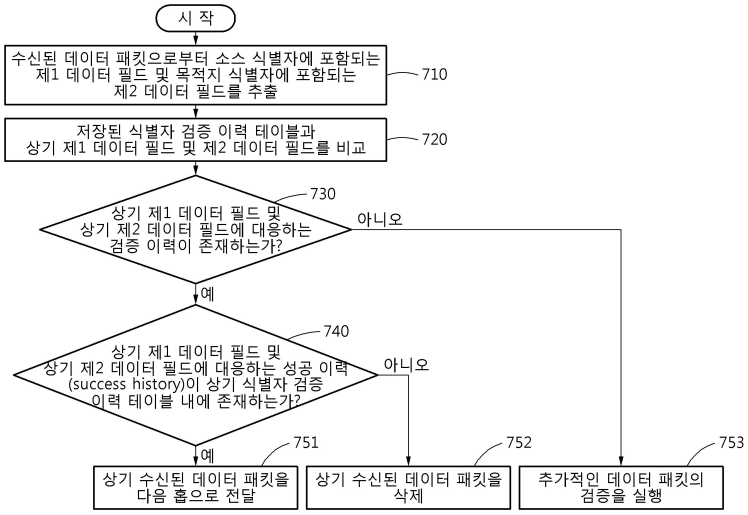
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **식별자 기반 네트워크의 식별자 생성 장치 및 방법**

## (57) 요 약

공개키 기반의 식별자를 생성하는 컴퓨팅 장치가 제공된다. 상기 컴퓨팅 장치는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서에 의해 적어도 일시적으로 구현될 수 있다. 상기 컴퓨팅 장치는 식별자 기반 네트워크에 접속하는 단말로부터 고유 정보를 추출하는 추출부 및 상기 추출된 고유 정보를 키 값으로 이용하여 상기 식별자 기반 네트워크에 대응하는 공개키(publication key) 기반의 식별자(identifier)를 생성하는 생성부를 포함할 수 있다.

## 대 표 도



(52) CPC특허분류
*H04L 9/30* (2013.01)
*H04L 9/3226* (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 CRC-15-05-ETRI
부처명 국가과학기술연구회
연구관리전문기관 국가과학기술연구회
연구사업명 융합연구사업
연구과제명 자가학습형 지식융합 슈퍼브레인 핵심기술개발
기 여 율 1/1
주관기관 한국전자통신연구원
연구기간 2015.12.01 ~ 2016.11.30

# 명 세 서

## 청구범위

### 청구항 1

적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서에 의해 적어도 일시적으로 구현되는:

식별자 기반 네트워크에 접속하는 단말로부터 고유 정보를 추출하는 추출부; 및

상기 추출된 고유 정보를 키 값으로 이용하여 상기 식별자 기반 네트워크에 대응하는 공개키(publication key) 기반의 식별자(identifier)를 생성하는 생성부

를 포함하는 컴퓨팅 장치.

### 청구항 2

제1항에 있어서,

상기 추출부는 상기 식별자 기반 네트워크에 접속하는 복수의 단말로부터 각각의 고유 정보를 추출하고, 상기 생성부는 상기 식별자 기반 네트워크에 대응하는 고유한 공개키 및 상기 각각의 고유 정보를 해시 함수에 입력하여 복수의 공개키 기반의 식별자를 생성하는 컴퓨팅 장치.

### 청구항 3

제2항에 있어서,

상기 생성부는 상기 고유한 공개키 및 상기 각각의 고유 정보를 상기 해시 함수에 입력하여 복수의 해시 기반의 메시지 인증 코드(HMAC: Hash based Message Authentication Code)를 상기 복수의 공개키 기반의 식별자로서 생성하는 컴퓨팅 장치.

### 청구항 4

제1항에 있어서,

상기 생성부는 상기 추출된 고유 정보의 제1 비트열을 상기 키 값으로서 해시 함수에 입력하여 해시 기반의 메시지 인증 코드를 생성하는 컴퓨팅 장치.

### 청구항 5

제4항에 있어서,

상기 생성부는 미리 지정된 비트 수에 따라 상기 해시 기반의 메시지 인증 코드에 대응하는 제2 비트열 및 상기 고유 정보에 대응하는 제3 비트열의 결합으로 상기 식별자 기반 네트워크에 대응하는 공개키 기반의 식별자를 생성하는 컴퓨팅 장치.

### 청구항 6

제1항에 있어서,

상기 단말이 제1 식별자 기반 네트워크에 접속하는 경우에 상기 생성부는 상기 추출된 고유 정보를 키 값으로 이용하여 상기 제1 식별자 기반 네트워크에 대응하는 제1 공개키 기반의 제1 식별자를 생성하고,

상기 단말이 제2 식별자 기반 네트워크에 접속하는 경우에 상기 생성부는 상기 추출된 고유 정보를 키 값으로 이용하여 상기 제2 식별자 기반 네트워크에 대응하는 제2 공개키 기반의 제2 식별자를 생성하는 컴퓨팅 장치.

**청구항 7**

제1항에 있어서,

상기 추출부는 상기 단말의 시리얼 넘버 및 맥 어드레스 중 적어도 하나를 상기 고유 정보로서 추출하는 컴퓨팅 장치.

**청구항 8**

제1항에 있어서,

상기 단말에 대응하는 식별자 및 상기 식별자 기반 네트워크에 대응하는 공개키를 매칭하여 저장하는 데이터베이스

를 더 포함하는 컴퓨팅 장치.

**청구항 9**

수신된 데이터 패킷으로부터 소스 식별자(source ID)에 포함되는 제1 데이터 필드 및 목적지 식별자(destination ID)에 포함되는 제2 데이터 필드를 추출하는 단계;

미리 지정된 공개키로 상기 제1 데이터 필드를 해시하고, 해시된 제1 결과값와 상기 소스 식별자를 비교하는 단계;

상기 공개키로 상기 제2 데이터 필드를 해시하고, 해시된 제2 결과값과 상기 목적지 식별자를 비교하는 단계; 및

상기 제1 결과값에 관한 비교 결과 및 상기 제2 결과값에 관한 비교 결과에 기초하여 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계

를 포함하는 데이터 패킷의 검증 방법.

**청구항 10**

제9항에 있어서,

상기 해시된 제1 결과값과 상기 소스 식별자를 비교하는 단계는,

상기 해시된 제1 결과값과 상기 소스 식별자 내의 해시 기반의 메시지 인증 코드를 비교하는 단계를 포함하고,

상기 해시된 제2 결과값과 상기 목적지 식별자를 비교하는 단계는,

상기 해시된 제2 결과값과 상기 목적지 식별자 내의 해시 기반의 메시지 인증 코드를 비교하는 단계를 포함하는 데이터 패킷의 검증 방법.

**청구항 11**

제9항에 있어서,

상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는

상기 해시된 제1 결과값과 상기 소스 식별자 내의 제3 데이터 필드가 동일하고, 상기 해시된 제2 결과값과 상기

목적지 식별자 내의 제4 데이터 필드가 동일한 경우에 상기 수신된 데이터 패킷을 다음 홉(hop)으로 전달하는 단계

를 포함하는 데이터 패킷의 검증 방법.

**청구항 12**

제9항에 있어서,

상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는

상기 해시된 제1 결과값과 상기 소스 식별자 내의 제3 데이터 필드의 불일치 및 상기 해시된 제2 결과값과 상기 목적지 식별자 내의 제4 데이터 필드의 불일치 중 적어도 어느 하나가 발생한 경우에 상기 수신된 데이터 패킷을 삭제하는 단계

를 포함하는 데이터 패킷의 검증 방법.

