(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0130440
(43) 공개일자 2019년11월22일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/08* (2006.01)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
H04W 12/04 (2009.01)
(52) CPC특허분류
H04L 9/3226 (2013.01)
H04L 67/12 (2013.01)
(21) 출원번호 10-2018-0094825
(22) 출원일자 2018년08월14일
심사청구일자 2018년08월14일
(30) 우선권주장
1020180047887 2018년04월25일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
윤현기
서울특별시 송파구 바람드리길 10 (풍납동)
민성기
서울 중랑구 상봉로 131, A동 3402호 (상봉동, 상봉 듀오트리스 주상복합)
(뒷면에 계속)
(74) 대리인
윤귀상

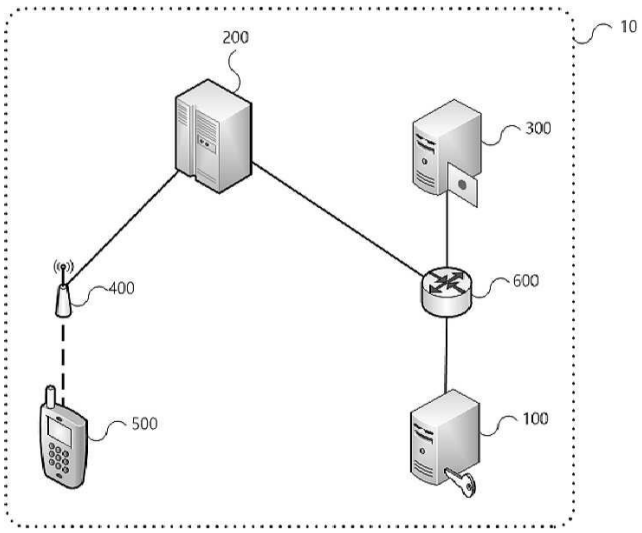
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **센서 장치의 인증을 위해 인증 프로토콜을 수행하는 센서 인증 서버, 소프트웨어 정의 네트워크 컨트롤러 및 방법, 이 방법을 수행하기 위한 기록 매체**

(57) 요 약

접속 장치(AP)로부터 센서 장치(STA)와 접속 장치(AP)와 관련된 정보를 포함한 메시지를 수신하여, 센서 장치(STA)의 인증 요청이 최초인 경우 인증을 수행하는 것으로 결정하고, 센서 인증 서버(S.AS) 및 상기 인증 서버(AS)와 인증 프로토콜을 수행하여, 제 1 마스터 키(PMK_0)의 생성 및 센서 인증 서버(S.AS)와 보안 연관(SA)을 생성한다. 제 1 마스터 키(PMK_0)를 이용하여 센서 장치(STA)를 위한 제 2 마스터 키(PMKs)와 접속 장치(AP)를 위한 제 3 마스터 키(PMKap)를 생성하여 접속 장치(AP)에게 송신한다. 제 2 마스터 키(PMKs)와 제 3 마스터 키(PMKap)를 이용하여 센서 장치(STA)와 접속 장치(AP)는 세션용 암호키를 생성함으로써 보안 연관(SA)을 생성하는 센서 장치를 위한 인증 프로토콜을 수행한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0618 (2013.01)
H04L 9/0869 (2013.01)
H04W 12/04 (2019.01)

(72) 발명자
최주호
서울특별시 성동구 행당로 82, 116동 2004호(행당동, 행당 한진타운)

김태윤
서울특별시 양천구 목동동로 130, 1404동 202호 (신정동, 목동신시가지14단지아파트)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711055347
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 SW중심대학 지원사업 (SW전문인력양성사업 / 정보통신창의인재양성)
연구과제명 SW중심대학(고려대)
기 여 율 1/1
주관기관 고려대학교산학협력단
연구기간 2015.10.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

센서 장치의 인증을 위한 인증 프로토콜 수행하는 센서 인증 서버(S.AS, Sensor Authentication Server)에 있어서,

소프트웨어 정의 네트워크 컨트롤러(SDNc, Software Defined Network controller)에 연결되어 메시지를 수신 및 송신하는 통신부;

상기 소프트웨어 정의 네트워크 컨트롤러(SDNc)로부터 수신한 상기 센서 장치(STA, Station)의 인증 요청이 최초인지 여부에 대해 응답하는 판단부;

상기 센서 장치(STA)의 인증 요청이 최초인 경우, 상기 소프트웨어 정의 네트워크 컨트롤러(SDNc) 및 인증 서버(AS, Authentication Server)와 인증 프로토콜을 수행하는 인증부;

인증 프로토콜의 수행을 완료하면, 제 1 마스터키(PMK_0, Pairwise Master Key)를 생성하고, 상기 소프트웨어 정의 네트워크 컨트롤러(SDNc)와 보안 연관(SA, Security Association)을 생성하는 연관부; 및

상기 제 1 마스터 키와 상기 센서 장치(STA)의 센서키(sensorkey)를 이용하여 상기 센서 장치(STA)와 접속 장치(AP, Access Point)의 보안 연관 생성을 위한 제 2 마스터 키(PMKs)를 생성하는 키 생성부;를 포함하는, 센서 인증 서버.

청구항 2

제 1항에 있어서,

미리 설정된 상기 센서 장치(STA)의 아이디(SensorID), 상기 센서 장치(STA)의 센서키(sensorkey) 및 상기 센서 장치(STA)의 인증 요청에 따른 인증 수행 여부를 저장하는 저장부를 더 포함하는, 센서 인증 서버.

청구항 3

제 1항에 있어서,

상기 제 1 마스터키(PMK_0)를 보관하는 키 관리부를 더 포함하는, 센서 인증 서버.

청구항 4

제 3항에 있어서, 상기 키 생성부는,

상기 센서 장치(STA)의 인증 요청이 최초가 아닌 경우, 상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관을 다시 생성하기 위해 상기 키 관리부에 보관된 제 1 마스터 키(PMK_0)를 이용하여 제 2 마스터 키(PMKs)를 생성하는, 센서 인증 서버.

청구항 5

센서 장치의 인증을 위한 인증 프로토콜을 수행하는 소프트웨어 정의 네트워크 컨트롤러(SDNc, Software Defined Network Controller)에 있어서,

접속 장치(AP), 인증 서버(AS), 센서 인증 서버(S.AS)와 네트워크를 통해 메시지를 수신 및 송신하는 통신부;

상기 센서 장치(STA)로부터 수신한 인증 요청이 최초인 경우 인증을 수행하는 것으로 결정하는 결정부;

인증을 수행하는 것으로 결정한 경우, 상기 센서 인증 서버(S.AS) 및 상기 인증 서버(AS)와 인증 프로토콜을 수행하는 인증부;

인증 프로토콜의 수행을 완료하면, 제 1 마스터 키(PMK_0)를 생성하며, 상기 센서 인증 서버(S.AS)와 보안 연관(SA)을 생성하는 연관부; 및

상기 제 1 마스터 키(PMK_0)를 이용하여 상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관(SA) 생성을 위한 제 2 마스터 키(PMKap)를 생성하는 키 생성부를 포함하는, 소프트웨어 정의 네트워크 컨트롤러.

청구항 6

제5항에 있어서,

상기 센서 인증 서버의 아이디(S.ASID) 및 상기 센서 장치(STA)의 인증 요청에 따른 인증 수행 여부를 저장하는 저장부를 더 포함하는, 소프트웨어 정의 네트워크 컨트롤러.

청구항 7

제5항에 있어서,

상기 제 1 마스터키(PMK_0)를 보관하는 키 관리부를 더 포함하는, 소프트웨어 정의 네트워크 컨트롤러.

청구항 8

제7항에 있어서, 상기 키 생성부는,

상기 센서 장치(STA)의 인증 요청이 최초가 아닌 경우, 상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관을 다시 생성하기 위해 상기 키 관리부에 보관된 제 1 마스터 키(PMK_0)를 이용하여 제 2 마스터 키(PMKap) 생성하는, 소프트웨어 정의 네트워크 컨트롤러.

청구항 9

소프트웨어 정의 네트워크 컨트롤러(SDNc)에 의해 수행되는 센서 장치의 인증을 위한 인증 프로토콜 수행 방법에 있어서,

상기 센서 장치(STA)와 접속 장치(AP)의 정보를 포함한 제 1 메시지를 수신하며, 상기 센서 장치(STA)의 인증 요청이 최초인 경우 인증 프로토콜을 수행하는 것으로 결정하는 단계;

인증 프로토콜을 수행하는 것으로 결정한 경우, 센서 인증 서버(S.AS) 및 인증 서버(AS)와 인증 프로토콜을 수행하는 단계;

인증 프로토콜의 수행을 완료하면, 제 1 마스터키(PMK_0)를 생성하고, 상기 센서 인증 서버(S.AS)와 보안 연관(SA)을 생성하는 단계;

상기 제 1 마스터키(PMK_0)를 이용하여 상기 센서 인증 서버(S.AS)에 의해 생성된 제 2 마스터 키(PMKs)를 포함한 메시지에 상기 제 1 마스터키(PMK_0)를 이용하여 생성한 제 3 마스터 키(PMKap)를 부가하여 제 2 메시지를 생성하는 단계; 및

상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관(SA)을 생성하기 위해 상기 제 2 메시지를 송신하는 단계를 포함하는, 인증 프로토콜의 수행 방법.

