(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0098589
(43) 공개일자 2018년09월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/32 (2013.01)
H04L 63/0823 (2013.01)
(21) 출원번호 10-2018-7020968
(22) 출원일자(국제) 2016년12월08일
심사청구일자 없음
(85) 번역문제출일자 2018년07월20일
(86) 국제출원번호 PCT/EP2016/080161
(87) 국제공개번호 WO 2017/108412
국제공개일자 2017년06월29일
(30) 우선권주장
15201664.8 2015년12월21일
유럽특허청(EPO)(EP)

(71) 출원인
코닌클리케 필립스 엔.브이.
네덜란드, 아인트호벤 5656 에이이, 하이 테크 캠퍼스 5
(72) 발명자
베른센, 요하네스 아르놀뒤스 코르넬리스
네덜란드 5656 아에 아인드호펜 하이 테크 캠퍼스 5
(74) 대리인
장훈

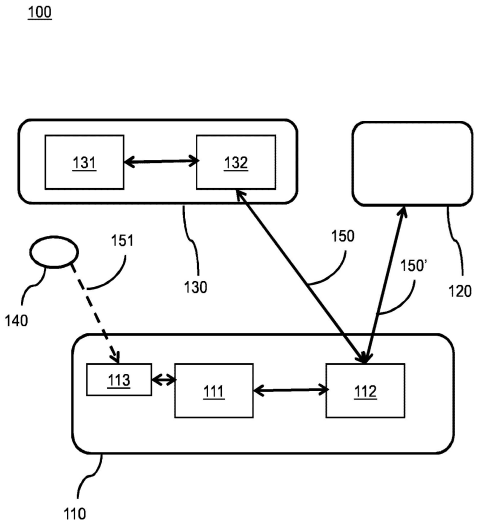
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **보안 통신을 위한 네트워크 시스템**

(57) 요 약

무선 통신을 위한 네트워크 시스템(100)에서, 피등록기(110)는 구성기(130)를 통해 네트워크에 액세스한다. 피등록기는 센서(113)에 의해 대역외 채널을 통해 네트워크 공개 키를 나타내는 데이터 패턴(140)을 획득한다. 피등록기는 네트워크 공개 키 및 제1 피등록기 비공개 키에 기초하여 제1 공유 키를 도출하고, 제1 공유 키를 사용하여 제2 피등록기 공개 키를 인코딩하고, 네트워크 액세스 요청을 생성한다. 구성기가 또한 제1 공유 키를 도출하고, 인코딩된 제2 피등록기 공개 키가 제1 공유 키에 의해 인코딩되었는지를 검증하고, 그렇다면, 보안 데이터를 생성하고 제2 공유 키를 사용하여 데이터를 암호화 방식으로 보호하고, 네트워크 액세스 메시지를 생성한다. 피등록기 프로세서가 또한 제2 공유 키를 도출하고, 데이터가 암호화 방식으로 보호되었는지를 검증하고, 그렇다면, 제2 피등록기 비공개 키 및 보안 데이터에 기초하여 보안 통신을 이행한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0825 (2013.01)
H04W 12/04 (2013.01)
H04W 12/06 (2013.01)
H04W 4/80 (2018.02)
H04W 84/12 (2013.01)

명 세 서

청구범위

청구항 1

영역 내의 네트워크 장치들 간의 무선 통신(150, 150')을 위해, 그리고 보안 프로토콜에 따른 보안 통신을 위해 배열된 네트워크 시스템에서 사용하기 위한 피등록기 장치(enrollee device)로서,

상기 네트워크 시스템은,

- 상기 네트워크에 액세스하기 위해 상기 보안 프로토콜에 따라 상기 피등록기 장치(110)로서 동작하도록 배열된 네트워크 장치, 및

- 상기 피등록기 장치에 의한 상기 네트워크에 대한 액세스를 가능하게 하기 위해 상기 보안 프로토콜에 따라 구성기 장치(130)로서 동작하도록 배열된 네트워크 장치를 포함하며,

상기 구성기 장치는,

상기 피등록기 장치로부터, 상기 보안 프로토콜에 따라 네트워크 액세스 요청을 수신하도록 배열된 구성기 통신 유닛(132)으로서, 상기 네트워크 액세스 요청은 인코딩된 제2 피등록기 공개 키 및 제1 피등록기 공개 키를 포함하는, 상기 구성기 통신 유닛(132), 및

상기 구성기 장치에 대해, 구성기 공개 키 및 대응하는 구성기 비공개 키를 갖고, 상기 네트워크 시스템에 대해, 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 갖도록 배열된 메모리를 포함하는 구성기 프로세서(131)를 포함하고,

상기 구성기 프로세서는,

- 상기 네트워크 비공개 키 및 상기 제1 피등록기 공개 키에 기초하여 제1 공유 키를 도출하고,

- 상기 제1 공유 키를 사용하여 상기 인코딩된 제2 피등록기 공개 키를 디코딩하고,

- 상기 인코딩된 제2 피등록기 공개 키가 상기 제1 공유 키에 의해 인코딩되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 공개 키 및 상기 구성기 비공개 키를 사용하여 보안 데이터를 생성하고,

- 상기 제1 피등록기 공개 키, 상기 제2 피등록기 공개 키 및 상기 네트워크 비공개 키에 기초하여 제2 공유 키를 도출하고,

- 상기 제2 공유 키를 사용하여, 상기 보안 데이터 및 상기 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호하고,

- 상기 보안 프로토콜에 따라, 상기 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나를 포함하는 네트워크 액세스 메시지를 생성하도록 배열되고,

상기 피등록기 장치는,

무선 통신을 위해 배열된 피등록기 무선 통신 유닛(112),

대역외 채널을 통해 데이터 패턴(140)을 획득하도록 배열된 피등록기 센서(113)로서, 상기 데이터 패턴은 상기 영역에서 제공되고 상기 네트워크 공개 키를 나타내는, 상기 피등록기 센서(113), 및

상기 제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키를 갖고, 상기 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 갖도록 배열된 메모리를 포함하는 피등록기 프로세서(111)를 포함하고,

상기 피등록기 프로세서(111)는,

- 상기 네트워크 공개 키 및 상기 제1 피등록기 비공개 키에 기초하여 상기 제1 공유 키를 도출하고,

- 상기 제1 공유 키를 사용하여 상기 제2 피등록기 공개 키를 인코딩하고,

- 상기 보안 프로토콜에 따라, 상기 인코딩된 제2 피등록기 공개 키 및 상기 제1 피등록기 공개 키를 포함하는

상기 네트워크 액세스 요청을 생성하고,

- 상기 피등록기 무선 통신 유닛을 통해 상기 네트워크 액세스 요청을 상기 구성기 장치로 전송하도록 배열되고,

상기 피등록기 프로세서는,

- 상기 피등록기 무선 통신 유닛을 통해 상기 구성기로부터 상기 네트워크 액세스 메시지를 수신하고,

- 상기 제1 피등록기 비공개 키, 상기 제2 피등록기 비공개 키 및 상기 네트워크 공개 키에 기초하여 상기 제2 공유 키를 도출하고,

- 상기 보호된 보안 데이터 및 상기 보호된 구성기 공개 키 중 적어도 하나가 상기 제2 공유 키에 의해 암호화 방식으로 보호되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 비공개 키 및 상기 보안 데이터에 기초하여 상기 보안 통신을 이행하도록 추가로 배열되는, 피등록기 장치.

청구항 2

제1항에 있어서,

- 상기 피등록기 프로세서(111)는 상기 제1 피등록기 공개 키 및 상기 대응하는 제1 피등록기 비공개 키를 구성하는, 임시 피등록기 공개 키 및 대응하는 임시 피등록기 비공개 키를 생성하도록 배열되고/되거나,

- 상기 피등록기 프로세서는 상기 제2 피등록기 공개 키 및 상기 대응하는 제2 피등록기 비공개 키를 구성하는, 추가의 임시 피등록기 공개 키 및 대응하는 추가의 임시 피등록기 비공개 키를 생성하도록 배열되는, 피등록기 장치.

청구항 3

제1항 또는 제2항에 있어서,

상기 구성기 프로세서(131)는,

- 구성기 세션 키를 제공하고 상기 구성기 세션 키를 상기 피등록기로 전송함으로써

상기 보안 데이터를 생성하도록 추가로 배열되고,

상기 피등록기 프로세서(111)는,

- 상기 구성기 세션 키를 수신하고,

- 상기 구성기 세션 키에 기초하여 상기 보안 통신을 이행하도록 추가로 배열되는, 피등록기 장치.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 구성기 프로세서(131)는,

- 구성기 세션 공개 키 및 대응하는 구성기 세션 비공개 키를 생성하고,

- 상기 구성기 세션 비공개 키 및 상기 제2 피등록기 공개 키에 기초하여 제3 공유 키를 도출하고,

- 상기 구성기 세션 공개 키를 상기 피등록기로 전송하도록 추가로 배열되고,

상기 피등록기 프로세서(111)는,

- 상기 구성기 세션 공개 키를 수신하고,

- 상기 제2 피등록기 비공개 키 및 상기 구성기 세션 공개 키에 기초하여 상기 제3 공유 키를 도출하고,

- 상기 제3 공유 키에 기초하여 보안 통신을 이행하도록 추가로 배열되는, 피등록기 장치.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 네트워크 시스템은,

- 상기 제2 피등록기 공개 키 및 상기 보안 데이터를 수신하고,

- 세션 네트워크 공개 키 및 대응하는 세션 네트워크 비공개 키를 제공하고,

- 상기 세션 네트워크 비공개 키 및 상기 제2 피등록기 공개 키에 기초하여 제5 공유 키를 도출하고, 상기 세션 네트워크 공개 키를 상기 피등록기로 전송하도록

배열된 추가의 네트워크 장치(120)를 포함하고,

상기 피등록기 프로세서(111)는,

- 상기 세션 네트워크 공개 키를 수신하고,

- 상기 제2 피등록기 비공개 키 및 상기 세션 네트워크 공개 키에 기초하여 상기 제5 공유 키를 도출하고,

- 상기 제5 공유 키에 기초하여 상기 추가의 네트워크 장치와의 보안 통신을 이행하도록 추가로 배열되는, 피등록기 장치.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 구성기 프로세서(131)는,

- 상기 구성기 비공개 키로 상기 제2 피등록기 공개 키에 디지털 서명함으로써 디지털 서명을 포함하는 상기 보안 데이터를 생성하고,

- 상기 피등록기와 제3 장치 간의 보안 통신을 가능하게 하기 위해 상기 디지털 서명을 상기 제3 장치 및/또는 상기 피등록기로 전송하도록 추가로 배열되고,

상기 피등록기 프로세서(111)는,

- 상기 디지털 서명을 수신하고,

- 상기 디지털 서명 및 상기 구성기 공개 키에 기초하여, 상기 제2 피등록기 공개 키가 올바르게 서명되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 비공개 키에 기초하여 상기 보안 통신을 이행하도록 추가로 배열되는, 피등록기 장치.

청구항 7

제6항에 있어서,

상기 네트워크 시스템은,

- 상기 구성기 공개 키를 획득하고,

- 상기 디지털 서명 및 상기 제2 피등록기 공개 키를 수신하고,

- 상기 디지털 서명 및 상기 구성기 공개 키에 기초하여, 상기 제2 피등록기 공개 키가 올바르게 서명되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 공개 키에 기초하여 상기 피등록기 장치와의 상기 보안 통신을 이행하도록

배열된 추가의 네트워크 장치(120)를 포함하는, 피등록기 장치.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 구성기 프로세서(131)는, 상기 구성기 비공개 키로, 추가의 네트워크 장치의 추가의 공개 키에 디지털 서명함으로써 추가의 디지털 서명을 포함하는 추가의 보안 데이터를 생성하도록 추가로 배열되고,

상기 피등록기 프로세서(111)는,

- 상기 추가의 공개 키 및 상기 추가의 디지털 서명을 수신하고,

- 상기 추가의 디지털 서명 및 상기 구성기 공개 키에 기초하여, 상기 추가의 공개 키가 올바르게 서명되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 비공개 키 및 상기 추가의 공개 키를 사용하여 상기 추가의 네트워크 장치와 보안 통신함으로써

상기 추가의 보안 데이터를 사용하도록 추가로 배열되는, 피등록기 장치.

청구항 9

제1항 내지 제8항 중 어느 한 항에 있어서,

상기 구성기 프로세서(131)는,

- 인코딩된 피등록기 테스트 데이터를 상기 제2 공유 키를 사용하여 디코딩하고,

- 상기 피등록기 테스트 데이터가 상기 피등록기에서 상기 제2 공유 키에 의해 인코딩되었는지를 검증하도록 추가로 배열되고,

상기 피등록기 프로세서(111)는,

- 상기 피등록기 테스트 데이터를 생성하고,

- 상기 제2 공유 키를 사용하여 상기 피등록기 테스트 데이터를 인코딩하고,

- 상기 인코딩된 피등록기 테스트 데이터를 상기 구성기로 전송하도록 추가로 배열되는, 피등록기 장치.

청구항 10

제1항 내지 제9항 중 어느 한 항에 있어서,

상기 구성기 프로세서(131)는,

- 구성기 테스트 데이터를 생성하고,

- 상기 제2 공유 키를 사용하여 상기 구성기 테스트 데이터를 인코딩하고,

- 상기 인코딩된 구성기 테스트 데이터를 상기 피등록기로 전송하도록 추가로 배열되고,

상기 피등록기 프로세서(111)는,

- 상기 제2 공유 키를 사용하여 상기 인코딩된 구성기 테스트 데이터를 디코딩하고,

- 상기 구성기 테스트 데이터가 상기 구성기에서 상기 제2 공유 키에 의해 인코딩되었는지를 검증하도록 추가로 배열되는, 피등록기 장치.

청구항 11

영역 내의 네트워크 장치들 간의 무선 통신(150, 150')을 위해, 그리고 보안 프로토콜에 따른 보안 통신을 위해 배열된 네트워크 시스템에서 사용하기 위한 피등록기 방법으로서,

상기 네트워크 시스템은,

- 상기 네트워크에 액세스하기 위해 상기 보안 프로토콜에 따라 피등록기 장치(110)로서 동작하도록 상기 피등록기 방법을 실행하는 네트워크 장치, 및

- 상기 피등록기 장치에 의한 상기 네트워크에 대한 액세스를 가능하게 하기 위해 상기 보안 프로토콜에 따라 구성기 장치(130)로서 동작하도록 배열된 네트워크 장치를 포함하고,

상기 구성기 장치는,

상기 피등록기 장치로부터, 상기 보안 프로토콜에 따라 네트워크 액세스 요청을 수신하도록 배열된 구성기 통신 유닛(132)으로서, 상기 네트워크 액세스 요청은 인코딩된 제2 피등록기 공개 키 및 제1 피등록기 공개 키를 포

함하는, 상기 구성기 통신 유닛(132), 및

상기 구성기 장치에 대해, 구성기 공개 키 및 대응하는 구성기 비공개 키를 갖고, 상기 네트워크 시스템에 대해, 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 갖도록 배열된 메모리를 포함하는 구성기 프로세서(131)를 포함하고,

상기 구성기 프로세서는,

- 상기 네트워크 비공개 키 및 상기 제1 피등록기 공개 키에 기초하여 제1 공유 키를 도출하고,

- 상기 제1 공유 키를 사용하여 상기 인코딩된 제2 피등록기 공개 키를 디코딩하고,

- 상기 인코딩된 제2 피등록기 공개 키가 상기 제1 공유 키에 의해 인코딩되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 공개 키 및 상기 구성기 비공개 키를 사용하여 보안 데이터를 생성하고,

- 상기 제1 피등록기 공개 키, 상기 제2 피등록기 공개 키 및 상기 네트워크 비공개 키에 기초하여 제2 공유 키를 도출하고,

- 상기 제2 공유 키를 사용하여, 상기 보안 데이터 및 상기 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호하고,

- 상기 보안 프로토콜에 따라, 상기 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나를 포함하는 네트워크 액세스 메시지를 생성하도록 배열되고,

상기 피등록기 방법은,

- 상기 제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키와, 상기 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 저장하는 단계,

- 대역외 채널을 통해 데이터 패턴(140)을 획득하는 단계로서, 상기 데이터 패턴은 상기 영역에서 제공되고 상기 네트워크 공개 키를 나타내는, 상기 데이터 패턴(140) 획득 단계,

- 상기 네트워크 공개 키 및 상기 제1 피등록기 비공개 키에 기초하여 상기 제1 공유 키를 도출하는 단계,

- 상기 제1 공유 키를 사용하여 상기 제2 피등록기 공개 키를 인코딩하는 단계,

- 상기 보안 프로토콜에 따라 상기 네트워크 액세스 요청을 생성하는 단계로서, 상기 네트워크 액세스 요청은 상기 인코딩된 제2 피등록기 공개 키 및 상기 제1 피등록기 공개 키를 포함하는, 상기 네트워크 액세스 요청 생성 단계, 및

- 상기 피등록기 무선 통신 유닛을 통해 상기 네트워크 액세스 요청을 상기 구성기 장치로 전송하는 단계를 포함하고,

상기 피등록기 방법은,

- 상기 구성기로부터 상기 네트워크 액세스 메시지를 수신하는 단계,

- 상기 제1 피등록기 비공개 키, 상기 제2 피등록기 비공개 키 및 상기 네트워크 공개 키에 기초하여 상기 제2 공유 키를 도출하는 단계,

- 상기 보호된 보안 데이터 및 상기 보호된 구성기 공개 키 중 적어도 하나가 상기 제2 공유 키에 의해 암호화 방식으로 보호되었는지를 검증하는 단계, 및, 그렇다면,

- 상기 제2 피등록기 비공개 키 및 상기 보안 데이터에 기초하여 상기 보안 통신을 이행하는 단계를 추가로 포함하는, 피등록기 방법.

청구항 12

영역 내의 네트워크 장치들 간의 무선 통신(150, 150')을 위해, 그리고 보안 프로토콜에 따른 보안 통신을 위해 배열된 네트워크 시스템에서 사용하기 위한 구성기 방법으로서,

상기 네트워크 시스템은,

- 상기 네트워크에 액세스하기 위해 상기 보안 프로토콜에 따라 피등록기 장치(110)로서 동작하도록 배열된 네

트워크 장치, 및

- 상기 피등록기 장치에 의한 상기 네트워크에 대한 액세스를 가능하게 하기 위해 상기 보안 프로토콜에 따라 구성기 장치(130)로서 동작하도록 상기 구성기 방법을 실행하는 네트워크 장치를 포함하고,

상기 피등록기 장치는,

무선 통신을 위해 배열된 피등록기 무선 통신 유닛(112),

대역외 채널을 통해 데이터 패턴(140)을 획득하도록 배열된 피등록기 센서(113)로서, 상기 데이터 패턴은 상기 영역에서 제공되고 네트워크 공개 키를 나타내는, 상기 피등록기 센서(113), 및

제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키를 갖고, 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 갖도록 배열된 메모리를 포함하는 피등록기 프로세서(111)를 포함하고,

상기 피등록기 프로세서(111)는,

- 상기 네트워크 공개 키 및 상기 제1 피등록기 비공개 키에 기초하여 제1 공유 키를 도출하고,

- 상기 제1 공유 키를 사용하여 상기 제2 피등록기 공개 키를 인코딩하고,

- 상기 보안 프로토콜에 따라, 상기 인코딩된 제2 피등록기 공개 키 및 상기 제1 피등록기 공개 키를 포함하는 네트워크 액세스 요청을 생성하고,

- 상기 피등록기 무선 통신 유닛을 통해 상기 네트워크 액세스 요청을 상기 구성기 장치로 전송하도록 배열되고,

상기 피등록기 프로세서는,

- 상기 피등록기 무선 통신 유닛을 통해 상기 구성기로부터, 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나를 포함하는 네트워크 액세스 메시지를 수신하고,

- 상기 제1 피등록기 비공개 키, 상기 제2 피등록기 비공개 키 및 상기 네트워크 공개 키에 기초하여 제2 공유 키를 도출하고,

- 상기 보호된 보안 데이터 및 상기 보호된 구성기 공개 키 중 적어도 하나가 상기 제2 공유 키에 의해 암호화 방식으로 보호되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 비공개 키 및 상기 보안 데이터에 기초하여 상기 보안 통신을 이행하도록 추가로 배열되고,

상기 구성기 방법은,

- 상기 구성기 장치에 대해, 상기 구성기 공개 키 및 대응하는 구성기 비공개 키를, 그리고, 상기 네트워크 시스템에 대해, 상기 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 저장하는 단계,

- 상기 피등록기 장치로부터, 상기 보안 프로토콜에 따라 상기 네트워크 액세스 요청을 수신하는 단계로서, 상기 네트워크 액세스 요청은 상기 인코딩된 제2 피등록기 공개 키 및 상기 제1 피등록기 공개 키를 포함하는, 상기 네트워크 액세스 요청 수신 단계,

- 상기 네트워크 비공개 키 및 상기 제1 피등록기 공개 키에 기초하여 상기 제1 공유 키를 도출하는 단계,

- 상기 제1 공유 키를 사용하여 상기 인코딩된 제2 피등록기 공개 키를 디코딩하는 단계,

- 상기 인코딩된 제2 피등록기 공개 키가 상기 제1 공유 키에 의해 인코딩되었는지를 검증하는 단계, 및, 그렇다면,

- 상기 제2 피등록기 공개 키 및 상기 구성기 비공개 키를 사용하여 상기 보안 데이터를 생성하는 단계,

- 상기 제1 피등록기 공개 키, 상기 제2 피등록기 공개 키 및 상기 네트워크 비공개 키에 기초하여 상기 제2 공유 키를 도출하는 단계,

- 상기 제2 공유 키를 사용하여, 상기 보안 데이터 및 상기 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호하는 단계, 및

- 상기 보안 프로토콜에 따라 상기 네트워크 액세스 메시지를 생성하는 단계를 포함하는, 구성기 방법.

