(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년03월08일
(11) 등록번호 10-2224264
(24) 등록일자 2021년03월02일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 63/0853 (2013.01)
H04L 63/062 (2013.01)
(21) 출원번호 10-2020-0102133
(22) 출원일자 2020년08월14일
심사청구일자 2020년08월14일
(56) 선행기술조사문헌
JP2019161256 A*
KR101968417 B1*
KR1020190130206 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
부산대학교 산학협력단
부산광역시 금정구 부산대학로63번길 2 (장전동, 부산대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호(신천동, 파크리오)
남일구
서울특별시 송파구 올림픽로 435, 311동 2001호(신천동, 파크리오)
조민재
서울특별시 동작구 사당로 180-6, 201호 (사당동)
(74) 대리인
두호특허법인

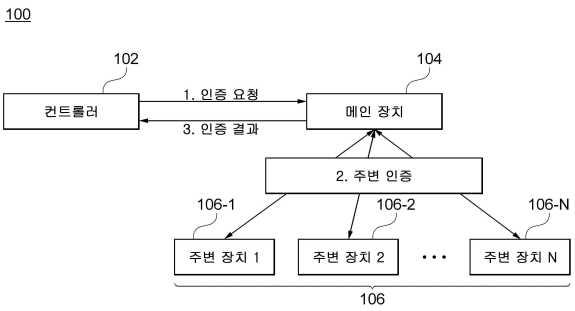
전체 청구항 수 : 총 18 항 심사관 : 문형섭

(54) 발명의 명칭 **주변 장치를 이용한 인증 시스템 및 방법**

(57) 요 약

주변 장치를 이용한 인증 시스템 및 방법이 개시된다. 일 실시예에 따른 인증 시스템은 컨트롤러; 및, 상기 컨트롤러로부터 인증 요청이 수신되는 경우, 상기 컨트롤러 및 하나 이상의 주변 장치로 주변 인증을 요청하고, 상기 주변 인증의 결과에 따라 상기 컨트롤러로 인증 응답을 송신하는 메인 장치를 포함한다.

대 표 도



(52) CPC특허분류
H04L 63/12 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711116145
과제번호 2018-0-01423-003
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 대학ICT연구센터육성지원사업
연구과제명 지능형 비행로봇 융합 기술 연구
기 여 율 60/100
과제수행기관명 세종대학교 산학협력단
연구기간 2020.01.01 ~ 2020.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711112410
과제번호 2019R1A2C109093512
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 중견연구자지원사업
연구과제명 자율주행차 사용자를 위한 5G-ATSC3.0 기반 차세대 방송-통신 융합 송수신기 연구
기 여 율 40/100
과제수행기관명 부산대학교 산학협력단
연구기간 2020.03.01 ~ 2021.02.28

명 세 서

청구범위

청구항 1

컨트롤러; 및

상기 컨트롤러로부터 인증 요청이 수신되는 경우, 상기 컨트롤러 및 하나 이상의 주변 장치로 주변 인증 요청 메시지를 송신하고, 상기 컨트롤러 및 상기 하나 이상의 주변 장치로부터 수신되는 주변 인증 응답 메시지를 이용하여 상기 컨트롤러를 인증하고, 상기 인증 결과에 따라 상기 컨트롤러로 인증 응답을 송신하는 메인 장치를 포함하며,

상기 주변 장치는 상기 메인 장치와 물리적으로 근접하여 근거리 무선 통신을 통해 상기 메인 장치와 통신이 가능한 장치이고,

상기 메인 장치는,

유효한 주변 인증 응답 메시지를 회신한 주변 장치의 개수가 기준값 이상이고,

상기 컨트롤러로부터 유효한 주변 인증 응답 메시지가 수신되었으며,

수신된 상기 주변 인증 응답 메시지의 수신 시각이 모두 기 설정된 타임아웃 이내인 경우, 상기 컨트롤러의 인증에 성공한 것으로 판단하는, 인증 시스템.

청구항 2

청구항 1에 있어서,

상기 메인 장치는,

상기 컨트롤러로부터 인증 요청이 수신되는 경우, 임의의 논스(nonce)를 포함하는 주변 인증 요청 메시지를 브로드캐스팅하는, 인증 시스템.

청구항 3

청구항 2에 있어서,

상기 주변 인증 요청 메시지를 수신한 상기 컨트롤러 및 상기 하나 이상의 주변 장치는, 상기 주변 인증 요청 메시지에 포함된 상기 논스 및 자신의 식별 정보를 포함하는 주변 인증 응답 메시지를 상기 메인 장치로 송신하는, 인증 시스템.

청구항 4

청구항 3에 있어서,

상기 메인 장치는, 상기 하나 이상의 주변 장치의 식별 정보로부터 생성된 블룸 필터를 저장 및 관리하며,

상기 논스 및 상기 블룸 필터를 이용하여 상기 하나 이상의 주변 장치로부터 수신되는 상기 주변 인증 응답 메시지의 유효성을 검증하는, 인증 시스템.

청구항 5

청구항 4에 있어서,

상기 메인 장치는,

수신된 주변 인증 응답 메시지에 포함된 논스가 기 브로드캐스팅된 논스와 동일하고,

상기 수신된 주변 인증 응답 메시지에 포함된 식별 정보가 상기 블룸 필터에 존재하는 경우,

상기 수신된 주변 인증 응답 메시지를 유효한 것으로 판단하는, 인증 시스템.

청구항 6

삭제

청구항 7

청구항 3에 있어서,

상기 하나 이상의 주변 장치는, 상기 메인 장치와 공유되는 대칭키로 상기 주변 인증 응답 메시지를 암호화하여 상기 메인 장치로 송신하는, 인증 시스템.

청구항 8

청구항 7에 있어서,

상기 메인 장치는, 상기 대칭키로 상기 암호화된 주변 인증 응답 메시지의 유효성을 검증하는, 인증 시스템.

청구항 9

청구항 3에 있어서,

상기 하나 이상의 주변 장치는, 자신의 식별 정보에 대응되는 비밀키로 상기 주변 인증 응답 메시지를 서명하여 상기 메인 장치로 송신하는, 인증 시스템.

청구항 10

청구항 9에 있어서,

상기 메인 장치는, 상기 비밀키에 대응되는 주변 장치의 식별 정보를 이용하여 상기 서명된 주변 인증 응답 메시지의 유효성을 검증하는, 인증 시스템.

청구항 11

메인 장치에서 수행되는 방법으로서,

컨트롤러로부터 인증 요청을 수신하는 단계;

상기 인증 요청에 따라 상기 컨트롤러 및 하나 이상의 주변 장치로 주변 인증 요청 메시지를 송신하는 단계;

상기 컨트롤러 및 상기 하나 이상의 주변 장치로부터 수신되는 주변 인증 응답 메시지를 이용하여 상기 컨트롤러를 인증하는 단계; 및

상기 인증 결과에 따라 상기 컨트롤러로 인증 응답을 송신하는 단계를 포함하며,

상기 주변 장치는 상기 메인 장치와 물리적으로 근접하여 근거리 무선 통신을 통해 상기 메인 장치와 통신이 가능한 장치이고,

상기 인증하는 단계는,

유효한 주변 인증 응답 메시지를 회신한 주변 장치의 개수가 기준값 이상이고,

상기 컨트롤러로부터 유효한 주변 인증 응답 메시지가 수신되었으며,

수신된 상기 주변 인증 응답 메시지의 수신 시각이 모두 기 설정된 타임아웃 이내인 경우, 상기 컨트롤러의 인증에 성공한 것으로 판단하는, 인증 방법.

청구항 12

청구항 11에 있어서,

상기 주변 인증을 요청하는 단계는,

상기 컨트롤러로부터 인증 요청이 수신되는 경우, 임의의 논스(nonce)를 포함하는 주변 인증 요청 메시지를 브로드캐스팅하는, 인증 방법.

청구항 13

청구항 12에 있어서,

상기 주변 인증 요청 메시지를 수신한 상기 컨트롤러 및 상기 하나 이상의 주변 장치는, 상기 주변 인증 요청 메시지에 포함된 상기 논스 및 자신의 식별 정보를 포함하는 주변 인증 응답 메시지를 상기 메인 장치로 송신하는, 인증 방법.

청구항 14

청구항 13에 있어서,

상기 메인 장치는, 상기 하나 이상의 주변 장치의 식별 정보로부터 생성된 블룸 필터를 저장 및 관리하며,

상기 인증 응답을 송신하는 단계는, 상기 논스 및 상기 블룸 필터를 이용하여 상기 하나 이상의 주변 장치로부터 수신되는 상기 주변 인증 응답 메시지의 유효성을 검증하는 단계를 더 포함하는, 인증 방법.

청구항 15

청구항 14에 있어서,

상기 유효성을 검증하는 단계는,

수신된 주변 인증 응답 메시지에 포함된 논스가 기 브로드캐스팅된 논스와 동일하고,

상기 수신된 주변 인증 응답 메시지에 포함된 식별 정보가 상기 블룸 필터에 존재하는 경우,

상기 수신된 주변 인증 응답 메시지를 유효한 것으로 판단하는, 인증 방법.

청구항 16

삭제

청구항 17

청구항 13에 있어서,

상기 하나 이상의 주변 장치는, 상기 메인 장치와 공유되는 대칭키로 상기 주변 인증 응답 메시지를 암호화하여 상기 메인 장치로 송신하는, 인증 방법.

청구항 18

청구항 17에 있어서,

상기 메인 장치는, 상기 대칭키로 상기 암호화된 주변 인증 응답 메시지의 유효성을 검증하는, 인증 방법.

청구항 19

청구항 13에 있어서,

상기 하나 이상의 주변 장치는, 자신의 식별 정보에 대응되는 비밀키로 상기 주변 인증 응답 메시지를 서명하여 상기 메인 장치로 송신하는, 인증 방법.