청구항 10

제9항에 있어서,

상기 인증 프로토콜의 수행을 완료하여 생성된 제 1 마스터 키(PMK_0)를 보관하는 단계를 더 포함하는, 인증 프로토콜의 수행 방법.

청구항 11

제 10항에 있어서, 인증 프로토콜을 수행하는 것으로 결정하는 단계는,

상기 센서 장치(STA)의 인증 요청이 최초가 아닌 경우, 인증 프로토콜을 수행하지 않는 것으로 결정하고, 상기 인증 프로토콜을 수행하는 단계 및 상기 센서 인증 서버(S.SA)와 보안 연관(SA)을 생성하는 단계를 수행하지 않는, 인증 프로토콜의 수행 방법.

청구항 12

제 11항에 있어서, 상기 제 2 메시지를 생성하는 단계는,

상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관(SA)을 다시 생성하기 위해, 상기 보관된 제 1 마스터키(PMK_0)를 이용하여 상기 센서 인증 서버(S.AS)에 의해 생성된 제 2 마스터 키(PMKs)를 포함한 메시지에 상기 보관된 제 1 마스터키(PMK_0)를 이용하여 생성한 제 3 마스터 키(PMKap)를 부가하여 제 2 메시지를 생성하는, 인증 프로토콜의 수행 방법.

청구항 13

제 12항에 있어서,

상기 센서 장치(STA)와 같은 사물 인터넷 서비스 도메인(IoT Service Domain)에 포함된 네트워크에 다른 센서 장치(STA)가 인증을 요청 하는 경우, 상기 센서 장치(STA)의 인증 요청이 최초가 아닌 경우와 동일한 과정을 수행하는, 인증 프로토콜의 수행 방법.

청구항 14

제9항에 있어서, 상기 제 2 메시지를 생성하는 단계는,

상기 센서 장치(STA)에 의해 제 2 마스터 키(PMKs)를 생성할 때 사용한 것과 동일한 키 파생 함수(KDF, Key Derivation Function)를 이용하여 상기 제 3 마스터 키(PMKap)를 생성하는, 인증 프로토콜의 수행 방법.

청구항 15

제9항 내지 제 14항 중 어느 한 항에 따른 인증 프로토콜의 수행 방법을 실행하기 위한 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 센서 장치의 인증을 위해 인증 프로토콜을 수행하는 센서 인증 서버(S.AS, Sensor Authentication Server), 소프트웨어 정의 네트워크 컨트롤러(SDNc, Software Defined Network controller) 및 방법에 관한 것

으로서, 더욱 상세하게는 소프트웨어 정의 네트워크 컨트롤러를 이용하여 사물 인터넷(IoT) 환경과 같은 센서 네트워크에서 수행되는 센서 장치의 인증 프로토콜에 관한 것이다.

배 경 기 술

[0003] 사물 인터넷(IoT, Internet-of-Things)은 사물에 센서 기능과 통신기능을 내장하여 실시간으로 데이터를 주고받는 기술 혹은 환경을 의미한다.

[0004] 사물이 연결되는 유/무선 네트워크인 센서 네트워크는 IEEE 802.15나 IEEE 802.11과 같은 무선네트워크 또는 유선네트워크 등 다양한 방법으로 연결 될 수 있다. 연결 과정에서 악의적이거나 정책에 반하는 장치를 걸러내기 위해 인증과정을 수행할 수도 있다. 이러한 인증 프로토콜 중에서 가장 대표적인 프로토콜이 IEEE 802.1x이다.

[0005] IEEE 802.1x은 네트워킹 프로토콜인 IEEE 802.1 그룹의 일부로 포트 기반 네트워크 액세스 제어(PNAC, Port-based Network Access Control)를 위한 IEEE 표준이다. 네트워크에 연결하려는 장치에 인증 메커니즘을 제공하며, 인증 메시지를 교환할 때에는 기존의 통신 규약인 확장 가능 인증 프로토콜(EAP, Extensible Authentication Protocol)를 사용한다.

[0006] IEEE 802.1x 인증 프로토콜의 수행을 위해서는 많은 패킷의 교환이 발생한다. 가장 간단한 방식인 EAP/MD5를 사용하는 경우에도 인증을 받으려는 장치(Supplicant)와 인증을 중계하는 장치(Authenticator)간에 6번의 패킷의 교환이 필요하다.

[0007] 각 패킷에 대한 해시 연산은 높은 연산 능력을 필요로 하고, 많은 송신, 수신 및 해시 연산의 수행으로 높은 배터리 성능을 필요로 하여 과도한 리소스 낭비로 이어지게 되는 문제점이 있었다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국공개특허 제10-2013-0085170호

(특허문헌 0002) 한국공개특허 제10-2007-0092571호

발명의 내용

해결하려는 과제

[0010] 이에, 본 발명의 기술적 과제는 이러한 점에서 착안된 것으로 본 발명의 목적은, 센서 장치가 인증을 하려고 할 때, 필요한 배터리 성능과 연산 능력을 감소시키기 위해 센서 장치를 대신하여 인증 과정을 수행하는 센서 인증 서버를 제공하는 것이다.

[0011] 본 발명의 다른 목적은 상기 인증 과정을 수행하는 소프트웨어 정의 네트워크 컨트롤러를 제공하는 것이다.

[0012] 본 발명의 다른 목적은 상기 인증 과정을 수행하는 방법을 제공하는 것이다.

[0013] 본 발명의 다른 목적은 상기 인증 과정을 수행하기 위한 기록 매체를 제공하는 것이다.

[0014] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0016] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른 센서 장치의 인증을 위한 인증 프로토콜 수행하는 센서 인증 서버(S.AS)는, 소프트웨어 정의 네트워크 컨트롤러(SDNc)에 연결되어 메시지를 수신 및 송신하는 통신부; 상기 소프트웨어 정의 네트워크 컨트롤러(SDNc)로부터 수신한 상기 센서 장치(STA, Station)의 인증 요청이

최초인지 여부에 대해 응답하는 판단부; 상기 센서 장치(STA)의 인증 요청이 최초인 경우, 상기 소프트웨어 정의 네트워크 컨트롤러(SDNc) 및 인증 서버(AS, Authentication Server)와 인증 프로토콜을 수행하는 인증부; 인증 프로토콜의 수행을 완료하면, 제 1 마스터키(PMK_0, Pairwise Master Key)를 생성하고, 상기 소프트웨어 정의 네트워크 컨트롤러(SDNc)와 보안 연관(SA, Security Association)을 생성하는 연관부; 및 상기 제 1 마스터 키와 상기 센서 장치(STA)의 센서키(sensorkey)를 이용하여 상기 센서 장치(STA)와 접속 장치(AP, Access Point)의 보안 연관 생성을 위한 제 2 마스터 키(PMKs)를 생성하는 키 생성부;를 포함한다.

[0017] 본 발명의 실시예에서, 상기 센서 인증 서버(S.AS)는 미리 설정된 상기 센서 장치(STA)의 아이디(SensorID), 상기 센서 장치(STA)의 센서키(sensorkey) 및 상기 센서 장치(STA)의 인증 요청에 따른 인증 수행 여부를 저장하는 저장부를 더 포함할 수 있다.

[0018] 본 발명의 실시예에서, 상기 센서 인증 서버(S.AS)는 제 1 마스터키(PMK_0)를 보관하는 키 관리부를 더 포함할 수 있다.

[0019] 본 발명의 실시예에서, 상기 키 생성부는, 상기 센서 장치(STA)의 인증 요청이 최초가 아닌 경우, 상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관을 다시 생성하기 위해 상기 키 관리부에 보관된 제 1 마스터 키(PMK_0)를 이용하여 제 2 마스터 키(PMKs)를 생성할 수 있다.

[0020] 상기한 본 발명의 목적을 실현하기 위한 다른 실시예에 따른 센서 장치의 인증을 위한 인증 프로토콜을 수행하는 소프트웨어 정의 네트워크 컨트롤러(SDNc, Software Defined Network Controller)는, 접속 장치(AP), 인증 서버(AS), 센서 인증 서버(S.AS)와 네트워크를 통해 메시지를 수신 및 송신하는 통신부; 상기 센서 장치(STA)로부터 수신한 인증 요청이 최초인 경우 인증을 수행하는 것으로 결정하는 결정부; 인증을 수행하는 것으로 결정한 경우, 상기 센서 인증 서버(S.AS) 및 상기 인증 서버(AS)와 인증 프로토콜을 수행하는 인증부; 인증 프로토콜의 수행을 완료하면, 제 1 마스터 키(PMK_0)를 생성하며, 상기 센서 인증 서버(S.AS)와 보안 연관(SA)을 생성하는 연관부; 및 상기 제 1 마스터 키(PMK_0)를 이용하여 상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관(SA) 생성을 위한 제 3 마스터 키(PMKap)를 생성하는 키 생성부를 포함한다.