청구항 13

영역 내의 네트워크 장치들 간의 무선 통신(150, 150')을 위해, 그리고 보안 프로토콜에 따른 보안 통신을 위해 배열된 네트워크 시스템에서 사용하기 위한 구성기 장치로서,

상기 네트워크 시스템은,

- 상기 네트워크에 액세스하기 위해 상기 보안 프로토콜에 따라 피등록기 장치(110)로서 동작하도록 배열된 네트워크 장치, 및

- 상기 피등록기 장치에 의한 상기 네트워크에 대한 액세스를 가능하게 하기 위해 상기 보안 프로토콜에 따라 상기 구성기 장치(130)로서 동작하도록 배열된 네트워크 장치를 포함하고,

상기 피등록기 장치는,

무선 통신을 위해 배열된 피등록기 무선 통신 유닛(112),

대역외 채널을 통해 데이터 패턴(140)을 획득하도록 배열된 피등록기 센서(113)로서, 상기 데이터 패턴은 상기 영역에서 제공되고 네트워크 공개 키를 나타내는, 상기 피등록기 센서(113), 및

제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키를 갖고, 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 갖도록 배열된 메모리를 포함하는 피등록기 프로세서(111)를 포함하고,

상기 피등록기 프로세서(111)는,

- 상기 네트워크 공개 키 및 상기 제1 피등록기 비공개 키에 기초하여 제1 공유 키를 도출하고,

- 상기 제1 공유 키를 사용하여 상기 제2 피등록기 공개 키를 인코딩하고,

- 상기 보안 프로토콜에 따라, 상기 인코딩된 제2 피등록기 공개 키 및 상기 제1 피등록기 공개 키를 포함하는 네트워크 액세스 요청을 생성하고,

- 상기 피등록기 무선 통신 유닛을 통해 상기 네트워크 액세스 요청을 상기 구성기 장치로 전송하도록 배열되고,

상기 피등록기 프로세서는,

- 상기 피등록기 무선 통신 유닛을 통해 상기 구성기로부터, 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나를 포함하는 네트워크 액세스 메시지를 수신하고,

- 상기 제1 피등록기 비공개 키, 상기 제2 피등록기 비공개 키 및 상기 네트워크 공개 키에 기초하여 제2 공유 키를 도출하고,

- 상기 보호된 보안 데이터 및 상기 보호된 구성기 공개 키 중 적어도 하나가 상기 제2 공유 키에 의해 암호화 방식으로 보호되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 비공개 키 및 상기 보안 데이터에 기초하여 상기 보안 통신을 이행하도록 추가로 배열되고,

상기 구성기 장치는,

상기 피등록기 장치로부터, 상기 보안 프로토콜에 따라 상기 네트워크 액세스 요청을 수신하도록 배열된 구성기 통신 유닛(132)으로서, 상기 네트워크 액세스 요청은 상기 인코딩된 제2 피등록기 공개 키 및 상기 제1 피등록기 공개 키를 포함하는, 상기 구성기 통신 유닛(132), 및

상기 구성기 장치에 대해, 상기 구성기 공개 키 및 대응하는 구성기 비공개 키를 갖고, 상기 네트워크 시스템에 대해, 상기 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 갖도록 배열된 메모리를 포함하는 구성기 프로세서(131)를 포함하고,

상기 구성기 프로세서는,

- 상기 네트워크 비공개 키 및 상기 제1 피등록기 공개 키에 기초하여 상기 제1 공유 키를 도출하고,

- 상기 제1 공유 키를 사용하여 상기 인코딩된 제2 피등록기 공개 키를 디코딩하고,

- 상기 인코딩된 제2 피등록기 공개 키가 상기 제1 공유 키에 의해 인코딩되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 공개 키 및 상기 구성기 비공개 키를 사용하여 상기 보안 데이터를 생성하고,

- 상기 제1 피등록기 공개 키, 상기 제2 피등록기 공개 키 및 상기 네트워크 비공개 키에 기초하여 상기 제2 공유 키를 도출하고,

- 상기 제2 공유 키를 사용하여, 상기 보안 데이터 및 상기 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호하고,

- 상기 보안 프로토콜에 따라 상기 네트워크 액세스 메시지를 생성하도록 배열되는, 구성기 장치.

청구항 14

제13항에 있어서, 상기 구성기 프로세서(131)는 상기 네트워크 공개 키 및 상기 대응하는 네트워크 비공개 키를 구성하는, 임시 네트워크 공개 키 및 대응하는 임시 네트워크 비공개 키를 생성하도록 배열되는, 구성기 장치.

청구항 15

제13항 또는 제14항에 있어서,

상기 피등록기 프로세서(111)는,

- 구성기 세션 공개 키를 수신하고,

- 상기 제2 피등록기 비공개 키 및 상기 구성기 세션 공개 키에 기초하여 제3 공유 키를 도출하고,

- 상기 제3 공유 키에 기초하여 보안 통신을 이행하도록 추가로 배열되고,

상기 구성기 프로세서(131)는,

- 상기 구성기 세션 공개 키 및 대응하는 구성기 세션 비공개 키를 생성하고,

- 상기 구성기 세션 비공개 키 및 상기 제2 피등록기 공개 키에 기초하여 상기 제3 공유 키를 도출하고,

- 상기 구성기 세션 공개 키를 상기 피등록기로 전송하도록 추가로 배열되는, 구성기 장치.

청구항 16

제13항 내지 제15항 중 어느 한 항에 있어서, 상기 구성기 프로세서(131)는,

- 상기 구성기 비공개 키로 상기 제2 피등록기 공개 키에 디지털 서명함으로써 디지털 서명을 포함하는 상기 보안 데이터를 생성하고,

- 상기 피등록기와 제3 장치 간의 보안 통신을 가능하게 하기 위해 상기 디지털 서명을 상기 제3 장치 및/또는 상기 피등록기로 전송하도록 추가로 배열되는, 피등록기 장치.

청구항 17

제13항 내지 제16항 중 어느 한 항에 있어서,

상기 피등록기 프로세서(111)는,

- 추가의 공개 키 및 추가의 디지털 서명을 수신하고,

- 상기 추가의 디지털 서명 및 상기 구성기 공개 키에 기초하여, 상기 추가의 공개 키가 올바르게 서명되었는지를 검증하고, 그렇다면,

- 상기 제2 피등록기 비공개 키 및 상기 추가의 공개 키를 사용하여 추가의 네트워크 장치와 보안 통신함으로써

추가의 보안 데이터를 사용하도록 추가로 배열되고,

상기 구성기 프로세서(131)는, 상기 구성기 비공개 키로, 상기 추가의 네트워크 장치의 상기 추가의 공개 키에 디지털 서명함으로써 상기 추가의 디지털 서명을 포함하는 상기 추가의 보안 데이터를 생성하도록 추가로 배열

되는, 구성기 장치.

청구항 18

제13항 내지 제17항 중 어느 한 항에 있어서,

상기 피등록기 프로세서(111)는,

- 피등록기 테스트 데이터를 생성하고,

- 상기 제2 공유 키를 사용하여 상기 피등록기 테스트 데이터를 인코딩하고,

- 상기 인코딩된 피등록기 테스트 데이터를 상기 구성기로 전송하도록 추가로 배열되고,

상기 구성기 프로세서(131)는,

- 상기 제2 공유 키를 사용하여 상기 인코딩된 피등록기 테스트 데이터를 디코딩하고,

- 상기 피등록기 테스트 데이터가 상기 피등록기에서 상기 제2 공유 키에 의해 인코딩되었는지를 검증하도록 추가로 배열되는, 구성기 장치.

청구항 19

제13항 내지 제18항 중 어느 한 항에 있어서,

상기 피등록기 프로세서(111)는,

- 인코딩된 구성기 테스트 데이터를 상기 제2 공유 키를 사용하여 디코딩하고,

- 상기 구성기 테스트 데이터가 상기 구성기에서 상기 제2 공유 키에 의해 인코딩되었는지를 검증하도록 추가로 배열되고,

상기 구성기 프로세서(131)는,

- 상기 구성기 테스트 데이터를 생성하고,

- 상기 제2 공유 키를 사용하여 상기 구성기 테스트 데이터를 인코딩하고,

- 상기 인코딩된 구성기 테스트 데이터를 상기 피등록기로 전송하도록 추가로 배열되는, 구성기 장치.

청구항 20

네트워크로부터 다운로드 가능하고/하거나 컴퓨터 판독 가능 매체 및/또는 마이크로프로세서 실행 가능 매체에 저장된 컴퓨터 프로그램 제품으로서, 상기 제품은 컴퓨터 상에서 실행될 때 제11항 또는 제12항에 따른 방법을 구현하기 위한 프로그램 코드 명령어들을 포함하는, 컴퓨터 프로그램 제품.

발명의 설명

기 술 분 야

[0001] 본 발명은 영역 내의 네트워크 장치들 사이의 무선 통신을 위한 네트워크 시스템에 관한 것이며, 네트워크 시스템은 보안 프로토콜에 따른 보안 통신을 위해 배열된다.

[0002] 본 발명은 일반적으로 현장 무선 네트워킹(예를 들어, 와이파이), 특히 무선 네트워크들을 보안 방식으로 구성하는 것에 관한 것이다.

배 경 기 술

[0003] 지난 수십 년 동안, 많은 위치에 무선 네트워크들이 제공되었다. 네트워크의 사용, 네트워크에 대한 액세스 또는 네트워크 상의 데이터 트래픽을 위해 어느 정도의 보안을 제공하는 것은 일반적인 요건이다. 네트워크를 사용하기를 원하는 새로운 장치, 즉 무선 네트워크에 가입하고자 장치는 일반적으로 피등록기(enrollee)로 지칭된다. 피등록기는 몇몇 증명서들을 가져야 하는 반면, 네트워크는 네트워크 액세스를 계속 추적해야 한다. 그러한 기능은 소위 등록기(registrar) 또는 구성기, 즉 네트워크에 대한 액세스를 발행 및 취소할 수 있는 권한을 갖는 장치에 의해 수행될 수 있으며, 이러한 장치는 무선 액세스 포인트(AP)에 통합되거나 별개의 장치로서 제

공될 수 있다. 액세스 포인트는 등록기와 피등록기 사이에서 프록시로서 기능할 수 있다.

[0004] 그러나, 그러한 증명서들이 무선 통신을 통해 교환되는 경우, 메시지들을 수신하는 제삼자들도 증명서들에 액세스할 수 있으며, 액세스 권리들을 조작하고/하거나, 피등록기의 개인 정보 및 네트워크와 피등록기 사이에서 교환되는 추가의 데이터에 대한 원치 않는 액세스를 획득하는 것이 가능할 수 있다. 예를 들어, 레스토랑 및 카페와 같은 공공 장소들은 그러한 네트워크들을 운영할 수 있다.

[0005] 그러한 다소 개방된 네트워크들에 대한 보안 액세스를 획득하기 위해, 네트워크에 대한 액세스를 획득하기 위한 식별자 및/또는 증명서들의 교환에 대한 다양한 옵션들이 제안되었다. 그러한 증명서들은 예를 들어, 네트워크에 대해 선택되고 일반적으로는 비밀로 유지되지만 피등록기의 사용자에게는 공개되어 피등록기에 입력되는 패스프레이즈를 포함할 수 있다. 그러한 패스프레이즈는 피등록기와 네트워크 사이의 공유 키를 생성하는 데 사용될 수 있다. 더 진보된 보안 시스템들은 RSA 공개 키 시스템과 같은, 일반적으로 공개 키 및 비공개 키로 지칭되는 키 데이터의 쌍 세트들의 잘 알려진 시스템을 사용할 수 있다. RSA 공개 키 시스템은 보안 데이터 전송에 널리 사용된다. 그러한 암호 시스템에서, 암호화 키는 공개적이며, 비밀로 유지되는 해독 키와는 상이하다. RSA에서, 이러한 비대칭은 2개의 큰 소수의 곱의 인수 분해의 실질적인 어려움, 즉 인수 분해 문제에 기초한다. RSA는 1977년에 알고리즘을 처음 공개적으로 설명한 리베스트 론(Ron Rivest), 샤미르 아디(Adi Shamir) 및 아델먼 레오나드(Leonard Adleman)의 성의 머리글자들로 이루어진다. RSA의 사용자는, 보조 값과 함께, 2개의 큰 소수에 기초하여 공개 키를 생성한 후에 공개한다. 소수들은 비밀로 유지되어야 한다. 누구나 공개 키를 사용하여 메시지를 암호화할 수 있지만, 현재 공개된 방법들을 이용하는 경우, 공개 키가 충분히 크다면, 소수들을 알고 있는 누군가만이 메시지를 실행 가능하게 해독할 수 있다. 따라서, 공개 키는 보안 장치와의 보안 통신을 원하는 누구에게나 공개될 수 있는 반면, 대응하는 비공개 키는 보안 장치에만 알려진다. 디피-헬먼(Diffie-Hellman) 키 교환(DH)이 또한 공개/비공개 타원 곡선 암호화(ECC, Elliptic Curve Cryptography) 키 쌍들에 기초할 수 있고 여러 키 쌍들에. 공유 비밀은 $(PubKey_1 + PubKey_2 + ... + PubKey_N) * (PrivKey_{N+1} + ... + PrivKey_{N+M})$으로서 계산될 수 있으며, 이는 $(PubKey_{N+1} + PubKey_{N+2} + ... + PubKey_{N+M}) * (PrivKey_1 + ... + PrivKey_N)$과 동일하고, 덧셈들 및 곱셈들은 통상적인 대수적 덧셈들 및 곱셈들이 아니라, 타원 곡선 상의 점들에 대해 수행되고, 하나의 장치가 $\{PrivKey_{1,...,} PrivKey_N\}$ 비밀을 유지하지만, 대응하는 공개 키들$\{PubKey_{1,...,} PubKey_N\}$을 다른 장치들이 이용 가능하게 하고, $\{PubKey_{N+1}, PubKey_{N+2,.....,}Key_{N+M}\}$을 알며, 따라서 공유 비밀을 도출할 수 있고, 그 반대도 가능하다. 아래의 예들은 N=1 및 M=2를 사용한다.

[0006] 피등록기 및 구성기 둘 모두에서 양측에서 공개 키 및 비공개 키 둘 모두를 사용하여 소위 공유 키 재료(shared key material)를 생성하는 것에 기초하여 추가의 보안이 달성될 수 있다. 그러한 공유 키는 공개 네트워크 키 및 비공개 피등록기 키에 기초하여 피등록기에서 생성되는 반면, 동일 키(따라서, 공유 키라고 함)가 비공개 네트워크 키 및 공개 피등록기 키에 기초하여 구성기 측에서 생성될 수 있다. 그러한 공유 키들을 생성하기 위한 다양한 암호화 방법들, 예를 들어 디피-헬먼 키 교환(DH)이 알려져 있다. DH는 공개 채널을 통해 암호화 키들을 안전하게 교환하는 특정 방법이며, 암호화 분야 내에서 구현되는 공개 키 교환의 가장 초기의 실제 예들 중 하나이다. 전통적으로, 두 당사자 간의 보안 암호화 통신은 그들이 신뢰되는 운반자에 의해 운반되는 종이 키 리스트들과 같은 어떤 보안 물리 채널에 의해 먼저 키들을 교환할 것을 요구하였다. 디피-헬먼 키 교환 방법은 서로에 대한 사전 지식이 없는 두 당사자가 비보안 채널을 통해 공유 비밀 키를 공동으로 설정하는 것을 가능하게 한다. 이어서, 이 키는 대칭 키 암호를 사용하여 후속 통신들을 암호화하는 데 사용될 수 있다.

[0007] 디피-헬먼 키 교환 방법은 프로토콜 교환을 청취하는 어느 누구도 디피-헬먼 키를 계산할 수 없게 한다. 그러나, 어느 하나의 당사자는 다른 당사자로부터 수신한 공개 키가 실제로 올바른 당사자로부터 온 것임을 확인해야 한다. 일반적으로 중간자로 지칭되는 악의적인 제삼자가 의도된 각자의 공개 키 대신에 그의 공개 키를 두 당사자에게 줄 수 있고, 따라서 이들 둘 각각에 대한 디피-헬먼 키를 셋업할 수 있는 반면, 이들 두 당사자는 그들이 직접 통신한다고 생각한다. 따라서, 이 경우, 중간자는 두 당사자가 모르게 하나의 당사자로부터의 통신을 해독하고, 그것을 마음대로 사용하고, 그것을 다른 당사자에 대한 DH 키로 암호화하고, 그것을 다른 당사자에게 전송할 수 있다. 두 당사자 중 적어도 하나가 후술하는 바와 같이 그들이 신뢰하는 대역외(OOB) 채널을 사용하여 그의 공개 키를 다른 당사자에게 전송하는 경우, 또는 두 당사자가 신뢰되는 OOB 채널을 사용하여 그들의 공개 키들을 교환하는 경우, 그들은 OOB를 수신하지 않은 공개 키를 가진 당사자에 대해 DH 프로토콜을 수행하는 것을 거부함으로써 중간자가 존재하지 않는 것을 확실히 할 수 있다. OOB를 통해 공개 키를 전송하는 대신에, 공개 키의 파생물, 예를 들어 공개 키의 해시가 또한 전송될 수 있다. 당사자가 그의 공개 키를 다른 당사자에 제공하는 경우, 다른 당사자는 그 공개 키의 해시를 계산하고, 계산된 해시가 OOB를 통해 수신된 해시

와 동일한지를 체크한다. 이것의 예는 문헌[Wi-Fi Simple Configuration Technical Specification Version 2.05](참고문헌 1)의 10.1.3 절의 "접속 핸드오버" 방법에서 OOB 채널로서의 근거리 장 통신(NFC)의 사용이다.

[0008] 비밀들을 파괴하려고 시도하는 공격자들에 대한 더욱 개선된 내구력은 타원 곡선 암호화를 사용하여 달성될 수 있다. 타원 곡선 암호화(ECC)는 유한 장들에 대한 타원 곡선들의 대수 구조에 기초한 공개 키 암호화에 대한 접근법이다. ECC는 동등한 보안을 제공하기 위해 (평평한 갈루아 장들(plain Galois fields)에 기초한) 논(non)-ECC 암호화에 비해 더 작은 키들을 요구한다. 타원 곡선들은 암호화, 디지털 서명들, 의사 난수 생성기들 및 다른 태스크들에 적용 가능하다. 그들은 또한 렌스트라(Lenstra) 타원 곡선 인수 분해와 같은, 암호화에서의 응용들을 갖는 여러 정수 인수 분해 알고리즘에서 사용된다. 공개 키 암호화는 소정의 수학 문제들의 난해함에 기초한다. 초기 공개 키 시스템들은 2개 이상의 큰 소인수로 구성된 큰 정수를 인수 분해하기 어렵다고 가정하면 안전하다. 타원 곡선 기반 프로토콜들의 경우, 공지된 기점에 대한 무작위 타원 곡선 요소의 이산 로그를 찾는 것이 실행 불가능하다고 가정하는데, 이는 "타원 곡선 이산 로그 문제"로 지칭된다. ECC의 보안은 점 곱셈 계산의 능력, 및 원점 및 곱 점이 주어질 경우의 피승수 계산의 무능력에 의존한다. 타원 곡선의 크기는 문제의 난이도를 결정한다. 다양한 암호화 스킴들이 그러한 타원 곡선들에 기초하여 적응되었다.