청구항 20

청구항 19에 있어서,

상기 메인 장치는, 상기 비밀키에 대응되는 주변 장치의 식별 정보를 이용하여 상기 서명된 주변 인증 응답 메시지의 유효성을 검증하는, 인증 방법.

발명의 설명

기 술 분 야

[0001] 개시되는 실시예들은 네트워크 상에서 단말 장치간의 인증 기술과 관련된다.

배 경 기 술

[0003] 스마트폰, 웨어러블 디바이스 등의 스마트 디바이스가 보편화되면서, 이를 이용하여 다른 장치들을 제어하려는 수요 또한 증가하고 있다. 예를 들어, 스마트폰이나 스마트 워치 등의 사용자 디바이스를 이용하여 텔레비전, 차량, 드론, 도어락, 공장의 스마트 기기 등의 다양한 기기를 조작함으로써 생활 및 업무의 편의성을 높일 수 있다.

[0004] 사용자 디바이스를 이용하여 다른 기기를 제어하기 위해서는 먼저 제어 대상 기기로부터 사용자 디바이스에 대한 접근 권한을 부여받아야 한다. 특히 최근에는 대부분의 전자 기기들이 네트워크에 연결되는 추세이며, 일단 접근 권한을 부여받은 사용자 디바이스는 제어 대상 기기에 대한 전면적인 제어가 가능하므로, 디바이스 인증시 충분한 보안성을 유지하는 것은 중요한 과제이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 공개특허공보 제10-2011-0071366호 (2011. 06. 29)

발명의 내용

해결하려는 과제

[0007] 개시되는 실시예들은 메인 디바이스에 접근하여 이를 제어하려는 컨트롤러의 인증 시 보안성을 높이기 위한 기술적인 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0009] 예시적인 실시예에 따르면, 컨트롤러; 및, 상기 컨트롤러로부터 인증 요청이 수신되는 경우, 상기 컨트롤러 및 하나 이상의 주변 장치로 주변 인증을 요청하고, 상기 주변 인증의 결과에 따라 상기 컨트롤러로 인증 응답을 송신하는 메인 장치를 포함하는 인증 시스템이 제공된다

[0010] 상기 메인 장치는, 상기 컨트롤러로부터 인증 요청이 수신되는 경우, 임의의 논스(nonce)를 포함하는 주변 인증 요청 메시지를 브로드캐스팅할 수 있다.

[0011] 상기 주변 인증 요청 메시지를 수신한 상기 컨트롤러 및 상기 하나 이상의 주변 장치는, 상기 주변 인증 요청 메시지에 포함된 상기 논스 및 자신의 식별 정보를 포함하는 주변 인증 응답 메시지를 상기 메인 장치로 송신할 수 있다.

[0012] 상기 메인 장치는, 상기 하나 이상의 주변 장치의 식별 정보로부터 생성된 블룸 필터를 저장 및 관리하며, 상기 논스 및 상기 블룸 필터를 이용하여 상기 하나 이상의 주변 장치로부터 수신되는 상기 주변 인증 응답 메시지의 유효성을 검증할 수 있다.

[0013] 상기 메인 장치는, 수신된 주변 인증 응답 메시지에 포함된 논스가 기 브로드캐스팅된 논스와 동일하고, 상기 수신된 주변 인증 응답 메시지에 포함된 식별 정보가 상기 블룸 필터에 존재하는 경우, 상기 수신된 주변 인증 응답 메시지를 유효한 것으로 판단할 수 있다.

[0014] 상기 메인 장치는, 유효성이 검증된 주변 인증 응답 메시지의 개수가 기준값 이상이고, 상기 컨트롤러로부터 유효한 주변 인증 응답 메시지가 수신되었으며, 수신된 상기 주변 인증 응답 메시지의 수신 시각이 모두 기 설정된 타임아웃 이내인 경우, 상기 컨트롤러의 인증에 성공한 것으로 판단할 수 있다.

[0015] 상기 하나 이상의 주변 장치는, 상기 메인 장치와 공유되는 대칭키로 상기 주변 인증 응답 메시지를 암호화하여 상기 메인 장치로 송신할 수 있다.

[0016] 상기 메인 장치는, 상기 대칭키로 상기 암호화된 주변 인증 응답 메시지의 유효성을 검증할 수 있다.

[0017] 상기 하나 이상의 주변 장치는, 자신의 식별 정보에 대응되는 비밀키로 상기 주변 인증 응답 메시지를 서명하여 상기 메인 장치로 송신할 수 있다.

[0018] 상기 메인 장치는, 상기 비밀키에 대응되는 주변 장치의 식별 정보를 이용하여 상기 서명된 주변 인증 응답 메시지의 유효성을 검증할 수 있다.

[0019] 다른 예시적인 실시예에 따르면, 컨트롤러로부터 인증 요청을 수신하는 단계; 상기 인증 요청에 따라 상기 컨트롤러 및 하나 이상의 주변 장치로 주변 인증을 요청하는 단계; 및, 상기 주변 인증의 결과에 따라 상기 컨트롤러로 인증 응답을 송신하는 단계를 포함하는 인증 방법이 제공된다.

[0020] 상기 주변 인증을 요청하는 단계는, 상기 컨트롤러로부터 인증 요청이 수신되는 경우, 임의의 논스(nonce)를 포함하는 주변 인증 요청 메시지를 브로드캐스팅하도록 구성될 수 있다.

[0021] 상기 주변 인증 요청 메시지를 수신한 상기 컨트롤러 및 상기 하나 이상의 주변 장치는, 상기 주변 인증 요청 메시지에 포함된 상기 논스 및 자신의 식별 정보를 포함하는 주변 인증 응답 메시지를 상기 메인 장치로 송신할 수 있다.

[0022] 상기 메인 장치는, 상기 하나 이상의 주변 장치의 식별 정보로부터 생성된 블룸 필터를 저장 및 관리하며, 상기 인증 응답을 송신하는 단계는, 상기 논스 및 상기 블룸 필터를 이용하여 상기 하나 이상의 주변 장치로부터 수신되는 상기 주변 인증 응답 메시지의 유효성을 검증하는 단계를 더 포함할 수 있다.

[0023] 상기 유효성을 검증하는 단계는, 수신된 주변 인증 응답 메시지에 포함된 논스가 기 브로드캐스팅된 논스와 동일하고, 상기 수신된 주변 인증 응답 메시지에 포함된 식별 정보가 상기 블룸 필터에 존재하는 경우, 상기 수신된 주변 인증 응답 메시지를 유효한 것으로 판단할 수 있다.

[0024] 상기 메인 장치는, 유효성이 검증된 주변 인증 응답 메시지의 개수가 기준값 이상이고, 상기 컨트롤러로부터 유효한 주변 인증 응답 메시지가 수신되었으며, 수신된 상기 주변 인증 응답 메시지의 수신 시각이 모두 기 설정된 타임아웃 이내인 경우, 상기 컨트롤러의 인증에 성공한 것으로 판단할 수 있다.

[0025] 상기 하나 이상의 주변 장치는, 상기 메인 장치와 공유되는 대칭키로 상기 주변 인증 응답 메시지를 암호화하여 상기 메인 장치로 송신할 수 있다.

[0026] 상기 메인 장치는, 상기 대칭키로 상기 암호화된 주변 인증 응답 메시지의 유효성을 검증할 수 있다.

[0027] 상기 하나 이상의 주변 장치는, 자신의 식별 정보에 대응되는 비밀키로 상기 주변 인증 응답 메시지를 서명하여 상기 메인 장치로 송신할 수 있다.

[0028] 상기 메인 장치는, 상기 비밀키에 대응되는 주변 장치의 식별 정보를 이용하여 상기 서명된 주변 인증 응답 메시지의 유효성을 검증할 수 있다.

발명의 효과

[0030] 개시되는 실시예들에 따르면, 메인 디바이스에 주변의 디바이스를 컨트롤러의 인증을 위한 인증 매체로 활용함으로써 컨트롤러의 인증 시 보안성 높일 수 있으며, 이 과정에서 발생할 수 있는 컨트롤러 및 주변 장치의 릴레이 공격을 효과적으로 차단할 수 있다.

도면의 간단한 설명

[0032] 도 1은 일 실시예에 따른 주변 장치를 이용한 인증 시스템(100)을 설명하기 위한 블록도

도 2는 제1 실시예에 따른 주변 장치를 이용한 인증에서의 셋업 과정(S200)을 설명하기 위한 흐름도

도 3은 제1 실시예에 따른 주변 장치를 이용한 인증 과정(S300)을 설명하기 위한 흐름도

도 4는 제2 실시예에 따른 주변 장치를 이용한 인증에서의 셋업 과정(S400)을 설명하기 위한 흐름도

도 5는 제2 실시예에 따른 주변 장치를 이용한 인증 과정(S500)을 설명하기 위한 흐름도

도 6은 제3 실시예에 따른 주변 장치를 이용한 인증에서의 셋업 과정(S600)을 설명하기 위한 흐름도

도 7은 제3 실시예에 따른 주변 장치를 이용한 인증 과정(S700)을 설명하기 위한 흐름도

도 8은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0033] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0034] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0036] 도 1은 일 실시예에 따른 주변 장치를 이용한 인증 시스템(100)을 설명하기 위한 블록도이다. 도시된 바와 같이, 일 실시예에 따른 인증 시스템(100)은 컨트롤러(102), 메인 장치(104) 및 하나 이상의 주변 장치(106)를 포함한다.

[0037] 컨트롤러(102)는 메인 장치(104)에 접근하여 메인 장치(104)를 제어하고자 하는 사용자의 디바이스이다. 컨트롤러(102)는 메인 장치(104)에 접속하여 인증을 수행함으로써 메인 장치(104)로의 접근 권한을 획득할 수 있다. 개시되는 실시예들에서, 컨트롤러(102)는 휴대 전화, 스마트폰, 태블릿, 웨어러블 디바이스, 랩탑 컴퓨터 등 다양한 종류의 사용자 디바이스를 포함할 수 있다.