[0021] 본 발명의 실시예에서, 상기 소프트웨어 정의 네트워크 컨트롤러(SDNc)는 상기 센서 인증 서버의 아이디(S.ASID) 및 상기 센서 장치(STA)의 인증 요청에 따른 인증 수행 여부를 저장하는 저장부를 더 포함할 수 있다.

[0022] 본 발명의 실시예에서, 상기 소프트웨어 정의 네트워크 컨트롤러(SDNc)는 상기 제 1 마스터 키(PMK_0)를 보관하는 키 관리부를 더 포함할 수 있다.

[0023] 본 발명의 실시예에서, 상기 키 생성부는, 상기 센서 장치(STA)의 인증 요청이 최초가 아닌 경우, 상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관을 다시 생성하기 위해 상기 키 관리부에 보관된 제 1 마스터 키(PMK_0)를 이용하여 제 2 마스터 키(PMKap) 생성할 수 있다.

[0024] 상기한 본 발명의 목적을 실현하기 위한 다른 실시예에 따른 소프트웨어 정의 네트워크 컨트롤러(SDNc)에 의해 수행되는 센서 장치의 인증을 위한 인증 프로토콜 수행 방법은, 상기 센서 장치(STA)와 접속 장치(AP)의 정보를 포함한 제 1 메시지를 수신하며, 상기 센서 장치(STA)의 인증 요청이 최초인 경우 인증 프로토콜을 수행하는 것으로 결정하고, 인증 프로토콜을 수행하는 것으로 결정한 경우, 센서 인증 서버(S.AS) 및 인증 서버(AS)와 인증 프로토콜을 수행하고, 인증 프로토콜의 수행을 완료하면, 제 1 마스터키(PMK_0)를 생성하고, 상기 센서 인증 서버(S.AS)와 보안 연관(SA)을 생성하고, 상기 제 1 마스터키(PMK_0)를 이용하여 상기 센서 인증 서버(S.AS)에 의해 생성된 제 2 마스터 키(PMKs)를 포함한 메시지에 상기 제 1 마스터키(PMK_0)를 이용하여 생성한 제 3 마스터 키(PMKap)를 부가하여 제 2 메시지를 생성하며, 상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관(SA)을 생성하기 위해 상기 제 2 메시지를 송신한다.

[0025] 본 발명의 실시예에서, 상기 소프트웨어 정의 네트워크 컨트롤러(SDNc)에 의해 수행되는 센서 장치의 인증을 위한 인증 프로토콜 수행 방법은, 상기 인증 프로토콜의 수행을 완료하여 생성된 제 1 마스터 키(PMK_0)를 보관하는 단계를 더 포함할 수 있다.

[0026] 본 발명의 실시예에서, 상기 인증 프로토콜을 수행하는 것으로 결정하는 단계는, 상기 센서 장치(STA)의 인증 요청이 최초가 아닌 경우, 인증 프로토콜을 수행하지 않는 것으로 결정하고, 상기 인증 프로토콜을 수행하지 않

고, 상기 센서 인증 서버(S.SA)와 보안 연관(SA)을 생성하는 과정을 수행하지 않을 수 있다.

[0027] 본 발명의 실시예에서, 상기 제 2 메시지를 생성하는 것은 상기 센서 장치(STA)와 상기 접속 장치(AP)의 보안 연관(SA)을 다시 생성하기 위해, 상기 보관된 제 1 마스터키(PMK_0)를 이용하여 상기 센서 인증 서버(S.AS)에 의해 생성된 제 2 마스터 키(PMKs)를 포함한 메시지에 상기 보관된 제 1 마스터키(PMK_0)를 이용하여 생성한 제 3 마스터 키(PMKap)를 부가하여 생성할 수 있다.

[0028] 본 발명의 실시예에서, 상기 센서 장치(STA)와 같은 사물 인터넷 서비스 도메인(IoT Service Domain)에 포함된 네트워크에 다른 센서 장치(STA)가 인증을 요청 하는 경우, 상기 센서 장치(STA)의 인증 요청이 최초가 아닌 경우와 동일한 과정을 수행할 수 있다.

[0029] 본 발명의 실시예에서, 상기 제 2 메시지를 생성하는 것은 상기 센서 장치(STA)에 의해 제 2 마스터 키(PMKs)를 생성할 때 사용한 것과 동일한 키 파생 함수(KDF, Key Derivation Function)를 이용하여 상기 제 3 마스터 키(PMKap)를 생성할 수 있다.

[0030] 상기한 본 발명의 목적을 실현하기 위한 다른 실시예에 따른 컴퓨터로 판독 가능한 저장 매체에는, 인증 프로토콜의 수행 방법을 실행하기 위한 컴퓨터 프로그램이 기록되어 있다.

발명의 효과

[0032] 본 발명의 일 측면에 따른 센서 장치의 인증을 위한 인증 프로토콜 수행 방법은, 기존의 IEEE 802.1x를 사용하는 인증을 하는 경우보다 센서 장치(STA)와 접속 장치가(AP) 송신 및 수신하는 패킷의 양이 줄어 배터리 소모량 및 연산량을 감소시킬 수 있다. 따라서, 감소한 부담에 따라 연산 능력 및 배터리 능력을 낮출 수 있어 센서 장치(STA)의 하드웨어 비용을 줄일 수 있다.

[0033] 센서네트워크를 이용한 무인 자동 전력 검침, 수도관 누수 감시 시스템 과 같은 사물 인터넷(IoT)의 특성상 서비스를 제공하기 위한 센서가 다량으로 필요하고, 이런 상황에서 단가의 감소는 매우 긍정적인 영향을 미칠 것이다.

[0034] 또한, 넓은 공간에서 데이터를 수집해야 하는 서비스에 있어서 민감한 데이터를 교환하는 통신 채널에 인증되지 않은 사용자의 접근 제어가 필요하다.

[0035] 제안된 인증 프로토콜에서는 센서 인증 서버(S.AS)가 인증 서버(AS)와 인증과정을 거치기 때문에 인증되지 않은 사용자의 접근을 원천 봉쇄할 수 있어 네트워크의 보안 능력의 향상을 기대할 수 있다.

[0036] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0038] 도 1은 본 발명의 센서 장치(STA)의 인증을 위한 인증 프로토콜을 수행하는 시스템의 개략적인 구성이 도시된 도면이다.

도 2는 본 발명의 센서 장치(STA)의 인증을 위한 인증 프로토콜을 수행하는 시스템에 존재하는 두 개의 도메인(Domain)을 나타낸 구성도이다.

도 3은 본 발명의 일 실시예에 따른 센서 인증 서버(S.AS)를 도시한 블록도이다.

도 4는 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크 컨트롤러(SDNc)를 도시한 블록도이다.

도 5는 본 발명의 일 실시예에 따른 센서 인증 서버(S.AS)를 이용한 인증 프로토콜을 수행하는 방법을 도시한 흐름도이다.

도 6는 제안된 센서 인증 서버(S.AS)를 이용한 인증 프로토콜의 전체 과정을 개략적으로 나타낸 흐름도이다.

도 7은 도 6의 인증 협상(S4000)을 세분화한 흐름도이다.

도 8는 도 6의 인증 시작(S5000)을 세분화한 흐름도이다.

도 9은 도 6의 키 생성(S6000)을 세분화한 흐름도이다.

도 10은 도 6의 보안 연관 생성(S7000)을 세분화한 흐름도이다.

도 11은 도 6의 보안 연관 생성 과정(S8000)을 세분화한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0039] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0040] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0041] 도 1은 본 발명의 센서 장치(500)의 인증을 위한 인증 프로토콜을 수행하는 시스템(10)의 구성도이다.

[0042] 도 1을 참조하면, 본 발명의 센서 장치(500)의 인증을 위한 인증 프로토콜을 수행하는 시스템(10)은 센서 인증 서버(100), 소프트웨어 정의 네트워크 컨트롤러(200), 인증 서버(300), 접속 장치(400), 센서 장치(500), 중계기(600)를 포함할 수 있고, 각각의 장치는 다수 개로 구성될 수 있다.

[0043] 센서 인증 서버(100)는 인증에 관련한 센서 장치(500)의 정보를 포함하여 사전에 구성될 수 있다. 소프트웨어 정의 네트워크 컨트롤러(200)는 네트워크 상의 메시지의 경로를 설정할 수 있고, 복잡한 데이터 처리를 수행할 수 있다.

[0044] 인증 서버(300)는 인증 프로토콜의 수행과정에서 필요한 메시지를 인증 중계자(Authenticator)가 아닌 소프트웨어 정의 네트워크 컨트롤러(200)와 주고 받을 수 있다. 접속 장치(400)는 네트워크에 접속하기 위해 거쳐야 하는 모든 장치를 포함할 수 있다. 센서 장치(500)는 센서를 내장하는 모든 장치를 포함할 수 있다. 중계기(600)는 네트워크 패킷이 경유하는 모든 장치를 포함할 수 있다.

[0045] 도 2는 센서 장치의 인증을 위한 인증 프로토콜을 수행하는 시스템 에 존재하는 두 개의 도메인(Domain)을 나타낸 구성도이다.