**청구항 13**

제11항에 있어서,

상기 해시된 제1 결과값, 상기 해시된 제2 결과값 및 검증 결과를 저장하여 식별자 검증 이력 테이블(ID checksum table)을 업데이트하는 단계

를 더 포함하는 데이터 패킷의 검증 방법.

**청구항 14**

제9항에 있어서,

상기 추출된 제1 데이터 필드 및 상기 추출된 제2 데이터 필드를 비교하여 미리 지정된 접근 제어 조건을 만족하는지 여부를 판단하는 단계

를 더 포함하는 데이터 패킷의 검증 방법.

**청구항 15**

제9항에 있어서,

상기 제1 데이터 필드 및 상기 제2 데이터 필드를 추출하는 단계는,

상기 소스 식별자의 접근 제어 필드(access control field)를 확인하여 상기 제1 데이터 필드로서 추출하고, 상기 목적지 식별자의 접근 제어 필드를 확인하여 상기 제2 데이터 필드로서 추출하는 단계

를 포함하는 데이터 패킷의 검증 방법.

**청구항 16**

수신된 데이터 패킷으로부터 소스 식별자에 포함되는 제1 데이터 필드 및 목적지 식별자에 포함되는 제2 데이터 필드를 추출하는 단계; 및

저장된 식별자 검증 이력 테이블과 상기 제1 데이터 필드 및 제2 데이터 필드를 비교하여 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계

를 포함하고,

상기 소스 식별자 및 상기 목적지 식별자는 소스 및 목적지 각각에 대응하는 고유 정보를 키 값으로 이용하여 식별자 기반 네트워크에 대응하는 공개키 기반의 식별자로서 생성되는 데이터 패킷의 검증 방법.

**청구항 17**

제16항에 있어서,

상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는,

상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 성공 이력(success history)이 상기 식별자 검증 이력 테이블 내에 존재하는 경우에, 상기 수신된 데이터 패킷을 다음 홉으로 전달하는 단계

를 포함하는 데이터 패킷의 검증 방법.

**청구항 18**

제16항에 있어서,

상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는,

상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 실패 이력(failure history)이 상기 식별자 검증 이력 테이블 내에 존재하는 경우에, 상기 수신된 데이터 패킷을 삭제하는 단계

를 포함하는 데이터 패킷의 검증 방법.

**청구항 19**

제16항에 있어서,

상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는,

상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 검증 이력이 존재하지 않는 경우에 상기 식별자 기반 네트워크에 대응하는 공개키를 이용하여 상기 제1 데이터 필드 및 상기 제2 데이터 필드를 각각 해시하는 단계

를 더 포함하는 데이터 패킷의 검증 방법.

**청구항 20**

제19항에 있어서,

상기 제1 데이터 필드에 대응하는 해시된 제1 결과값과 상기 소스 식별자를 비교하는 단계;

상기 제2 데이터 필드에 대응하는 해시된 제2 결과값과 상기 목적지 식별자를 비교하는 단계; 및

상기 제1 결과값에 관한 비교 결과 및 상기 제2 결과값에 관한 비교 결과에 기초하여 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계

를 더 포함하는 데이터 패킷의 검증 방법.

## *발명의 설명*

### *기 술 분 야*

[0001] 식별자 생성 장치 및 방법에 연관되고, 보다 구체적으로 식별자 기반 네트워크 내에서 복수의 단말에 관한 식별자를 생성하고, 식별자를 검증하는 장치 및 방법에 연관된다.

## 배 경 기 술

[0002] 사물 단말의 인터넷 접속을 허용하는 IoT(Internet of Things) 서비스가 활발해짐에 따라 복수의 사물 단말들의 접근을 제어하는 기술과 관련하여서도 다양한 연구가 진행되고 있다.

[0003] 서비스 서버에 보안 스위치나 방화벽을 설치하고, IP(Internet Protocol) 주소나 포트 번호 등을 리스트로서 관리하여 접근을 제어하는 LBAC(ACL based access control) 방식, 미리 지정된 인증 절차를 통과한 제3자에게 토큰(capability)을 부여하고, 통신 패킷에 토큰 정보를 삽입하여 서비스를 제어하는 CBAC(capability based access control) 방식 및 통신 개체의 역할을 정의하고 역할에 따라 시스템에 접근을 제어하는 RBAC(role based access control) 방식 등이 존재하고 있다.

## 발명의 내용

### 해결하려는 과제

### 과제의 해결 수단

[0004] 일측에 따르면, 공개키 기반의 식별자를 생성하는 컴퓨팅 장치가 제공된다. 상기 컴퓨팅 장치는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서에 의해 적어도 일시적으로 구현될 수 있다. 상기 컴퓨팅 장치는 식별자 기반 네트워크에 접속하는 단말로부터 고유 정보를 추출하는 추출부 및 상기 추출된 고유 정보를 키 값으로 이용하여 상기 식별자 기반 네트워크에 대응하는 공개키(publication key) 기반의 식별자(identifier)를 생성하는 생성부를 포함할 수 있다.

[0005] 일실시예에 따르면, 상기 추출부는 상기 식별자 기반 네트워크에 접속하는 복수의 단말로부터 각각의 고유 정보를 추출하고, 상기 생성부는 상기 식별자 기반 네트워크에 대응하는 고유한 공개키 및 상기 각각의 고유 정보를 해시 함수에 입력하여 복수의 공개키 기반의 식별자를 생성할 수 있다.

[0006] 다른 일실시예에 따르면, 상기 생성부는 상기 고유한 공개키 및 상기 각각의 고유 정보를 상기 해시 함수에 입력하여 복수의 해시 기반의 메시지 인증 코드(HMAC: Hash based Message Authentication Code)를 상기 복수의 공개키 기반의 식별자로서 생성할 수 있다.

[0007] 또 다른 일실시예에 따르면, 상기 생성부는 상기 추출된 고유 정보의 제1 비트열을 상기 키 값으로서 해시 함수에 입력하여 해시 기반의 메시지 인증 코드를 생성할 수 있다. 보다 구체적으로, 생성부는 미리 지정된 비트 수에 따라 상기 해시 기반의 메시지 인증 코드에 대응하는 제2 비트열 및 상기 고유 정보에 대응하는 제3 비트열의 결합으로 상기 식별자 기반 네트워크에 대응하는 공개키 기반의 식별자를 생성할 수 있다.

[0008] 또 다른 일실시예에 따르면, 상기 단말이 제1 식별자 기반 네트워크에 접속하는 경우에 상기 생성부는 상기 추출된 고유 정보를 키 값으로 이용하여 상기 제1 식별자 기반 네트워크에 대응하는 제1 공개키 기반의 제1 식별자를 생성하고, 상기 단말이 제2 식별자 기반 네트워크에 접속하는 경우에 상기 생성부는 상기 추출된 고유 정보를 키 값으로 이용하여 상기 제2 식별자 기반 네트워크에 대응하는 제2 공개키 기반의 제2 식별자를 생성할 수 있다.

[0009] 또 다른 일실시예에 따르면, 상기 추출부는 상기 단말의 시리얼 넘버 및 맥 어드레스 중 적어도 하나를 상기 고유 정보로서 추출할 수 있다.

[0010] 또 다른 일실시예에 따르면, 상기 컴퓨팅 장치는 상기 단말에 대응하는 식별자 및 상기 식별자 기반 네트워크에 대응하는 공개키를 매칭하여 저장하는 데이터베이스를 더 포함할 수 있다.