[0038] 메인 장치(104)는 컨트롤러(102)가 접근하고자 하는 대상 기기이다. 개시되는 실시예들에서, 메인 장치(104)는 스마트 TV, 차량, 데스크탑 또는 노트북 컴퓨터, 스마트 도어록, 드론, 또는 각종 계측기 등 원격 제어가 가능한 모든 종류의 기기를 포함할 수 있다. 예컨대, 사용자가 자신의 스마트폰을 이용하여 스마트 TV를 제어할 경

우, 스마트폰이 컨트롤러(102)가 되고 스마트 TV가 메인 장치(104)가 될 수 있다. 이 밖에도, 본 발명의 컨트롤러(102) 및 메인 장치(104)는 모든 종류의 네트워크를 활용한 원격 제어 환경에 적용될 수 있다.

[0039] 주변 장치(106)는 메인 장치(104)의 요청에 따라 컨트롤러(102)를 인증하기 위한 인증 매체이다. 일 실시예에서, 주변 장치(106)는 메인 장치(104)와 물리적으로 근접하여 근거리 무선 통신을 통해 메인 장치(104)와 통신이 가능한 장치일 수 있다. 예를 들어, 주변 장치(106)는 메인 장치(104)와 동일 공간 내에 위치한 프린터, 복합기, 스캐너 등의 주변 기기, 컨트롤러(102)와는 별도의 휴대 단말 내지 태블릿 디바이스, IoT 기능을 내장한 가전 기기 등일 수 있다. 컨트롤러(102)의 사용자는 사전에 메인 장치(104)에 컨트롤러(102)를 인증하는데 사용될 하나 이상의 주변 장치(106)를 등록해 둘 수 있다.

[0040] 메인 장치(104)에 접근하려는 컨트롤러(102)로부터 인증 요청이 수신되는 경우, 메인 장치(104)는 컨트롤러(102) 및 하나 이상의 주변 장치(106)로 주변 인증을 요청한다. 일 실시예에서 메인 장치(104)는 임의의 논스(nonce)를 생성하고, 생성된 상기 논스를 포함하는 주변 인증 요청 메시지를 브로드캐스트(broadcast)하는 방식으로 주변 인증을 요청할 수 있다.

[0041] 주변 인증 요청을 수신한 컨트롤러(102) 및 하나 이상의 주변 장치(106)는 상기 주변 인증에 따른 주변 인증 응답을 메인 장치(104)로 회신하고, 메인 장치(104)는 주변 인증의 결과에 따라 컨트롤러(102)로 인증 응답을 회신한다. 이때 상기 인증 응답 메시지에는 상기 주변 인증 요청 메시지에 포함된 논스가 포함될 수 있다. 즉, 기본적으로 메인 장치(104)는 인증 응답 메시지에 기 브로드캐스팅된 논스와 동일한 논스가 포함되어 있는지 여부에 따라 주변 인증을 수행할 수 있다.

[0042] 일 실시예에서, 메인 장치(104)는 n 개의 주변 장치(106) 중 유효한 인증 응답을 회신한 주변 장치(106)의 개수가 k(k<=n)개 이상이고, 컨트롤러(102)로부터 유효한 인증 응답이 수신되며, 또한 주변 장치(106)로부터 수신된 인증 응답 및 컨트롤러(102)로부터 수신된 인증 응답의 수신 시각이 모두 기 설정된 타임아웃(t) 내인 경우 컨트롤러(102)의 인증에 성공한 것으로 판단할 수 있다. 이때 상기 k 및 t는 요구되는 보안 수준, 주변 장치(106)의 개수 및 네트워크 환경 등 다양한 요소를 고려하여 적절히 설정될 수 있다.

[0043] 일 실시예에서, 컨트롤러(102), 메인 장치(104) 및 하나 이상의 주변 장치(106)는 네트워크(미도시)를 통해 연결될 수 있다. 몇몇 실시예들에서, 네트워크는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wide area networks), 셀룰러 네트워크, 모바일 네트워크, 블루투스(Bluetooth), 지그비(Zigbee) 등의 근거리 통신 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0044] 개시되는 실시예들에서, 주변 장치(106)를 이용한 주변 인증 방법은 다음의 세 가지로 구분될 수 있다.

[0045] 1) 블룸 필터 기반의 인증 방식

[0046] 2) 대칭키 기반의 인증 방식

[0047] 3) 비대칭키 기반의 인증 방식

[0048] 위의 세 가지 방식은 모두 셋업 단계와 인증 단계를 포함하는 두 가지 단계로 구성된다. 또한 1)의 블룸 필터 기반의 인증 방식은 2) 및 3)의 인증에도 선택적으로 적용 가능하다.

[0050] 도 2는 제1 실시예에 따른 주변 장치를 이용한 인증에서의 셋업 과정(S200)을 설명하기 위한 흐름도이다. 제1 실시예에 따른 인증은 블룸 필터를 기반으로 한 인증 방식이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0051] 단계 S202에서, 메인 장치(104)는 하나 이상의 주변 장치(106)로부터 각 주변 장치(106)의 식별 정보(아이디)를 수신한다. 일 실시예에서, 상기 식별 정보는 하나 이상의 주변 장치(106)의 아이피 주소, 맥 어드레스 등 각각의 주변 장치(106)를 다른 장치와 구별하기 위한 모든 종류의 정보를 포함할 수 있다. 이하의 설명에서는 n의 주변 장치(106) 중 i번째의 주변 장치(106-i)의 식별 정보를 N_i로 칭하기로 한다.

[0052] 단계 S204에서, 메인 장치(104)는 수신된 상기 각 주변 장치(106)의 식별 정보를 이용하여 블룸 필터(BF_N)를 생성한다. 일 실시예에서, 메인 장치(104)는 n의 주변 장치(106)로부터 수신된 n의 식별 정보(N_1 ~ N_n)를 해시하여

얻은 해시값을 이용하여 상기 블룸 필터를 생성할 수 있다.

[0053] 또한, 이와 별도로 메인 장치(104)는 인증 파라미터인 k 및 t를 사전에 정의할 수 있다. k는 컨트롤러(102)의 인증을 위하여 필요한 주변 장치(106)의 개수로서 k <= n의 관계를 가진다. 즉, 컨트롤러(102)의 인증을 위해서는 n개의 주변 장치(106) 중 적어도 k개의 주변 장치(106)로부터 유효한 인증 응답을 수신하여야 한다. 또한 t는 타임아웃으로서, 컨트롤러(102)의 인증을 위해서는 k개의 인증 응답이 모두 t 시간 이내에 메인 장치(104)로 수신되어야 한다.

[0055] 도 3은 제1 실시예에 따른 주변 장치를 이용한 인증 과정(S300)을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0056] 단계 S302에서, 컨트롤러(102)는 메인 장치(104)로 인증을 요청한다.

[0057] 단계 S304에서, 메인 장치(104)는 새로운 논스(nonce)를 생성한다.

[0058] 단계 S306 및 단계 S308에서, 메인 장치(104)는 생성된 논스를 포함하는 주변 인증 요청 메시지를 컨트롤러(102) 및 주변 장치(106)에 브로드캐스팅한다.

[0059] 단계 S310 및 단계 S312에서, 상기 주변 인증 요청 메시지를 수신한 주변 장치(106)는 주변 인증 응답 메시지를 생성하고 이를 메인 장치(104)로 송신한다. 이때 상기 주변 인증 응답 메시지는 자신이 수신한 논스 및 주변 장치(106)의 식별 정보가 포함된다.

[0060] 단계 S314 및 단계 S316에서, 상기 주변 인증 요청 메시지를 수신한 컨트롤러(102) 또한 주변 인증 응답 메시지를 생성하고 이를 메인 장치(104)로 송신한다. 이때 상기 주변 인증 응답 메시지는 자신이 수신한 논스 및 컨트롤러(102)의 식별 정보가 포함된다.

[0061] 본 발명의 실시예들에서, 주변 장치(106) 뿐 아니라 컨트롤러(102) 또한 주변 인증 응답을 회신하는 이유는 릴레이 공격(relaying attack)을 차단하기 위한 것이다. 릴레이 공격이란 컨트롤러(102) 또는 주변 장치(106)가 실제로 메인 장치(104)에 물리적으로 근접하지 않은 상황에서 리피터(repeater) 등을 이용하여 메시지 전송 거리를 늘리거나 인터넷 또는 여타의 무선 네트워크 등을 이용하여, 원거리에서 메인 장치(104)에 인접한 것처럼 메인 장치(104)를 속이는 공격을 의미한다. 개시되는 실시예에서는, 주변 장치(106) 및 컨트롤러(102)에 주변 인증 요청을 송신하고 이에 따른 주변 인증 응답이 기 설정된 타임아웃(t) 내에 수신되는지의 여부를 파악함으로써 주변 장치(106) 뿐 아니라 컨트롤러(102)가 실제로 메인 장치(104)에 물리적으로 근접해 있는지의 여부를 확인할 수 있으며, 이에 따라 릴레이 공격을 효과적으로 차단할 수 있다. 예컨대, 블루투스나 WiFi 등의 경우 메시지 전송에 소요되는 시간이 거리에 비례하여 증가하는 특성을 보인다. 따라서 네트워크의 종류 및 공간의 특성에 따라 타임아웃을 적절히 설정함으로써 원격에서 메인 장치(104)에 접근하는 것을 막을 수 있다.

[0062] 단계 S318에서, 메인 장치(104)는 수신된 주변 인증 응답 메시지를 검증한다. 메인 장치(104)는 앞서 설명한 셋업 과정을 통해 하나 이상의 주변 장치(106)의 식별 정보로부터 생성된 블룸 필터(BF_N)를 저장 및 관리하도록 구성된다. 메인 장치(104)는 기 송신된 논스 및 상기 블룸 필터(BF_N)를 이용하여 하나 이상의 주변 장치(106) 및 컨트롤러(102)로부터 수신되는 주변 인증 응답 메시지의 유효성을 검증할 수 있다.