[0009] 증명서들의 교환은 네트워크를 통해 제공되는 무선 통신과는 다른 근접 기반 통신 채널의 사용을 초기에 요구함으로써 미리 정의된 위치 내에 있도록 추가로 제어될 수 있다. 잘 알려진 예는 2006년에 소개된 와이파이 보호 셋업(WPS, 참고문헌 1 참조)으로 지칭되며, 이 프로토콜의 목표는 무선 보안을 거의 모르고 이용 가능한 보안 옵션들에 의해 위협받을 수 있는 가정 사용자들이 와이파이 보호 액세스를 셋업하는 것을 가능하게 하는 것뿐만 아니라, 긴 패스프레이즈들을 입력함이 없이 기존 네트워크에 새로운 장치들을 추가하는 것을 쉽게 만드는 것이다. WPS 표준은 유용성과 보안을 강조하며, 새로운 장치를 네트워크에 추가하기 위한 홈 네트워크에서의 몇 가지 모드: PIN, 푸시 버튼 또는 NFC를 허용한다. PIN 방법에서, 개인 식별 번호(PIN)가 새로운 무선 장치 상의 스티커 또는 디스플레이로부터 판독되어야 한다. 이어서, 이 PIN은 일반적으로 네트워크의 액세스 포인트인 네트워크의 관리자를 나타내는 장치에 입력되어야 한다. 대안적으로, 액세스 포인트에 의해 제공되는 PIN이 새로운 장치에 입력될 수 있다. 푸시 버튼 방법에서, 사용자는 액세스 포인트 및 새로운 무선 클라이언트 장치 둘 모두 상의 버튼(실제 또는 가상 버튼)을 눌러야 한다. 대부분의 장치들에서, 이러한 발견 모드는 어느 것이 먼저 오든지 접속이 설정되자마자 또는 지연(전형적으로 2분 이하) 후에 스스로 턴오프되어서, 그의 취약성을 최소화한다. 세 번째 방법은 근거리 장 통신(NFC)에 기초하며, 이 경우에 사용자는 장치들 간의 근거리 장 통신을 가능하게 하기 위해 새로운 클라이언트를 액세스 포인트 가까이에 가져와야 한다. NFC 포럼 준수 RFID 태그들이 또한 WPS 시스템에서 사용될 수 있다. 이러한 모드의 지원은 선택적이다. 그러한 추가의 근접 기반 통신 채널은 일반적으로 대역외 채널(OOB)이라고 한다.

[0010] 무선 주파수 식별(RFID)은 물체들에 부착된 태그들을 자동으로 식별하고 추적할 목적들을 위한, 데이터를 전송하기 위한 전자기장들의 무선 사용이다. 태그들은 전자적으로 저장된 정보를 포함한다. 몇몇 태그들은 판독기 근처에 생성되는 자기장들로부터의 전자기 유도에 의해 급전된다. 일부 타입들은 송신 무선파들로부터 에너지를 수집하며, 수동 트랜스폰더로서 동작한다. 다른 타입들은 배터리와 같은 국지적 전원을 가지며, 판독기로부터 수백 미터에서 동작할 수 있다. 바코드와는 달리, 태그는 반드시 판독기의 시선 내에 있어야 할 필요는 없으며, 추적되는 물체에 내장될 수 있다.

[0011] 근거리 장 통신(NFC)에 기초한 추가의 예는 참고문헌 1의 10장 WLAN 구성을 위한 "NFC 대역외 인터페이스 사양"에 설명되어 있다. 여기서, NFC 태그가 피등록기 장치에서 제공되어야 한다. NFC 태그는 가까운 범위에서 피등록기로부터 NFC 인에이블드 등록기로 장치 패스워드를 물리적으로 전송하는 데 사용된다. 이어서, 장치 패스워드는 대역내 등록 프로토콜과 함께 사용되어 피등록기에 WLAN 구성 데이터를 프로비저닝할 것이다. 장치가 휴대 가능하고, 제조자가 사용자에게 장치를 등록기 NFC 장치 근처로 물리적으로 이동시키는 데 실질적인 어려움을 주지 않는 경우 NFC 패스워드 토큰이 장치에 통합될 수 있다. 새로운 장치가 네트워크에 액세스할 수 있게 하는, 즉 피등록기와 네트워크가 보안 방식으로 필요한 증명서들을 교환하게 함으로써 네트워크 및 피등록기의 구성을 가능하게 하는 그러한 네트워크 등록기 장치는 여기서부터 구성기라고 한다. 참고문헌 1의 알려진 시스템에서, 피등록기는 OOB 채널을 통해 가까운 범위에서 구성기에 피등록기 패스워드를 제공하도록 요구될 수 있다. OOB 채널을 사용하기 위한 더 많은 방법, 예를 들어 공개 키들의 해시들의 교환이 참고문헌 1에 설명되어 있다.

[0012] WO2010/023506호는 무선 장치들에 대한 보안 페어링 및 연관을 설명하며, 여기서 장치들은 순방향 비밀을 손상시킴이 없이 제1 장치와 제2 장치의 페어링 및 연관에 사용하기 위한 제1 장치에서의 고정 비밀 값 및 고정 공개 키의 사용을 가능하게 한다. 제1 및 제2 장치들은 제1 장치의 고정 공개 키 및 제2 장치와 연관된 공개 키

에 적어도 부분적으로 기초하여 공개 키 협의 프로토콜에 따라 제1 공유 비밀 키를 설정할 수 있다. 제1 공유 비밀 키는 제2 공유 비밀 키의 검증을 위해 사용될 수 있다. 제2 공유 비밀 키는 제2 장치와 연관된 공개 키 및 제1 장치에 의해 생성된 새로운 공개 키에 적어도 부분적으로 기초하여 설정될 수 있고, 장치들 간의 암호화된 통신을 용이하게 하는 데 사용될 수 있다.

발명의 내용

[0013] 공개적인 장소들에서의 보안 방식의 증명서들의 교환이 요구되며, 피등록기는 그의 증명서들을 구성기에게 제공하도록 요구될 수 있다. 그러나, 사용자가 그의 장치를 구성기에 근접시키는 것은 귀찮을 수 있고/있거나, 네트워크의 운영자가 네트워크 액세스를 원하는 각각의 고객에 대해 구성기에 대한 물리적 액세스를 제공하는 것은 귀찮을 수 있다. 그럼에도 불구하고, 그러한 네트워크의 운영자는, 제삼자가 피등록기와 네트워크 사이에서 전송되는 데이터에 액세스할 수 없고 방해하거나 중간자 역할을 할 수 없다는 것을 피등록기 및 구성기 둘 모두가 확신할 수 있으면서, 그의 고객들이 매우 간단한 방식으로 그의 네트워크에 대한 보안 액세스를 획득할 수 있기를 바랄 것이다.

[0014] 피등록기들에 대해 더 편리한 액세스를 가능하게 하는 공개 무선 네트워크에 대한 보안 액세스를 위한 시스템을 제공하는 것이 본 발명의 목적이다.

[0015] 이러한 목적을 위해, 첨부된 청구항들에 한정된 바와 같은 네트워크 시스템, 장치들 및 방법들이 제공된다.

[0016] 네트워크 시스템은 영역 내의 네트워크 장치들 간의 무선 통신을 위해, 그리고 보안 프로토콜에 따른 보안 통신을 위해 배열된다. 네트워크 시스템은,

[0017] - 무선 통신을 위해 배열되며, 네트워크에 대한 액세스를 획득하기 위해 보안 프로토콜에 따라 피등록기로서 동작하고, 제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키를 갖고, 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 갖도록 배열된 적어도 하나의 네트워크 장치,

[0018] - 구성기로서 동작하도록 배열되며, 보안 프로토콜에 따라 피등록기에 대한 보안 통신을 가능하게 하고, 구성기 공개 키 및 대응하는 구성기 비공개 키를 갖고, 네트워크 시스템에 대해, 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 갖도록 배열된 네트워크 장치를 포함하며,

[0019] 피등록기는 피등록기 센서 및 피등록기 프로세서를 포함하고, 피등록기 프로세서는,

[0020] - 피등록기 센서에 의해 대역외 채널을 통해, 영역에서 제공되고 네트워크 공개 키를 나타내는 데이터 패턴을 획득하고,

[0021] - 네트워크 공개 키 및 제1 피등록기 비공개 키에 기초하여 제1 공유 키를 도출하고,

[0022] - 제1 공유 키를 사용하여 제2 피등록기 공개 키를 인코딩하고,

[0023] - 보안 프로토콜에 따라, 인코딩된 제2 피등록기 공개 키 및 제1 피등록기 공개 키를 포함하는 네트워크 액세스 요청을 생성하고,

[0024] - 무선 통신을 통해 네트워크 액세스 요청을 구성기로 전송하도록 배열되고,

[0025] 구성기는,

[0026] - 무선 통신을 통해 피등록기로부터 네트워크 액세스 요청을 수신하고,

[0027] - 네트워크 비공개 키 및 제1 피등록기 공개 키에 기초하여 제1 공유 키를 도출하고,

[0028] - 제1 공유 키를 사용하여 인코딩된 제2 피등록기 공개 키를 디코딩하고,

[0029] - 인코딩된 제2 피등록기 공개 키가 제1 공유 키에 의해 인코딩되었는지를 검증하고, 그렇다면,

[0030] - 제2 피등록기 공개 키 및 구성기 비공개 키를 사용하여 보안 데이터를 생성하고,

[0031] - 제1 피등록기 공개 키, 제2 피등록기 공개 키 및 네트워크 비공개 키에 기초하여 제2 공유 키를 도출하고,

[0032] - 제2 공유 키를 사용하여 보안 데이터 및 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호하고,

[0033] - 보안 프로토콜에 따라, 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나를 포함하는 네트워크 액세스 메시지를 생성하도록

[0034] 배열된 구성기 프로세서를 포함하고,

[0035] 피등록기 프로세서는,

[0036] - 무선 통신을 통해 구성기로부터 네트워크 액세스 메시지를 수신하고,

[0037] - 제1 피등록기 비공개 키, 제2 피등록기 비공개 키 및 네트워크 공개 키에 기초하여 제2 공유 키를 도출하고,

[0038] - 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나가 제2 공유 키에 의해 암호화 방식으로 보호되었는지를 검증하고, 그렇다면,

[0039] - 제2 피등록기 비공개 키 및 보안 데이터에 기초하여 보안 통신을 이행하도록 추가로 배열된다.

[0040] 제1 네트워크 장치는 구성기로도 불리는 구성기 장치로서 동작한다. 구성기 장치는 피등록기 장치로부터 보안 프로토콜에 따라 네트워크 액세스 요청을 수신하도록 배열된 구성기 통신 유닛으로서, 네트워크 액세스 요청은 인코딩된 제2 피등록기 공개 키 및 제1 피등록기 공개 키를 포함하는, 상기 구성기 통신 유닛, 및, 구성기 장치에 대해, 구성기 공개 키 및 대응하는 구성기 비공개 키를 갖고, 네트워크 시스템에 대해, 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 갖도록 배열된 메모리를 포함하는 구성기 프로세서를 포함한다. 구성기 프로세서는,

[0041] - 네트워크 비공개 키 및 제1 피등록기 공개 키에 기초하여 제1 공유 키를 도출하고,

[0042] - 제1 공유 키를 사용하여 인코딩된 제2 피등록기 공개 키를 디코딩하고,

[0043] - 인코딩된 제2 피등록기 공개 키가 제1 공유 키에 의해 인코딩되었는지를 검증하고, 그렇다면,

[0044] - 제2 피등록기 공개 키 및 구성기 비공개 키를 사용하여 보안 데이터를 생성하고,

[0045] - 제1 피등록기 공개 키, 제2 피등록기 공개 키 및 네트워크 비공개 키에 기초하여 제2 공유 키를 도출하고,

[0046] - 제2 공유 키를 사용하여, 보안 데이터 및 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호하고,

[0047] - 보안 프로토콜에 따라 네트워크 액세스 메시지를 생성하도록 배열된다.

[0048] 구성기가 네트워크 및 네트워크에 진입하는 네트워크 장치들, 소위 피등록기들을 구성함에 따라, 구성기 장치는, 직접 또는 액세스 포인트와 같은 무선 통신 장치를 통해 간접적으로, 다른 네트워크 장치들과 무선으로 통신할 수 있어야 한다. 그렇기 때문에, 구성기는 네트워크 자체의 일부일 필요가 없는데, 즉 구성되고 있는 네트워크를 통해 통신에 참여하는 것이 가능할 수 있거나 가능하지 않을 수 있다.

[0049] 제2 네트워크 장치는 피등록기로도 불리는 피등록기 장치로서 동작한다. 피등록기 장치는,

[0050] 무선 통신을 위해 배열된 피등록기 무선 통신 유닛;

[0051] 대역외 채널을 통해 데이터 패턴을 획득하도록 배열된 피등록기 센서로서, 데이터 패턴은 영역에서 제공되고 네트워크 공개 키를 나타내는, 상기 피등록기 센서; 및

[0052] 제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키를 갖고, 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 갖도록 배열된 메모리를 포함하는 피등록기 프로세서를 포함한다. 피등록기 프로세서는,

[0053] - 네트워크 공개 키 및 제1 피등록기 비공개 키에 기초하여 제1 공유 키를 도출하고,

[0054] - 제1 공유 키를 사용하여 제2 피등록기 공개 키를 인코딩하고,

[0055] - 보안 프로토콜에 따라, 인코딩된 제2 피등록기 공개 키 및 제1 피등록기 공개 키를 포함하는 네트워크 액세스 요청을 생성하고,

[0056] - 피등록기 무선 통신 유닛을 통해 네트워크 액세스 요청을 구성기 장치로 전송하도록 배열된다.

[0057] 피등록기 프로세서는,

[0058] - 피등록기 무선 통신 유닛을 통해 구성기로부터 네트워크 액세스 메시지를 수신하고,

[0059] - 제1 피등록기 비공개 키, 제2 피등록기 비공개 키 및 네트워크 공개 키에 기초하여 제2 공유 키를 도출하고,

[0060] - 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나가 제2 공유 키에 의해 암호화 방식으로 보호되

었는지를 검증하고, 그렇다면,

[0061] - 제2 피등록기 비공개 키 및 보안 데이터에 기초하여 보안 통신을 이행하도록 추가로 배열된다.

[0062] 현재 네트워크 시스템의 맥락에서, 피등록기는 이러한 정보를 나타내는 소위 데이터 패턴, 예를 들어 네트워크 공개 키를 나타내는 데이터 패턴을 포함하는 QR 코드, 컬러 패턴 또는 NFC 태그로부터, 전술한 바와 같이, 소위 대역외(OOB) 채널을 통해 정보를 수신할 수 있는 피등록기 센서를 갖는다.

[0063] 일반적으로, 데이터의 프라이버시 및/또는 무결성을 보호하는 것은 키 재료에 기초하여 암호화 해시를 암호화 및/또는 추가하는 형태를 포함하며, 이는 일반적인 단어 '인코딩'에 의해 표현될 수 있다. 따라서, 키로 정보를 인코딩하는 것은, 예를 들어 AES를 사용함으로써, 키로 정보를 암호화하는 것을 의미할 수 있다. 예를 들어, "제2 공유 키를 사용하여 보안 데이터 및 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호하는" 단계는 다음의 기능을 갖는다. 이 단계에서, 보호는 보안 데이터 및 구성기 공개 키가 비밀로 유지될 수 있는 (그러나 그럴 필요는 없음) 인코딩의 타입이며, 따라서 이 단계는 키를 이용한 암호화를 포함할 수 있거나 포함하지 않을 수 있다. 그러나, 수신 당사자는 "보호된 데이터"가 올바른지 확인해야 하며, 따라서 그들의 무결성을 체크하는 것이 가능해야 한다. 따라서, '보호'는 암호화 서명의 생성 및/또는 추가의 체크 데이터, 체크섬들 또는 다른 고유 데이터를 포함한 재료의 '암호화'와 같은 '무결성에 대한 보호'로 해석되어야 한다. 정보를 키로 암호화 방식으로 보호하는 것은 또한 그러한 키로 정보의 무결성을 보호하는 것을 의미할 수 있으며, 이는 정보 위에 키를 사용하여 암호화 해시를 추가함으로써 행해질 수 있으며, 따라서 키를 알고 있는 당사자들이 정보의 무결성을 체크할 수 있다. 암호화 해시는 정보를 키를 알고 있는 당사자로부터 유래하는 것으로 인증한다고 말할 수도 있다. 암호화 해시 함수는, 입력으로서 해싱될 데이터 외에, 입력으로서의 키를 또한 요구하는 해시 함수이며, 이때 결과적인 해시는 물론 키에 의존하는데, 예를 들어 AES-SIV(RFC 5297, [2] 참조)는 키에 기초하여 암호화 및 무결성 보호 둘 모두를 달성한다. 수신된 바와 같은 데이터에 대해 '~인지를 검증하는' 단계는 무결성 체크를 구현하여 무결성 보호를 달성한다. 이 단계는, 사용되는 보호 방법에 따라, 해독을 포함할 수 있다. 예를 들어 보호를 위해 AES-SIV(RFC 5297, [2] 참조)가 사용되는 경우, '~인지를 검증하는' 단계는 데이터의 해독을 또한 포함한다. 또한, '제2 공유 키를 사용하여 보안 데이터 및 구성기 공개 키 중 적어도 하나를 보호하는 것'은 "제2 공유 키를 사용하여 보안 데이터 및 구성기 공개 키 중 적어도 하나에 대한 무결성 보호 정보를 생성하고", 이어서 무결성 보호 정보와 보안 데이터 및 구성기 공개 키 중 적어도 하나를 네트워크 액세스 메시지에 넣는 것으로 해석될 수 있다.

[0064] 유리하게는, 네트워크 시스템에서, 피등록기는 그 자신의 제2 피등록기 비공개 키 및 네트워크 액세스 메시지를 통해 수신된 바와 같은 보안 데이터에 기초하여 보안 통신을 효율적으로 이행하는 것이 가능해진다. 또한, 피등록기는 먼저 데이터 패턴을 획득하기 위해 피등록기 센서를 사용함으로써 형성된 유효 대역외 채널을 설정한다. 데이터 패턴은 네트워크 시스템 관리자가 피등록기들이 네트워크 시스템에 액세스하도록 허용하려고 하는 영역에서 이용 가능하게 된다. 이어서, 피등록기는 무선 통신을 사용하여 보안 프로토콜을 개시한다.

[0065] 더 유리하게는, 시스템 관리자는 피등록기들이 시스템에 들어갈 수 있는 영역을 제어하는 반면, 증명서들은 중간자 공격을 방지하는 방식으로 구성기와 안전하게 교환된다. 대역외 채널을 통해 피등록기 자신에 의해 등록 프로세스가 개시되게 함으로써, 최소 수의 무선 메시지, 즉 네트워크 요청 메시지 및 후속 네트워크 액세스 메시지가 상기의 안전한 증명서 교환에 충분하다.

[0066] 선택적으로, 구성기 장치는 구성기 장치를 대신하여 공개 키들에 서명하도록 다른 장치를 셋업할 수 있다. 장치들의 그러한 조합은 네트워크 시스템에서 한정된 바와 같은 구성기의 구현인 것으로 간주된다. 구성기 장치에 의해 행해져야 하는 것들 중 하나는 이러한 다른 장치에 그의 서명 비공개 키를 제공하거나, 다른 장치의 서명 공개 키를 획득하고, 그것에 구성기의 서명 비공개 키로 서명하고, 서명된 다른 장치의 서명 공개 키, 및 구성기의 서명 공개 키를 다른 장치로 전송하는 것이다. 다른 장치가 피등록기로부터의 공개 키에 서명할 때, 그것은 두 번째 경우에 그의 공개 서명 키, 구성기에 의해 제공된 서명 및 구성기의 공개 서명 키를 피등록기로 전송하며, 따라서 피등록기는 그의 공개 키의 서명 및 다른 장치의 공개 서명 키에 대한 서명을 체크할 수 있다.

[0067] 선택적으로, 상기의 네트워크 시스템에서, 구성기 프로세서는 임시 네트워크 공개 키 및 대응하는 임시 네트워크 비공개 키를 생성하도록 배열되며, 이들 키는 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 구성한다. 이것은 네트워크 키 쌍을 일시적인(임시, 일회용) 것으로 만드는 것을 정의한다. 네트워크 공개 키가 정적인 시스템에서, 이전의 피등록기들 중 하나는 이 공개 키를 인터넷 상에 두었을 수 있으며, 누구나 구성기와 접촉할 수 있다. 일시적인 키의 이점은, 피등록기가 와이파이를 통해 구성기와 접촉하고 네트워크 공개

키가 방금 생성된 경우, 피등록기는 이 네트워크 공개 키만을 알 수 있다는 것인데, 이는 그것이 대역외 메커니즘을 통해 바로 전에 이 키를 획득했기 때문이다.