[0046] 도 2를 참조하면, 센서 인증 서버(100)와 센서 장치(500) 사이에 사전에 보안 연관(SA)이 구성된 사물 인터넷 서비스 도메인(700, IoT Server Domain)과 소프트웨어 정의 네트워크 컨트롤러(200), 인증 서버(300) 및 접속 장치(400) 사이에 사전에 보안 연관(SA)이 구성된 접속 네트워크 도메인(800, Access Network Domain)에 새로운 센서 장치(500)가 연결될 수 있다.

[0047] 보안 연관(SA) 구성된 네트워크에 속하는 장치 간에는 보안 통신을 수행할 수 있다.

[0048] 도 3은 본 발명의 일 실시예에 따른 센서 인증 서버(100)를 도시한 블록도이다.

[0049] 도 3을 참조하면, 본 발명의 일 실시예에 따른 센서 인증 서버(100)는 통신부(110), 판단부(120), 인증부(130), 연관부(140) 및 키생성부(150)를 포함한다.

[0050] 본 발명의 다른 실시예에 따른 센서 인증 서버(100)는 저장부(160)를 더 포함할 수 있다. 본 발명의 다른 실시예에 따른 센서 인증 서버(100)는 키관리부(170)를 더 포함할 수 있다.

[0051] 통신부(110), 판단부(120), 인증부(130), 연관부(140), 키생성부(150), 저장부(160) 및 키관리부(170)의 구성은 통합 모듈로 형성되거나, 하나 이상의 모듈로 이루어질 수 있다. 그러나, 이와 반대로 각 구성은 별도의 모듈로 이루어질 수도 있다.

[0052] 통신부(110)는 소프트웨어 정의 네트워크 컨트롤러(200)에 연결되어 메시지를 수신 및 송신할 수 있다. 판단부(120)는 소프트웨어 정의 네트워크 컨트롤러(200)를 통해 수신한 센서 장치(500)의 인증 요청이 최초인지를 판

단하여 대해 응답할 수 있다.

[0053] 인증부(130)는 센서 장치(500)의 인증 요청이 최초인 경우, 소프트웨어 정의 네트워크 컨트롤러(200) 및 인증 서버(300)와 인증 프로토콜을 수행할 수 있다. 연관부(140)는 인증 프로토콜의 수행을 완료하면, 제 1 마스터키(PMK_0)를 생성하고, 소프트웨어 정의 네트워크 컨트롤러(200)와 보안 연관(SA)을 생성할 수 있다.

[0054] 키생성부(150)는 제 1 마스터 키(PMK_0)와 센서 장치(500)의 센서 키(sensorkey)를 이용하여 센서 장치(500)와 접속 장치(400)의 보안 연관을 생성할 때 센서 장치(500)에서 필요한 제 2 마스터 키(PMKs)를 생성할 수 있다.

[0055] 저장부(160)는 미리 설정된 센서 장치(500)의 아이디(SensorID), 센서 장치(500)의 센서키(sensorkey) 및 센서 장치(500)의 인증 요청에 따른 인증 수행 여부를 저장할 수 있다. 센서 장치(500)의 아이디(SensorID)는 센서 인증 서버(100)가 센서 장치를 위한 식별자이고, 센서키(sensorkey)는 센서 인증 서버(100)가 센서 장치(500)를 위해 제 2 마스터 키(PMKs)를 암호화하여 생성할 때 필요한 것이며, 인증 수행 여부는 센서 장치(500)의 인증 요청이 최초인지 아닌지 판단하기 위해 보관할 수 있다.

[0056] 키관리부(170)는 제 1 마스터키(PMK_0)를 보관할 수 있다. 제 1 마스터 키(PMK_0)는 센서 장치(500)의 인증 요청이 최초인 경우 센서 인증 서버(100), 소프트웨어 정의 네트워크 컨트롤러(200) 및 인증 서버(300)의 3자간 통신에 의해 인증 프로토콜을 수행한 결과 생성된 것으로, 센서 장치(500)의 인증 요청이 최초가 아니거나 같은 사물 인터넷 서비스 도메인(700, IoT Service Domain)에 포함된 다른 센서 장치가 인증 요청을 하는 경우에 제 2 마스터 키(PMKs)를 생성하기 위해 제공될 수 있다.

[0057] 도 4는 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크 컨트롤러(200)를 도시한 블록도이다.

[0058] 도 4를 참조하면, 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크 컨트롤러(200)는 통신부(210), 결정부(220), 인증부(230), 연관부(240) 및 키생성부(250)을 포함한다.

[0059] 본 발명의 다른 실시예에 따른 소프트웨어 정의 네트워크 컨트롤러(200)는 저장부(260)를 더 포함할 수 있다. 본 발명의 다른 실시예에 따른 소프트웨어 정의 네트워크 컨트롤러(200)는 키관리부(770)를 더 포함할 수 있다.

[0060] 통신부(210)는 접속 장치(400), 인증 서버(300), 센서 인증 서버(100)와 네트워크를 통해 메시지를 수신 및 송신할 수 있다. 결정부(220)는 센서 장치(500)로부터 수신한 인증 요청이 최초인지 여부를 기준으로 인증 프로토콜의 수행 여부를 결정할 수 있다.

[0061] 인증부(230)는 인증을 수행하는 것으로 결정한 경우, 센서 인증 서버(100) 및 인증 서버(300)와 인증 프로토콜을 수행할 수 있다. 연관부(240)는 인증 프로토콜의 수행을 완료하면, 제 1 마스터 키(PMK_0)를 생성하며, 센서 인증 서버(100)와 보안 연관(SA)을 생성할 수 있다.

[0062] 키 생성부(250)은 제 1 마스터 키(PMK_0)를 이용하여 센서 장치(500)와 접속 장치(400)의 보안 연관(SA)을 생성할 때 접속 장치(400)에서 사용되는 마스터 키(PMKap)를 생성할 수 있다.

[0063] 저장부(260)는 센서 인증 서버(100)의 아이디(S.ASID) 및 센서 장치(500)의 인증 요청에 따른 인증 수행 여부를 저장할 수 있다. 센서 장치(500)의 아이디(SensorID)는 센서 인증 서버(100)가 센서 장치를 위한 식별자이고, 인증 수행 여부는 센서 장치(500)의 인증 요청이 최초인지 아닌지 판단하기 위해 보관할 수 있다.

[0064] 키관리부(270)는 제 1 마스터키(PMK_0)를 보관할 수 있다. 제 1 마스터 키(PMK_0)는 센서 장치(500)의 인증 요청이 최초인 경우 센서 인증 서버(100), 소프트웨어 정의 네트워크 컨트롤러(200) 및 인증 서버(300)의 3자간 통신에 의해 인증 프로토콜을 수행한 결과 생성된 것으로, 센서 장치(500)의 인증 요청이 최초가 아니거나 같은 사물 인터넷 서비스 도메인(700, IoT Server Domain)에 포함된 다른 센서 장치가 인증 요청을 하는 경우에 접속 장치(400)를 위한 마스터 키(PMKap)를 생성하기 위해 제공될 수 있다.

[0065] 도 5는 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크 컨트롤러(200)에 의해 수행되는 센서 인증 서버(100)를 이용한 인증 프로토콜을 수행하는 방법을 도시한 흐름도이다.

[0066] 도 5를 참조하면, 센서 장치(500)의 센서 인증 서버(100) 아이디(S.ASID)와 센서 장치(500)의 아이디(SensorID)를 포함한 메시지에 접속 장치(500)의 아이디(APID)를 부가한 제 1 메시지를 접속 장치(500)로부터 수신하고(S1100), 센서 장치(500)의 인증요청이 최초인지를 소프트웨어 정의 네트워크 컨트롤러(200)의 저장부(260)에 저장된 인증 수행 여부를 참조하거나 센서 인증 서버(100)의 판단부(120)에 요청하여 응답을 받아 결정

할 수 있고, 센서 장치(500)의 인증 요청이 최초인 경우 인증 프로토콜을 수행하는 것으로 결정할 수 있다(S1200).

[0067] 인증 프로토콜을 수행하는 것으로 결정한 경우, 센서 인증 서버(100) 및 인증 서버(300)와 인증 프로토콜을 수행하고(S1300), 제 1 마스터키(PMK_0)를 생성한다(S1400). 제 1 마스터 키(PMK_0)는 별도로 보관될 수 있다(S1500)

[0068] 제 1 마스터 키(PMK_0)를 이용하여 센서 인증 서버(100)와 보안 연관(SA)을 생성할 수 있다(S1600).

[0069] 제 1 마스터키(PMK_0)를 이용하여 센서 인증 서버(100)에 의해 생성된 센서 장치(500)를 위한 제 2 마스터 키(PMKs)를 포함한 메시지를 수신할 수 있고(S1700), 수신한 메시지에 제 1 마스터키(PMK_0)를 이용하여 생성한 접속 장치(400)를 위한 제 3 마스터 키(PMKap)를 부가하여 제 2 메시지를 생성할 수 있다(S1800).

[0070] 센서 장치(STA)와 접속 장치(AP)의 보안 연관(SA)을 생성하기 위해 제 2 메시지를 송신할 수 있다(S1900).