[0063] 구체적으로 메인 장치(104)는, 주변 장치(106)로부터 수신된 주변 인증 응답 메시지에 포함된 논스가 기 브로드캐스팅된 논스와 동일하고, 주변 인증 응답 메시지에 포함된 주변 장치(106)의 식별 정보가 블룸 필터(BF_N)에 존재하는 경우, 해당 주변 인증 응답 메시지를 유효한 것으로 판단할 수 있다.

[0064] 또한, 메인 장치(104)는, 컨트롤러(102)로부터 수신된 주변 인증 응답 메시지에 포함된 논스가 기 브로드캐스팅된 논스와 동일하고, 주변 인증 응답 메시지에 포함된 컨트롤러(102)의 식별 정보가 인증 요청을 송신한 컨트롤러(102)와 동일한 경우, 해당 주변 인증 응답 메시지를 유효한 것으로 판단할 수 있다.

[0065] 메인 장치(104)는 1) 주변 장치(106)로부터 수신된 인증 응답 메시지 중 유효성이 검증된 주변 인증 응답 메시지의 개수(j)가 기준값(k) 이상이고 (j >= k), 2) 컨트롤러(102)로부터 유효한 주변 인증 응답 메시지가 수신되었으며, 3) 1) 및 2)에서 수신된 주변 인증 응답 메시지의 수신 시각이 모두 기 설정된 타임아웃(t) 이내인 경우, 컨트롤러(102)의 인증에 성공한 것으로 판단할 수 있다. 그러나 이와 달리 위 1), 2), 3)의 조건 중 하나라도 만족하지 못하는 경우에는 컨트롤러(102)의 인증에 실패한 것으로 판단할 수 있다.

[0066] 단계 S320에서, 메인 장치(104)는 상기 판단에 따른 인증 결과를 컨트롤러(102)로 회신한다.

[0068] 도 4는 제2 실시예에 따른 주변 장치를 이용한 인증에서의 셋업 과정(S400)을 설명하기 위한 흐름도이다. 제2 실시예에 따른 인증은 대칭키 기반의 인증 방식이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0069] 단계 S402에서, 주변 장치(106)는 신뢰 가능한 인증 기관(TKG; Trusted Key Generator, 108)에 자신의 식별 정보(주변 장치 식별 정보)를 송신한다.

[0070] 단계 S404에서, 컨트롤러(102) 또한 신뢰 가능한 인증 기관(108)에 자신의 식별 정보(컨트롤러 식별 정보)를 송신한다.

[0071] 단계 S406에서, 인증 기관(108)은 식별 정보를 송신한 주변 장치(106) 및 컨트롤러(102) 각각에 대한 대칭키를 생성한다. 일 실시예에서, 인증 기관(108)은 메시지 인증 코드(MAC; Message Authentication Code)를 이용하여 상기 대칭키를 생성할 수 있다. 예를 들어, i번째의 주변 장치(106-i)의 대칭키 K_{Ni}는 다음의 수학식 1과 같이 생성될 수 있다.

[0072] [수학식 1]

$$K_{N_i} = MAC.Gen(1^k)$$

[0073]

[0074] 상기 수학식에서 k는 시큐리티 파라미터, MAC.Gen은 대칭키 생성 함수이다. 컨트롤러(102)의 식별 정보에 대응되는 대칭키(K_C) 또한 동일한 방법으로 생성될 수 있다.

[0075] 단계 S408에서, 인증 기관(108)은 수신된 주변 장치(106) 및 컨트롤러(102)의 식별 정보 및 S406 단계에서 생성된 대칭키 쌍을 대칭키 테이블(T)에 저장한다.

[0076] 단계 S410에서, 인증 기관(108)은 각 주변 장치(106)로 S406 단계에서 생성된 대칭키를 전달한다.

[0077] 마찬가지로 단계 S412에서, 인증 기관(108)은 컨트롤러(102)로 S406 단계에서 생성된 대칭키를 전달한다.

[0078] 단계 S414에서, 인증 기관(108)은 S408 단계에서 생성된 대칭키 테이블을 메인 장치(104)로 전달한다.

[0079] 한편, 제1 실시예와 마찬가지로 메인 장치(104)는 인증 파라미터인 k 및 t를 사전에 정의할 수 있다. k는 컨트롤러(102)의 인증을 위하여 필요한 주변 장치(106)의 개수로서 k <= n의 관계를 가진다. 즉, 컨트롤러(102)의 인증을 위해서는 n개의 주변 장치(106) 중 적어도 k개의 주변 장치(106)로부터 유효한 인증 응답을 수신하여야 한다. 또한 t는 타임아웃으로서, 컨트롤러(102)의 인증을 위해서는 k개의 인증 응답이 모두 t 시간 이내에 메인 장치(104)로 수신되어야 한다.

[0081] 도 5는 제2 실시예에 따른 주변 장치를 이용한 인증 과정(S500)을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0082] 단계 S502에서, 컨트롤러(102)는 메인 장치(104)로 인증을 요청한다.

[0083] 단계 S504에서, 메인 장치(104)는 새로운 논스(nonce)를 생성한다.

[0084] 단계 S506 및 단계 S508에서, 메인 장치(104)는 생성된 논스를 포함하는 주변 인증 요청 메시지를 컨트롤러(102) 및 주변 장치(106)에 브로드캐스팅한다.

[0085] 단계 S510 및 단계 S512에서, 상기 주변 인증 요청 메시지를 수신한 주변 장치(106)는 주변 인증 응답 메시지를 생성하고 셋업 과정에서 인증 기관(108)으로부터 수신한 주변 장치 대칭키를 이용하여 주변 인증 응답을 암호화한다. 상기 암호화는 다음의 수학식 2와 같이 수행될 수 있다.

[0086] [수학식 2]

$$m = C \parallel M \parallel N_i \parallel nonce$$

[0087]

$$t_i = MAC.Mac_{K_{N_i}}(m)$$

[0088]

[0089] 상기 수학식에서, C는 컨트롤러(102)의 식별 정보, M은 메인 장치(104)의 식별 정보, N_i는 i번째 주변 장치(106)의 식별 정보, nonce는 주변 인증 요청 메시지에 포함된 논스이다. 컨트롤러(102)의 식별 정보(C) 및 메인 장치(104)의 식별 정보(M)는 논스와 함께 주변 인증 요청 메시지에 포함되어 주변 장치(106)로 전달될 수 있다. 또한 m은 주변 인증 응답 메시지, K_{Ni}는 i번째 주변 장치(106)의 대칭키, MAC.Mac는 대칭키 암호화 함수, t_i는 암호화된 주변 인증 응답 메시지이다.

[0090] 단계 S514에서, 주변 장치(106)는 암호화된 주변 인증 응답 메시지(t_i)를 메인 장치(104)로 송신한다.

[0091] 단계 S516 및 단계 S518에서, 상기 주변 인증 요청 메시지를 수신한 컨트롤러(102)는 주변 인증 응답 메시지를 생성하고 셋업 과정에서 인증 기관(108)으로부터 수신한 컨트롤러 대칭키를 이용하여 주변 인증 응답을 암호화한다. 상기 암호화는 다음의 수학식 3과 같이 수행될 수 있다.

[0092] [수학식 3]

$$m_C = C \parallel M \parallel nonce$$

[0093]

$$t_C = MAC.Mac_{K_C}(m_C)$$

[0094]

[0095] 상기 수학식에서, C는 컨트롤러(102)의 식별 정보, M은 메인 장치(104)의 식별 정보, nonce는 주변 인증 요청 메시지에 포함된 논스이다. 메인 장치(104)의 식별 정보(M)는 논스와 함께 주변 인증 요청 메시지에 포함되어 컨트롤러(102)로 전달될 수 있다. 또한 m_C는 컨트롤러(102)의 주변 인증 응답 메시지, K_C는 컨트롤러(102)의 대칭키, MAC.Mac는 대칭키 암호화 함수, t_C는 암호화된 주변 인증 응답 메시지이다.

[0096] 단계 S520에서, 주변 장치(106)는 암호화된 주변 인증 응답 메시지(t_C)를 메인 장치(104)로 송신한다.

[0097] 본 발명의 실시예들에서, 주변 장치(106) 뿐 아니라 컨트롤러(102) 또한 주변 인증 응답을 회신하는 이유는 릴레이 공격(relaying attack)을 차단하기 위한 것임은 제1 실시예에서 이미 기술하였으므로 여기서는 반복되는 설명을 생략한다.

[0098] 단계 S522에서, 메인 장치(104)는 수신된 주변 인증 응답 메시지를 검증한다. 주변 장치(106)로부터 수신되는 주변 인증 응답 메시지(t_i)의 검증은 다음의 수학식 4와 같이 이루어질 수 있다.

[0099] [수학식 4]

$$b = MAC.Vrfy_{K_i}(m, t_i)$$

[0100]

[0101] 상기 수학식에서, MAC.Vrfy는 대칭키 기반의 검증 함수로서 t_i가 유효한 인증 응답 메시지인 경우 1을 반환하고 그렇지 않은 경우 0을 반환하는 함수이고, b는 검증값이다.

[0102] 마찬가지로, 컨트롤러(102)로부터 수신되는 주변 인증 응답 메시지(t_C)의 검증은 다음의 수학식 5와 같이 이루어질 수 있다.

[0103] [수학식 5]

$$a = MAC.Vrfy_{K_i}(m, t_c)$$

[0104]

[0105] 상기 수학식에서, MAC.Vrfy는 대칭키 기반의 검증 함수로서 t_C가 유효한 인증 응답 메시지인 경우 1을 반환하고 그렇지 않은 경우 0을 반환하는 함수, a는 검증값이다.