[0068] 선택적으로, 상기의 네트워크 시스템에서, 피등록기 프로세서는 임시 피등록기 공개 키 및 대응하는 임시 피등록기 비공개 키를 생성하도록 배열되며, 이들 키는 제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키를 구성하고/하거나; 피등록기 프로세서는 추가의 임시 피등록기 공개 키 및 대응하는 추가의 임시 피등록기 비공개 키를 생성하도록 배열되며, 이들 키는 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 구성한다. 그러한 일시적인 키의 이점은, 피등록기가 와이파이를 통해 구성기와 통신하고 키가 방금 생성된 경우, 피등록기 및 구성기만이 이 키를 알 수 있다는 것인데, 이는 그것이 방금 생성되었기 때문이다.

[0069] 선택적으로, 상기의 시스템에서, 보안 데이터는 구성기로부터의 허가 정보이며, 이 허가 정보는 피등록기가 네트워크에 액세스하는 것을 허가한다. 유리하게는, 그러한 보안 데이터는 피등록기가 네트워크에 액세스하는 것을 허가하는 데 사용될 수 있다.

[0070] 선택적으로, 상기의 네트워크 시스템에서, 구성기 프로세서는 구성기 세션 키를 제공하고 구성기 세션 키를 피등록기로 전송함으로써 보안 데이터를 생성하도록 추가로 배열되고; 피등록기 프로세서는 구성기 세션 키를 수신하고 구성기 세션 키에 기초하여 보안 통신을 이행하도록 추가로 배열된다. 예를 들어, 구성기 세션 키는 그와 같이 알려진 와이파이 패스프레이즈일 수 있다. 실시예는 레거시 액세스 포인트의 와이파이 패스프레이즈를 본 발명에 따라 구현되는 피등록기로 전송할 수 있게 한다.

[0071] 선택적으로, 상기의 네트워크 시스템에서, 구성기 프로세서는 제2 피등록기 공개 키 및 디지털 서명을 포함하는 추가의 메시지를 생성하고, 피등록기와 추가의 장치 간의 보안 통신을 가능하게 하기 위해 추가의 메시지를 추가의 장치로 전송하도록 추가로 배열된다. 유리하게는, 구성기는 또한 제2 피등록기 공개 키 및 디지털 서명을 추가의 네트워크 장치들에 배포하며, 따라서 피등록기와의 보안 통신을 제어하고 허가한다. 유사한 메시지가 서명을 검증하기 위해 피등록기로 전송될 수 있다.

[0072] 선택적으로, 상기의 네트워크 시스템에서, 피등록기 프로세서는 구성기로부터 또는 추가의 네트워크 장치로부터 추가의 공개 키 및 추가의 디지털 서명을 수신하도록 추가로 배열된다. 유리하게는, 피등록기는, 구성기로부터 또는 추가의 네트워크 장치로부터, 구성기에 의해 허가된 증명서들을 수신한다. 피등록기가 추가의 네트워크 장치로부터 그러한 증명서들을 수신할 때, 추가의 장치에 대한 보안 통신의 직접적인 셋업이 가능해진다.

[0073] 선택적으로, 상기의 네트워크 시스템에서, 구성기 프로세서는 구성기 세션 공개 키 및 대응하는 구성기 세션 비공개 키를 생성하고, 구성기 세션 비공개 키 및 제2 피등록기 공개 키에 기초하여 제3 공유 키를 도출하고, 구성기 세션 공개 키를 피등록기로 전송함으로써 보안 데이터를 생성하도록 추가로 배열된다. 피등록기 프로세서는 구성기 세션 공개 키를 수신하고, 제2 피등록기 비공개 키 및 구성기 세션 공개 키에 기초하여 제3 공유 키를 도출하고, 제3 공유 키에 기초하여 보안 통신을 이행하도록 추가로 배열된다. 유리하게는, 그러한 구성기 세션 공개/비공개 키 쌍을 생성하는 것은 제3 공유 키에 기초하여 피등록기와 구성기 사이의 추가의 보안 통신을 가능하게 한다.

[0074] 선택적으로, 상기의 네트워크 시스템에서, 피등록기 프로세서는 피등록기 세션 공개 키 및 대응하는 피등록기 세션 비공개 키를 생성하고, 피등록기 세션 비공개 키 및 구성기 공개 키에 기초하여 제4 공유 키를 도출하고, 피등록기 세션 공개 키를 구성기로 전송하도록 추가로 배열되며; 구성기 프로세서는 구성기 비공개 키 및 피등록기 세션 공개 키에 기초하여 제4 공유 키를 도출하고, 제4 공유 키에 기초하여 보안 통신을 이행하도록 추가로 배열된다. 유리하게는, 피등록기는 따라서 세션 키 쌍을 생성할 수 있고, 추가의 공유 키를 도출하기 위해 비공개/공개 키 쌍을 사용할 수 있다.

[0075] 선택적으로, 상기의 네트워크 시스템에서, 네트워크 시스템은 제2 피등록기 공개 키 및 보안 데이터를 수신하고, 세션 네트워크 공개 키 및 대응하는 세션 네트워크 비공개 키를 제공하고, 세션 네트워크 비공개 키 및 제2 피등록기 공개 키에 기초하여 제5 공유 키를 도출하고, 세션 네트워크 공개 키를 피등록기로 전송하도록 배열된 추가의 네트워크 장치를 포함한다. 피등록기 프로세서는 세션 네트워크 공개 키를 수신하고, 제2 피등록기 비공개 키 및 세션 네트워크 공개 키에 기초하여 제5 공유 키를 도출하고, 제5 공유 키에 기초하여 추가의 네트워크 장치와의 보안 통신을 이행하도록 추가로 배열된다. 유리하게는, 그러한 추가의 세션 네트워크 공개/비공개 키 쌍을 생성하는 것은 제5 공유 키에 기초하여 피등록기와 추가의 네트워크 장치 사이의 추가의 보안 통신을 가능하게 한다.

[0076] 선택적으로, 상기의 네트워크 시스템에서, 구성기 프로세서는 구성기 비공개 키로 제2 피등록기 공개 키에 디지

털 서명함으로써 디지털 서명을 포함하는 보안 데이터를 생성하고, 피등록기와 제3 장치 사이의 보안 통신을 가능하게 하기 위해 디지털 서명을 제3 장치 및/또는 피등록기로 전송하도록 추가로 배열된다. 구성기의 디지털 서명을 제3 장치로 전송함으로써, 디지털 서명은 피등록기와 제3 장치 사이의 보안 통신을 가능하게 한다. 유리하게는, 구성기는 제2 피등록기 공개 키에 대한 보안 데이터로서 디지털 서명을 제공하며, 따라서 제3 장치는 상기 제2 피등록기 공개 키가 신뢰되어야 한다는 것을 검증할 수 있다.

[0077] 또한, 선택적으로, 이전의 네트워크 시스템에서, 피등록기 프로세서는 디지털 서명을 수신하고, 디지털 서명 및 구성기 공개 키에 기초하여, 제2 피등록기 공개 키가 올바르게 서명되었는지를 검증하고, 그렇다면, 제2 피등록기 비공개 키에 기초하여 보안 통신을 이행하도록 추가로 배열된다. 유리하게는, 피등록기는 구성기가 제2 피등록기 공개 키에 올바르게 서명했는지를 검출할 수 있다.

[0078] 또한, 선택적으로, 이전의 네트워크 시스템에서, 네트워크 시스템은 구성기 공개 키를 획득하고, 디지털 서명 및 제2 피등록기 공개 키를 수신하고, 디지털 서명 및 구성기 공개 키에 기초하여, 제2 피등록기 공개 키가 올바르게 서명되었는지를 검증하고, 그렇다면, 제2 피등록기 공개 키에 기초하여 피등록기와의 보안 통신을 이행하도록 배열된 추가의 네트워크 장치를 포함한다. 유리하게는, 추가의 네트워크 장치는 구성기가 제2 피등록기 공개 키에 올바르게 서명했는지를 검출하고, 보안 통신을 이행할 수 있다.

[0079] 선택적으로, 상기의 네트워크 시스템에서, 구성기 프로세서는, 구성기 비공개 키로, 추가의 네트워크 장치의 추가의 공개 키에 디지털 서명함으로써 추가의 디지털 서명을 포함하는 추가의 보안 데이터를 생성하도록 추가로 배열된다. 피등록기 프로세서는 추가의 공개 키 및 추가의 디지털 서명을 수신하고, 추가의 디지털 서명 및 구성기 공개 키에 기초하여, 추가의 공개 키가 올바르게 서명되었는지를 검증하고, 그렇다면, 제2 피등록기 비공개 키 및 추가의 공개 키를 사용하여 추가의 네트워크 장치와 보안 통신함으로써 추가의 보안 데이터를 사용하도록 추가로 배열된다. 유리하게는, 피등록기는 구성기가 추가의 공개 키에 올바르게 서명했는지를 검출하고, 보안 통신을 이행할 수 있다.

[0080] 선택적으로, 상기의 네트워크 시스템에서, 피등록기 프로세서는 피등록기 테스트 데이터를 생성하고, 제2 공유 키를 사용하여 피등록기 테스트 데이터를 인코딩하고, 인코딩된 피등록기 테스트 데이터를 구성기로 전송하도록 추가로 배열된다. 구성기 프로세서는 제2 공유 키를 사용하여 인코딩된 피등록기 테스트 데이터를 디코딩하고, 피등록기 테스트 데이터가 피등록기에서 제2 공유 키에 의해 인코딩되었는지를 검증하도록 추가로 배열된다. 유리하게는, 피등록기가 지금까지 프로토콜 내의 어딘가에서 잘못된 어떤 것을 수행한 경우, 예를 들어 우연히 구성기들을 섞어서 잘못된 것에 응답한 경우, 구성기는 수신된 테스트 데이터 및 그가 스스로 계산하는 테스트에 기초하여 에러를 알 수 있다. 그러한 테스트 데이터는 피등록기를 구성기에 대해 허가하는 것으로 간주될 수 있다.

[0081] 선택적으로, 상기의 네트워크 시스템에서, 구성기 프로세서는 구성기 테스트 데이터를 생성하고, 제2 공유 키를 사용하여 구성기 테스트 데이터를 인코딩하고, 인코딩된 구성기 테스트 데이터를 피등록기로 전송하도록 추가로 배열된다. 피등록기 프로세서는 제2 공유 키를 사용하여 인코딩된 구성기 테스트 데이터를 디코딩하고, 구성기 테스트 데이터가 구성기에서 제2 공유 키에 의해 인코딩되었는지를 검증하도록 추가로 배열된다. 유리하게는, 구성기가 지금까지 프로토콜 내의 어딘가에서 잘못된 어떤 것을 수행한 경우, 예를 들어 우연히 피등록기들을 섞어서 잘못된 것에 응답한 경우, 피등록기는 수신된 테스트 데이터 및 그가 스스로 계산하는 테스트에 기초하여 에러를 알 수 있다. 그러한 테스트 데이터는 구성기를 피등록기에 대해 허가하는 것으로 간주될 수 있다.

[0082] 상기의 시스템에서의 다양한 동작 요소들은 첨부된 청구항들에 또한 추가로 한정된 바와 같은 각자의 방법을 수행함으로써 구현될 수 있다.

[0083] 피등록기 방법은,

[0084] - 제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키와, 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 저장하는 단계,

[0085] - 대역외 채널을 통해 데이터 패턴(140)을 획득하는 단계로서, 데이터 패턴은 영역에서 제공되고 네트워크 공개 키를 나타내는, 상기 데이터 패턴(140) 획득 단계,

[0086] - 네트워크 공개 키 및 제1 피등록기 비공개 키에 기초하여 제1 공유 키를 도출하는 단계,

[0087] - 제1 공유 키를 사용하여 제2 피등록기 공개 키를 인코딩하는 단계,

[0088] - 보안 프로토콜에 따라 네트워크 액세스 요청을 생성하는 단계로서, 네트워크 액세스 요청은 인코딩된 제2 피

등록기 공개 키 및 제1 피등록기 공개 키를 포함하는, 상기 네트워크 액세스 요청 생성 단계, 및

[0089] - 피등록기 무선 통신 유닛을 통해 네트워크 액세스 요청을 구성기 장치로 전송하는 단계를 포함한다.

[0090] 피등록기 방법은,

[0091] - 구성기로부터 네트워크 액세스 메시지를 수신하는 단계,

[0092] - 제1 피등록기 비공개 키, 제2 피등록기 비공개 키 및 네트워크 공개 키에 기초하여 제2 공유 키를 도출하는 단계,

[0093] - 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나가 제2 공유 키에 의해 암호화 방식으로 보호되었는지를 검증하는 단계, 및, 그렇다면,

[0094] - 제2 피등록기 비공개 키 및 보안 데이터에 기초하여 보안 통신을 이행하는 단계를 추가로 포함한다.

[0095] 구성기 방법은,

[0096] - 구성기 장치에 대해, 구성기 공개 키 및 대응하는 구성기 비공개 키를, 그리고 네트워크 시스템에 대해, 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 저장하는 단계,

[0097] - 피등록기 장치로부터, 보안 프로토콜에 따라 네트워크 액세스 요청을 수신하는 단계로서, 네트워크 액세스 요청은 인코딩된 제2 피등록기 공개 키 및 제1 피등록기 공개 키를 포함하는, 상기 네트워크 액세스 요청 수신 단계,

[0098] - 네트워크 비공개 키 및 제1 피등록기 공개 키에 기초하여 제1 공유 키를 도출하는 단계,

[0099] - 제1 공유 키를 사용하여 인코딩된 제2 피등록기 공개 키를 디코딩하는 단계,

[0100] - 인코딩된 제2 피등록기 공개 키가 제1 공유 키에 의해 인코딩되었는지를 검증하는 단계, 및, 그렇다면,

[0101] - 제2 피등록기 공개 키 및 구성기 비공개 키를 사용하여 보안 데이터를 생성하는 단계,

[0102] - 제1 피등록기 공개 키, 제2 피등록기 공개 키 및 네트워크 비공개 키에 기초하여 제2 공유 키를 도출하는 단계,

[0103] - 제2 공유 키를 사용하여, 보안 데이터 및 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호하는 단계, 및

[0104] - 보안 프로토콜에 따라 네트워크 액세스 메시지를 생성하는 단계를 포함한다.

[0105] 또한, 상기의 시스템에서의 요소들 또는 방법들은 위에서 한정된 바와 같은 네트워크 시스템에서 사용하기 위한 각자의 장치에 의해 구현될 수 있다. 장치는 무선 통신을 위해 배열된 무선 송수신기를 포함한다. 장치는 구성기로서 동작하도록 배열되며, 상기의 시스템에서 한정된 바와 같은 구성기 프로세서이도록 배열된 장치 프로세서를 포함한다. 장치는 대안적으로 피등록기로서 동작하도록 배열될 수 있으며, 상기의 시스템에서 한정된 바와 같은 피등록기 프로세서이도록 배열된 장치 프로세서를 포함할 수 있다.

[0106] 본 발명에 따른 방법은 컴퓨터 구현 방법으로서 컴퓨터 상에서, 또는 전용 하드웨어에서, 또는 이들 둘 모두의 조합으로 구현될 수 있다. 본 발명에 따른 방법을 위한 실행 가능 코드는 컴퓨터 프로그램 제품에 저장될 수 있다. 컴퓨터 프로그램 제품들의 예들은 메모리 스틱과 같은 메모리 장치들, 광 디스크와 같은 광학 저장 장치들, 집적 회로들, 서버들, 온라인 소프트웨어 등을 포함한다. 바람직하게는, 컴퓨터 프로그램 제품은 상기 프로그램 제품이 컴퓨터 상에서 실행될 때 본 발명에 따른 방법을 수행하기 위해 컴퓨터 판독 가능 매체에 저장된 비일시적 프로그램 코드 수단을 포함한다.

[0107] 바람직한 실시예에서, 컴퓨터 프로그램은 컴퓨터 프로그램이 컴퓨터 상에서 실행될 때 본 발명에 따른 방법의 모든 단계들 또는 스테이지들을 수행하도록 적응되는 컴퓨터 프로그램 코드 수단을 포함한다. 바람직하게는, 컴퓨터 프로그램은 컴퓨터 판독 가능 매체 상에 구현된다.

[0108] 본 발명의 다른 태양은 컴퓨터 프로그램을, 예를 들어 위치 기반 애플리케이션의 다운로드가 가능하게 하는 방법을 제공한다. 이 태양은 컴퓨터 프로그램이 예를 들어 애플(Apple)의 앱 스토어(App Store), 구글(Google)의 플레이 스토어(Play Store), 또는 마이크로소프트(Microsoft)의 윈도우 스토어(Windows Store)에 업로드될 때, 그리고 컴퓨터 프로그램이 그러한 스토어로부터 다운로드가 가능할 때 사용된다.

[0109] 본 발명에 따른 장치들 및 방법들의 추가의 바람직한 실시예들이 첨부된 청구항들에서 주어지며, 그 개시 내용은 본 명세서에 참고로 포함된다.

도면의 간단한 설명

[0110] 본 발명의 이들 및 다른 태양들이 아래의 설명에서 그리고 첨부 도면들을 참조하여 예로서 설명되는 실시예들로부터 명백할 것이고 그 실시예들을 참조하여 추가로 설명될 것이다.

도 1은 네트워크 시스템을 도시한다.

도 2는 네트워크 시스템 및 보안 프로토콜의 제1 예를 도시한다.

도 3은 네트워크 시스템 및 보안 프로토콜의 제2 예를 도시한다.

도 4는 네트워크 시스템 및 보안 프로토콜의 제3 예를 도시한다.

도 5는 네트워크 시스템 및 보안 프로토콜의 제4 예를 도시한다.

도 6은 네트워크 시스템 및 보안 프로토콜의 제5 예를 도시한다.

도 7은 피등록기 방법의 예를 도시한다.

도 8은 구성기 방법의 예를 도시한다.

도 9a는 컴퓨터 판독 가능 매체를 도시한다.

도 9b는 프로세서 시스템의 개략도를 도시한다.

도면들은 전적으로 도식적인 것이며, 일정한 축척으로 작성된 것은 아니다. 도면들에서, 이미 설명된 요소들에 대응하는 요소들은 동일한 도면 부호들을 가질 수 있다.

발명을 실시하기 위한 구체적인 내용

[0111] 네트워크에 대한 액세스를 획득하기 위해, 피등록기는 그의 정보를 네트워크 상의 하나 이상의 다른 장치, 예를 들어 와이파이 네트워크 내의 구성기 및/또는 액세스 포인트(AP)로 전송해야 한다. 이어서, 피등록기는 서명된 네트워크 액세스 정보를 수신 및 체크하고, 에러를 발견한 경우에는, 예를 들어 서명된 네트워크 액세스 정보의 서명 검증이 실패한 경우에는 중지한다. 서명된 네트워크 액세스 정보를 수신하는 다른 장치는 서명된 네트워크 액세스 정보에 대해 서명 검증을 수행하여, 그것이 공통 구성기에 의해 올바르게 서명되었음을 발견할 수 있다. 그렇다면, 다른 장치는 수신된 서명된 네트워크 액세스 정보에 포함된 피등록기 공개 네트워크 액세스 암호화 정보를 신뢰할 수 있고, 공유 키 도출 알고리즘에서 이 정보를 사용하여 피등록기와 그 자신 사이에서 링크 키를 생성할 수 있음을 안다. 다른 장치는 그 자신의 서명된 네트워크 액세스 정보를 피등록기로 전송해야 할 것이며, 따라서 피등록기는 유사한 체크를 수행하고 동일한 링크 키를 도출할 수 있다. 그 이후로, 피등록기 및 다른 장치는 그들의 무선 링크의 보호를 도출된 링크 키에 기초할 수 있다. 도출된 링크 키는 예를 들어 와이파이 네트워크에서 쌍 마스터 키(pairwise master key, PMK)로서 사용할 수 있다. 피등록기 공개 네트워크 액세스 암호화 정보는 공개 타원 곡선 암호화(ECC) 키 또는 공개 RSA(Rivest-Shamir-Adleman cryptosystem) 키의 형태일 수 있거나, HIMMO [3]과 같은 식별자 기반 암호 시스템의 공개 식별자일 수 있다.