[0011] 다른 일측에 따르면, 식별자 기반 네트워크 내에서 데이터 패킷을 검증하는 방법이 제공된다. 상기 데이터 패킷의 검증 방법은 수신된 데이터 패킷으로부터 소스 식별자(source ID)에 포함되는 제1 데이터 필드 및 목적지 식별자(destination ID)에 포함되는 제2 데이터 필드를 추출하는 단계, 미리 지정된 공개키로 상기 제1 데이터 필드를 해시하고, 해시된 제1 결과값와 상기 소스 식별자를 비교하는 단계, 상기 공개키로 상기 제2 데이터 필드를 해시하고, 해시된 제2 결과값과 상기 목적지 식별자를 비교하는 단계 및 상기 제1 결과값에 관한 비교 결과 및 상기 제2 결과값에 관한 비교 결과에 기초하여 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계를 포함할 수 있다.

[0012] 일실시예에 따르면, 상기 해시된 제1 결과값과 상기 소스 식별자를 비교하는 단계는 상기 해시된 제1 결과값과 상기 소스 식별자 내의 해시 기반의 메시지 인증 코드를 비교하는 단계를 포함하고, 상기 해시된 제2 결과값과 상기 목적지 식별자를 비교하는 단계는 상기 해시된 제2 결과값과 상기 목적지 식별자 내의 해시 기반의 메시지 인증 코드를 비교하는 단계를 포함할 수 있다.

[0013] 다른 일실시예에 따르면 상기 해시된 제1 결과값과 상기 소스 식별자를 비교하는 단계는 상기 해시된 제1 결과값과 상기 소스 식별자 내의 해시 기반의 메시지 인증 코드를 비교하는 단계를 포함하고, 상기 해시된 제2 결과값과 상기 목적지 식별자를 비교하는 단계는 상기 해시된 제2 결과값과 상기 목적지 식별자 내의 해시 기반의 메시지 인증 코드를 비교하는 단계를 포함할 수 있다.

[0014] 또 다른 일실시예에 따르면 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는 상기 해시된 제1 결과값과 상기 소스 식별자 내의 제3 데이터 필드의 불일치 및 상기 해시된 제2 결과값과 상기 목적지 식별자 내의 제4 데이터 필드의 불일치 중 적어도 어느 하나가 발생한 경우에 상기 수신된 데이터 패킷을 삭제하는 단계를 포함할 수 있다.

[0015] 또 다른 일실시예에 따르면 상기 데이터 패킷의 검증 방법은 상기 해시된 제1 결과값, 상기 해시된 제2 결과값 및 검증 결과를 저장하여 식별자 검증 이력 테이블(ID checksum table)을 업데이트하는 단계를 더 포함할 수 있다.

[0016] 또 다른 일실시예에 따르면 상기 데이터 패킷의 검증 방법은 상기 추출된 제1 데이터 필드 및 상기 추출된 제2 데이터 필드를 비교하여 미리 지정된 접근 제어 조건을 만족하는지 여부를 판단하는 단계를 더 포함할 수 있다.

[0017] 또 다른 일실시예에 따르면, 상기 제1 데이터 필드 및 상기 제2 데이터 필드를 추출하는 단계는 상기 소스 식별자의 접근 제어 필드(access control field)를 확인하여 상기 제1 데이터 필드로서 추출하고, 상기 목적지 식별자의 접근 제어 필드를 확인하여 상기 제2 데이터 필드로서 추출하는 단계를 포함할 수 있다.

[0018] 또 다른 일측에 따르면 식별자 검증 이력 테이블을 이용하여 데이터 패킷을 검증하는 방법이 제공된다. 데이터 패킷의 검증 방법은 수신된 데이터 패킷으로부터 소스 식별자에 포함되는 제1 데이터 필드 및 목적지 식별자에 포함되는 제2 데이터 필드를 추출하는 단계 및 저장된 식별자 검증 이력 테이블과 상기 제1 데이터 필드 및 제2 데이터 필드를 비교하여 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계를 포함할 수 있다. 또한, 상기 소스 식별자 및 상기 목적지 식별자는 소스 및 목적지 각각에 대응하는 고유 정보를 키 값으로 이용하여 식별자 기반 네트워크에 대응하는 공개키 기반의 식별자로서 생성될 수 있다.

[0019] 일실시예에 따르면 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는 상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 성공 이력(success history)이 상기 식별자 검증 이력 테이블 내에 존재하는 경우에, 상기 수신된 데이터 패킷을 다음 홉으로 전달하는 단계를 포함할 수 있다.

[0020] 다른 일실시예에 따르면 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는 상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 실패 이력(failure history)이 상기 식별자 검증 이력 테이블 내에 존재하는 경우에, 상기 수신된 데이터 패킷을 삭제하는 단계를 포함할 수 있다.

[0021] 또 다른 일실시예에 따르면 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계는 상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 검증 이력이 존재하지 않는 경우에 상기 식별자 기반 네트워크에 대응하는 공개키를 이용하여 상기 제1 데이터 필드 및 상기 제2 데이터 필드를 각각 해시하는 단계를 더 포함할 수 있다. 또한, 상기 제1 데이터 필드에 대응하는 해시된 제1 결과값과 상기 소스 식별자를 비교하는 단계, 상기 제2 데이터 필드에 대응하는 해시된 제2 결과값과 상기 목적지 식별자를 비교하는 단계 및 상기 제1 결과값에 관한 비교 결과 및 상기 제2 결과값에 관한 비교 결과에 기초하여 상기 수신된 데이터 패킷의 전달여부를 결정하는 단계를 더 포함할 수 있다.

## *도면의 간단한 설명*

[0022] 도 1은 식별자 기반 네트워크를 도시하는 예시도이다.

도 2a 및 도 2b는 일실시예에 따른 식별자 기반 네트워크를 구성하는 프로토콜 스택을 나타내는 예시도이다.

도 3a는 일실시예에 따라 식별자를 생성하는 컴퓨팅 장치를 도시하는 블록도이다.

도 3b는 일실시예에 따라 공개키 기반의 식별자를 생성하는 방법을 도시하는 흐름도이다.

도 4는 일실시예에 따른 접근 제어 필드의 구조를 도시하는 예시도이다.

도 5는 일실시예에 따라 생성된 공개키 기반의 식별자의 구조를 도시하는 예시도이다.

도 6은 일실시예에 따라 식별자 기반 네트워크 내의 식별자 패킷의 구조를 도시하는 예시도이다.

도 7은 일실시예에 따라 식별자 검증 이력을 이용하여 데이터 패킷을 검증하는 과정을 나타내는 흐름도이다.

도 8은 일실시예에 따라 미리 지정된 공개키를 이용하여 데이터 패킷을 검증하는 과정을 나타내는 흐름도이다.

## *발명을 실시하기 위한 구체적인 내용*

[0023] 실시예들에 대한 특정한 구조적 또는 기능적 설명들은 단지 예시를 위한 목적으로 개시된 것으로서, 다양한 형태로 변경되어 실시될 수 있다. 따라서, 실시예들은 특정한 개시형태로 한정되는 것이 아니며, 본 명세서의 범위는 기술적 사상에 포함되는 변경, 균등물, 또는 대체물을 포함한다.

[0024] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 이런 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 해석되어야 한다. 예를 들어, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[0025] 어떤 구성요소가 다른 구성요소에 "연결 되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.