[0106] 메인 장치(104)는, 1) 주변 장치(106)로부터 수신된 인증 응답 메시지 중 유효성이 검증된 주변 인증 응답 메시지의 개수(j)가 기준값(k) 이상이고 (j >= k), 2) 컨트롤러(102)로부터 유효한 주변 인증 응답 메시지가 수신되었으며, 3) 1) 및 2)에서 수신된 주변 인증 응답 메시지의 수신 시각이 모두 기 설정된 타임아웃(t) 이내인 경우, 컨트롤러(102)의 인증에 성공한 것으로 판단할 수 있다. 그러나 이와 달리 위 1), 2), 3)의 조건 중 하나라도 만족하지 못하는 경우에는 컨트롤러(102)의 인증에 실패한 것으로 판단할 수 있다.

[0107] 한편, 실시예에 따라 메인 장치(104)는 주변 인증 응답 메시지(t_i)의 검증을 수행하기 이전에 제1 실시예에 따른 블룸 필터(BF_N)를 이용한 주변 인증 응답 메시지의 검증을 추가로 실시할 수도 있다. 예를 들어, 주변 장치(106)는 주변 인증 응답 메시지에 자신의 식별 정보를 부가하여 메인 장치(104)로 송신하고, 메인 장치(104)는 수신된 주변 인증 응답 메시지에 포함된 식별 정보가 블룸 필터(BF_N)에 포함되어 있는지를 확인할 수 있다. 만약 해당 식별 정보가 블룸 필터(BF_N)에 포함되어 있지 않은 경우, 메인 장치(104)는 검증 함수를 이용한 메시지의 유효성 검증을 수행할 필요 없이 해당 주변 인증 응답 메시지를 삭제(discard)할 수 있다.

[0108] 단계 S524에서, 메인 장치(104)는 상기 판단에 따른 인증 결과를 컨트롤러(102)로 회신한다.

[0109] 본 실시예의 경우 블룸 필터만을 기반으로 하는 제1 실시예에 비해 보안성이 강화될 수 있다. 특히 메인 장치(104)와 주변 장치(106)간에만 공유되는 대칭키를 이용하여 메시지를 암호화하여 전송하므로 메시지의 위변조나 man in the middle 공격에 강하고, 별도의 메시지 타임아웃을 설정함으로써 릴레이 공격을 차단할 수 있다.

[0111] 도 6은 제3 실시예에 따른 주변 장치를 이용한 인증에서의 셋업 과정(S600)을 설명하기 위한 흐름도이다. 제3 실시예에 따른 인증은 비대칭키 기반의 인증 방식이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0112] 단계 602에서, 신뢰 가능한 인증 기관(TKG; Trusted Key Generator, 108)은 아이디 기반 시그니처 스킴(Identity Based Signature scheme)의 셋업 함수(IBS.Setup)를 이용하여 공개 파라미터(params) 및 마스터 비밀키(msk)를 생성한다.

[0113] 단계 S604에서, 주변 장치(106)는 신뢰 가능한 인증 기관(TKG; Trusted Key Generator, 108)에 자신의 식별 정보(주변 장치 식별 정보)를 송신한다.

[0114] 단계 S606에서, 컨트롤러(102) 또한 신뢰 가능한 인증 기관(108)에 자신의 식별 정보(컨트롤러 식별 정보)를 송신한다.

[0115] 단계 S608에서, 인증 기관(108)은 식별 정보를 송신한 주변 장치(106) 및 컨트롤러(102) 각각에 대한 비밀키를 생성한다. 일 실시예에서, 인증 기관(108)은 아이디 기반 시그니처 스킴(Identity Based Signature scheme)을 이용하여 상기 비밀키를 생성할 수 있다. 예를 들어, i번째의 주변 장치(106-i)의 식별 정보를 N_i라 할 때, 이에 대한 비밀키 SK_{Ni}는 다음의 수학식 6과 같이 생성될 수 있다.

[0116] [수학식 6]

$$SK_{N_i} = IBS.KeyGen(msk, N_i)$$

[0117]

[0118] 상기 수학식에서 IBS.KeyGen은 아이디 기반 시그니처 스킴의 비밀키 생성 함수이다. 컨트롤러(102)의 식별 정보에 대응되는 비밀키(SK_C) 또한 동일한 방법으로 생성될 수 있다.

[0119] 단계 S610에서, 인증 기관(108)은 수신된 주변 장치(106) 및 컨트롤러(102)의 식별 정보를 테이블(T)에 저장한다.

[0120] 단계 S612에서, 인증 기관(108)은 각 주변 장치(106)로 S608 단계에서 생성된 비밀키(주변 장치 비밀키)를 전달한다.

[0121] 마찬가지로 단계 S614에서, 인증 기관(108)은 컨트롤러(102)로 S608 단계에서 생성된 비밀키(컨트롤러 비밀키)를 전달한다.

[0122] 단계 S616에서, 인증 기관(108)은 S608 단계에서 생성된 식별 정보 테이블을 메인 장치(104)로 전달한다.

[0123] 한편, 제1 실시예와 마찬가지로 메인 장치(104)는 인증 파라미터인 k 및 t를 사전에 정의할 수 있다. k는 컨트롤러(102)의 인증을 위하여 필요한 주변 장치(106)의 개수로서 k <= n의 관계를 가진다. 즉, 컨트롤러(102)의 인증을 위해서는 n개의 주변 장치(106) 중 적어도 k개의 주변 장치(106)로부터 유효한 인증 응답을 수신하여야 한다. 또한 t는 타임아웃으로서, 컨트롤러(102)의 인증을 위해서는 k개의 인증 응답이 모두 t 시간 이내에 메인 장치(104)로 수신되어야 한다.

[0125] 도 7은 제3 실시예에 따른 주변 장치를 이용한 인증 과정(S700)을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0126] 단계 S702에서, 컨트롤러(102)는 메인 장치(104)로 인증을 요청한다.

[0127] 단계 S704에서, 메인 장치(104)는 새로운 논스(nonce)를 생성한다.

[0128] 단계 S706 및 단계 S708에서, 메인 장치(104)는 생성된 논스를 포함하는 주변 인증 요청 메시지를 컨트롤러(102) 및 주변 장치(106)에 브로드캐스팅한다.

[0129] 단계 S710 및 단계 S712에서, 상기 주변 인증 요청 메시지를 수신한 주변 장치(106)는 주변 인증 응답 메시지를 생성하고 셋업 과정에서 인증 기관(108)으로부터 수신한 주변 장치 비밀키를 이용하여 주변 인증 응답을 서명한다. 상기 서명은 다음의 수학식 7과 같이 수행될 수 있다.

[0130] [수학식 7]

$$m = C \parallel M \parallel N_i \parallel nonce$$

[0131]

$$\sigma_i = IBS.Sign_{SK_{N_i}}(m)$$

[0132]

[0133] 상기 수학식에서, C는 컨트롤러(102)의 식별 정보, M은 메인 장치(104)의 식별 정보, N_i는 i번째 주변 장치(106)의 식별 정보, nonce는 주변 인증 요청 메시지에 포함된 논스이다. 컨트롤러(102)의 식별 정보(C) 및 메인 장치(104)의 식별 정보(M)는 논스와 함께 주변 인증 요청 메시지에 포함되어 주변 장치(106)로 전달될 수 있다. 또한 m은 주변 인증 응답 메시지, SK_{Ni}는 i번째 주변 장치(106)의 비밀키, IBS.Sign은 아이디 기반 시그니처 스킴의 서명 함수, σ_i는 서명된 주변 인증 응답 메시지이다.

[0134] 단계 S714에서, 주변 장치(106)는 서명된 주변 인증 응답 메시지(σ_i)를 메인 장치(104)로 송신한다.

[0135] 단계 S716 및 단계 S718에서, 상기 주변 인증 요청 메시지를 수신한 컨트롤러(102)는 주변 인증 응답 메시지를 생성하고 셋업 과정에서 인증 기관(108)으로부터 수신한 컨트롤러 비밀키를 이용하여 주변 인증 응답을 서명한다. 상기 서명은 다음의 수학식 8과 같이 수행될 수 있다.

[0136] [수학식 8]

$$m_C = C \parallel M \parallel nonce$$

[0137]

$$\sigma_C = IBS.Sign_{SK_C}(m_C)$$

[0138]

[0139] 상기 수학식에서, C는 컨트롤러(102)의 식별 정보, M은 메인 장치(104)의 식별 정보, nonce는 주변 인증 요청 메시지에 포함된 논스이다. 메인 장치(104)의 식별 정보(M)는 논스와 함께 주변 인증 요청 메시지에 포함되어 컨트롤러(102)로 전달될 수 있다. 또한 m_C는 컨트롤러(102)의 주변 인증 응답 메시지, SK_C는 컨트롤러(102)의 비

밀키, IBS.Sign은 아이디 기반 시그니처 스킴의 서명 함수, σ_C는 서명된 주변 인증 응답 메시지이다.

[0140] 단계 S720에서, 주변 장치(106)는 서명된 주변 인증 응답 메시지(t_C)를 메인 장치(104)로 송신한다.

[0141] 본 발명의 실시예들에서, 주변 장치(106) 뿐 아니라 컨트롤러(102) 또한 주변 인증 응답을 회신하는 이유는 릴레이 공격(relaying attack)을 차단하기 위한 것임은 제1 실시예에서 이미 기술하였으므로 여기서는 반복되는 설명을 생략한다.

[0142] 단계 S724에서, 메인 장치(104)는 수신된 주변 인증 응답 메시지를 검증한다. 주변 장치(106)로부터 수신되는 주변 인증 응답 메시지(σ_i)의 검증은 다음의 수학식 9와 같이 이루어질 수 있다.