[0112] 공개 네트워크 시스템으로도 지칭되는 제안된 네트워크 시스템은 선택된 영역에서, 예를 들어 상점이나 공항 라운지, 대합실 또는 게이트에서 모바일 장치들에 대한 무선 통신을 셋업하는 편리한 방법을 제공한다. 그러한 경우들에서, 네트워크 소유자는 그의 네트워크에 누가 액세스하는지에 대해 신경 쓰지 않지만 네트워크 셋업(SSID, 주파수 대역, 채널 등)에 관해 신경을 쓰며, 그의 네트워크 상에서 링크 보호를 제공하여 네트워크 상의 모든 장치들의 통신 프라이버시를 보호하기를 원한다. 레스토랑 및 카페와 같은 공공 장소들은 그러한 네트워크들을 운영할 수 있다. 네트워크의 운영자가 네트워크 액세스를 원한 각각의 고객에 대해 구성기 장치를 지원하는 것은 매우 성가신 일이다. 전형적으로 이러한 타입의 네트워크에서, 그것을 담당하는 것은 AP이지만, AP와 같은 장치들은 일반적으로 카메라를 구비하지 않으며, 구비하더라도, 네트워크에 액세스하기를 원하는 사용자가 그러한 AP(심지어 천장에 장착될 수도 있음) 근처에 가서 그의 카메라를 작동시켜 액세스하는 것은 매우 불편하다. 다른 OOB 방법들을 사용하는 것도 이 경우에 매우 번거롭다(천장에 장착된 AP와 USB 접속을 행해야 하나? 천장의 AP와 NFC 터치를 수행해야 하나? AP와 보안 블루투스 링크를 셋업해야 하나?). 그러한 네트워크의 운영자는 그의 고객들이 매우 간단한 방식으로 그의 네트워크에 대한 보안 액세스를 획득할 수 있기를 바랄

것이다.

[0113] 예를 들어 관리되는 환경 내의 공개 프린터에 대해 유사하게, 프린터 소유자는 그의 구내에서 스펙트럼 사용을 관리하고 공개 프린터의 주파수 대역 및 채널을 설정하기를 원할 것이다. 그럼에도 불구하고, 소유자는 모든 사람이, 그러나 보안 방식으로, 이 프린터에 액세스하기를 원한다. 그러한 프린터는 사용자가 어떤 것을 인쇄하고자 하는 스마트폰으로부터 공개 암호화 정보를 판독하기 위해 카메라 또는 스캐너를 구비할 수 있지만, 프린터의 사용자 인터페이스는 스마트폰의 사용자 인터페이스보다 사용하기 쉽고 직관적이기가 훨씬 더 어렵다. 그러나, 자신의 스마트폰 상에서 어떤 것을 인쇄하고 싶은 사용자가 스마트폰의 카메라를 이용하여, 예를 들어 공개 RSA 또는 ECC 키 또는 식별자 기반 암호화 스킴의 공개 식별자의 형태의, 프린터의 공개 암호화 정보를 캡처하고, 이어서 인쇄 작업의 목적지로서 카메라를 이용하여 캡처된 정보를 사용하여 그의 스마트폰 상에서 인쇄 작업을 시작하는 것이 편리할 것이다.

[0114] 공개 무선 도킹 센터에 대해 유사하게, 무선 도킹 센터는 무선으로 또는 유선 방식으로 모니터, 키보드, 마우스, 스피커 등과 같은 여러 주변 장치에 접속되거나 이들 중 일부를 내장 주변 장치로서 가질 수 있고, 이러한 주변 장치들의 사용을 무선 채널들을 통해 무선 도키들(dockees)에 제공하는 것이 가능할 수 있다. 그러한 무선 도킹 센터는 구성기를 사용하여 셋업될 수 있으며, 따라서 무선 도킹 센터는 무선 주변 장치들에 안전하게 접속될 것이다. 이어서, 구성기는 무선 도킹 센터가 그 자신 및 무선 접속된 주변 장치들의 구성기가 되도록 무선 도킹 센터를 셋업할 것이다. 구성기는 무선 도키들이 무선 도킹 센터를 사용하도록 허용되는 몇몇 규칙들을 무선 도킹 센터에 제공할 수 있다. 그러한 무선 도킹 센터는 사용자가 무선 도킹 센터를 사용하기를, 즉 무선 도킹 센터와 도킹하기를 원하는 스마트폰으로부터 공개 암호화 정보, 예를 들어 공개 ECC 또는 RSA 키를 판독하기 위해 카메라 또는 스캐너를 구비할 수 있다. 그러나, 자신의 스마트폰으로 무선 도킹 센터에 도킹하기를 원하는 사용자가 스마트폰의 카메라로 무선 도킹 센터의 공개 암호화 정보를 캡처한 다음에 무선 도킹 센터를 사용하는 것이 편리할 것이다. 무선 도킹 센터는 예를 들어 그의 스크린 상에 (아마도 동적인) 공개 암호화 정보를 표시하거나, 예를 들어 그의 하우징 상에 인쇄된 정적인 공개 암호화 정보를 가질 수 있다.

[0115] 제안된 네트워크 시스템에서, 구성기가 피등록기의 대역외 공개 암호화 정보를 판독하는 대신, 피등록기가 구성기의 대역외 공개 암호화 정보를 판독한다. 많은 OOB 방법의 경우, OOB 정보가 판독되는 장치는 이 정보가 판독되는 것을 알 필요가 없음에 유의한다. 이것은 예를 들어 카메라, 스캐너 또는 인간에 의해 코드가 판독될 때, 장치에 대한 전기적 접속이 없는 NFC 태그가 판독되고 있을 때 등의 경우에 그러하다.

[0116] 선택적으로, 프로토콜의 무선 부분의 시작에서, 어느 장치가 다른 장치를 구성할지가 결정될 수 있다. 이는 장치들이 누가 누구를 구성할 것인지에 대한 협상을 수행함을 의미한다. 또한, 상호 구성이 이행될 수 있다. 프로토콜에 그러한 협상 단계를 추가하는 것은 간단한 방식으로 행해지는 경우에 (적어도) 2개 이상의 메시지를 추가할 것이다.

[0117] 피등록기가 예를 들어 네트워크 공개 키를 나타내는 구성기의 대역외 공개 암호화 정보를 판독하고, 프로토콜의 무선 부분을 개시하여서, 피등록기가 이제 프로토콜의 개시기인 것이 제안된다. 네트워크 공개 키는 "구성기 식별자 공개 키"로도 지칭될 수 있다.

[0118] 이어서, 피등록기는 아래에 설명되는 바와 같이 피등록기 공개 네트워크 액세스 암호화 정보(이후 제2 피등록기 공개 키라고 함) 내지 공유 키로 암호화된 추가의 정보를 포함하는 제1 메시지를 전송한다. 이것은 다른 당사자, 구성기 또는 응답기에게 프로토콜의 개시기를 구성하기로 되어 있다는 것을 지시한다. 그러한 액션을 통해, 응답기는 그가 관리하고 있는 네트워크에 대한 액세스를 개시기에 제공하기 위해 그가 서명해야 하는 공개 네트워크 액세스 암호화 정보를 갖는다.

[0119] 대안적으로 또는 추가적으로, 응답기가 그의 공개 네트워크 액세스 암호화 정보를 개시기로 전송하는 경우, 이것은 응답기가 또한 개시기에 의해 구성되기를 원한다는 것을 신호하는 데 사용될 수 있다.

[0120] 무선 기술들은 일반적으로 장치들이 다른 장치들로 하여금 그들이 무엇을 할 수 있는지를 무선으로 알게 할 수 있는 방법들을 지원한다. 그들은 예를 들어 그들의 능력들을 광고할 수 있는데, 즉 그들은 그들의 능력들을 갖는 특수 메시지를 방송한다. 그들은 예를 들어 발견 메시지들을 청취하고, 그들이 그들에게 의도된 것으로 생각하는 그러한 메시지의 수신시에 그들의 능력들에 대한 정보 및 아마도 다른 정보를 포함하는 메시지로 응답할 수 있다. 제안된 바와 같은 구성기 장치는 그가 제안된 보안 프로토콜에 따라 다른 장치들(피등록기들)을 구성할 수 있는 그의 능력 리스트를 가질 수 있으며, 이는 피등록기들이 OOB 공개 암호화 정보를 판독하고 스스로 구성되기를 요청할 것을 필요로 한다.

[0121] 프로토콜에 따라 협력하는 네트워크 장치들은 피등록기(또는 개시기) 및 구성기(또는 응답기)로 지칭되었다. 일반적으로, 어느 것이 다른 것을 구성할 것인지가 불확실한 경우, 다른 이름들이 사용될 수 있다. 제1 네트워크 액세스 메시지가 공개 네트워크 액세스 암호화 정보를 포함하는 경우, 송신기는 응답기 내의 구성기에 의해 구성되기를 원한다. 이어서, 응답기는 서명된 네트워크 액세스 정보를 전송한다. 속성과 같은 추가적의 등록 정보가 또한 제안된 프로토콜의 초기 메시지에 공개 네트워크 액세스 암호화 정보와 함께 포함될 수 있다.

[0122] 도 1은 네트워크 시스템을 도시한다. 네트워크 시스템은 영역 내의 네트워크 장치들 사이의 와이파이와 같은 무선 통신(150, 150')을 위해 배열되고, 아래에 설명되는 바와 같이 보안 프로토콜에 따른 보안 통신을 위해 배열된다. 프로토콜의 추가의 특정 태양들이 도 2 내지 5를 참조하여 설명된다.

[0123] 네트워크 시스템(100)은 다수의 네트워크 장치(110, 120, 130)를 포함하며, 각각의 네트워크 장치는 미리 정의된 통신 프로토콜들 및 보안 프로토콜들을 사용하여 네트워크를 통해 상호 작용할 수 있다. 네트워크는 예를 들어 근처에 있는 장치들에 네트워크 서비스들을 제공하기 위해 영역 내의 추가의 네트워크 장치들에 대한 액세스를 제공하도록 배열된다. 예를 들어, 네트워크 시스템은 액세스 포인트(AP)로서, 그 AP와 연관된 다른 네트워크 장치들, 예를 들어 AP와 링크 키를 셋업한 모바일 폰들 또는 랩탑들에 대한 결합 센터로서 동작하는, 상기 AP를 포함할 수 있다. 네트워크 장치들 서로 간의 그리고 다른 네트워크들, 예를 들어 기업 인트라넷 또는 인터넷과의 통신은 AP를 통해 진행될 수 있다. 장치들은 직접, 따라서 AP와 같은 장치들을 통하지 않고 통신하는 것이 가능할 수 있으며, 서로 링크 키들을 셋업하는 것이 가능할 수 있다.

[0124] 도면은 피등록기(110), 즉 상기 영역에서 네트워크에 참여하여 피등록기로서 동작하고자 하는 네트워크 장치를 도시한다. 도시된 바와 같은 피등록기는 미리 정의된 통신 프로토콜들 및 보안 프로토콜들에 따라 보안 통신을 이행하도록 배열된 피등록기 센서(113), 피등록기 프로세서(111) 및 피등록기 무선 통신 유닛(112)을 갖는다.

[0125] 도면은 구성기(130), 즉 구성기로서 동작하는 네트워크 시스템 내의 추가의 네트워크 장치를 도시한다. 이것은 별도의 네트워크 장치, 또는 액세스 포인트 또는 다른 네트워크 장치에 내장된 역할일 수 있다. 도시된 바와 같은 구성기는 구성기 프로세서(131) 및 구성기 통신 유닛(132)을 가지며, 이들 유닛은 후술하는 바와 같이 미리 정의된 통신 프로토콜들 및 보안 프로토콜들에 따라 피등록기와 통신하도록 배열된다. 구성기 통신 유닛은 무선 통신 유닛일 수 있다. 구성기 통신 유닛은 또한 어떤 다른 네트워크 채널을 통해 액세스 포인트에 통신할 수 있으며, 이어서 액세스 포인트는 피등록기와 무선 통신한다. 구성기가 아래에 설명되는 바와 같이 네트워크 시스템에 대한 액세스를 제어하는 것을 가능하게 하기 위해, 구성기는 구성기 공개 키 및 대응하는 구성기 비공개 키와 같은 다양한 증명서들을 갖는다.

[0126] 네트워크 시스템(100)은, 이미 네트워크의 일부이고 피등록기와의 보안 통신을 위해 이용 가능할 수 있는 적어도 하나의 추가의 네트워크 장치(120)를 포함할 수 있다. 추가의 장치는 미리 정의된 통신 프로토콜들 및 보안 프로토콜들에 따라 보안 통신을 이행하도록 배열된 추가의 장치 프로세서 및 추가의 무선 통신 유닛을 갖는다.

[0127] 피등록기는 네트워크에 대한 액세스를 획득하기 위해 보안 프로토콜에 따라 동작하도록 배열된다. 동작시에, 피등록기는, 피등록기 프로세서의 메모리에, 제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키를 가지며, 또한 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 갖는다. 구성기는 보안 프로토콜에 따라 피등록기에 대한 보안 통신을 가능하게 하도록 배열된다. 동작시, 구성기는, 구성기 프로세서의 메모리에, 구성기 장치에 대한 구성기 공개 키 및 대응하는 구성기 비공개 키 및, 네트워크 시스템에 대한, 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 갖는다.

[0128] 피등록기 센서 및 피등록기 프로세서는 도면에 점선 화살표(151)에 의해 지시되는 바와 같이 피등록기 센서(113)를 통해 데이터 패턴(140)을 획득하도록 배열된다. 데이터 패턴은 영역에서 제공되며 네트워크 공개 키를 나타낸다. 예를 들어, 데이터 패턴은 바코드 또는 QR 패턴일 수 있다. 센서를 통해 데이터 패턴을 획득하는 것은 대역외 채널(OOB)을 구성한다. 그러한 OOB 채널들 및 패턴들의 다양한 예들은 서론에서 논의되었다. 패턴을 획득하는 센서에 의해 구성되는 바와 같은 OOB는 한 방향으로 동작하는데, 즉 네트워크로부터 피등록기로의 정보를 획득한다. 피등록기 센서는 실제 시스템 셋업에서 사용되는 패턴을 검출하거나 수신할 수 있는 임의의 적합한 검출기 또는 수신기일 수 있는데, 이는 그러한 패턴이 여러 가지 방식으로 제공될 수 있기 때문이다. 이 패턴은 네트워크에 액세스하도록 잠재적으로 허용되는 다른 네트워크 장치들의 사용자들을 위해 의도되는 영역 내의 네트워크 시스템에 대해 제공된다. 영역은 사무실, 상점, 공공 장소, 비행장 등일 수 있다. 패턴은 예를 들어 QR 코드 또는 바코드일 수 있고, 대응하는 센서는 모바일 네트워크 장치의 카메라 또는 IR 빔 검출기이다. 패턴은 종이, 예를 들어 메뉴 또는 영수증 상에 제공될 수 있거나, 디스플레이 상에 또는 어떤 다른 물리적 형태로 나타내어질 수 있다. OOB 채널은 또한 네트워크 통신(대역내)이 와이파이에 기초하는 경우 NFC 또

는 블루투스일 수 있으며, 따라서 피등록기 센서는 블루투스 유닛 또는 NFC 태그 검출기이다. 따라서, 센서는 대역외 채널, 즉 네트워크의 무선 통신 기술 이외의 다른 기술을 이용하는 채널을 사용하여 데이터 패턴을 검출하기 위한 임의의 적합한 검출기 또는 수신기를 지칭한다.

[0129] 피등록기 프로세서는 네트워크 공개 키 및 제1 피등록기 비공개 키에 기초하여 제1 공유 키를 도출하도록 배열된다. 그렇기 때문에, 공개/비공개 키 쌍들을 사용하여 공유 키들을 도출하는 것은 알려져 있으며 서론에서 설명되었다. 피등록기 프로세서는 제1 공유 키를 사용하여 제2 피등록기 공개 키를 후속하여 인코딩하도록 배열된다. 이어서, 피등록기 프로세서는 보안 프로토콜에 따라 네트워크 액세스 요청을 생성한다. 네트워크 액세스 요청은 인코딩된 제2 피등록기 공개 키 및 제1 피등록기 공개 키를 포함한다. 피등록기 프로세서는 무선 통신을 통해 네트워크 액세스 요청을 구성기로 전송하도록 배열된다. 네트워크 액세스 요청 메시지 및 후속 메시지들은 IEEE 802.11(2012) [4]에 의해 정의된 바와 같은 소위 액션 프레임들 또는 자기 보호 액션 프레임들의 형태일 수 있다.

[0130] 구성기 프로세서(131)는, 구성기 통신 유닛(132)을 통해 직접 또는 액세스 포인트와 같은 네트워크 내의 어떤 다른 무선 수신기를 통해, 무선 통신을 통해 피등록기로부터 네트워크 액세스 요청을 수신하도록 배열된다. 구성기 프로세서는 또한 네트워크 비공개 키 및 제1 피등록기 공개 키에 기초하여 제1 공유 키를 도출한다. 구성기 프로세서는 예를 들어 제1 공유 키를 사용하여 미리 정의된 암호화 방법에 의해 인코딩된 데이터를 해독함으로써 제1 공유 키를 사용하여 인코딩된 제2 피등록기 공개 키를 후속 디코딩한다. 다음에, 구성기 프로세서는 인코딩된 제2 피등록기 공개 키가 제1 공유 키에 의해 인코딩되었는지를 암호화 방식으로 검증한다. 인코딩이 올바른 경우, 구성기 프로세서는 피등록기에 대해 네트워크에 대한 액세스를 허용하기로 결정하고, 제2 피등록기 공개 키 및 구성기 비공개 키를 사용하여 보안 데이터를 생성하기를 계속한다. 구성기 프로세서는 제1 피등록기 공개 키, 제2 피등록기 공개 키 및 네트워크 비공개 키에 기초하여 제2 공유 키를 도출한다. 다수의 키를 사용할 수 있는 방법이 앞서 서론에서 설명되었다. 다음에, 구성기 프로세서는 제2 공유 키를 사용하면서 보안 데이터 및 구성기 공개 키 중 적어도 하나를 암호화 방식으로 보호한다. 예를 들어, 보안 데이터로서, 서명이 계산될 수 있거나, 추가의 세션 키가 생성될 수 있다. 추가의 상세한 예들이 아래에서 논의된다. 이어서, 구성기 프로세서는 보안 프로토콜에 따라 네트워크 액세스 메시지를 생성한다. 네트워크 액세스 메시지는 암호화 방식으로 보호된 데이터, 즉 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나를 포함한다.

[0131] 구성기 역할은 적어도 2개의 키 쌍을 갖는다. 제1 쌍은 피등록기와의 제1 공유 비밀을 셋업하기 위한 것이다. 이 키는 시간에 따라 변할 수 있거나 일정할 수 있다. 제2 쌍은 피등록기의 제2 피등록기 공개 키(또는 공개 네트워크 키)에 서명하는 데 사용되는 키 쌍이며, 따라서 동일한 구성기에 의해 등록된 다른 장치들(또는 구성기를 대신하여 서명할 수 있는 장치)은 그들이 제2 피등록기 공개 키를 신뢰할 수 있고 그것을 링크 키를 도출하는 데 사용할 수 있음을 안다. 구성기의 가능한 제3 키 쌍을 사용하여 추가의 공유 비밀을 셋업할 수 있다. 이 제3 쌍은 일시적인 쌍(즉, 일회용의 임시 키 재료)일 것이다.

[0132] 구성기에 의해 서명된 자신들의 제2 피등록기 공개 키를 갖는 네트워크 내의 모든 장치들(또는 구성기를 대신하여 동작하는 장치들 중 하나)은 그들의 제2 공개 키들을 교환하고, 이들을 디피-헬먼 공유 키 도출 프로토콜, 예를 들어 IEEE 802.11(2012) [4]로부터의 4 방향 핸드셰이크에서 사용하여 그들의 미래 무선 통신을 보호하기 위한 링크 키를 도출할 수 있다. 이러한 서명된 공개 키들은 '서명된 네트워크 액세스 정보'로 지칭될 수 있다.

[0133] 피등록기 프로세서는 무선 통신을 통해 구성기로부터 네트워크 액세스 메시지를 수신하도록 추가로 배열된다. 그러한 메시지가 수신되면, 피등록기 프로세서는 다음과 같이 등록 프로세스를 진행한다. 피등록기 프로세서는 제1 피등록기 비공개 키, 제2 피등록기 비공개 키 및 네트워크 공개 키에 기초하여 제2 공유 키를 도출한다. 다음에, 피등록기 프로세서는 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나가 제2 공유 키에 의해 암호화 방식으로 보호되었는지를 검증한다. 인코딩이 올바르면, 피등록기 프로세서는 네트워크에 액세스하기로 결정하고, 그의 제2 피등록기 비공개 키 및 보안 데이터에 기초하여 보안 통신을 이행하기를 계속한다. 보안 통신은 구성기와의, 또는 네트워크 내의 다른 장치들과의 추가의 통신일 수 있다. 이제, 적절한 경우에 조합될 수 있는 실시예들의 다양한 예들이 논의된다.

[0134] 상기의 네트워크 시스템의 실시예에서, 피등록기 프로세서는 임시 피등록기 공개 키 및 대응하는 임시 피등록기 비공개 키를 생성하도록 배열되며, 이들 키는 제1 피등록기 공개 키 및 대응하는 제1 피등록기 비공개 키를 구성한다. 그러한 임시 키들은 예를 들어 서론에서 설명된 바와 같이 필요한 수의 무작위 비트를 생성하고, 비공개 키를 정의하고, 후속하여 대응하는 공개 키를 계산하는 무작위 데이터 생성기에 의해 생성될 수 있다. 그러

한 임시 키들의 사용은 보안을 향상시키는데, 이는 공격자들이 이전 세션들로부터의 어떠한 지식도 사용할 수 없기 때문이다.