[0026] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 설명된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함으로 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0027] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 해당 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0028] 도 1은 식별자 기반 네트워크를 도시하는 예시도이다. 도 1을 참조하면, 식별자 기반 네트워크(110) 및 IP(Internet Protocol) 네트워크(120)를 통해 데이터를 송수신하는 복수의 사물 단말(141, 142, 143, 144)들이 도시된다. 이하의 설명에서 사물 단말(141, 142, 143, 144)들은 IoT 서비스를 제공하기 위해 인터넷에 연결되는 다양한 형태의 전자 기기를 나타낼 수 있다. 예시적으로, 사물 단말(141, 142, 143, 144)은 사용자 단말로부터 턴 온, 턴 오프, 온도 조절과 같은 다양한 제어 입력을 수신하는 가전제품(141), 지정 구역 내의 온도, 습도, 영상 등을 센싱하여 서버로 전송하는 센서(142), 스마트 폰, 스마트 패드와 같은 사용자 단말(143, 144)과 같이 다양한 형태의 전자 기기로 구현될 수 있을 것이다. 복수의 사물 단말(141, 142, 143, 144)들은 식별자 기반 네트워크(110)를 통해 원하는 데이터를 송수신할 수 있고, 미리 지정된 컴퓨팅 장치(131, 132)에 접속되어 있을 수 있다.

[0029] 컴퓨팅 장치(131, 132)는 식별자 기반 네트워크에 사물 단말(141, 142, 143, 144)들을 연결할 수 있다. 본 실시예에서 컴퓨팅 장치(131, 132)는 식별자 기반 네트워크로의 액세스포인트 또는 게이트웨이로서 동작할 수 있다. 컴퓨팅 장치(131, 132)는 식별자 패킷을 IP 패킷으로 변환할 수 있다. 또한, 컴퓨팅 장치(131, 132)는 IP 패킷을 식별자 패킷으로 변환할 수도 있다. 컴퓨팅 장치(131, 132)는 상기 식별자 패킷 및 상기 IP 패킷 모두를 송수신할 수 있다.

[0030] 도 2a 및 도 2b는 일실시예에 따른 식별자 기반 네트워크를 구성하는 프로토콜 스택을 나타내는 예시도이다. 도 2a를 참조하면, 컴퓨팅 장치(131, 132)에 의해 구현되는 프로토콜 스택이 도시된다. 보다 구체적으로, 컴퓨팅 장치(131, 132)는 물리/데이터 링크 계층(241), 네트워크 계층 및 식별자 계층(231), 전송 계층(221) 및 응용 계층(211)을 프로토콜 스택으로서 포함할 수 있다. 또한, 컴퓨팅 장치(131, 132)는 상기 식별자 패킷을 상기 IP 패킷으로 변환하고, 상기 IP 패킷을 상기 식별자 패킷으로 변환하도록 지원하는 듀얼 프로토콜 스택을 포함할 수 있다. 보다 구체적으로, 컴퓨팅 장치(131, 132)는 제3 계층을 IP 패킷에 상응하는 네트워크 계층 및 식별자 패킷에 상응하는 식별자 계층으로 각각 포함할 수 있다.

[0031] 도 2b를 참조하면, 식별자 기반 네트워크에 접속하는 사물 단말(141, 142, 143, 144)에 의해 구현되는 프로토콜 스택이 도시된다. 보다 구체적으로, 사물 단말(141, 142, 143, 144)은 물리/데이터 링크 계층(242), 식별자 계층(232), 전송 계층(222) 및 응용 계층(212)을 프로토콜 스택으로서 포함할 수 있다. 각각의 사물 단말(141, 142, 143, 144)들을 식별자 통신을 수행하기 위한 식별자 계층(232)을 포함할 수 있다.

[0032] 도 3a는 일실시예에 따라 식별자를 생성하는 컴퓨팅 장치를 도시하는 블록도이다. 컴퓨팅 장치(300)는 프로세서(310) 및 데이터베이스(320)를 포함할 수 있다. 프로세서(310)는 식별자 기반 네트워크에 접속하는 단말로부터 고유 정보를 추출하는 추출부 및 상기 추출된 고유 정보를 키 값으로 이용하여 상기 식별자 기반 네트워크에 대응하는 공개키 기반의 식별자를 생성하는 생성부를 적어도 일시적으로 구현할 수 있다. 추출부는 식별자 기반 네트워크에 접속하는 복수의 단말으로부터 각각의 고유 정보를 추출할 수 있다. 일실시예로서, 상기 추출부는 복수의 단말 각각의 맥 어드레스를 상기 고유 정보로서 추출할 수 있다. 다른 일실시예로서, 상기 추출부는 복수의 단말 기기에 대응하는 시리얼 번호를 상기 고유 정보로서 추출할 수 있다. 예시적으로, 단말이 휴대전화인 경우에 상기 시리얼 번호는 국제모바일기기 식별코드(IMEI: International Mobile Equipment Identity)로 구현될 수 있다. 또 다른 일실시예로서, 상기 추출부는 복수의 단말에 연관되는 사용자로부터 고유 정보를 직접 입력 받을 수도 있다. 이를테면, 미리 지정된 QR 코드를 사용자가 촬영하면 해당 전자기기의 고유 정보가 컴퓨팅 장치(300)로 전송되도록 하여 상기 추출부는 고유 정보를 추출할 수 있다.

[0033] 생성부는 식별자 기반 네트워크에 대응하는 고유한 공개키 및 단말의 고유 정보를 해시 함수에 입력할 수 있다. 또한, 생성부는 고유한 공개키 및 단말의 고유 정보를 해시 함수에 입력하여 해시 기반의 메시지 인증 코드(HMAC: Hash based Message Authentication Code)를 식별자로서 생성할 수 있다. 본 실시예에 따른 컴퓨팅 장치(300)는 식별자 기반 네트워크에 대응하는 어느 하나의 공개키를 미리 지정할 수 있다. 그에 따라, 컴퓨팅 장치(300)는 하나의 공개키를 이용하여 서로 다른 고유 정보를 갖는 복수의 단말에 대응하는 각각의 식별자를 생성할 수 있다. 해시 함수를 이용하여 HMAC를 생성하는 구체적 과정은 기술 분야의 전문가에게는 straight forward한 내용이므로 자세한 설명은 생략하기로 한다.

[0034] 또 다른 일실시예로서, 생성부는 추출된 고유 정보의 제1 비트열을 키 값으로서 해시 함수에 입력할 수 있다. 상기 제1 비트열은 미리 설정된 조건에 따라 고유 정보의 제1 비트에서부터 제2 비트까지의 데이터를 추출한 비트열을 나타낼 수 있다. 전자 기기의 유형에 따라 시리얼 넘버의 크기가 상이할 경우가 존재할 수 있다. 본 실시예에 따른 컴퓨팅 장치(300)는 미리 지정된 크기에 대응하는 비트열을 이용하여 해시 함수에 키 값으로서 입력할 수 있어, 상이한 전자 기기들도 동일한 길이를 갖는 식별자를 생성할 수 있도록 제어할 수 있다.

[0035] 데이터베이스(320)는 단말에 대응하는 식별자 및 식별자 기반 네트워크에 대응하는 공개키를 매칭하여 저장할 수 있다. 식별자를 할당 받은 단말은 프로토콜 스택 내의 식별자 계층에 할당 받은 식별자를 등록할 수 있다.

[0036] 도 3b는 일실시예에 따라 공개키 기반의 식별자를 생성하는 방법을 도시하는 흐름도이다. 도 3b를 참조하면, 공개키 기반의 식별자를 생성하는 방법은 식별자 기반 네트워크에 접속하는 단말로부터 고유 정보를 추출하는 단계(330) 및 상기 식별자 기반 네트워크에 대응하는 공개키 및 고유 정보를 해시 함수에 입력하여 공개키 기반의 식별자를 생성하는 단계(340)를 포함할 수 있다.