[0071] 인증 요청이 최초가 아닌 경우(S1250), 인증 프로토콜을 수행하지 않을 수 있고(S1300), 제 1 마스터 키(PMK_0)는 생성 되지 않을 수 있으며(S1400), 센서 인증 서버(100)와 소프트웨어 정의 네트워크 컨트롤러(200)는 최초의 인증 요청에 의한 인증 프로토콜의 수행으로 보안 연관이 이미 생성되어 있으므로 보안 연관의 생성을 수행하지 않을 수 있다.

[0072] 최초의 인증 요청에 의한 인증 프로토콜의 수행으로 생성되어 별도로 보관된 제 1 마스터 키(PMK_0)를 제공받아 센서 인증 서버(100)에 의해 생성된 센서 장치(500)를 위한 제 2 마스터 키(PMKs)를 포함한 메시지를 수신할 수 있다(S1700).

[0073] 최초의 인증 요청에 의한 인증 프로토콜의 수행으로 생성되어 별도로 보관된 제 1 마스터 키를 제공받아 생성한 접속 장치(400)를 위한 제 3 마스터 키(PMKap)를 부가하여 제 2 메시지를 생성할 수 있다(S1800)

[0074] 도 6은 제안된 센서 인증 서버를 이용한 인증 프로토콜의 전체 과정을 개략적으로 나타낸 흐름도이다.

[0075] 도 6을 참조하면, 센서 장치(500)와 접속 장치(400)가 인증 프로토콜을 협상(negotiate)할 수 있고(S4000), 센서 장치(400)가 접속 장치(400)를 통해 소프트웨어 정의 네트워크 컨트롤러(200)에게 인증 시작을 위한 메시지를 송신할 수 있다(S5000),

[0076] 소프트웨어 정의 네트워크 컨트롤러(200)는 센서 장치(500)의 인증 요청에 따른 인증 프로토콜을 수행할 것이지 결정하기 위해 인증 요청이 최초인지 판단할 수 있고, 이를 위해 소프트웨어 정의 네트워크 컨트롤러(200)가 저장하고 있는 인증 정보 여부를 참조하거나 센서 인증 서버(100)가 저장하고 있는 인증 정보 여부를 문의하여 수신한 응답을 기초로 판단할 수 있다.

[0077] 센서 장치(500)의 인증 요청이 최초인 경우 인증 프로토콜을 수행할 것으로 결정할 수 있고, 센서 장치(500)의 인증 요청이 최초가 아니거나 같은 사물 인터넷 서비스 도메인(700, IoT Service Domain)에 포함된 다른 센서 장치가 인증을 요청할 경우 아래에서 설명할 인증 수행(S6000)을 생략하는 것으로 결정할 수 있다(S5500).

[0078] 센서 장치(500)의 인증 요청이 최초인 경우, 센서 인증 서버(100), 소프트웨어 정의 네트워크 컨트롤러(200) 및 인증 서버(300)의 3자간 통신에 의해 인증을 수행 할 수 있다(S6000),

[0079] 인증 수행 결과 생성된 제 1 마스터 키(PMK_0)를 이용하여 센서 장치(500)를 위한 제 2 마스터 키(PMKs)와 접속 장치를 위한 제 3 마스터 키(PMKap)를 생성하여 접속 장치에게 송신할 수 있다(S7000).

[0080] 수신한 제 2 마스터 키(PMKs)와 제 3 마스터 키(PMKap)를 이용하여 센서 장치(500)와 접속 장치(400)가 보안 연관(SA)을 생성하여 보안 통신을 할 수 있게 된다(S8000).

[0081] 도 7은 도 6의 인증 협상(S4000)을 세분화한 흐름도이다.

[0082] 도 7을 참조하면, 센서 장치(500)는 네트워크에 연결되기 위해 Prove Request를 송신할 수 있고(S4100), 이를 수신한 접속 장치(400)는 Prove Response를 송신할 수 있다(S4200).

[0083] Prove Response를 수신한 센서 장치(500)는 Authentication-Request을 송신할 수 있고(S4300), 이를 수신한 접속 장치(400)는 Authentication-Response를 송신할 수 있다(S4400).

[0084] Authentication-Response를 수신한 센서 장치(400)는 센서 장치(400)가 사물 인터넷 인증 프로토콜(IoT Authentication Protocol) 기능을 제공하는 의미의 IoT-A 태그를 Associate-Request에 추가하여 송신할 수 있다(S4500).

[0085] 이를 수신한 접속 장치(400)는 접속 장치(400)가 연결된 네트워크가 사물 인터넷 인증 프로토콜(IoT Authentication Protocol) 기능을 제공하는 의미의 IoT-A 태그를 Associate-Response에 추가하여 송신할 수 있다(S4600).

[0086] 도 8는 도 6의 인증 시작(S5000)을 세분화한 흐름도이다.

[0087] 도 8을 참조하면, 센서 장치(500)가 인증을 대신 수행할 센서 인증 서버(100)의 아이디(S.ASID)와 해당 센서 장치(500)의 신원을 확인시키기 위한 (SensorID)를 메시지에 포함하여 접속 장치(400)에게 송신할 수 있다(S5100).

[0088] 메시지를 수신한 접속 장치(400)는 해당 접속 장치(400)의 아이디(APID)를 부가하여 소프트웨어 정의 네트워크 컨트롤러(200)에게 송신할 수 있다(S5200).

[0089] 도 9는 도 6의 인증 수행(S6000)을 세분화한 흐름도이다.

[0090] 도 9를 참조하면, 센서 장치(500)-접속 장치(400)-인증 서버(300) 3자간 통신으로 인증을 수행하였던 종래와 달리, 센서 인증 서버(100)-소프트웨어 정의 네트워크 컨트롤러(200)-인증 서버(300)의 3자통신에 의해 인증 프로토콜을 수행할 수 있다(S6100 내지 S6420).

[0091] 이때 인증 서버(300)는 마스터 세션 키(S6800 / MSK, Master Session Key)를 생성하여 소프트웨어 정의 네트워크 컨트롤러(200) 및 센서 인증 서버(100)에게 송신할 수 있다.

[0092] 센서 인증 서버(100)는 수신한 마스터 세션 키(S6820 / MSK)의 정보를 이용하여 제 1 마스터 키(S6860 / PMK_0, Pairwise Master Key)를 생성할 수 있고, 소프트웨어 정의 네트워크 컨트롤러(300)는 수신한 마스터 세션 키(S6840 / MSK)의 정보를 이용하여 제 1 마스터 키(S6880 / PMK_0, Pairwise Master Key)를 생성할 수 있다. 이때, 센서 인증 서버(100)가 생성한 마스터 키(S6860)와 소프트웨어 정의 네트워크 컨트롤러(200)가 생성한 마스터 키(S6880)는 각각의 장치에 저장되어 인증 키 관리(AKM, Authenitcation Key Management)를 수행할 수 있다.

[0093] 센서 인증 서버(100)는 소프트웨어 정의 네트워크 컨트롤러(300)와 소프트웨어 정의 네트워크 컨트롤러(200)의 임의값(ENonce), 센서 인증 서버(100)의 임의값(SNonce), 메시지 인증 코드(MIC, Message authentication code) 및 RNS정보 요소(RSNE, Robust Securit Netowrk Element)의 정보를 포함한 EAPoL-Key를 교환(S6600 내지 S6640)하여 센서 인증 서버(100)를 위한 세션용 암호 키(S6900 / PTK, Pairwise Transient Key)를 생성할 수 있고, 소프트웨어 정의 네트워크 컨트롤러(200)를 위한 세션용 암호 키(S6920)를 생성함으로써 보안 연관을 생성할 수 있다(S6660).

[0094] 도 10은 도 6의 키 생성(S7000)을 세분화한 흐름도이다.

[0095] 도 10을 참조하면, 소프트웨어 정의 네트워크 컨트롤러(200)는 센서 장치(500)의 아이디(SensorID)와 접속 장치(400) 아이디(APID)를 포함한 메시지를 센서 인증 서버(100)에게 송신할 수 있고(S7100), 이를 수신한 센서 인증 서버(100)는 저장한 제 1 마스터키(S6860)을 이용하여 센서 장치(500)를 위해 생성한 제 2 마스터 키(PMKs)를 포함한 메시지를 송신할 수 있다(S7200).

[0096] 이를 수신한 소프트웨어 정의 네트워크 컨트롤러(200)는 저장한 제 1 마스터키(S6880)을 이용하여 접속 장치(400)를 위해 생성한 제 3 마스터 키(PMKap)를 포함한 메시지를 접속 장치(400)에게 송신할 수 있다(S7200).

[0097] 이 때, 제 2 마스터 키(PMKs)와 제 3 마스터 키(PMKap)는 사용하는 기기가 다르기 때문에 분류한 것이지 실제론 동일한 키이며, 두 가지키를 생성하는 키 파생 함수(KDF, Key Derivation Function)는 센서 인증 서버(100)와 인증 서버(300)가 동일한 함수(Function)를 사용하기만 한다면 어떠한 키 파생 함수(KDF)를 사용해도 무방하다.