[0135] 상기의 네트워크 시스템의 실시예에서, 피등록기 프로세서는 추가의 임시 피등록기 공개 키 및 대응하는 추가의 임시 피등록기 비공개 키를 생성하도록 배열되며, 이들 키는 제2 피등록기 공개 키 및 대응하는 제2 피등록기 비공개 키를 구성한다. 추가의 임시 피등록기 공개 및 비공개 키 쌍의 사용은 상이한 네트워크 장치들과의 보안 통신을 이행하기 위해 그러한 임시 키들을 사용할 때 보안을 더욱 향상시킨다.

[0136] 상기의 네트워크 시스템의 실시예에서, 구성기 프로세서는 임시 네트워크 공개 키 및 대응하는 임시 네트워크 비공개 키를 생성하도록 배열되며, 이들 키는 네트워크 공개 키 및 대응하는 네트워크 비공개 키를 구성한다. 임시 네트워크 공개 및 비공개 키 쌍의 사용은 구성기에 의해 그러한 임시 키들을 사용할 때 보안을 더욱 향상시킨다. 또한, 임시 네트워크 공개 키를 OOB 채널을 통해 이용 가능하게 하기 위해 대응하는 데이터 패턴이 생성되고 노출(예를 들어, 인쇄 또는 표시)되어야 한다.

[0137] 상기의 네트워크 시스템의 실시예에서, 보안 데이터는 구성기로부터의 허가 정보이고, 이 허가 정보는 피등록기가 네트워크에 액세스하는 것을 허가한다. 예를 들어, 허가 정보는 피등록기에 이미 알려진 데이터의 구성기에 의해 생성된 서명, 또는 구성기 또는 네트워크의 식별 데이터 및 하나 이상의 대응하는 서명을 포함하는 증명서와 같은 추가의 데이터, 및/또는 각자의 공개 키(들), 또는 (커넥터라고도 하는) 피등록기의 서명된 공개 키를 포함한다.

[0138] 상기의 네트워크 시스템의 실시예에서, 구성기 프로세서는 구성기 세션 키를 제공하고 구성기 세션 키를 피등록기로 전송함으로써 보안 데이터를 생성하도록 추가로 배열된다. 또한, 피등록기 프로세서는 구성기 세션 키를 수신하고 구성기 세션 키에 기초하여 보안 통신을 이행하도록 추가로 배열된다. 구성기 세션 키는 전송 중에 암호화에 의해 보호될 수 있다. 예를 들어, 구성기 세션 키는 그와 같이 알려진 와이파이 패스프레이즈일 수 있다. 실시예는 레거시 액세스 포인트의 와이파이 패스프레이즈를 본 발명에 따라 구현되는 피등록기로 전송할 수 있게 한다.

[0139] 상기의 네트워크 시스템의 실시예에서, 구성기 프로세서는 구성기 세션 공개 키 및 대응하는 구성기 세션 비공개 키를 생성하고, 구성기 세션 비공개 키 및 제2 피등록기 공개 키에 기초하여 제3 공유 키를 도출하고, 구성기 세션 공개 키를 피등록기로 전송함으로써 보안 데이터를 생성하도록 추가로 배열된다. 또한, 피등록기 프로세서는 구성기 세션 공개 키를 수신하고, 제2 피등록기 비공개 키 및 구성기 세션 공개 키에 기초하여 제3 공유 키를 도출하고, 제3 공유 키에 기초하여 보안 통신을 이행하도록 추가로 배열된다.

[0140] 선택적으로, 상기의 시스템에서, 피등록기 프로세서는 피등록기 세션 공개 키 및 대응하는 피등록기 세션 비공개 키를 생성하고, 피등록기 세션 비공개 키 및 구성기 공개 키에 기초하여 제4 공유 키를 도출하고, 피등록기 세션 공개 키를 구성기로 전송하도록 추가로 배열되며; 구성기 프로세서는 구성기 비공개 키 및 피등록기 세션 공개 키에 기초하여 제4 공유 키를 도출하고, 제4 공유 키에 기초하여 보안 통신을 이행하도록 추가로 배열된다.

[0141] 실시예에서, 상기의 네트워크 시스템은, 제2 피등록기 공개 키 및 보안 데이터를 수신하고, 세션 네트워크 공개 키 및 대응하는 세션 네트워크 비공개 키를 제공하도록 배열된 추가의 네트워크 장치를 포함한다. 추가의 네트워크 장치는 세션 네트워크 비공개 키 및 제2 피등록기 공개 키에 기초하여 제5 공유 키를 도출하고, 세션 네트워크 공개 키를 피등록기로 전송한다. 또한, 피등록기 프로세서는 세션 네트워크 공개 키를 수신하고, 제2 피등록기 비공개 키 및 세션 네트워크 공개 키에 기초하여 제5 공유 키를 도출하도록 추가로 배열된다. 다음에, 피등록기는 제5 공유 키에 기초하여 추가의 네트워크 장치와의 보안 통신을 이행할 수 있다.

[0142] 상기의 네트워크 시스템의 실시예에서, 구성기 프로세서는 구성기 비공개 키로 제2 피등록기 공개 키에 디지털 서명함으로써 디지털 서명을 포함하는 보안 데이터를 생성하고, 피등록기와 제3 장치 사이의 보안 통신을 가능하게 하기 위해 디지털 서명을 제3 장치 및/또는 피등록기로 전송하도록 추가로 배열된다. 유효한 서명은 서명이 장치에 신뢰를 제공하기 때문에 보안 통신을 가능하게 한다. 통신에 사용되는 키는 그와 같은 서명에 기초할 필요가 없다. 보안 통신은 키와 같은 여러 요소에, 그러나 또한 공개 키를 통한 서명에 기초할 수 있는데, 이는 서명된 공개 키를 수신하는 장치가 공개 키에 서명한 장치를 신뢰하므로 그러한 공개 키를 신뢰하고, 예를 들어 디피-헬먼을 사용하여 보안 채널을 셋업하기 위해 그것을 사용할 것이기 때문이다. 신뢰되는 서명자는 구성기일 수 있다.

[0143] 상기의 네트워크 시스템의 실시예에서, 구성기 프로세서는 제2 피등록기 공개 키 및 디지털 서명을 포함하는 추

가의 메시지를 생성하고, 추가의 메시지를 추가의 장치 및/또는 피등록기로 전송하도록 추가로 배열된다. 추가의 장치가 이제 구성기에 의해 제공되는 바와 같은 제2 피등록기 공개 키 및 디지털 서명을 가지므로, 피등록기와 추가의 장치 사이의 보안 통신이 가능해진다.

[0144] 상기의 네트워크 시스템의 실시예에서, 피등록기 프로세서는 디지털 서명을 수신하도록 추가로 배열된다. 피등록기 프로세서는, 디지털 서명 및 구성기 공개 키에 기초하여, 제2 피등록기 공개 키가 올바르게 서명되었는지를 암호화 방식으로 검증한다. 그렇다면, 피등록기는 의도된 구성기가 서명했음을 알고, 피등록기는, 제2 피등록기 비공개 키에 기초하여, 의도된 구성기를 통해 구성된 다른 네트워크 장치들과의 보안 통신을 이행할 수 있다.

[0145] 실시예에서, 상기의 네트워크 시스템은, 구성기 공개 키를 획득하고, 디지털 서명 및 제2 피등록기 공개 키를 수신하도록 배열된 추가의 네트워크 장치를 포함한다. 추가의 네트워크 장치는, 디지털 서명 및 구성기 공개 키에 기초하여, 제2 피등록기 공개 키가 올바르게 서명되었는지를 검증하고, 그렇다면, 제2 피등록기 공개 키에 기초하여 피등록기와의 보안 통신을 이행한다.

[0146] 상기의 네트워크 시스템의 실시예에서, 구성기 프로세서는, 구성기 비공개 키로, 추가의 네트워크 장치의 추가의 공개 키에 디지털 서명함으로써 추가의 디지털 서명을 포함하는 추가의 보안 데이터를 생성하도록 추가로 배열된다. 또한, 피등록기 프로세서는 추가의 공개 키 및 추가의 디지털 서명을 수신하고, 추가의 디지털 서명 및 구성기 공개 키에 기초하여, 추가의 공개 키가 올바르게 서명되었는지를 암호화 방식으로 검증함으로써 추가의 보안 데이터를 사용하도록 추가로 배열된다. 그렇다면, 피등록기는 제2 피등록기 비공개 키 및 추가의 공개 키를 사용하여 추가의 네트워크 장치와 보안 통신할 수 있다. 또한, 피등록기 프로세서는 구성기 또는 추가의 네트워크 장치로부터 추가의 공개 키 및 추가의 디지털 서명을 수신하도록 추가로 배열될 수 있다.

[0147] 상기의 네트워크 시스템의 실시예에서, 피등록기 프로세서는 피등록기 테스트 데이터를 생성하고, 제2 공유 키를 사용하여 피등록기 테스트 데이터를 인코딩하고, 인코딩된 피등록기 테스트 데이터를 구성기로 전송하도록 추가로 배열된다. 또한, 구성기 프로세서는 제2 공유 키를 사용하여 인코딩된 피등록기 테스트 데이터를 디코딩하고, 피등록기 테스트 데이터가 피등록기에서 제2 공유 키에 의해 인코딩되었는지를 암호화 방식으로 검증하도록 추가로 배열된다. 그러한 테스트 데이터는 피등록기를 구성기에 대해 허가하는 것으로 간주될 수 있다.

[0148] 상기의 네트워크 시스템의 실시예에서, 구성기 프로세서는 구성기 테스트 데이터를 생성하고, 제2 공유 키를 사용하여 구성기 테스트 데이터를 인코딩하고, 인코딩된 구성기 테스트 데이터를 피등록기로 전송하도록 추가로 배열된다. 또한, 피등록기 프로세서는 제2 공유 키를 사용하여 인코딩된 구성기 테스트 데이터를 디코딩하고, 구성기 테스트 데이터가 구성기에서 제2 공유 키에 의해 인코딩되었는지를 암호화 방식으로 검증하도록 추가로 배열된다. 그러한 테스트 데이터는 구성기를 피등록기에 대해 허가하는 것으로 간주될 수 있다.

[0149] 이하에서는 네트워크 시스템 및 보안 프로토콜들이 도 2 내지 도 5를 참조하여 상세하게 설명된다.

[0150] 도 2는 네트워크 시스템 및 보안 프로토콜의 제1 예를 도시한다. 도 1을 참조하여 전술한 시스템에 대응하는 시스템의 태양들은 여기서 반복되지 않는다. 피등록기(210)는 보안 프로토콜(200)에 따라 구성기(230)와 무선 통신하는 것으로 도시되어 있다. 둘 모두의 장치는 각자의 와이파이 유닛(240, 240')을 통해 통신하는 것으로 도시되어 있다.

[0151] 예에서, 보안 프로토콜은 2개의 메시지를 사용하여 인증을 제공한다. 제1 메시지는 다음 요소들: H(CI), EE, $\{E\text{-nonce, EN, E-Attributes}\}_{k1}$을 포함하는 네트워크 액세스 요청(250)이다.

[0152] 제2 메시지는 다음 요소들: H(CI), $\{E\text{-nonce, [C-name,] [C-sign-key,] SecurityData}\}_{k2}$를 갖는 네트워크 액세스 응답(260)이다.

[0153] 메시지에서, 다음 요소들이 주어진다:

[0154] 메시지 내의 H(CI)는 구성기 공개 키와 같은 구성기 식별 데이터에 대한 해시이고;

[0155] $\{Information\}_k$는 키 k로 암호화된 정보를 나타내고;

[0156] [Info]는 선택적인 정보를 나타내고;

[0157] 메시지 내의 EE는 제1 피등록기 공개 키이고;

[0158] 제1 메시지 내의 EN은 제2 피등록기 공개 키이고;

[0159] E-attributes는 필요한 네트워크 액세스를 정의하는 데이터이고;

[0160] K_1은 네트워크 공개 키 및 제1 피등록기 비공개 키에 기초하는 제1 공유 키이고;

[0161] K_2는 제1 피등록기 공개 키, 제2 피등록기 공개 키 및 네트워크 비공개 키에 기초하는 제2 공유 키이고;

[0162] E-nonce는 피등록기에 의해 제공된 논스이고;

[0163] C-name은 구성기에 의해 제공된 이름이고;

[0164] C-sign-key는 공개 서명 키 또는 구성기 공개 서명 키 자체의 구성기 참조이고;

[0165] SecurityData는 피등록기의 서명된 공개 키(EN), 와이파이 패스프레이즈 등일 수 있다.

[0166] H(CI)는, 구성기 공개 키를 세상의 나머지가 이용할 수 있게 함이 없이, 이 메시지가 구성기를 위한 것이라는 지시자로서 사용된다. 다른 메시지들 내의 H(CI)는 메시지들을 링크하는 간단한 방식으로서 사용된다. 메시지들 내의 논스들의 반복이 또한, 그러나 이제는 암호화 방식으로 보호되는 방식으로, 메시지들을 링크하기 위한 것인데, 이는 어떤 장치도 H(CI)로 시작하는 메시지로 응답할 수 있기 때문이다.

[0167] 제2 메시지는 구성기 이름(C-name), 서명 키의 구성기 참조(C-sign-key) 및 SecurityData로 구성될 수 있는 증명서를 포함할 수 있다. SecurityData는 구성기에 의해 서명될 수 있다. 피등록기의 공개 키(EN)는 SecurityData 내에 있을 수 있다.

[0168] 도 3은 네트워크 시스템 및 보안 프로토콜의 제2 예를 도시한다. 도 2를 참조하여 전술한 시스템에 대응하는 프로토콜의 태양들은 여기서 반복되지 않는다. 예에서, 보안 프로토콜(300)은 4개의 메시지를 사용하여 인증을 제공한다. 프로토콜은 위의 프로토콜(200)에 비해 더 안전한 인증을 위해 2개의 추가 메시지로 인증을 제공한다.

[0169] 제1 메시지는 다음 요소들: H(CI), EE, $\{E\text{-nonce}, EN\}_{k1}$을 포함하는 네트워크 액세스 요청(351)이다.

[0170] 제2 메시지는 인증 응답(352)이고, 다음의 요소들: H(CI), $\{C\text{-nonce} \mid E\text{-nonce}\}_{k1}$, $\{C\text{-testdata}\}_{k2}$를 포함한다.

[0171] 제3 메시지는 인증 확인(353)이며, 다음 요소들: H(CI), $\{E\text{-testdata}, E\text{-Attributes}\}_{k2}$를 포함한다.

[0172] 제4 메시지는 네트워크 액세스 응답(354)이고, 다음 요소들: H(CI), {[C-name,] [C-sign-key,] SecurityData}$_{k2}$를 포함한다.

[0173] 예시적인 실시예에서, 요소들은 다음과 같이 명명된다:

[0174] - 구성기(230)

[0175] - 구성기 공개 암호화 정보(CI)

[0176] - 구성기 비공개 암호화 정보(CIpr)

[0177] - 제1 허가 정보(C-testdata)

[0178] - 암호화된 제1 허가 정보({C-testdata})

[0179] - 제2 허가 정보(E-testdata)

[0180] - 암호화된 제2 허가 정보({E-testdata})

[0181] - 무선 출력 수단(240')

[0182] - 피등록기(210)

[0183] - 입력 수단(113)

[0184] - 피등록기 공개 네트워크 액세스 암호화 정보(EN)

[0185] - 피등록기 비공개 네트워크 액세스 암호화 정보(ENpr)

[0186] - 암호화된 피등록기 공개 네트워크 액세스 암호화 정보({EN})

[0187] - 피등록기 공개 임시 암호화 정보(EE)

[0188] - 피등록기 비공개 임시 암호화 정보(EEpr)

[0189] - 제2 피등록기(120)

[0190] - 제1의 서명된 네트워크 액세스 정보(SecurityData)

[0191] - 제1 공유 키(k1)

[0192] - 제2 공유 키(k2)

[0193] - 제2의 서명된 네트워크 액세스 정보(SecurityData2)

[0194] - 무선 통신(150, 150)

[0195] 네트워크 시스템의 예시적인 실시예에서, 프로토콜은 다음과 같이 진행한다. 무선 통신 시스템은 적어도 하나의 구성기(230) 및 적어도 하나의 피등록기(210)를 갖는다. 구성기(230) 및 피등록기(210)는 무선 통신을 통해 통신하도록 배열된다. 피등록기(210)는 구성기 공개 암호화 정보(CI)를 판독하거나 입력하기 위해 무선 통신 이외의 기술을 사용하는 피등록기 프로세서(112) 및 입력 수단(113)을 포함한다. 피등록기는 또한 피등록기 공개 네트워크 액세스 암호화 정보(EN) 및 관련 피등록기 비공개 네트워크 액세스 암호화 정보(ENpr)를 갖는다. 피등록기 프로세서는

[0196] o 피등록기 공개 임시 암호화 정보(EE) 및 관련 피등록기 비공개 임시 암호화 정보(EEpr)를 생성하고,

[0197] o 적어도 구성기 공개 암호화 정보(CI) 및 피등록기 비공개 임시 암호화 정보(EEpr)를 사용하여 제1 공유 키(k1)를 계산하고,

[0198] o 제1 공유 키(k1)로 피등록기 공개 네트워크 액세스 암호화 정보(EN)를 암호화하여, 암호화된 피등록기 공개 네트워크 액세스 암호화 정보({EN})를 형성하고,

[0199] o 암호화된 피등록기 공개 네트워크 액세스 암호화 정보({EN})와 함께 피등록기 공개 임시 암호화 정보(EE)를 무선 통신을 통해 구성기(230)로 전송하도록 배열된다.

[0200] 피등록기의 공개 네트워크 키(EN)를 전송하는 것은 프로토콜의 개시기가 응답 파트너의 네트워크에서 등록되기를 원하는 피등록기이고, 프로토콜의 개시기가 프로토콜의 개시기에 의해 관리되는 네트워크들 중 하나에서 응답기를 피등록기로서 구성하기를 원하는 구성기로서 동작하지 않는다는 것을 의미한다는 점에 유의한다.

[0201] 후속하여, 피등록기 프로세서는, 추가의 메시지에서,

[0202] o 구성기(230)로부터 암호화된 제1 허가 정보({C-testdata})를 무선 통신을 통해 수신하고,

[0203] o 적어도 구성기 공개 암호화 정보(CI), 피등록기 비공개 임시 암호화 정보(EEpr) 및 피등록기 비공개 네트워크 액세스 암호화 정보(ENpr)를 사용하여 제2 공유 키(k2)를 계산하고,

[0204] o 구성기(230)로부터 암호화된 제1 허가 정보({C-testdata})를 해독하여 제1 허가 정보(C-testdata)를 획득하고,

[0205] o 제1 허가 정보(C-testdata)를 획득하기 위한 프로세스가 에러를 검출한 경우에 절차를 중지하도록 배열될 수 있다.

[0206] 후속하여, 피등록기 프로세서는, 다음 메시지에서,

[0207] o 제2 허가 정보(E-testdata)를 생성하고,

[0208] o 제2 공유 키(k2)로 제2 허가 정보(E-testdata)를 암호화하여, 암호화된 제2 허가 정보({E-testdata})를 형성하고,

[0209] o 암호화된 제2 허가 정보({E-testdata})를 무선 통신을 통해 구성기(230)로 전송하도록 배열될 수 있다.

[0210] 후속하여, 피등록기 프로세서는, 동일한 또는 추가의 메시지에서,

[0211] o 암호화된 필요한 구성 정보({E-attributes})를 무선 통신을 통해 구성기(230)로 전송하도록 배열될 수 있다.

[0212] 후속하여, 피등록기 프로세서는, 다음 메시지에서,

[0213] o 구성기(230)로부터 제1의 서명된 네트워크 액세스 정보(SecurityData)를 무선 통신을 통해 수신하고,

[0214] o 제1의 서명된 네트워크 액세스 정보(SecurityData)가 올바르게 서명되지 않은 경우에 절차를 중지하도록 배열될 수 있다.

[0215] 마지막으로, 피등록기 프로세서는, 추가의 메시지에서,

[0216] o 제2 피등록기(120)로부터 제2의 서명된 네트워크 액세스 정보(SecurityData2)를 수신하고,

[0217] o 제1의 서명된 네트워크 액세스 정보(SecurityData) 및 제2의 서명된 네트워크 액세스 정보(SecurityData2) 및 아마도 또한 그의 비공개 네트워크 액세스 암호화 정보(ENpr)를 사용하여 제2 피등록기(120)와의 보안 통신을 셋업하도록 배열될 수 있다.