[0037] 단계(330)에서 식별자 기반 네트워크에 접속하는 단말로부터 고유 정보를 추출하는 과정에 대한 설명은 도 3a의 프로세서(310)에 관한 설명이 그대로 적용될 수 있어 중복되는 설명은 생략하기로 한다.

[0038] 단계(340)에서 컴퓨팅 장치는 식별자 기반 네트워크에 대응하는 공개키를 선택할 수 있다. 예시적으로, 단말이 제1 식별자 기반 네트워크에 접속하는 경우에 상기 단말은 상기 제1 식별자 기반 네트워크에 대응하는 제1 공개키 기반의 제1 식별자를 할당 받을 수 있다. 또한, 상기 단말이 제2 식별자 기반 네트워크에 접속하는 경우에 상기 단말은 상기 제2 식별자 기반 네트워크에 대응하는 제2 공개키 기반의 제2 식별자를 할당 받을 수 있다. 컴퓨팅 장치는 단말이 접속하려고 하는 식별자 기반 네트워크에 따라 식별자 생성에 이용되는 공개키를 선택할 수 있다.

[0039] 단계(340)에서 컴퓨팅 장치는 추출된 고유 정보의 제1 비트열을 키 값으로 이용하여 해시 함수에 입력할 수 있다. 컴퓨팅 장치는 해시 기반의 메시지 인증 코드를 생성할 수 있다. 컴퓨팅 장치는 미리 지정된 비트 수에 따라 상기 해시 기반의 메시지 인증 코드에 대응하는 제2 비트열 및 단말의 고유 정보에 대응하는 제3 비트열을 결합하여 공개키 기반의 식별자를 생성할 수 있다. 공개키 기반의 식별자의 예시적 구조는 이하에서 추가될 도면과 함께 자세하게 설명될 것이다.

[0040] 도 4는 일실시예에 따른 접근 제어 필드의 구조를 도시하는 예시도이다. 도 4를 참조하면, 공개키 기반의 식별

자에 포함되는 접근 제어 필드의 예시도가 도시된다. 일실시예로서, 접근 제어 필드는 고유 정보(410)를 포함하는 것으로 구현될 수 있다. 고유 정보(410)는 단말에 대응하는 식별 정보를 나타낼 수 있다. 예시적으로, 고유 정보(410)는 단말의 시리얼 번호 및 단말의 맥 어드레스 중 어느 하나로 구현될 수 있다. 또한, 고유 정보(410)는 단말에 대응하는 식별 정보 중 미리 지정된 비트수만큼 추출된 정보를 나타낼 수 있다.

[0041] 다른 일실시예로서, 접근 제어 필드는 고유 정보(410)에 디바이스 유형(420) 및 접근 제어 상태(430)를 추가적으로 더 포함하도록 구현될 수 있다. 접근 제어 상태(430)는 사물 단말에 관한 접근 제어의 실행 여부를 나타낼 수 있다. 예시적으로, 공개키 기반 네트워크 내에서 접근 제어 기능이 실행되면 특정 사용자의 공개키로 등록된 식별자로만 해당 사물 단말에 접속할 수 있을 것이다. 또한, 접근 제어 기능이 해제되면 어떤 식별자 이든지 해당 사물 디바이스에 접근할 수 있을 것이다.

[0042] 디바이스 유형(420)은 미리 지정된 필드값에 따라 사물 단말의 접근 제어를 결정하는 정보를 나타낼 수 있다. 예시적으로, 디바이스 유형(420)은 세 가지 유형으로 정의될 수 있다. 제1 디바이스 유형은 모든 유형의 식별자에 대해 접근 가능한 전자 기기를 나타내고, 제2 디바이스 유형은 제1 디바이스 유형 및 제2 디바이스 유형에 대해 접근이 가능하고, 제3 디바이스 유형은 제1 디바이스 유형 식별자 하나로만 접근이 가능한 디바이스를 나타낼 수 있다. 예시적으로, 제1 디바이스 유형은 사용자에 연관되는 스마트 폰, 컴퓨터, 랩탑 컴퓨터와 같은 디바이스 또는 센싱 데이터를 제공하는 센서 디바이스에 할당될 수 있다. 또한, 제2 디바이스 유형은 M2M(machine to machine) 통신을 필요로 하는 냉장고, 세탁기 등의 가전제품에 할당될 수 있다. 제3 디바이스 유형은 개인 전용의 접근을 허용하는 디바이스에 할당될 수 있다. 디바이스 유형(430)의 구체적 구현에 관한 위와 같은 설명은 이해를 돕기 위한 예시적 설명일 뿐, 다른 실시예들의 범위를 제한하거나 한정하는 것으로 해석되어서는 안될 것이다.

[0043] 도 5는 일실시예에 따라 생성된 공개키 기반의 식별자의 구조를 도시하는 예시도이다. 도 5를 참조하면, 공개키 기반의 식별자의 예시적 구조가 도시된다. 공개키 기반의 식별자는 식별자 헤더(510)(ID header) 및 식별자 바디(520)(ID body)를 포함할 수 있다. 식별자 헤더(510)는 공개키 기반의 식별자에 관한 버전 정보(511) 및 접근 제어 필드(512)를 포함할 수 있다. 버전 정보(511)는 식별자 기반 네트워크에 관한 식별 정보 및 접근 제어 필드(512)의 길이 정보를 포함할 수 있다. 접근 제어 필드(512)는 도 4와 함께 기재된 설명이 그대로 적용될 수 있어 중복되는 설명은 생략하기로 한다.

[0044] 식별자 바디(520)는 해시 기반의 메시지 인증 코드를 포함할 수 있다. 보다 구체적으로, 해시 기반의 메시지 인증 코드는 식별자 기반 네트워크에 대응하는 공개키를 대상으로 단말의 고유 정보를 키로 하여 생성될 수 있다. 예시적으로, 식별자 바디(520)가 생성되는 과정에는 MD5, SHA-1, RIPEMD-128/160등의 해시 함수가 이용될 수 있다. 앞서 기재한 해시 함수에 관한 설명은 예시적 기재일 뿐, 기술 분야의 전문가의 선택에 따라 다양한 변경이 가능하다는 것은 자명한 사실일 것이다.

[0045] 도 6은 일실시예에 따라 식별자 기반 네트워크 내의 식별자 패킷의 구조를 도시하는 예시도이다. 도 6을 참조하면, 식별자 기반 네트워크를 이용하여 제1 단말에서 제2 단말로 전송되는 데이터 패킷의 구체적 예시가 도시된다. 일실시예로서, 제1 단말 및 제2 단말은 동일한 식별자 기반 네트워크에 포함될 수 있다. 다른 일실시예로서 제1 단말 및 제2 단말 각각은 서로 상이한 식별자 기반 네트워크에 포함될 수 있다.

[0046] 식별자 패킷은 헤더(610)(header) 및 페이로드(620)(payload)를 포함할 수 있다. 헤더(610)는 버전 정보, 헤더 길이 정보, 전체 길이 정보 및 식별자 체크썸을 포함하는 제1 계층을 포함할 수 있다. 예시적으로, 식별자 체크썸(ID checksum)은 미리 지정된 해시 함수를 이용하여 발신지 식별자 및 목적지 식별자를 해시한 값을 나타낼 수 있다. 보다 구체적으로, 식별자 체크썸은 H(source ID||destination ID)를 나타낼 수 있다.