[0098] 소프트웨어 정의 네트워크 컨트롤러(200)와 접속 장치(400)는 상호 인증된 보안 연관(SA) 관계로 안전한 채널이기 때문에 제 3 마스터 키(PMKap)는 암호화하지 않고 송신할 수 있다.

[0099] 소프트웨어 정의 네트워크 컨트롤러(200)-센서 장치(500), 접속 장치(400)-센서 장치(500) 사이에는 보안 연관(SA)이 생성되지 않았고, 센서 인증 서버(100)와 센서 장치(500) 사이에는 보안 연관(SA)이 생성되어 있기 때문

에 제 2 마스터 키(PMKs)는 센서 장치(500)와 센서 인증 서버(100) 사이에 미리 설정된 키인 sensorkey를 이용하여 암호화하여 송신할 수 있다.

[0100] 도 11은 도 6의 보안 연관 생성 과정(S8000)을 세분화한 흐름도이다

[0101] 도 11을 참조하면, 보안 연관을 생성하기 위해 4-way handshaking을 수행하는 과정이다. 4-way handshaking은 무선구간 암호화를 위한 세션용 암호 키(PTK) 생성을 위한 키 교환 및 키 합의 과정이다.

[0102] 제 2 마스터 키(PMKs)와 제 3 마스터 키(PMKap) 모두 접속 장치(400)가 가지고 있으므로, 접속 장치(400)가 송신하는 첫 번째 메시지에는 암호화된 제 2 마스터 키(PMKs)가 포함된다(S8100).

[0103] 이후의 4-way handshaking 과정은 일반적인 4-way handshaking과 동일하게 진행되고, 진행 결과 접속 장치(400)위한 세션용 암호 키 (S8700)와 센서 장치(500)를 위한 세션용 암호 키(S8800)가 생성된다(S8200 내지 S8400).

[0104] 접속 장치(400)와 센서 장치(500)는 동일한 세션용 암호 키를 갖게 되며, 보안 연관(SA)을 생성하여 보안 통신을 할 수 있게 된다.

[0105] 이와 같은, 센서 장치(500)를 위한 인증 프로토콜을 이용한 인증 방법은 어플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

[0106] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거니와 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0107] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.

[0108] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0109] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0111] 10: 센서 장치를 위한 인증 프로토콜을 수행하는 시스템