[0218] 네트워크 시스템의 예시적인 실시예에서, 구성기(230)는 구성기 프로세서(131)를 포함한다. 구성기(230)는 구성기 공개 암호화 정보(CI) 및 관련 구성기 비공개 암호화 정보(CIpr)를 추가로 갖는다. 구성기는 무선 통신 이외의 기술을 사용하여 구성기 공개 암호화 정보(CI)를 출력 또는 표시하기 위한 출력 수단, 예를 들어 디스플레이를 가질 수 있다. 구성기 프로세서는

[0219] o 무선 통신을 통해 피등록기(210)로부터 암호화된 피등록기 공개 네트워크 액세스 암호화 정보({EN})와 함께 피등록기 공개 임시 암호화 정보(EE)를 수신하고,

[0220] o 적어도 구성기 비공개 암호화 정보(CIpr) 및 피등록기 공개 임시 암호화 정보(EE)를 사용하여 제1 공유 키(k1)를 계산하고,

[0221] o 암호화된 피등록기 공개 네트워크 액세스 암호화 정보({EN})를 제1 공유 키(k1)로 해독하여 피등록기 공개 네트워크 액세스 암호화 정보(EN)를 획득하고,

[0222] o 피등록기 공개 네트워크 액세스 암호화 정보(EN)를 획득하기 위한 프로세스가 에러를 검출한 경우에 절차를 중단하고,

[0223] o 제1 허가 정보(C-testdata)를 생성하고,

[0224] o 적어도 구성기 비공개 암호화 정보(CIpr), 피등록기 공개 임시 암호화 정보(EE) 및 피등록기 공개 네트워크 액세스 암호화 정보(EN)를 사용하여 제2 공유 키(k2)를 계산하고,

[0225] o 제1 허가 정보(C-testdata)를 암호화하여 암호화된 제1 허가 정보({C-testdata})를 형성하고,

[0226] o 암호화된 제1 허가 정보({C-testdata})를 무선 통신을 통해 피등록기(210)로 전송하도록 배열된다.

[0227] 후속하여, 구성기 프로세서는, 추가의 메시지에서,

[0228] o 무선 통신을 통해 피등록기(210)로부터 암호화된 제2 허가 정보({E-testdata})를 수신하고,

[0229] o 제2 공유 키(k2)로 암호화된 제2 허가 정보({E-testdata})를 해독하여 제2 허가 정보(E-testdata)를 획득하고,

[0230] o 제2 허가 정보(E-testdata)를 획득하기 위한 프로세스가 에러를 검출한 경우에 절차를 중지하도록 배열될 수 있다.

[0231] 후속하여, 구성기 프로세서는, 추가의 메시지에서,

[0232] o 피등록기 공개 네트워크 액세스 암호화 정보(EN)를 디지털 서명하고,

[0233] o 디지털 서명된 피등록기 공개 네트워크 액세스 암호화 정보(EN)를 사용하여 제1의 서명된 네트워크 액세스 정보(SecurityData)를 형성하고,

[0234] o 무선 통신을 통해 제1의 서명된 네트워크 액세스 정보(SecurityData)를 피등록기(210)로 전송하도록 배열될 수 있다.

[0235] 다양한 논스들(C-nonce, E-nonce)이 생성되고 메시지들 및/또는 그러한 메시지들의 암호화된 부분들에 추가되어 메시지들을 고유하게 만들 수 있다는 점에 유의한다.

[0236] 도 4는 네트워크 시스템 및 보안 프로토콜의 제3 예를 도시한다. 도 3을 참조하여 전술한 시스템에 대응하는

프로토콜의 태양들은 여기서 반복되지 않는다. 예에서, 보안 프로토콜(400)은 5개의 메시지를 사용하여 인증을 제공한다. 프로토콜은 위의 프로토콜들에 비하여 분리된 메시지들에서 인증 및 네트워크 액세스 프로비저닝 부분들을 제공한다.

[0237] 제1 메시지는 다음 요소들: H(CI), EE, $\{E\text{-nonce}, EN\}_{k1}$을 포함하는 네트워크 액세스 요청(451)이다.

[0238] 제2 메시지는 인증 응답(452)이며, 다음의 요소들: H(CI), $\{C\text{-nonce} \mid E\text{-nonce}\}_{k1}$, $\{C\text{-testdata}\}_{k2}$를 포함한다.

[0239] 제3 메시지는 인증 확인(453)이며, 다음 요소들: H(CI), $\{E\text{-testdata}\}_{k2}$를 포함한다.

[0240] 제4 메시지는 네트워크 액세스 정보(454)이며, 다음 요소들: H(CI), $\{E\text{-Attributes}\}_{k2}$를 포함한다.

[0241] 제5 메시지는 네트워크 액세스 응답(455)이며, 다음 요소들:

[0242] H(CI), $\{[C\text{-name},] [C\text{-sign-key},] SecurityData\}_{k2}$를 포함한다.

[0243] 처음 3개의 메시지는 인증을 제공하며, 여기서 네 번째 및 다섯 번째 메시지는 네트워크 액세스 프로비저닝을 제공한다.

[0244] 도 5는 네트워크 시스템 및 보안 프로토콜의 제4 예를 도시한다. 도 2를 참조하여 전술한 시스템에 대응하는 프로토콜의 태양들은 여기서 반복되지 않는다. 네트워크 장치 NDEV(510)는 액세스 포인트 AP(530)와 통신한다. 예에서, 보안 프로토콜(500)은 공개 키들에 기초하여 네트워크 액세스를 제공한다. 프로토콜은 SecurityData에 포함된 서명된 공개 키들을 교환하고, 디피-헬먼을 사용하는 4 방향 핸드셰이크를 위해 쌍 마스터 키(PMK), 예를 들어 IEEE 802.11i-2004 프로토콜에서 사용되는 공유 비밀 키를 계속하여 도출한다.

[0245] 제1 메시지(551)는 다음 요소들:

[0246] 네트워크 장치의 서명된 공개 키를 포함하는 SecurityData를 포함한다.

[0247] 제2 메시지(552)는 다음 요소들:

[0248] 액세스 포인트의 서명된 공개 키를 포함하는 SecurityData를 포함한다.

[0249] 추가의 메시지 시퀀스(553)는 4 방향 핸드셰이크 및 WPA2 보안 와이파이 통신을 제공한다. 와이파이 보호 액세스(WPA) 및 와이파이 보호 액세스 II(WPA2)는 무선 컴퓨터 네트워크들을 보호하기 위해 와이파이 동맹에 의해 개발된 2개의 보안 프로토콜 및 보안 증명 프로그램이다. 동맹은 연구자들이 이전 시스템인 유선 등가 프라이버시(WEP)에서 발견한 심각한 약점에 응답하여 이들을 정의했다. WPA(때때로 IEEE 802.11i 표준 초안이라고 함)는 2003년에 이용 가능하게 되었다. 와이파이 동맹은 더 안전하고 복잡한 WPA2의 가용성을 예측하여 그것을 중간 수단으로서 의도했다. WPA2는 2004년에 이용 가능하게 되었으며, 전체 IEEE 802.11i(또는 IEEE 802.11i-2004) 표준에 대한 일반적인 속기이며; IEEE 802.11(2012)은 IEEE 802.11i를 통합했다.

[0250] 도 6은 네트워크 시스템 및 보안 프로토콜의 제5 예를 도시한다. 도 5를 참조하여 전술한 시스템에 대응하는 프로토콜의 태양들은 여기서 반복되지 않는다. 예에서, 보안 프로토콜(600)은 와이파이 패스프레이즈에 기초하여 네트워크 액세스를 제공한다. 프로토콜은 SecurityData 내의 와이파이 패스프레이즈로부터 4 방향 핸드셰이크에 대한 PMK를 도출한다.

[0251] 메시지 시퀀스(651)는 다음을 제공한다: 4 방향 핸드셰이크 및 WPA2 보안 와이파이 통신.

[0252] 도 7은 피등록기 방법의 예를 도시한다. 방법은 전술한 바와 같이 네트워크 시스템에서 피등록기로서 동작하는 네트워크 장치에서 사용하기 위한 것이다. 방법은 노드 시작(701)에서 시작하고, 제1 스테이지 ACQP(702)로서, 피등록기 센서에 의해 대역외 채널을 통해 데이터 패턴을 획득하는 단계를 포함한다. 데이터 패턴은 영역에서 제공되며 네트워크 공개 키를 나타낸다. 다음 스테이지 D_E_K1(703)에서, 제1 공유 키가 네트워크 공개 키 및 제1 피등록기 비공개 키에 기초하여 도출되고, 제2 피등록기 공개 키는 제1 공유 키를 사용하여 인코딩된다. 다음 스테이지 G_NAR(704)에서, 보안 프로토콜에 따라 네트워크 액세스 요청이 생성된다. 네트워크 액세스 요청은 인코딩된 제2 피등록기 공개 키 및 제1 피등록기 공개 키를 포함한다. 네트워크 액세스 요청은 무선 통신을 통해 구성기로 전송된다. 다음 스테이지 R_NAM(705)에서, 네트워크 액세스 메시지가 무선 통신을 통해 구성기로부터 수신된다. 다음 스테이지 DV_K2(706)에서, 제2 공유 키가 제1 피등록기 비공개 키, 제2 피등록기 비공개 키 및 네트워크 공개 키에 기초하여 도출된다. 또한, 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나가 제2 공유 키에 의해 암호화 방식으로 보호되었는지가 검증된다. 보호가 올바르지 않으면, 방법

은 시작(701)로 돌아간다. 올바른 경우, 다음 스테이지 EN_SEC(707)에서, 제2 피등록기 비공개 키 및 보안 데이터에 기초하여 보안 통신이 이행된다. 방법은 노드 종료(708)에서 종료한다.

[0253] 도 8은 구성기 방법의 예를 도시한다. 방법은 전술한 바와 같이 네트워크 시스템에서 구성기로서 동작하는 네트워크 장치에서 사용하기 위한 것이다. 방법은 노드 시작(801)에서 시작하고, 제1 스테이지 R_NAR(802)로서, 무선 통신을 통해 피등록기로부터 네트워크 액세스 요청을 수신하는 단계를 포함한다. 다음 스테이지 D_D_K1(803)에서, 제1 공유 키가 네트워크 비공개 키 및 제1 피등록기 공개 키에 기초하여 도출된다. 또한, 인코딩된 제2 피등록기 공개 키가 제1 공유 키를 사용하여 디코딩된다. 다음 스테이지 V_K1(804)에서, 인코딩된 제2 피등록기 공개 키가 제1 공유 키에 의해 인코딩되었는지가 검증된다. 보호가 올바르지 않으면, 방법은 시작(801)로 돌아간다. 올바른 경우, 다음 스테이지 GSD(805)에서, 제2 피등록기 공개 키 및 구성기 비공개 키를 사용하여 보안 데이터가 생성된다. 다음 스테이지 D_P_K2(806)에서, 제2 공유 키가 제1 피등록기 공개 키, 제2 피등록기 공개 키 및 네트워크 비공개 키에 기초하여 도출된다. 또한, 보안 데이터 및 구성기 공개 키 중 적어도 하나가 제2 공유 키를 사용하여 암호화 방식으로 보호된다. 이어서, 다음 스테이지 G_NAM(807)에서, 보안 프로토콜에 따라 네트워크 액세스 메시지가 생성된다. 네트워크 액세스 메시지는 보호된 보안 데이터 및 보호된 구성기 공개 키 중 적어도 하나를 포함한다. 방법은 노드 종료(808)에서 종료한다.

[0254] 네트워크로부터 다운로드 가능하고/하거나 컴퓨터 판독 가능 매체 및/또는 마이크로프로세서 실행 가능 매체에 저장된 컴퓨터 프로그램 제품들이 제공되며, 컴퓨터 프로그램 제품들은 아래에 추가로 설명되는 바와 같이 위치 정보를 보호하기 위해 컴퓨터 상에서 실행될 때 상기의 방법들을 구현하기 위한 프로그램 코드 명령어들을 포함한다.

[0255] 전형적으로, 각각의 네트워크는 장치들에 저장된 적절한 소프트웨어를 실행하는 프로세서를 포함하며; 예를 들어 그러한 소프트웨어는 대응하는 메모리, 예를 들어 RAM과 같은 휘발성 메모리 또는 플래시(도시되지 않음)와 같은 비휘발성 메모리에 다운로드 및/또는 저장되었을 수 있다. 모바일 장치 및 서버들은 예를 들어 마이크로프로세서들 및 메모리들(도시되지 않음)을 구비할 수 있다. 대안적으로, 피등록기 및 구성기는. 전체적으로 또는 부분적으로. 프로그래머블 로직에서, 예를 들어 필드 프로그래머블 게이트 어레이(FPGA)로서 구현될 수 있다. 모바일 장치 및 서버들은, 전체적으로 또는 부분적으로, 소위 주문형 집적 회로(ASIC), 즉 그들의 특정 용도에 대해 맞춤화된 집적 회로(IC)로서 구현될 수 있다. 예를 들어, 회로들은 예를 들어 Verilog, VHDL 등과 같은 하드웨어 기술 언어를 사용하여 CMOS로 구현될 수 있다. 실제로, 위치 엔진은 모바일 장치의 운영 체제에 링크된 소프트웨어 서브루틴들의 라이브러리를 통해 구현될 수 있다.

[0256] 당업자에게 명백할 바와 같이, 방법을 실행하는 많은 상이한 방법이 가능하다. 예를 들어, 스테이지들 또는 단계들의 순서가 변경될 수 있거나, 몇몇 스테이지들이 병렬로 실행될 수 있다. 또한, 단계들 사이에 다른 방법 단계들이 삽입될 수 있다. 삽입된 단계들은 여기에 설명된 것과 같은 방법의 개선을 나타낼 수 있거나, 방법과 무관할 수 있다. 또한, 주어진 단계가 다음 단계가 시작되기 전에 완전히 종료되지 않았을 수 있다.

[0257] 본 발명에 따른 방법은 프로세서 시스템으로 하여금 각자의 방법을 수행하게 하기 위한 명령어들을 포함하는 소프트웨어를 사용하여 실행될 수 있다. 소프트웨어는 시스템의 특정 서브엔티티에 의해 취해지는 그러한 단계들만을 포함할 수 있다. 소프트웨어는 하드 디스크, 플로피, 메모리 등과 같은 적합한 저장 매체에 저장될 수 있다. 소프트웨어는 유선 또는 무선을 통해 또는 데이터 네트워크, 예를 들어 인터넷을 사용하여 신호로서 전송될 수 있다. 소프트웨어는 다운로드 및/또는 서버 상의 원격 사용이 가능하게 될 수 있다. 소프트웨어는 소스 코드, 객체 코드, 부분적으로 컴파일된 형태와 같은 코드 중간 소스 및 객체 코드의 형태, 또는 본 발명에 따른 방법의 구현에 사용하기에 적합한 임의의 다른 형태일 수 있다는 것이 인식될 것이다. 컴퓨터 프로그램 제품에 관한 실시예는 설명된 방법들 중 적어도 하나의 처리 단계들 각각에 대응하는 컴퓨터 실행 가능 명령어들을 포함한다. 이러한 명령어들은 서브루틴들로 세분되고/되거나, 정적 또는 동적으로 링크될 수 있는 하나 이상의 파일에 저장될 수 있다. 컴퓨터 프로그램 제품에 관한 다른 실시예는 설명된 시스템들 및/또는 제품들 중 적어도 하나의 수단들 각각에 대응하는 컴퓨터 실행 가능 명령어들을 포함한다.

[0258] 도 9a는 컴퓨터 프로그램(1020)을 포함하는 기입 가능 부분(1010)을 갖는 컴퓨터 판독 가능 매체(1000)를 도시하며, 컴퓨터 프로그램(1020)은 프로세서 시스템으로 하여금 도 2 내지 도 8을 참조하여 설명된 바와 같은 제공자 서버 방법, 위치 서버 방법, 위치 엔진 방법 또는 위치 기반 응용 방법의 실시예에 따라 위치 정보를 보호하기 위해 시스템에서 하나 이상의 방법을 수행하게 하기 위한 명령어들을 포함한다. 컴퓨터 프로그램(1020)은 물리적 마크들로서 또는 컴퓨터 판독 가능 매체(1000)의 자화에 의해 컴퓨터 판독 가능 매체(1000) 상에 구현될 수 있다. 그러나, 임의의 다른 적합한 실시예가 또한 구상될 수 있다. 또한, 컴퓨터 판독 가능 매체(1000)가

광학 디스크로서 여기에 도시되지만, 컴퓨터 판독 가능 매체(1000)는 하드 디스크, 고체 상태 메모리, 플래시 메모리 등과 같은 임의의 적합한 컴퓨터 판독 가능 매체일 수 있고, 기록 불가 또는 기록 가능할 수 있다는 것이 인식될 것이다. 컴퓨터 프로그램(1020)은 프로세서 시스템으로 하여금 상기 방법들을 수행하게 하기 위한 명령어들을 포함한다.

[0259] 도 9b는 제공자 서버, 위치 서버 또는 모바일 장치의 실시예에 따른 프로세서 시스템(1100)의 개략도를 도시한다. 프로세서 시스템은 하나 이상의 집적 회로(1110)를 포함한다. 하나 이상의 집적 회로(1110)의 아키텍처가 도면에 개략적으로 도시되어 있다. 회로(1110)는 실시예에 따른 방법을 실행하고/하거나 그의 모듈들 또는 유닛들을 구현하기 위해 컴퓨터 프로그램 컴포넌트들을 실행하기 위한 처리 유닛(1120), 예를 들어 CPU를 포함한다. 회로(1110)는 프로그래밍 코드, 데이터 등을 저장하기 위한 메모리(1122)를 포함한다. 메모리(1122)의 일부는 판독 전용일 수 있다. 회로(1110)는 통신 요소(1126), 예를 들어, 안테나, 커넥터 또는 이들 둘 모두 등을 포함할 수 있다. 회로(1110)는 방법에서 정의되는 처리의 일부 또는 전부를 수행하기 위한 전용 집적 회로(1124)를 포함할 수 있다. 프로세서(1120), 메모리(1122), 전용 IC(1124) 및 통신 요소(1126)는 인터커넥트(1130), 예를 들어 버스를 통해 서로 접속될 수 있다. 프로세서 시스템(1110)은 각각 안테나 및/또는 커넥터를 사용하여 접촉 및/또는 무접촉 통신을 위해 배열될 수 있다.

[0260] 명료함을 위해, 위의 설명은 상이한 기능 유닛들 및 프로세서들을 참조하여 본 발명의 실시예들을 설명하였음을 알 것이다. 그러나, 본 발명으로부터 벗어남이 없이 상이한 기능 유닛들 또는 프로세서들 간의 기능의 임의의 적합한 분산이 사용될 수 있음이 명백할 것이다. 예를 들어, 별개의 유닛들, 프로세서들 또는 제어기들에 의해 수행되도록 예시된 기능이 동일한 프로세서 또는 제어기에 의해 수행될 수 있다. 따라서, 특정 기능 유닛들에 대한 참조들은 오로지 엄격한 논리적 또는 물리적 구조 또는 조직을 나타내기보다는 설명된 기능을 제공하기 위한 적합한 수단에 대한 참조들로 간주되어야 한다. 본 발명은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 조합을 포함한 임의의 적합한 형태로 구현될 수 있다.

[0261] 이 문서에서 단어 '포함하는'은 열거된 것들 이외의 요소들 또는 단계들의 존재를 배제하지 않고, 요소에 선행하는 단어 'a' 또는 'an'은 복수의 그러한 요소의 존재를 배제하지 않으며, 임의의 도면 부호는 청구항들의 범위를 제한하지 않고, 본 발명은 하드웨어 및 소프트웨어 둘 모두에 의해 구현될 수 있으며, 여러 개의 '수단' 또는 '유닛'이 하드웨어 또는 소프트웨어의 동일한 아이템에 의해 표현될 수 있고, 프로세서는 아마도 하드웨어 요소들과 협력하여 하나 이상의 유닛의 기능을 수행할 수 있다는 점에 유의한다. 또한, 본 발명은 실시예들로 제한되지 않으며, 본 발명은 위에서 설명되거나 서로 상이한 종속 청구항들에 기재된 각각의 그리고 모든 신규한 특징 또는 특징들의 조합에 존재한다.