[0047] 또한, 헤더(610)는 옵션 필드를 제2 계층으로서 포함할 수 있다. 헤더(610)는 발신지 식별자(source ID)를 제3 계층으로서 포함할 수 있다. 보다 구체적으로, 발신지 식별자는 제1 단말의 고유 정보를 이용하여 생성된 공개키 기반의 식별자를 나타낼 수 있다. 헤더(610)는 목적지 식별자(destination ID)를 제4 계층으로서 포함할 수 있다. 보다 구체적으로, 목적지 식별자는 제2 단말의 고유 정보를 이용하여 공개키 기반의 식별자를 나타낼 수 있다.

[0048] 페이로드(620)는 제1 단말이 제2 단말로 전송하고자 하는 데이터를 포함할 수 있다.

[0049] 도 7은 일실시예에 따라 식별자 검증 이력을 이용하여 데이터 패킷을 검증하는 과정을 나타내는 흐름도이다. 단계(710)에서 컴퓨팅 장치는 수신된 데이터 패킷으로부터 소스 식별자에 포함되는 제1 데이터 필드 및 목적지 식별자에 포함되는 제2 데이터 필드를 추출할 수 있다. 본 실시예에서 컴퓨팅 장치는 식별자 기반 네트워크를

통해 단말 사이의 데이터 전송을 구현하는 엑세스포인트 또는 게이트웨이를 나타낼 수 있다. 예시적으로, 상기 제1 데이터 필드 및 상기 제2 데이터 필드는 소스 식별자 및 목적지 식별자 각각에 포함되는 접근 제어 필드를 나타낼 수 있다.

[0050] 단계(720)에서 컴퓨팅 장치는 저장된 식별자 검증 이력 테이블과 상기 제1 데이터 필드 및 상기 제2 데이터 필드를 비교할 수 있다. 보다 구체적으로, 컴퓨팅 장치는 미리 지정된 공개키 및 해시 함수를 이용하여 상기 제1 데이터 필드 및 상기 제2 데이터 필드 각각을 해시할 수 있다. 컴퓨팅 장치는 상기 제1 데이터 필드를 해시한 제1 결과값 및 상기 제2 데이터 필드를 해시한 제2 결과값을 식별자 검증 이력 테이블과 비교할 수 있다.

[0051] 도 7에서 도시되지 않았지만, 다른 일실시예로서 컴퓨팅 장치는 데이터 패킷으로부터 식별자 체크썸 자체를 추출할 수 있다. 보다 구체적으로, 상기 식별자 체크썸은 소스 식별자 및 목적지 식별자 각각이 미리 해시된 값, H(source ID||destination ID)을 나타낼 수 있다.

[0052] 단계(730)에서 컴퓨팅 장치는 상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 검증 이력이 존재하는지 여부를 확인할 수 있다. 상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 검증 이력이 존재하지 않는 경우에, 컴퓨팅 장치는 단계(753)를 수행할 수 있다. 보다 구체적으로, 단계(753)에서 컴퓨팅 장치는 추가적인 데이터 패킷의 검증을 실행할 수 있다. 추가적인 데이터 패킷의 검증 과정은 이하의 도 8과 함께 자세하게 설명될 것이다.

[0053] 상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 검증 이력이 존재하는 경우에, 컴퓨팅 장치는 단계(740)를 수행할 수 있다. 컴퓨팅 장치는 상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 성공 이력(success history)이 식별자 검증 이력 테이블 내에 존재하지는 여부를 확인할 수 있다. 상기 성공 이력이 존재하는 경우에, 컴퓨팅 장치는 단계(751)를 수행할 수 있다. 단계(751)에서 컴퓨팅 장치는 상기 수신된 데이터 패킷을 다음 홉으로 전달할 수 있다. 반면에, 상기 성공 이력이 존재하지 않고 실패 이력이 존재하는 경우에, 컴퓨팅 장치는 단계(752)를 수행할 수 있다. 단계(752)에서 컴퓨팅 장치는 상기 수신된 데이터 패킷을 삭제할 수 있다.

[0054] 도 8은 일실시예에 따라 미리 지정된 공개키를 이용하여 데이터 패킷을 검증하는 과정을 나타내는 흐름도이다. 단계(810)에서 컴퓨팅 장치는 수신된 데이터 패킷으로부터 소스 식별자에 포함되는 제1 데이터 필드 및 목적지 식별자에 포함되는 제2 데이터 필드를 추출할 수 있다. 예시적으로, 컴퓨팅 장치는 소스 식별자에 포함되는 접근 제어 필드를 상기 제1 데이터 필드로서 추출할 수 있다. 또한, 컴퓨팅 장치는 목적지 식별자에 포함되는 접근 제어 필드를 상기 제2 데이터 필드로서 추출할 수 있다.

[0055] 단계(820)에서 컴퓨팅 장치는 미리 지정된 공개키로 상기 제1 데이터 필드를 해시하고, 해시된 제1 결과값과 상기 소스 식별자를 비교할 수 있다. 보다 구체적으로, 컴퓨팅 장치는 소스 식별자의 접근 제어 필드를 키 값으로서 이용하여 해시된 제1 결과값을 생성할 수 있다. 또한, 단계(830)에서 컴퓨팅 장치는 미리 지정된 공개키로 상기 제2 데이터 필드를 해시하고, 해시된 제2 결과값과 상기 목적지 식별자를 비교할 수 있다. 보다 구체적으로, 컴퓨팅 장치는 목적지 식별자의 접근 제어 필드를 키 값으로서 이용하여 해시된 제2 결과값을 생성할 수 있다.

[0056] 단계(840)에서 컴퓨팅 장치는 상기 제1 결과값에 관한 비교 결과 및 상기 제2 결과값에 관한 비교 결과에 기초하여 상기 수신된 데이터 패킷의 전달여부를 결정할 수 있다. 보다 구체적으로, 컴퓨팅 장치는 상기 제1 결과값에 관한 비교 결과 및 상기 제2 결과값에 관한 비교 결과 모두가 일치한 경우에 데이터 패킷을 다음 홉으로 전달할 수 있다. 반면에, 컴퓨팅 장치는 상기 제1 결과값에 관한 비교 결과 및 상기 제2 결과값에 관한 비교 결과 중 적어도 하나가 불일치하는 경우에 데이터 패킷을 폐기할 수 있다.

[0057] 이상에서 설명된 실시예들은 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치, 방법 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소

(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

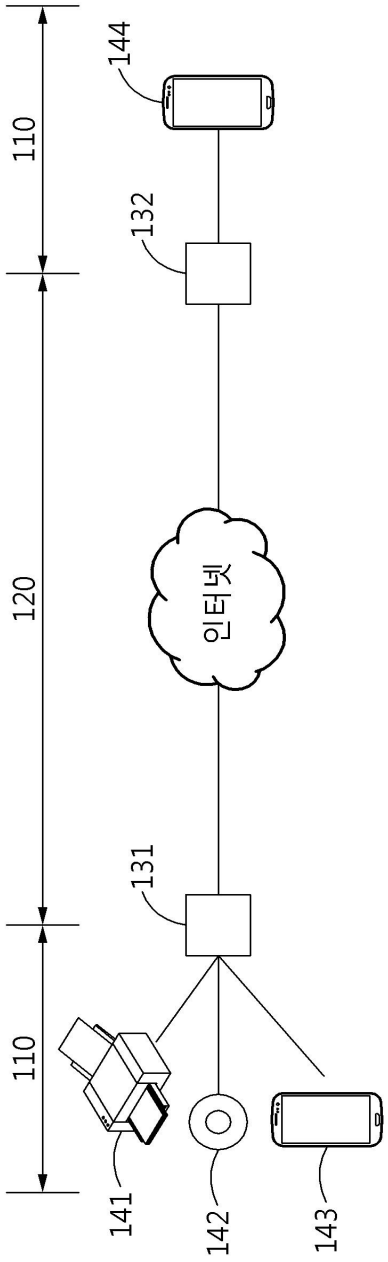
[0058] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0059] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