[0143] [수학식 9]

$$b = IBS.Vrfy(parmas, N_i, m, \sigma_i)$$

[0144]

[0145] 상기 수학식에서, IBS.Vrfy는 아이디 기반의 시그니처 스킴의 검증 함수로서 σ_i가 유효한 인증 응답 메시지인 경우 1을 반환하고 그렇지 않은 경우 0을 반환하는 함수이고, b는 검증값이다.

[0146] 마찬가지로, 컨트롤러(102)로부터 수신되는 주변 인증 응답 메시지(σ_C)의 검증은 다음의 수학식 10과 같이 이루어질 수 있다.

[0147] [수학식 10]

$$a = IBS.Vrfy(parmas, C, m, \sigma_c)$$

[0148]

[0149] 상기 수학식에서, IBS.Vrfy는 아이디 기반의 시그니처 스킴의 검증 함수로서 σ_i가 유효한 인증 응답 메시지인 경우 1을 반환하고 그렇지 않은 경우 0을 반환하는 함수이고, a는 검증값이다.

[0150] 메인 장치(104)는, 1) 주변 장치(106)로부터 수신된 인증 응답 메시지 중 유효성이 검증된 주변 인증 응답 메시지의 개수(j)가 기준값(k) 이상이고 (j >= k), 2) 컨트롤러(102)로부터 유효한 주변 인증 응답 메시지가 수신되었으며, 3) 1) 및 2)에서 수신된 주변 인증 응답 메시지의 수신 시각이 모두 기 설정된 타임아웃(t) 이내인 경우, 컨트롤러(102)의 인증에 성공한 것으로 판단할 수 있다. 그러나 이와 달리 위 1), 2), 3)의 조건 중 하나라도 만족하지 못하는 경우에는 컨트롤러(102)의 인증에 실패한 것으로 판단할 수 있다.

[0151] 한편, 실시예에 따라 메인 장치(104)는 주변 인증 응답 메시지(σ_i)의 검증을 수행하기 이전에 제1 실시예에 따른 블룸 필터(BF_N)를 이용한 주변 인증 응답 메시지의 검증을 추가로 실시할 수도 있다. 예를 들어, 주변 장치(106)는 주변 인증 응답 메시지에 자신의 식별 정보를 부가하여 메인 장치(104)로 송신하고, 메인 장치(104)는 수신된 주변 인증 응답 메시지에 포함된 식별 정보가 블룸 필터(BF_N)에 포함되어 있는지를 확인할 수 있다. 만약 해당 식별 정보가 블룸 필터(BF_N)에 포함되어 있지 않은 경우, 메인 장치(104)는 검증 함수를 이용한 메시지의 유효성 검증을 수행할 필요 없이 해당 주변 인증 응답 메시지를 삭제(discard)할 수 있다.

[0152] 단계 S724에서, 메인 장치(104)는 상기 판단에 따른 인증 결과를 컨트롤러(102)로 회신한다.

[0153] 본 실시예의 또한 블룸 필터만을 기반으로 하는 제1 실시예에 비해 보안성이 강화될 수 있다. 특히 아이디 기반의 시그니처 스킴을 이용하여 메시지를 서명하여 전송하므로 메시지의 위변조나 man in the middle 공격에 강하고, 별도의 메시지 타임아웃을 설정함으로써 릴레이 공격을 차단할 수 있다.

[0155] 도 8은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0156] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 본 발명의 실시예들에 따른 컨트롤러(102), 메인 장치(104) 및 주변 장치(106)일 수 있다. 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능

저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0157] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0158] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0159] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(102)와 연결될 수도 있다.

[0161] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0162] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0164] 100: 주변 장치를 이용한 인증 시스템

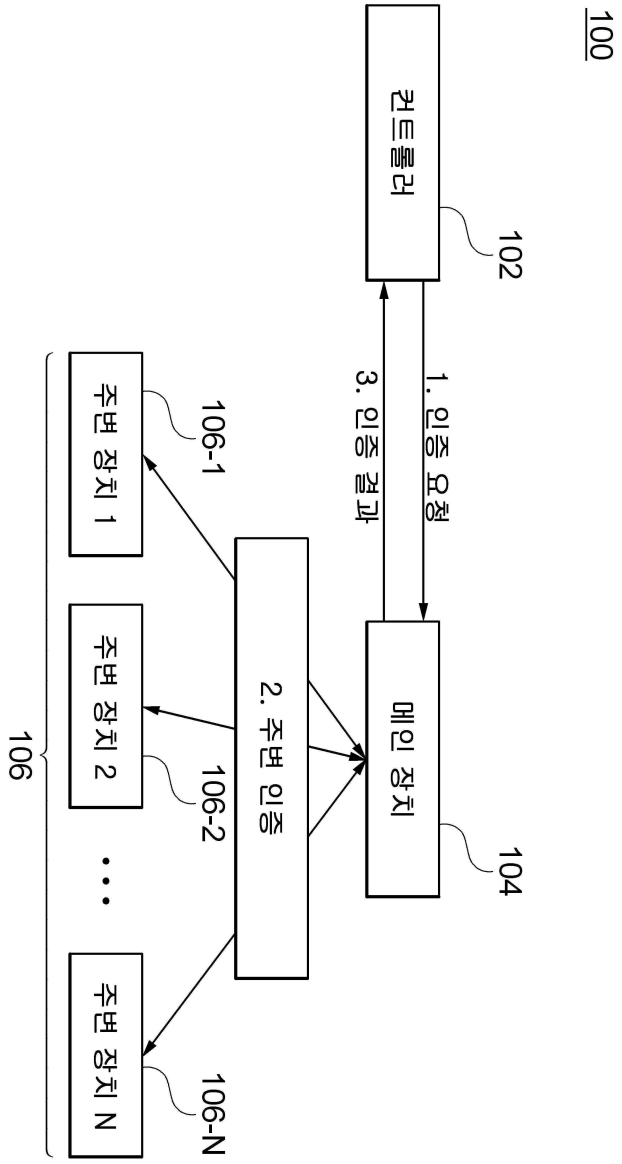
102: 컨트롤러

104: 메인 장치

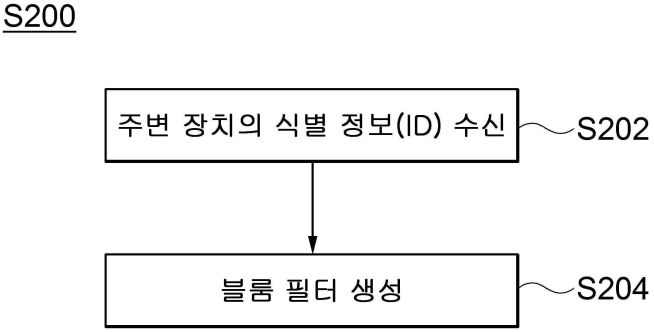
106: 주변 장치

도면

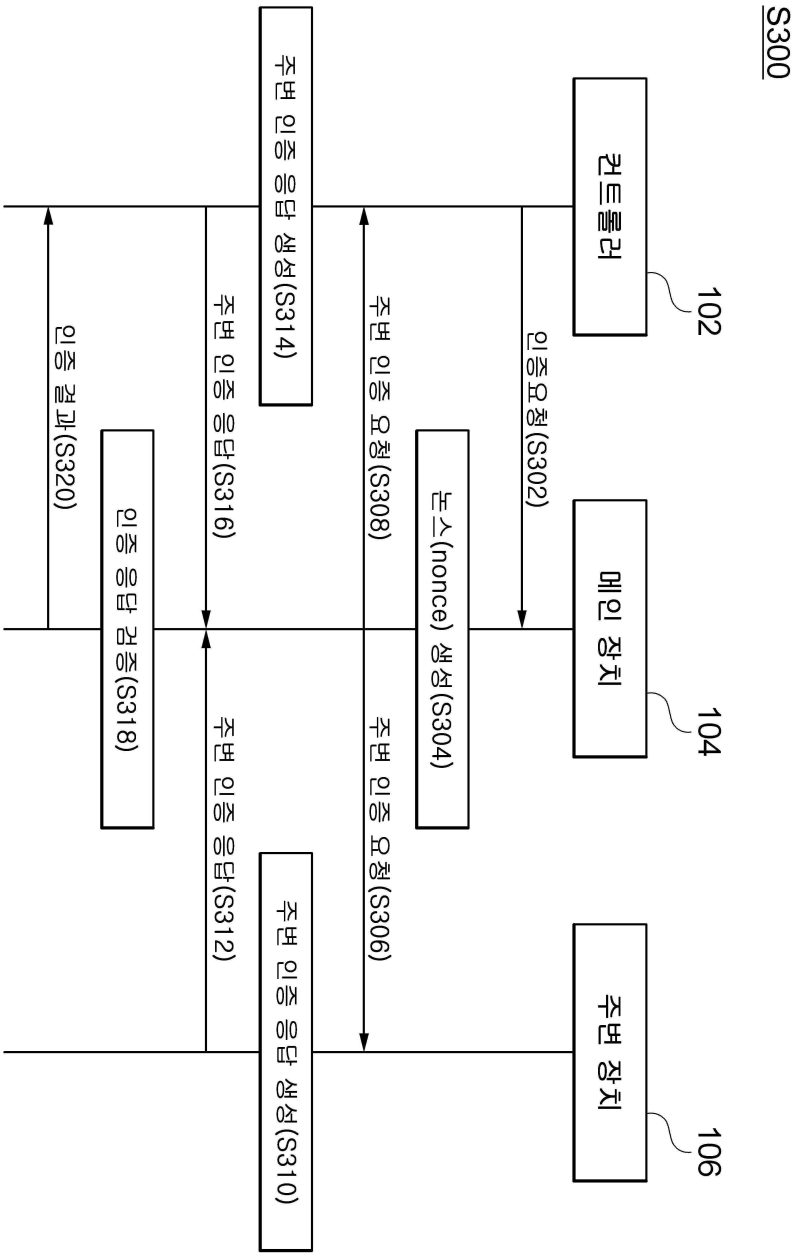
도면1


100
컨트롤러
102
1. 인증 요청
3. 인증 결과
메인 장치
104
2. 주변 인증
106
주변 장치 1
106-1
주변 장치 2
106-2
주변 장치 N
106-N