100: 센서 인증 서버

200: 소프트웨어 정의 네트워크 컨트롤러

300: 인증 서버

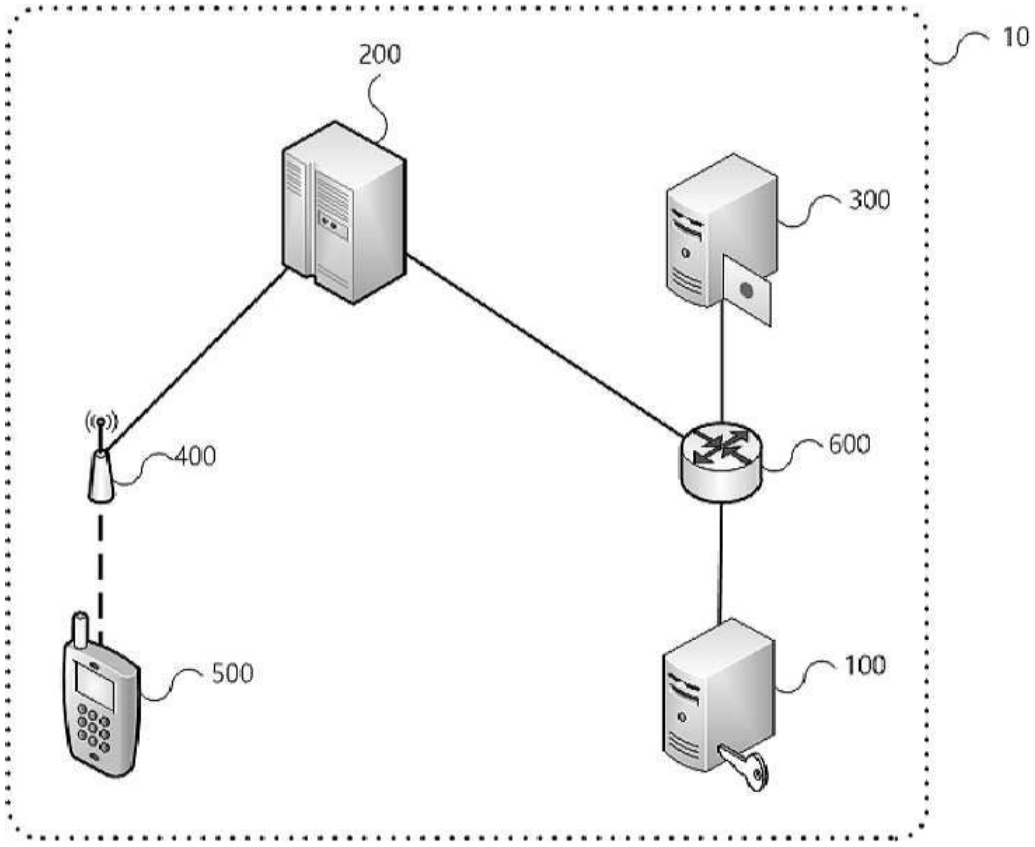
400: 접속 장치

500: 센서 장치

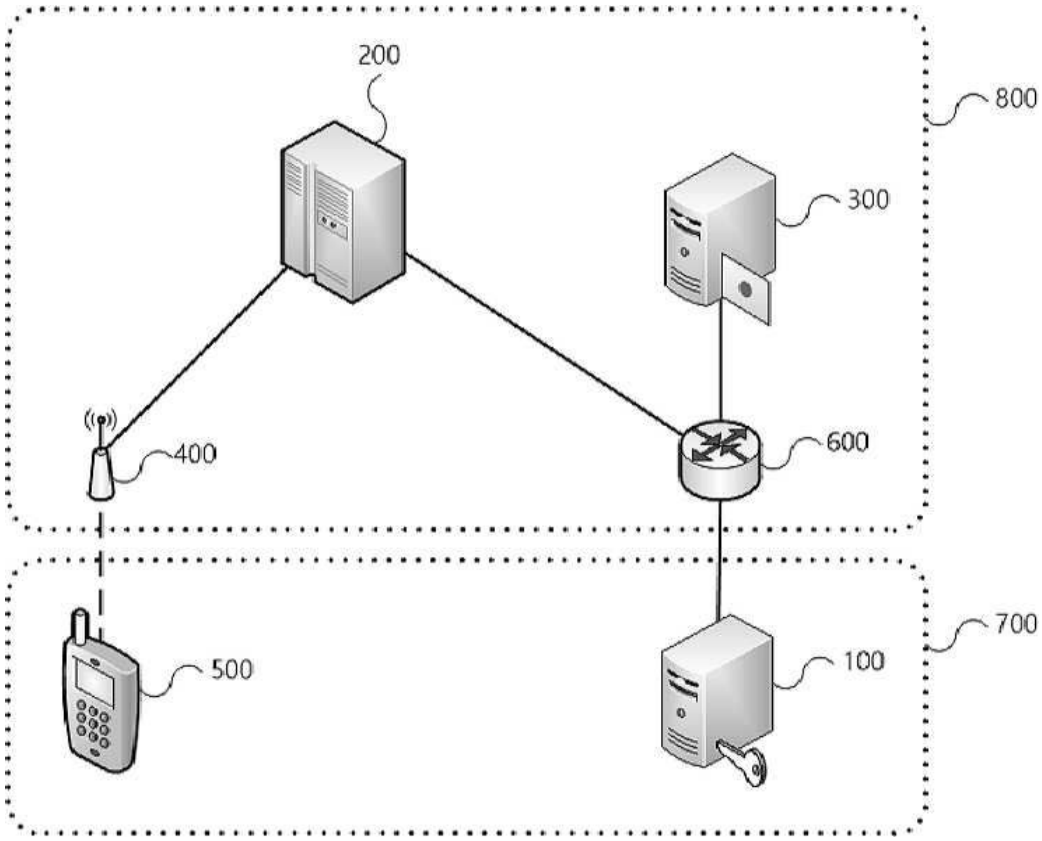
600: 중계기

도면

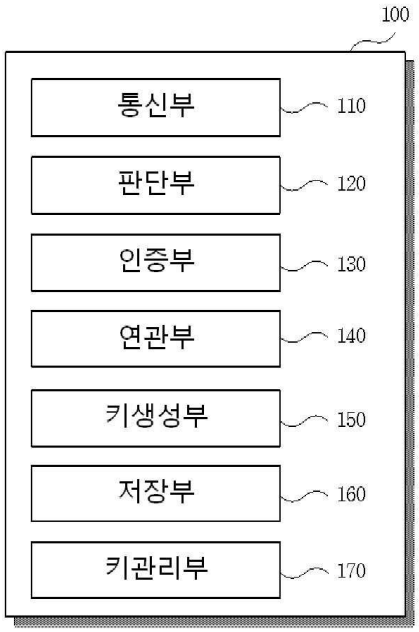
도면1



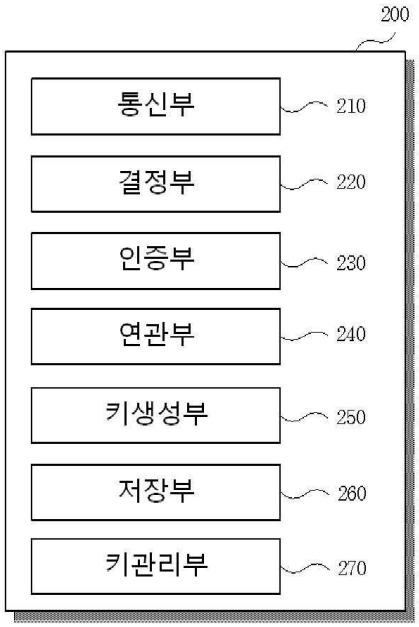
도면2


200
800
300
400
600
500
700
100

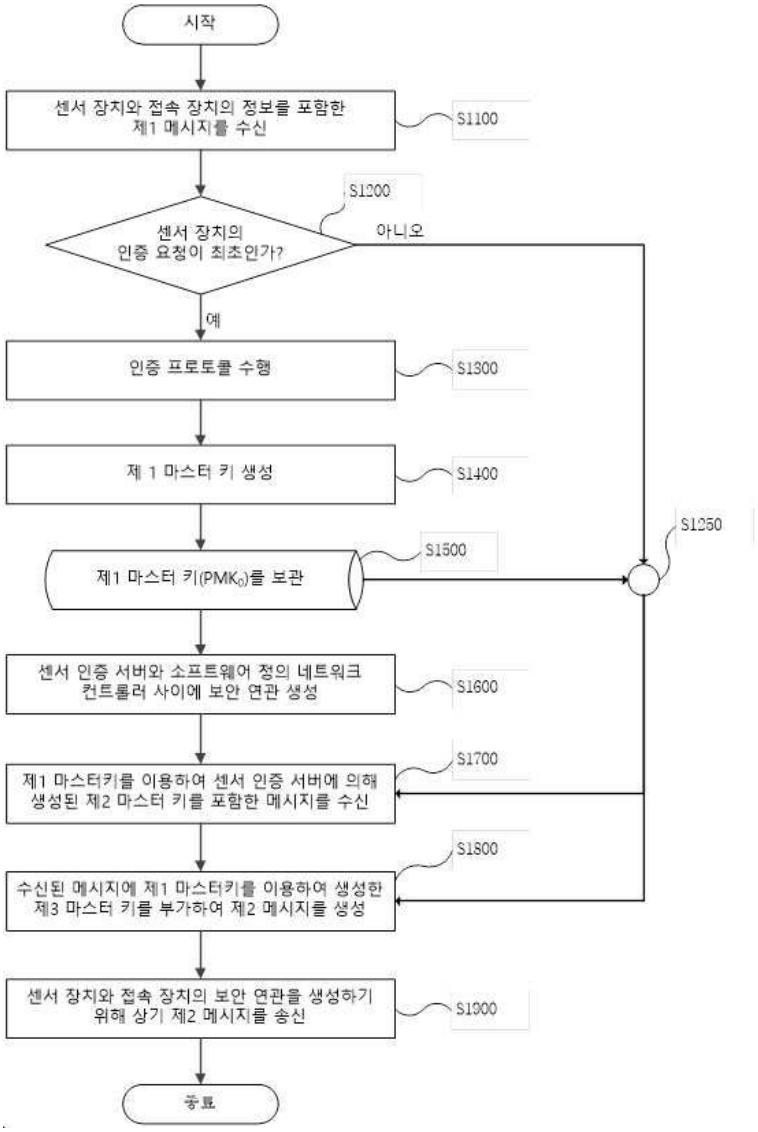
도면3


100
통신부
110
판단부
120
인증부
130
연관부
140
키생성부
150
저장부
160
키관리부
170

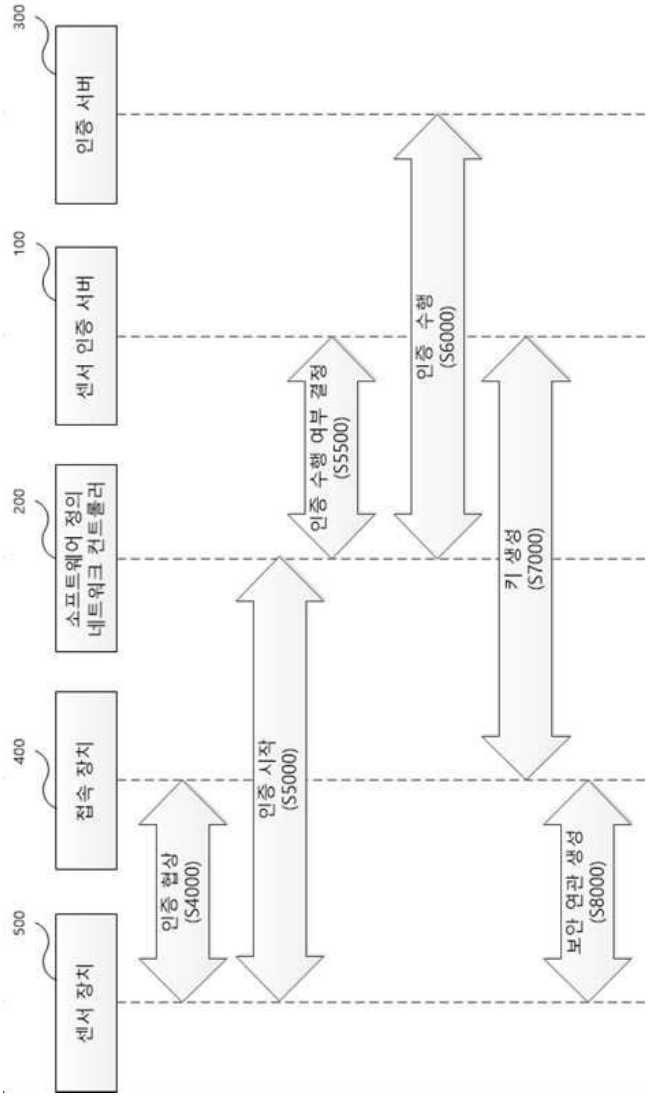
도면4



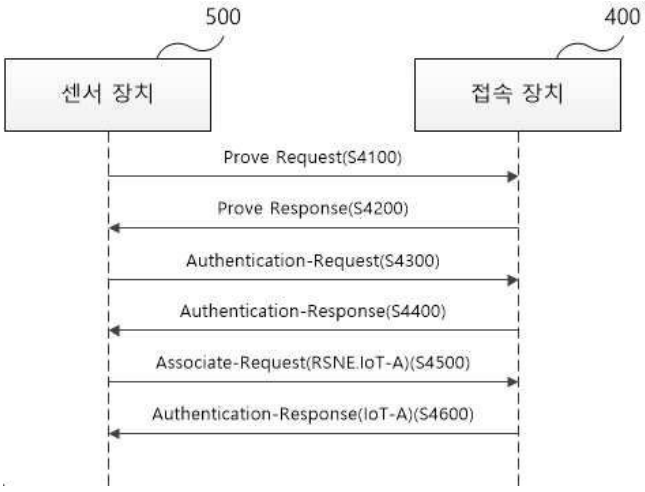
도면5


시작
센서 장치와 접속 장치의 정보를 포함한 제1 메시지를 수신
S1100
S1200
센서 장치의 인증 요청이 최초인가?
아니오
예
인증 프로토콜 수행
S1300
제 1 마스터 키 생성
S1400
S1250
제1 마스터 키(PMK0)를 보관
S1500
센서 인증 서버와 소프트웨어 정의 네트워크 컨트롤러 사이에 보안 연관 생성
S1600
제1 마스터키를 이용하여 센서 인증 서버에 의해 생성된 제2 마스터 키를 포함한 메시지를 수신
S1700
수신된 메시지에 제1 마스터키를 이용하여 생성한 제3 마스터 키를 부가하여 제2 메시지를 생성
S1800
센서 장치와 접속 장치의 보안 연관을 생성하기 위해 상기 제2 메시지를 송신
S1900
종료

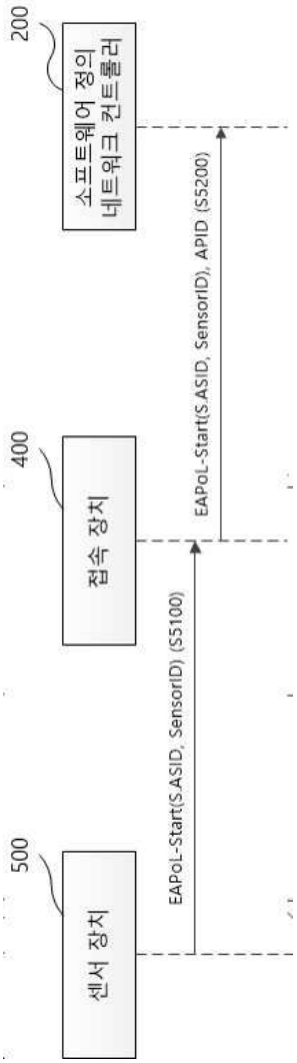
도면6


300
인증 서버
100
센서 인증 서버
200
소프트웨어 정의 네트워크 컨트롤러
400
접속 장치
500
센서 장치
인증 협상 (S4000)
인증 시작 (S5000)
인증 수행 여부 결정 (S5500)
인증 수행 (S6000)
키 생성 (S7000)
보안 연관 생성 (S8000)