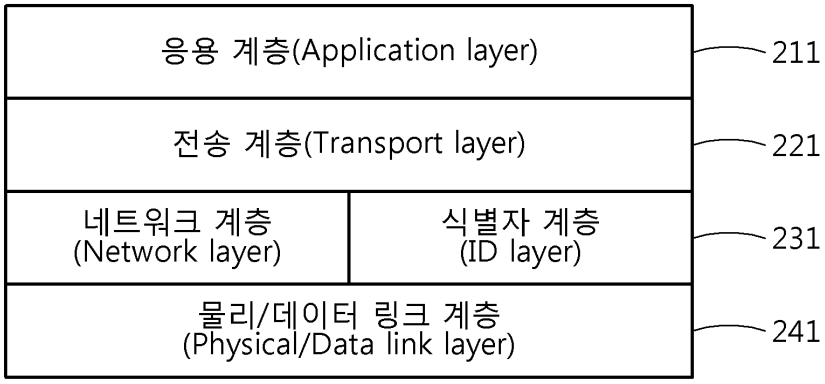
[0060] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기를 기초로 다양한 기술적 수정 및 변형을 적용할 수 있다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

도면

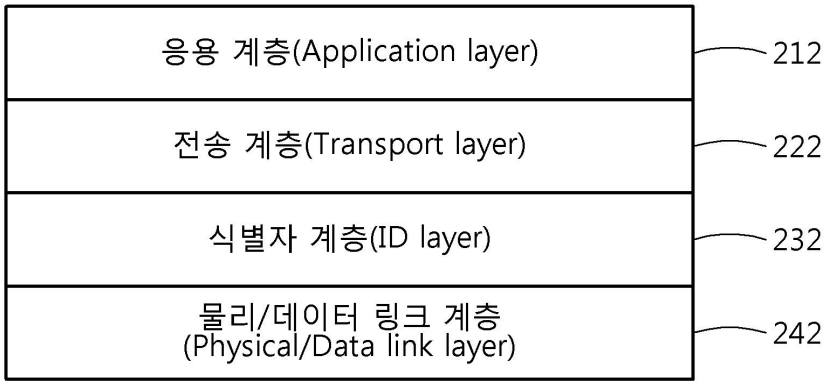
도면1



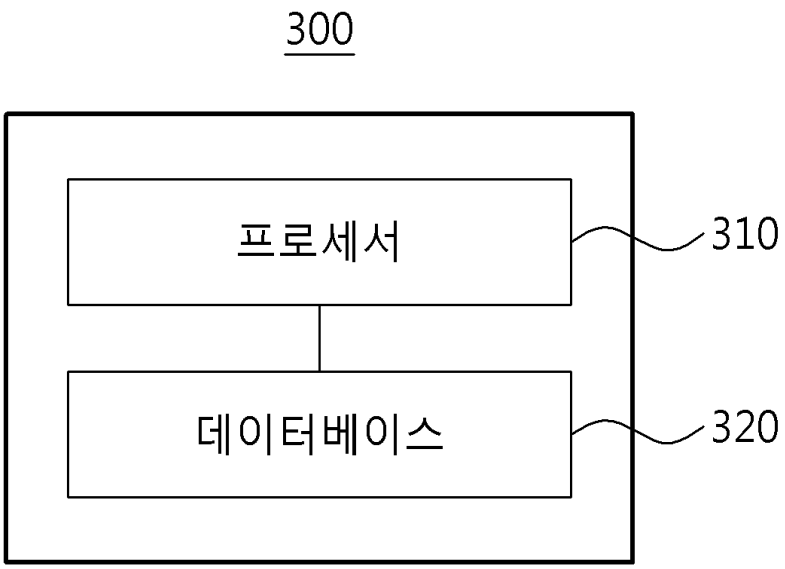
도면2a



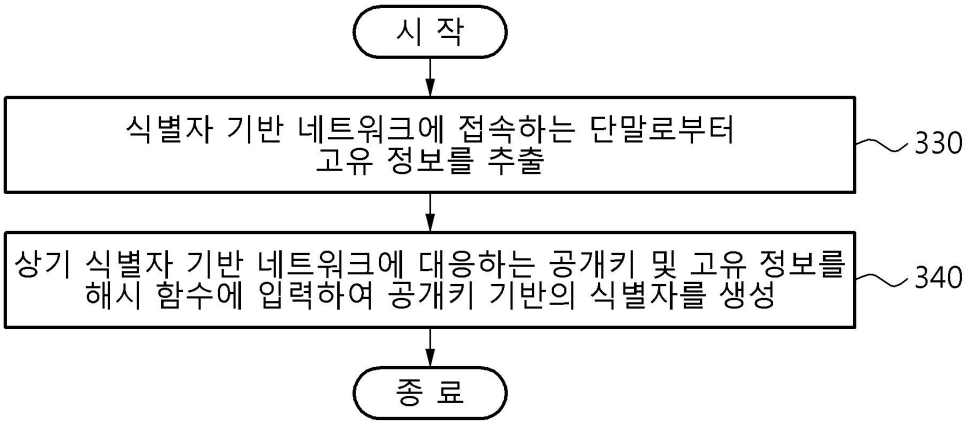

도면2b



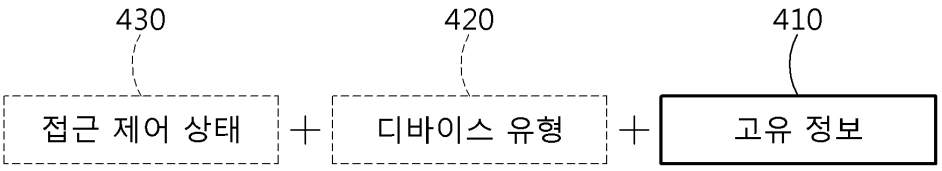

도면3a



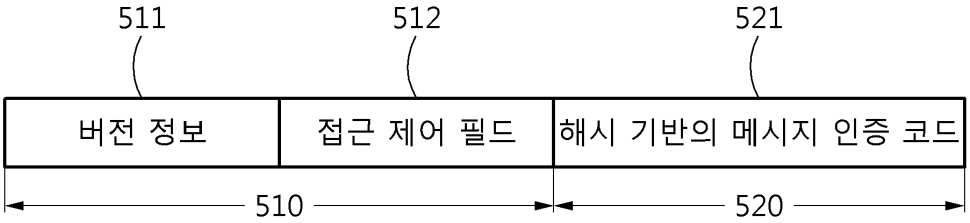
도면3b


시 작
식별자 기반 네트워크에 접속하는 단말로부터
고유 정보를 추출
330
상기 식별자 기반 네트워크에 대응하는 공개키 및 고유 정보를
해시 함수에 입력하여 공개키 기반의 식별자를 생성
340
종 료