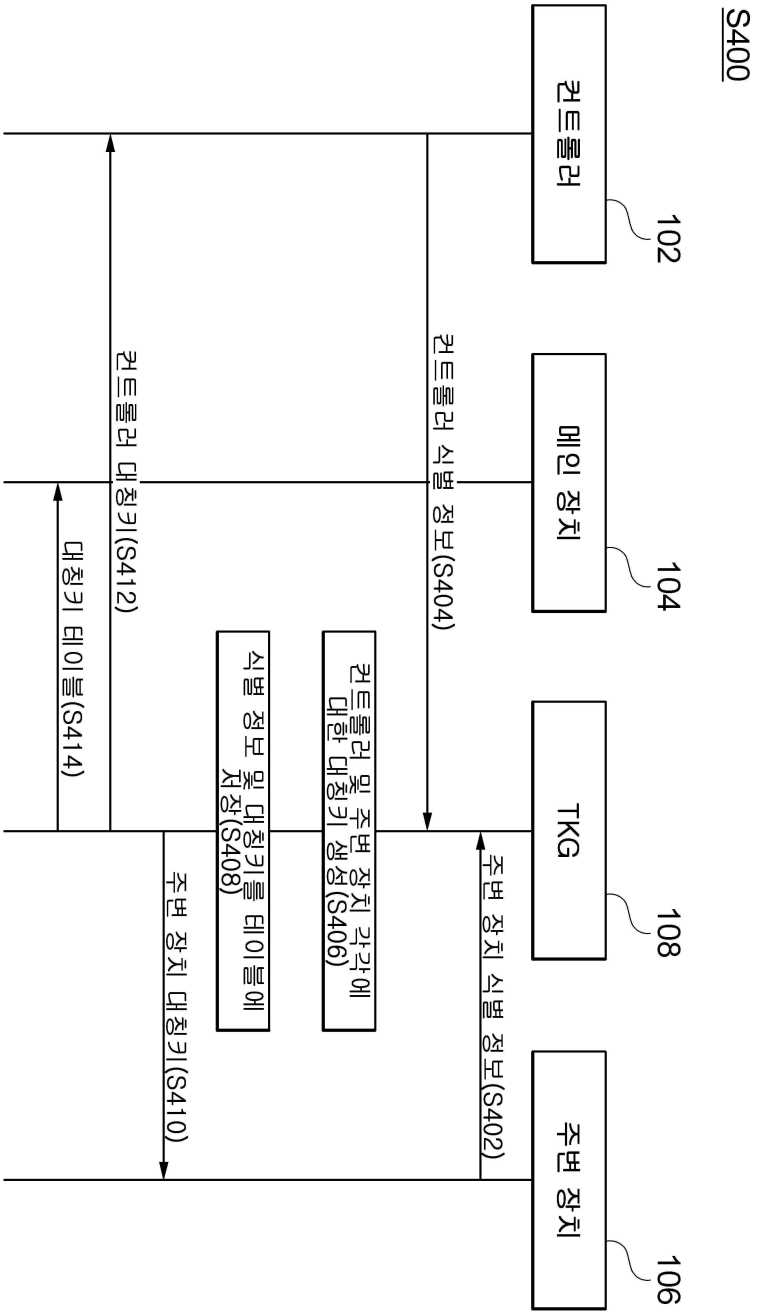
도면2


S200
주변 장치의 식별 정보(ID) 수신
S202
블룸 필터 생성
S204

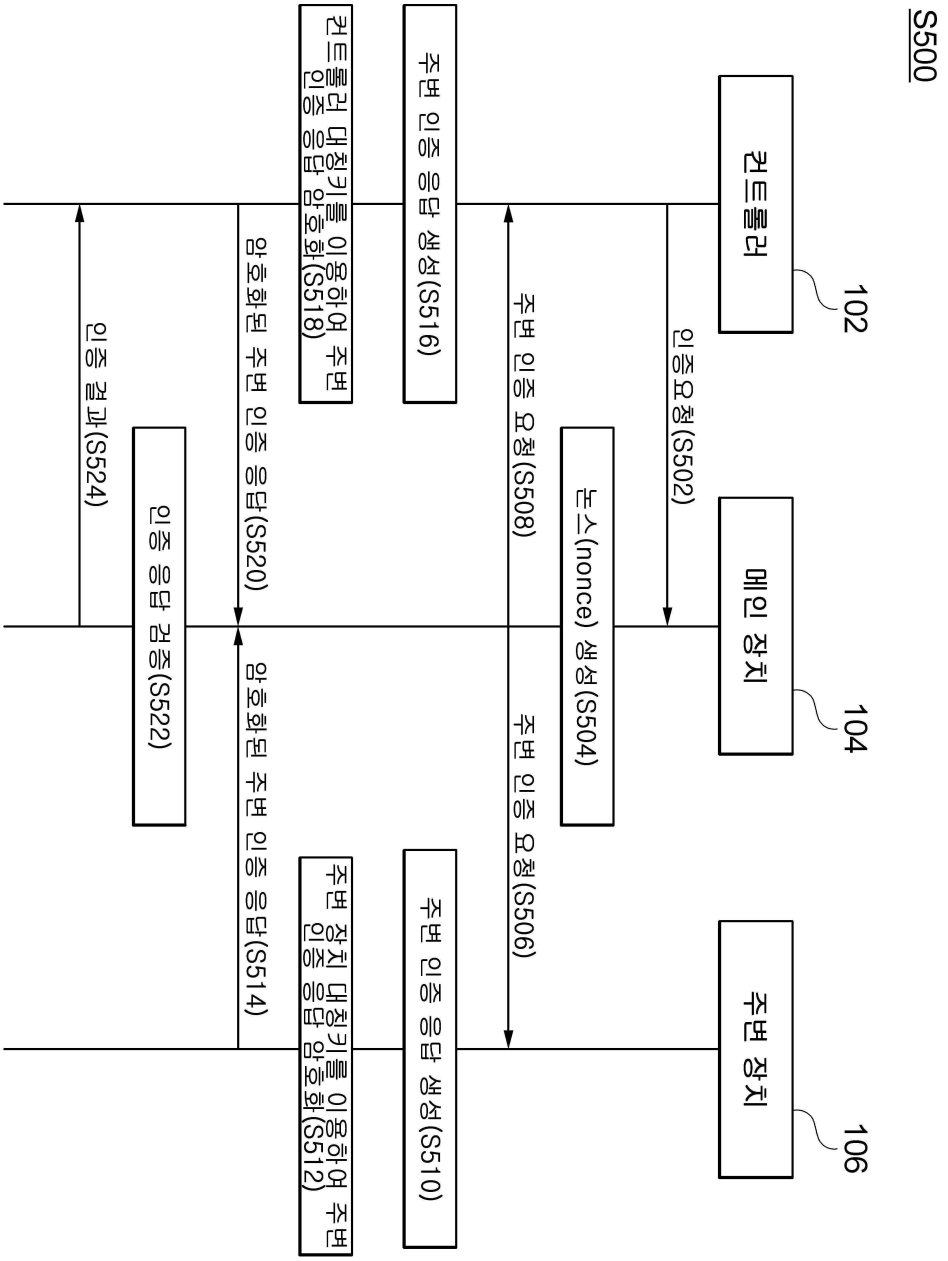
도면3


S300
컨트롤러
102
메인 장치
104
주변 장치
106
인증요청(S302)
논스(nonce) 생성(S304)
주변 인증 요청(S306)
주변 인증 응답 생성(S310)
주변 인증 응답(S312)
주변 인증 응답 생성(S314)
주변 인증 응답(S316)
인증 응답 검증(S318)
인증 결과(S320)