[0262] 참고 문헌들:

[0263] [1] Wi-Fi Simple Configuration Technical Specification Version 2.0.5, Wi-Fi Alliance 2014-08-04; https://www.wi-fi.org/file/wi-fi-simple-configuration-technical-specification-v205로부터 입수 가능

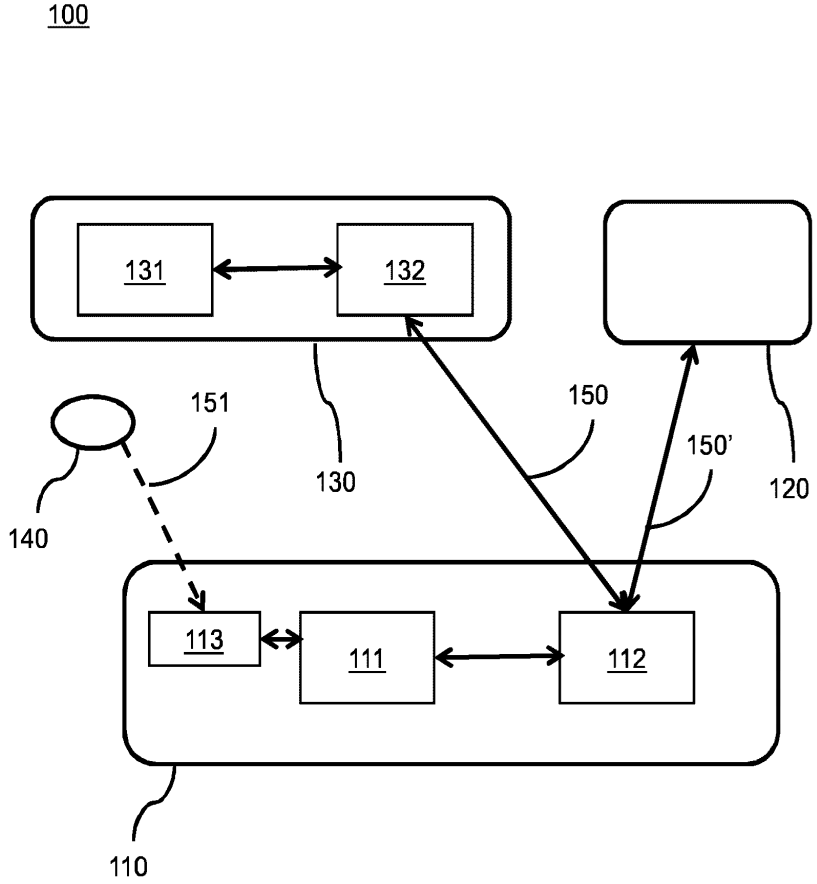
[0264] [2] RFC 5297, Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)

[0265] [3] DTLS-HIMMO: Efficiently Securing a PQ world with a fully-collusion resistant KPS, Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen, Jose Luis Torre-Arce; http://csrc.nist.gov/groups/ST/post-quantum-2015/presentations/session7-garcia-morchon.pdf

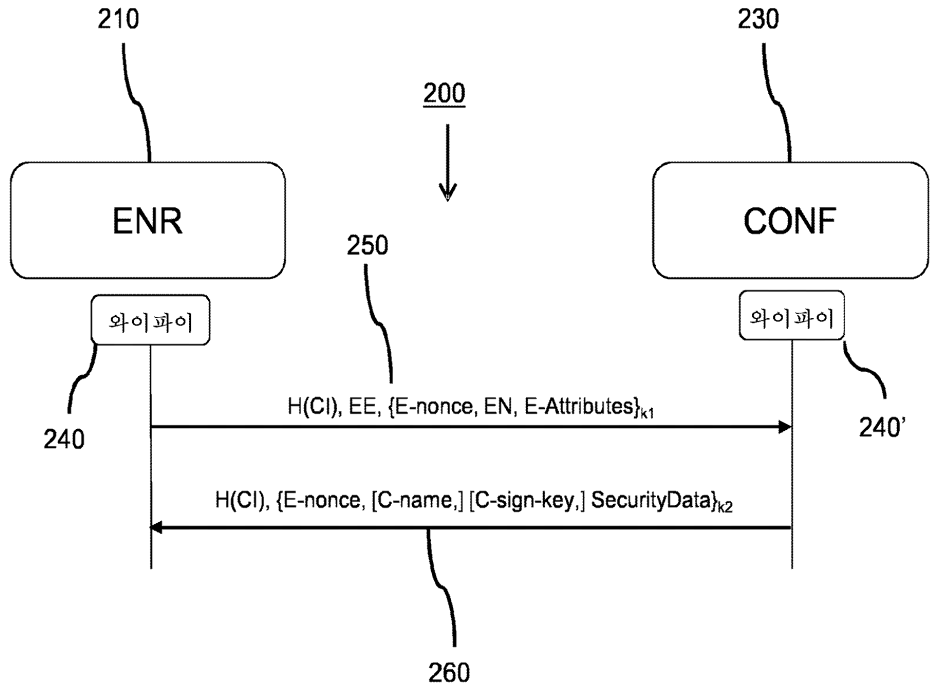
[0266] [4] IEEE Computer Society, "IEEE Standard for Information Technology— Telecommunications and Information Exchange Between Systems — Local and Metropolitan Area Networks — Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," (IEEE Std. 802.11-2012), March 2012

도면

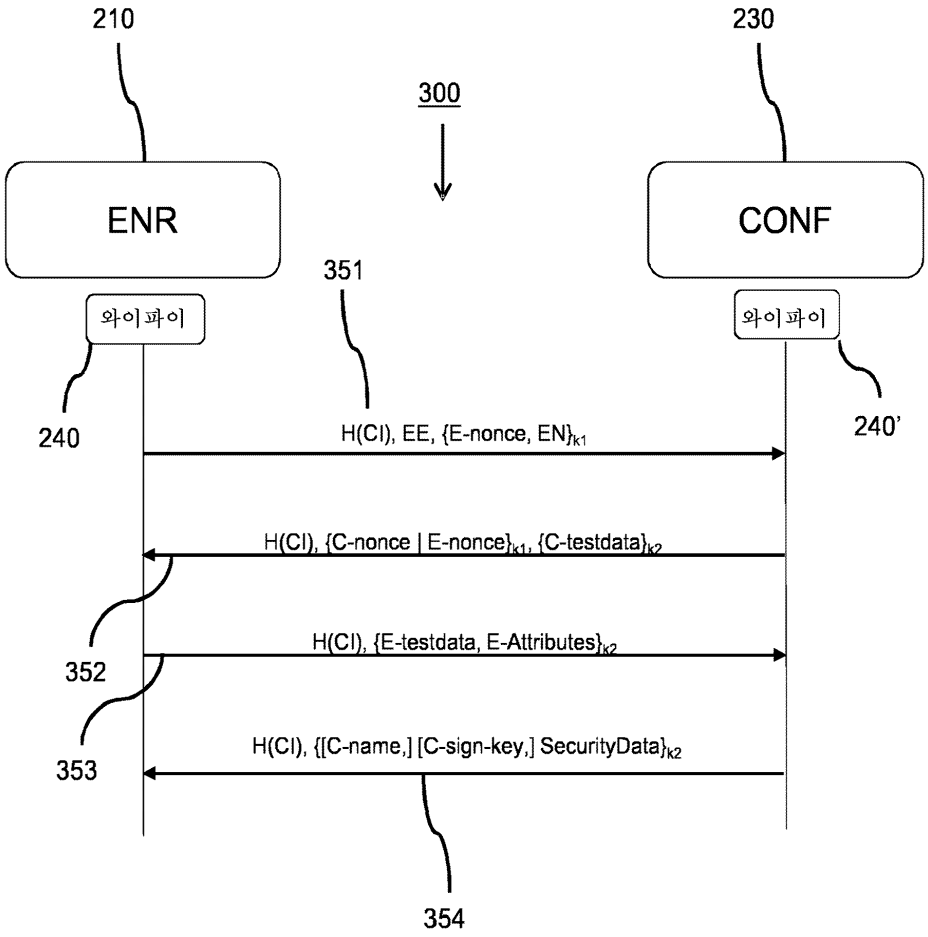
도면1


100
131
132
151
130
150
150'
120
140
113
111
112
110

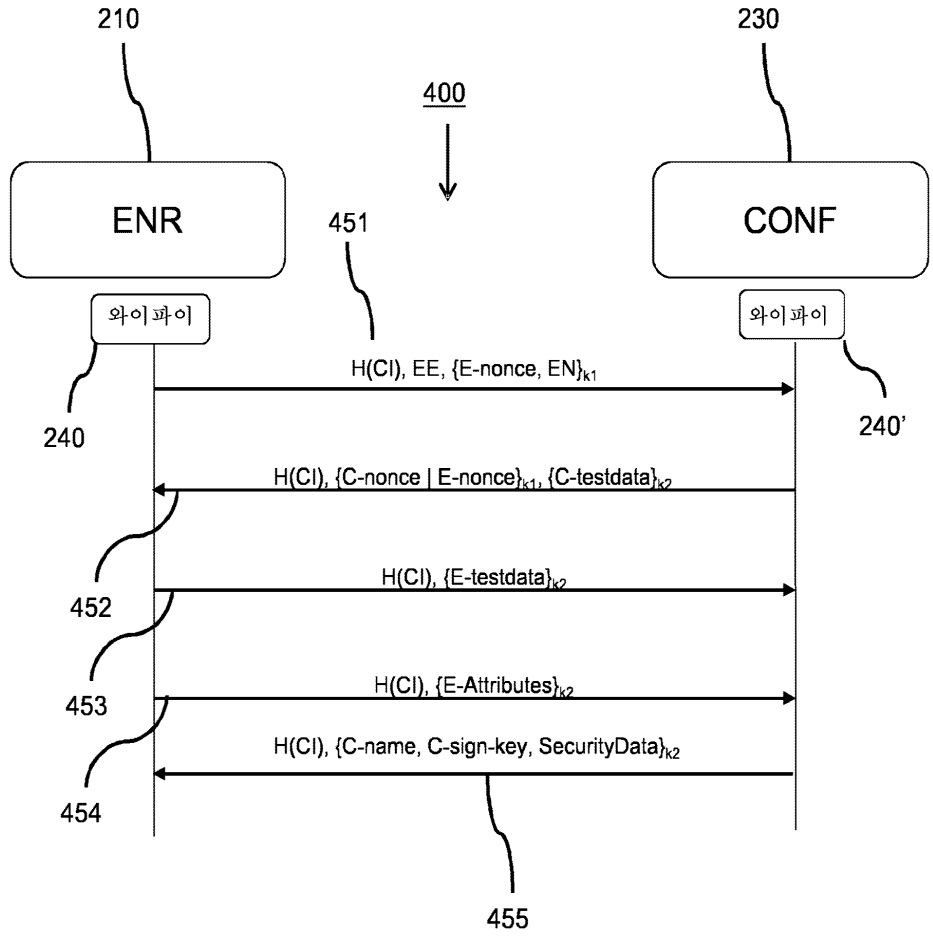
도면2


210
200
230
ENR
CONF
250
와이파이
와이파이
240
240'
H(CI), EE, {E-nonce, EN, E-Attributes}k1
H(CI), {E-nonce, [C-name,] [C-sign-key,] SecurityData}k2
260

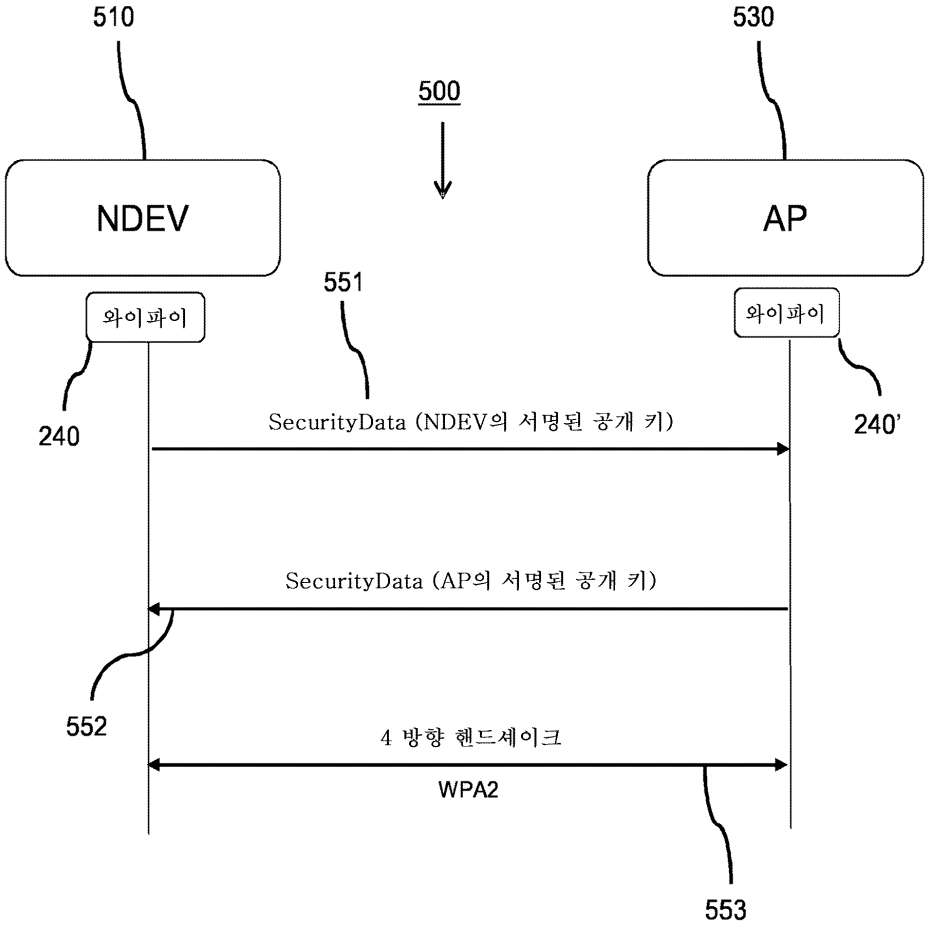
도면3


210
300
230
ENR
CONF
351
와이파이
와이파이
240
240'
H(CI), EE, {E-nonce, EN}k1
H(CI), {C-nonce | E-nonce}k1, {C-testdata}k2
352
H(CI), {E-testdata, E-Attributes}k2
353
H(CI), {[C-name,] [C-sign-key,] SecurityData}k2
354

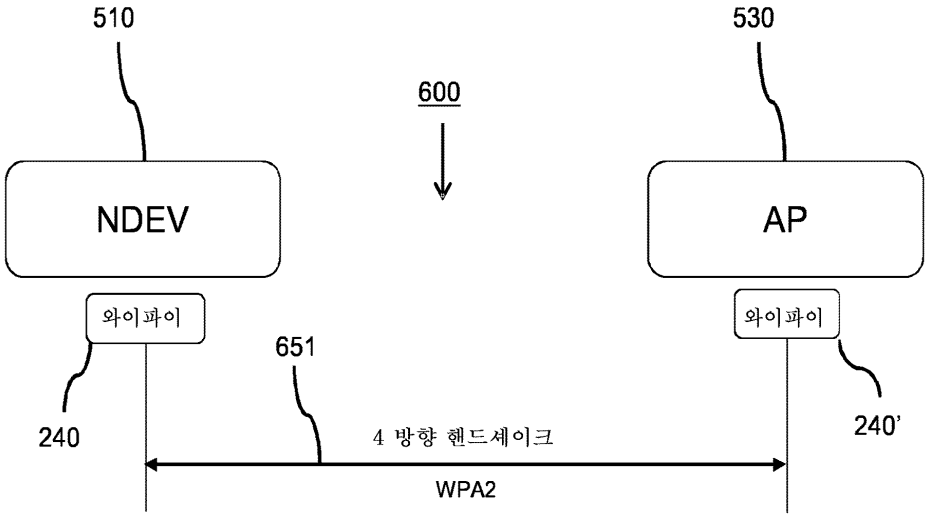
도면4


210
230
400
ENR
451
CONF
와이파이
와이파이
H(CI), EE, {E-nonce, EN}k1
240
240'
H(CI), {C-nonce | E-nonce}k1, {C-testdata}k2
452
H(CI), {E-testdata}k2
453
H(CI), {E-Attributes}k2
454
H(CI), {C-name, C-sign-key, SecurityData}k2
455

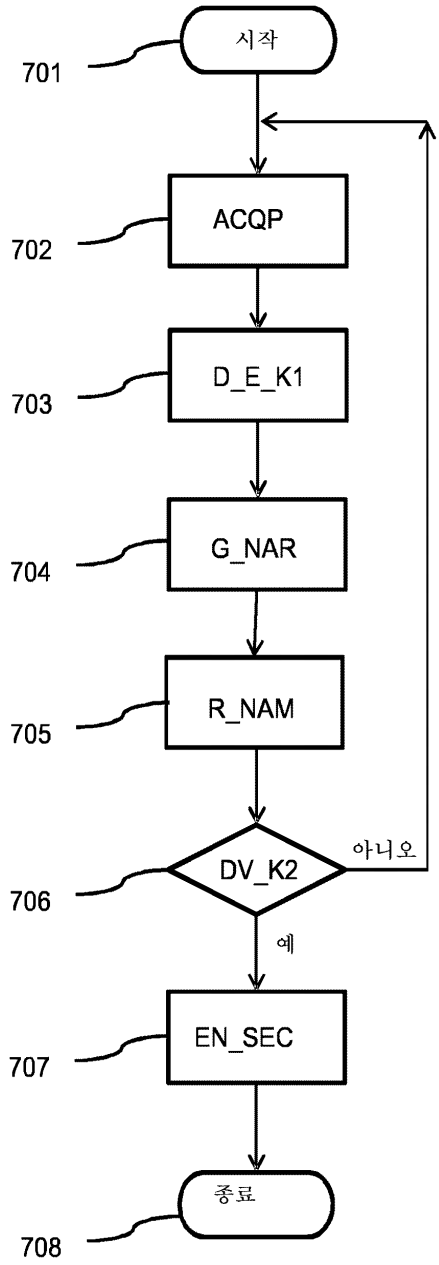
도면5


510
500
530
NDEV
AP
551
와이파이
와이파이
240
240'
SecurityData (NDEV의 서명된 공개 키)
SecurityData (AP의 서명된 공개 키)
552
4 방향 핸드셰이크
WPA2
553

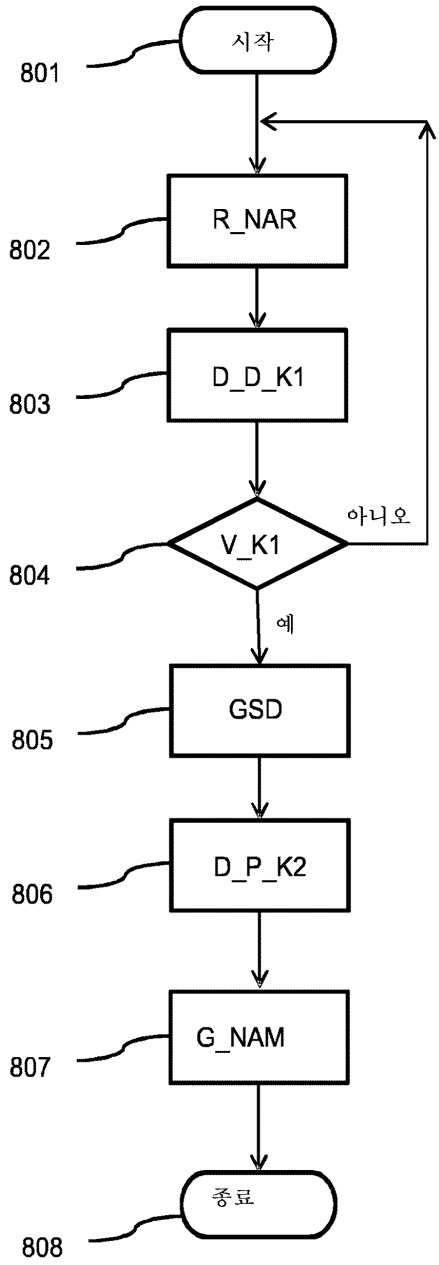
도면6


510
600
530
NDEV
AP
와이파이
와이파이
651
240
240'
4 방향 핸드셰이크
WPA2

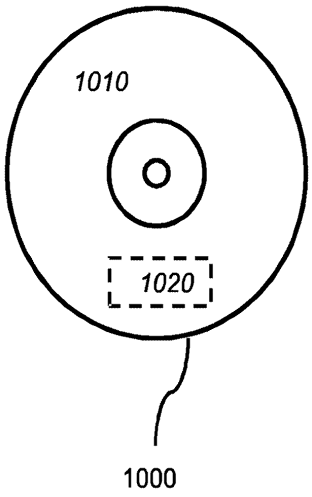
도면7


시작
701
ACQP
702
D_E_K1
703
G_NAR
704
R_NAM
705
DV_K2
706
아니오
예
EN_SEC
707
종료
708

도면8


시작
801
R_NAR
802
D_D_K1
803
V_K1
804
아니오
예
GSD
805
D_P_K2
806
G_NAM
807
종료
808

도면9a



도면9b