도면4

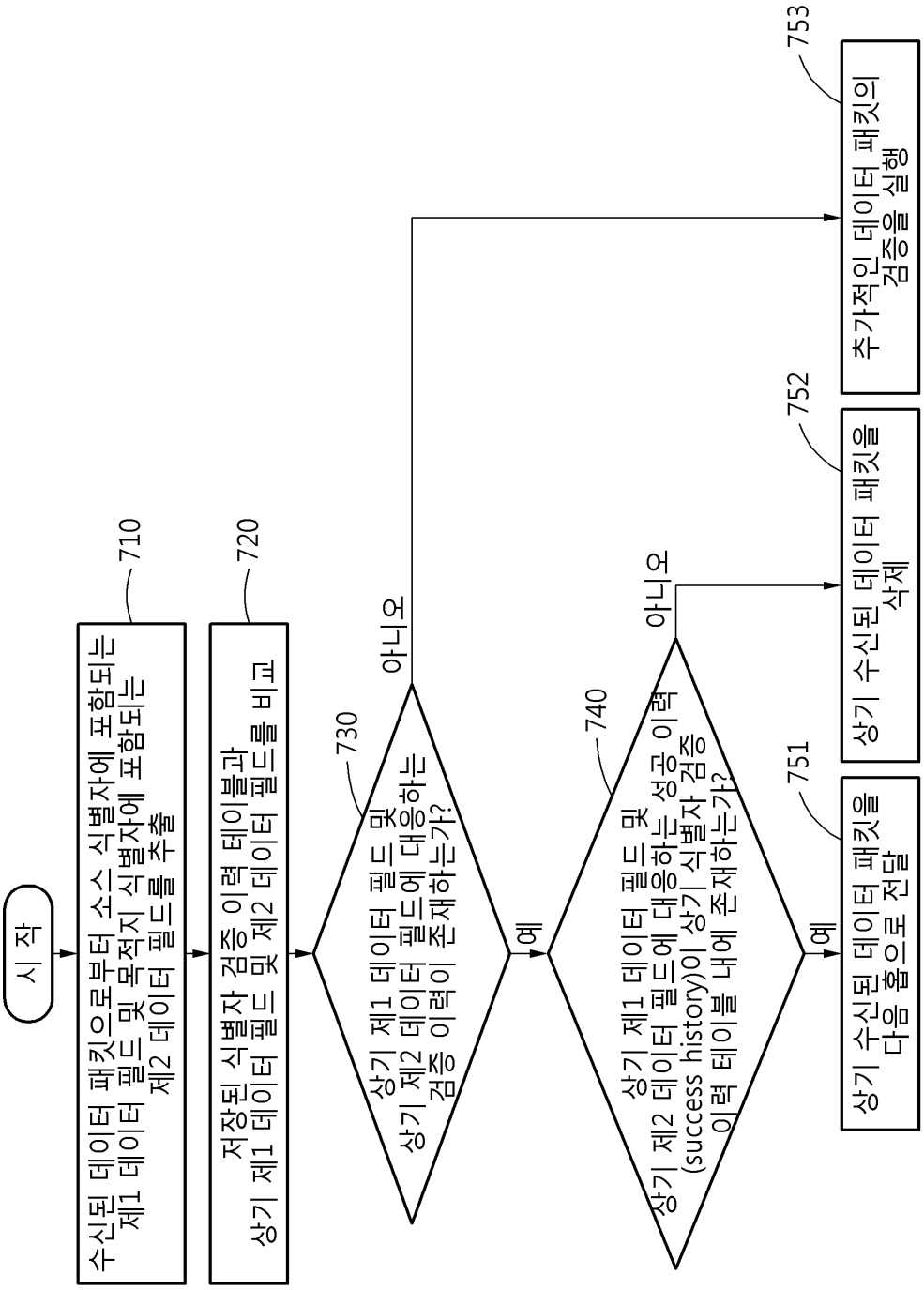

430
420
410
접근 제어 상태
+
디바이스 유형
+
고유 정보

도면5

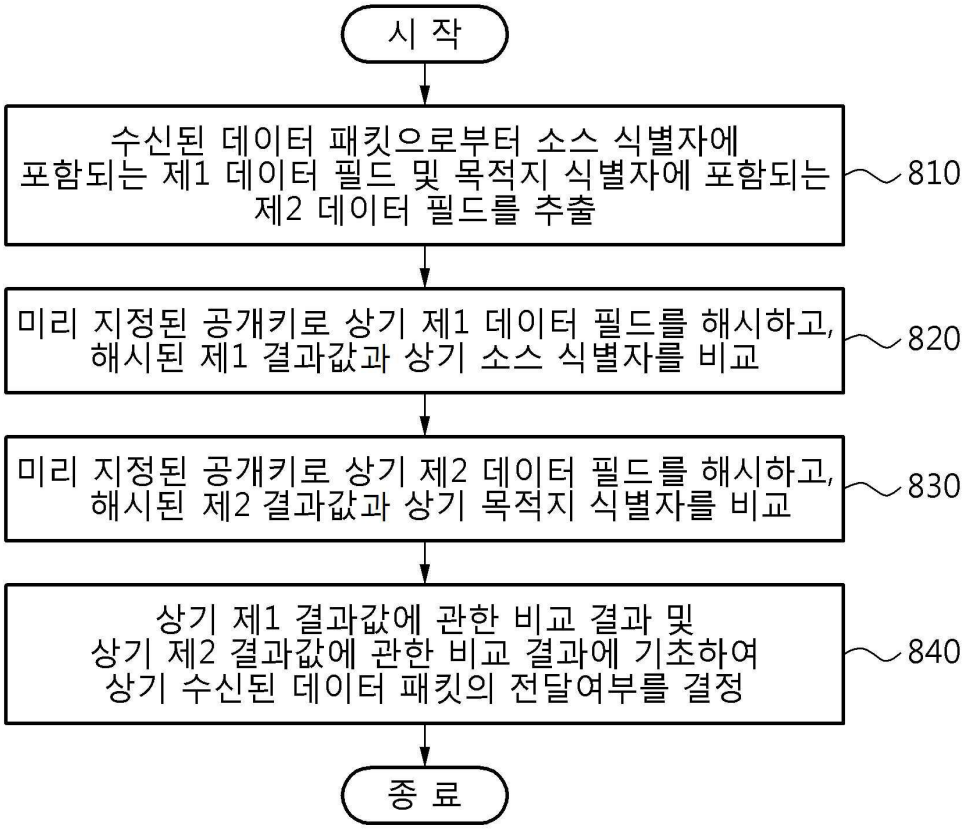

511
512
521
버전 정보
접근 제어 필드
해시 기반의 메시지 인증 코드
510
520

도면6

도면7


시 작
수신된 데이터 패킷으로부터 소스 식별자에 포함되는 제1 데이터 필드 및 목적지 식별자에 포함되는 제2 데이터 필드를 추출
710
저장된 식별자 검증 이력 테이블과 상기 제1 데이터 필드 및 제2 데이터 필드를 비교
720
상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 검증 이력이 존재하는가?
730
아니오
예
상기 제1 데이터 필드 및 상기 제2 데이터 필드에 대응하는 성공 이력(success history)이 상기 식별자 검증 이력 테이블 내에 존재하는가?
740
아니오
예
상기 수신된 데이터 패킷을 다음 홉으로 전달
751
상기 수신된 데이터 패킷을 삭제
752
추가적인 데이터 패킷의 검증을 실행
753

도면8


시 작
수신된 데이터 패킷으로부터 소스 식별자에 포함되는 제1 데이터 필드 및 목적지 식별자에 포함되는 제2 데이터 필드를 추출
810
미리 지정된 공개키로 상기 제1 데이터 필드를 해시하고, 해시된 제1 결과값과 상기 소스 식별자를 비교
820
미리 지정된 공개키로 상기 제2 데이터 필드를 해시하고, 해시된 제2 결과값과 상기 목적지 식별자를 비교
830
상기 제1 결과값에 관한 비교 결과 및 상기 제2 결과값에 관한 비교 결과에 기초하여 상기 수신된 데이터 패킷의 전달여부를 결정
840
종 료