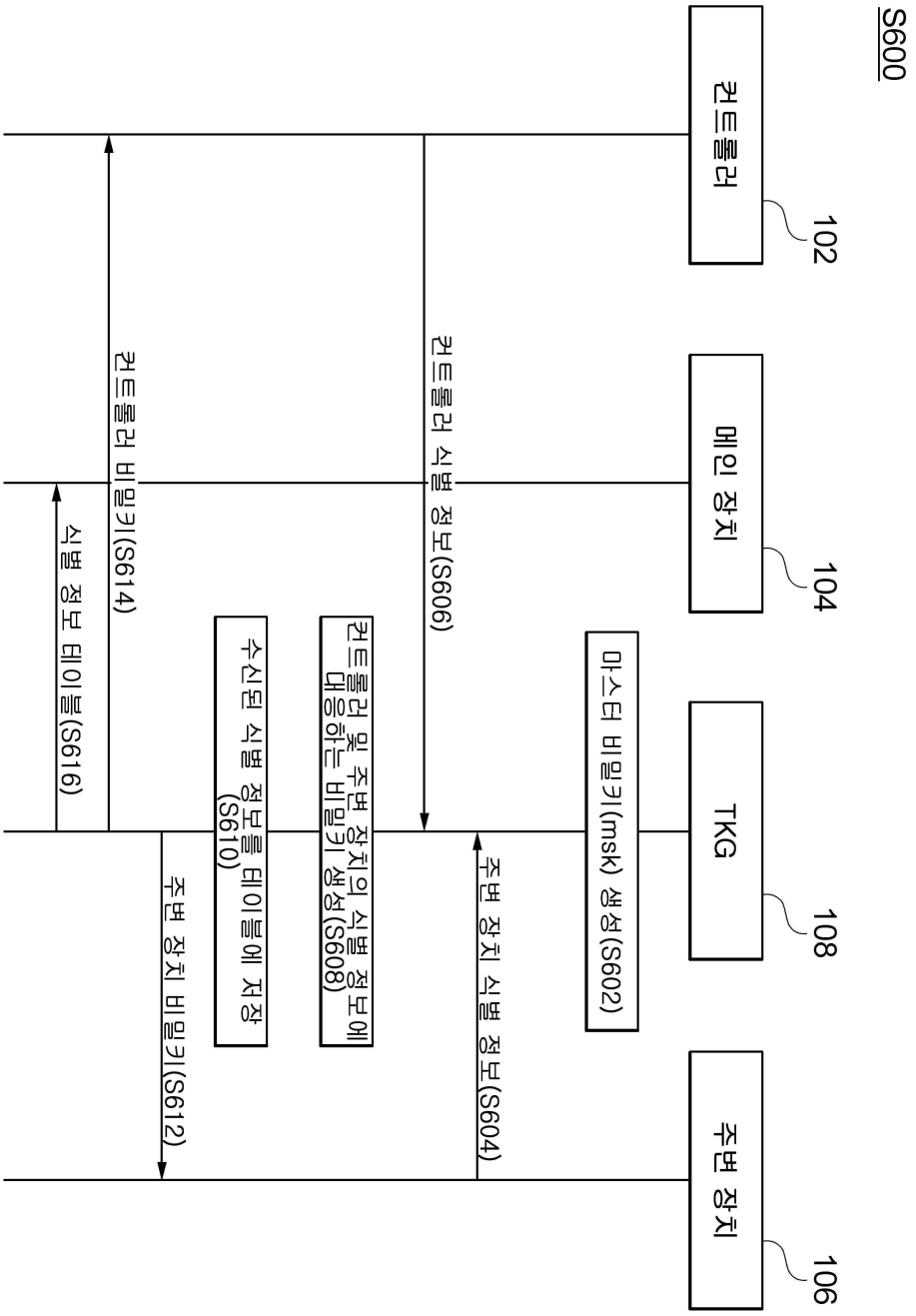
도면4


S400
컨트롤러
102
메인 장치
104
TKG
108
주변 장치
106
컨트롤러 식별 정보(S404)
주변 장치 식별 정보(S402)
컨트롤러 대칭키(S412)
대칭키 테이블(S414)
컨트롤러 및 주변 장치 각각에 대한 대칭키 생성(S406)
식별 정보 및 대칭키를 테이블에 저장(S408)
주변 장치 대칭키(S410)

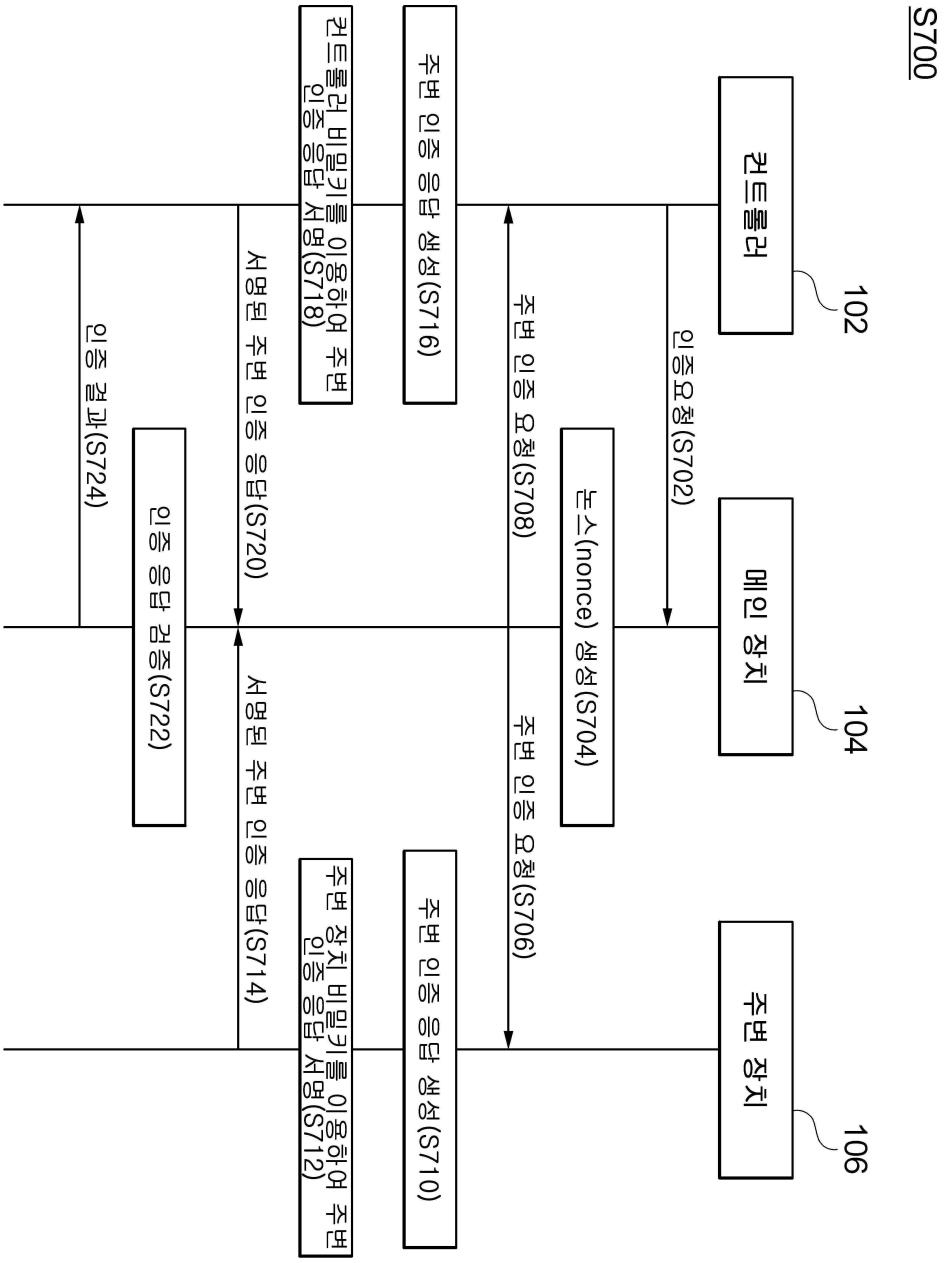
도면5


S500
컨트롤러
102
메인 장치
104
주변 장치
106
인증요청(S502)
논스(nonce) 생성(S504)
주변 인증 요청(S506)
주변 인증 응답 생성(S510)
주변 장치 대칭키를 이용하여 주변 인증 응답 암호화(S512)
암호화된 주변 인증 응답(S514)
주변 인증 요청(S508)
주변 인증 응답 생성(S516)
컨트롤러 대칭키를 이용하여 주변 인증 응답 암호화(S518)
암호화된 주변 인증 응답(S520)
인증 응답 검증(S522)
인증 결과(S524)

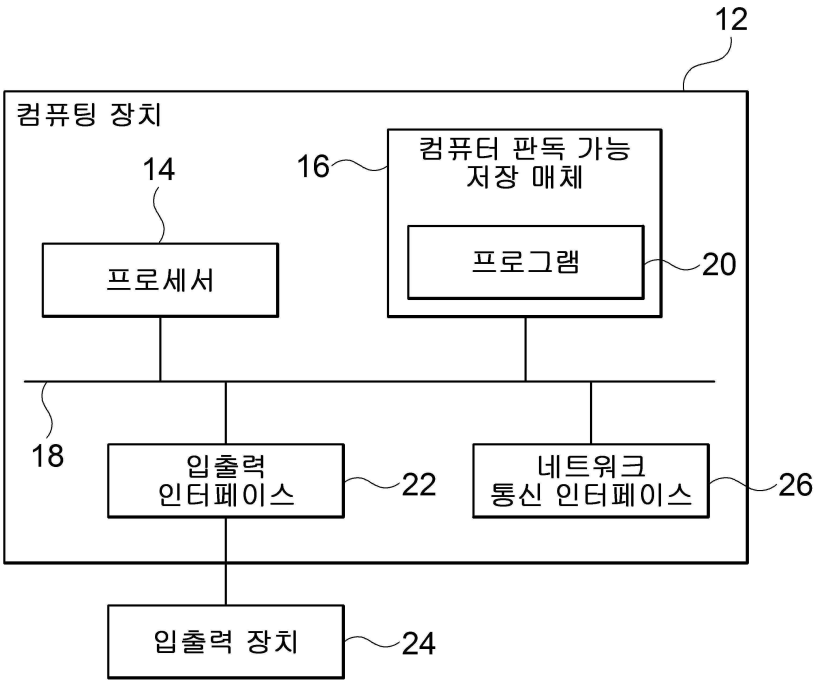
도면6


S600
컨트롤러
102
메인 장치
104
TKG
108
주변 장치
106
컨트롤러 비밀키(S614)
식별 정보 테이블(S616)
컨트롤러 식별 정보(S606)
주변 장치 비밀키(S612)
마스터 비밀키(msk) 생성(S602)
주변 장치 식별 정보(S604)
컨트롤러 및 주변 장치의 식별 정보에 대응하는 비밀키 생성(S608)
수신된 식별 정보를 테이블에 저장(S610)

도면7


S700
컨트롤러
102
메인 장치
104
주변 장치
106
인증요청(S702)
논스(nonce) 생성(S704)
주변 인증 요청(S706)
주변 인증 요청(S708)
주변 인증 응답 생성(S710)
주변 장치 비밀키를 이용하여 인증 응답 서명(S712)
서명된 주변 인증 응답(S714)
컨트롤러 비밀키를 이용하여 인증 응답 서명(S716)
서명된 주변 인증 응답(S718)
인증 응답 검증(S720)
인증 결과(S722)
인증 결과(S724)

도면8


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24