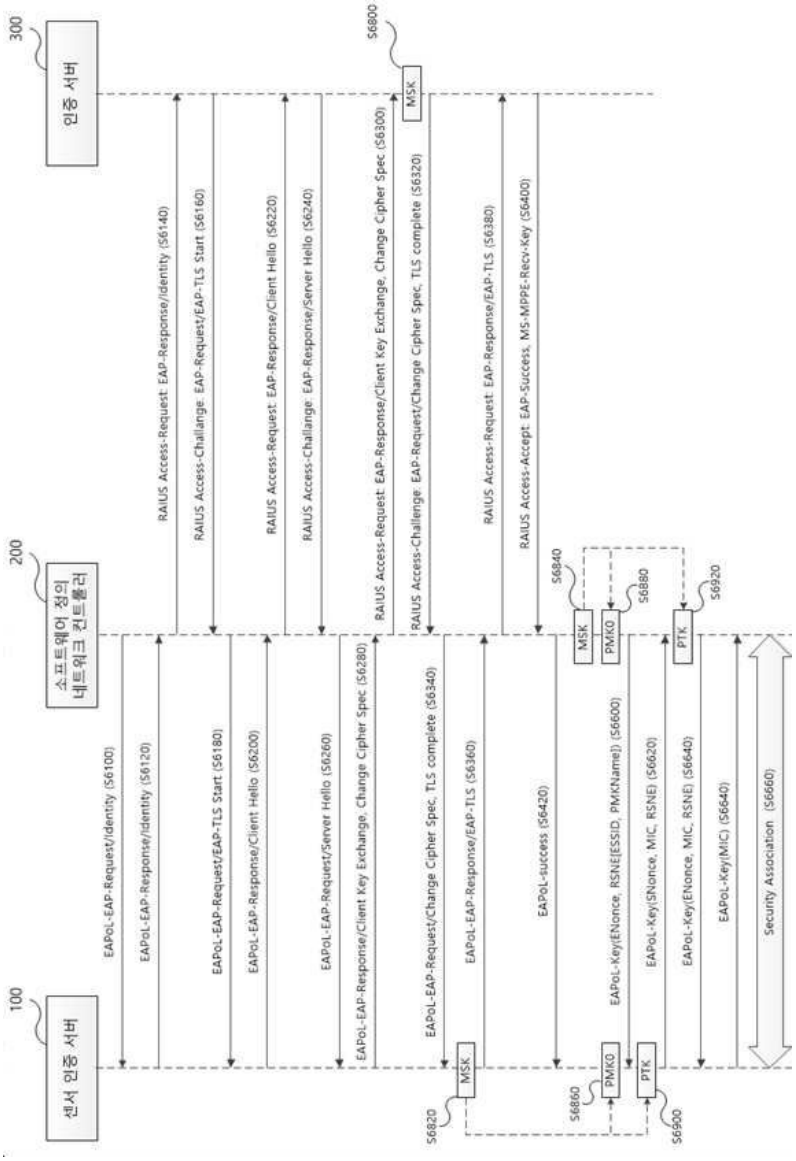
도면7


500
센서 장치
400
접속 장치
Prove Request(S4100)
Prove Response(S4200)
Authentication-Request(S4300)
Authentication-Response(S4400)
Associate-Request(RSNE.IoT-A)(S4500)
Authentication-Response(IoT-A)(S4600)

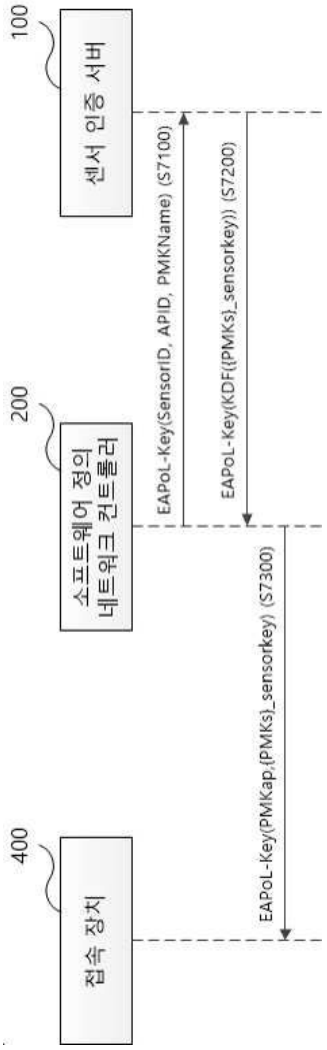
도면8


200
소프트웨어 정의 네트워크 컨트롤러
400
접속 장치
500
센서 장치
EAPoL-Start(S.ASID, SensorID), APID (S5200)
EAPoL-Start(S.ASID, SensorID) (S5100)

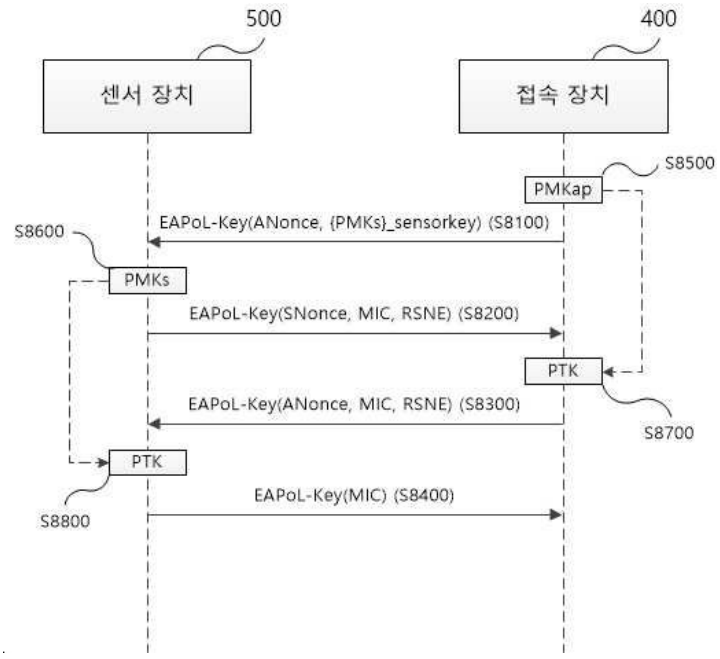
도면9


100
센서 인증 서버
200
소프트웨어 정의 네트워크 컨트롤러
300
인증 서버
EAPoL-EAP-Request/Identity (S6100)
EAPoL-EAP-Response/Identity (S6120)
RAIUS Access-Request: EAP-Response/Identity (S6140)
RAIUS Access-Challenge: EAP-Request/EAP-TLS Start (S6160)
EAPoL-EAP-Request/EAP-TLS Start (S6180)
EAPoL-EAP-Response/Client Hello (S6200)
RAIUS Access-Request: EAP-Response/Client Hello (S6220)
RAIUS Access-Challenge: EAP-Response/Server Hello (S6240)
EAPoL-EAP-Request/Server Hello (S6260)
EAPoL-EAP-Response/Client Key Exchange, Change Cipher Spec (S6280)
RAIUS Access-Request: EAP-Response/Client Key Exchange, Change Cipher Spec (S6300)
S6800
MSK
RAIUS Access-Challenge: EAP-Request/Change Cipher Spec, TLS complete (S6320)
EAPoL-EAP-Request/Change Cipher Spec, TLS complete (S6340)
MSK
S6820
EAPoL-EAP-Response/EAP-TLS (S6360)
RAIUS Access-Request: EAP-Response/EAP-TLS (S6380)
RAIUS Access-Accept: EAP-Success, MS-MPPE-Recv-Key (S6400)
S6840
MSK
EAPoL-success (S6420)
PMK0
S6860
S6880
EAPoL-Key(ENonce, RSNE(ESSID, PMKName)) (S6600)
PTK
S6900
EAPoL-Key(SNonce, MIC, RSNE) (S6620)
S6920
PTK
EAPoL-Key(ENonce, MIC, RSNE) (S6640)
EAPoL-Key(MIC) (S6640)
Security Association (S6660)

도면10


100
센서 인증 서버
200
소프트웨어 정의 네트워크 컨트롤러
400
접속 장치
EAPoL-Key(SensorID, APID, PMKName) (S7100)
EAPoL-Key(KDF({PMKs}_sensorkey)) (S7200)
EAPoL-Key(PMKap,{PMKs}_sensorkey) (S7300)

도면11


500
센서 장치
400
접속 장치
S8500
PMKap
S8600
EAPoL-Key(ANonce, {PMKs}_sensorkey) (S8100)
PMKs
EAPoL-Key(SNonce, MIC, RSNE) (S8200)
PTK
EAPoL-Key(ANonce, MIC, RSNE) (S8300)
S8700
PTK
S8800
EAPoL-Key(MIC) (S8400)