(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년09월18일
(11) 등록번호 10-1551315
(24) 등록일자 2015년09월02일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2014-7032060
(22) 출원일자(국제) 2013년04월16일
심사청구일자 2015년06월15일
(85) 번역문제출일자 2014년11월14일
(65) 공개번호 10-2015-0003334
(43) 공개일자 2015년01월08일
(86) 국제출원번호 PCT/US2013/036794
(87) 국제공개번호 WO 2013/158653
국제공개일자 2013년10월24일
(30) 우선권주장
13/658,268 2012년10월23일 미국(US)
61/625,627 2012년04월17일 미국(US)
(56) 선행기술조사문헌
US20070101136 A1
"Wi-Fi Protected Setup Specification Version 1.0h", pages 1-110 (2006.12)

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
체리안, 조지
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
마리넨, 조우니
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인 남앤드남

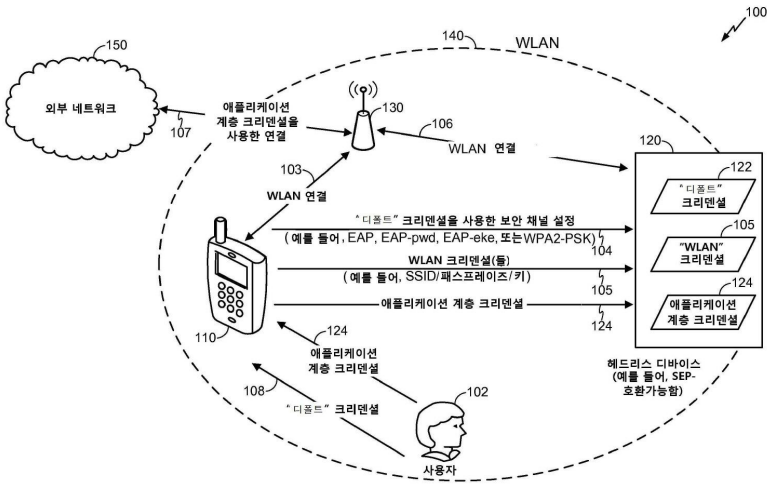
전체 청구항 수 : 총 38 항 심사관 : 송대종

(54) 발명의 명칭 **다른 디바이스가 무선 네트워크에 연결하는 것을 가능하게 하기 위한 모바일 디바이스의 사용**

(57) 요 약

방법은, 제 1 디바이스에서, 제 1 디바이스가 WLAN(wireless local area network)에 연결되고 제 2 디바이스가 WLAN에 연결되지 않은 동안, EAP 교환을 사용하여 제 2 디바이스로의 보안 채널을 설정하는 단계를 포함한다. 방법은 또한, 제 2 디바이스가 WLAN에 연결하는 것을 가능하게 하기 위해서, 보안 채널을 통해 제 2 디바이스로, WLAN과 연관된 적어도 하나의 크리덴셜을 전송하는 단계를 포함한다.

대 표 도



(72) 발명자

아브라함, 산토쉬, 폴

미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

틴나코른스리수팝, 피어라폴

미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

카푸어, 사미르

미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

데 베그트, 롤프

미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

명 세 서

청구범위

청구항 1

방법으로서,

제 1 디바이스에서, 상기 제 1 디바이스가 무선 로컬 영역 네트워크(WLAN)에 연결되고 제 2 디바이스가 상기 WLAN에 연결되지 않은 동안, 확장가능한 인증 프로토콜(extensible authentication protocol: EAP) 교환을 사용하여 상기 제 2 디바이스로의 보안 채널을 설정하는 단계;

상기 제 2 디바이스가 상기 WLAN에 연결하는 것을 가능하게 하기 위해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜(credential)을 상기 보안 채널을 통해 상기 제 2 디바이스로 전송하는 단계;

상기 제 1 디바이스에서, 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜(application layer credential)을 수신하는 단계; 및

상기 제 2 디바이스가 상기 WLAN의 외부의 네트워크로 액세스하게 하기 위해, 상기 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 보안 채널을 통해 상기 제 2 디바이스로 전송하는 단계를 포함하는,

방법.

청구항 2

제 1 항에 있어서,

상기 제 1 디바이스는, 모바일 전화, 휴대용 컴퓨팅 디바이스, 태블릿 컴퓨팅 디바이스, PDA(personal digital assistant), 휴대용 미디어 플레이어 또는 이들의 임의의 결합을 포함하는,

방법.

청구항 3

제 1 항에 있어서,

상기 제 2 디바이스는, SEP(smart energy profile)-호환가능한 디바이스를 포함하는,

방법.

청구항 4

제 1 항에 있어서,

상기 제 2 디바이스는, 적어도 하나의 네트워크 인터페이스를 포함하지만 입력 디바이스 또는 출력 디바이스를 포함하지 않는 헤드리스 디바이스(headless device)를 포함하는,

방법.

청구항 5

제 1 항에 있어서,

상기 적어도 하나의 크리덴셜은, SSID(service set identifier), 패스프레이즈(passphrase), 보안 키 또는 이들의 임의의 결합을 포함하는,

방법.

청구항 6

제 1 항에 있어서,

상기 제 2 디바이스와 연관된 보안 크리덴셜을 표시하는 입력을 상기 제 1 디바이스에서 수신하는 단계; 및

상기 EAP 교환 동안 상기 제 1 디바이스로부터 상기 제 2 디바이스로 상기 보안 크리덴셜을 전송하는 단계를 더 포함하는,

방법.

청구항 7

제 1 항에 있어서,

상기 제 2 디바이스는 헤드리스 디바이스(headless device)를 포함하고,

상기 애플리케이션 계층 크리덴셜은 상기 헤드리스 디바이스에서 계층-7 또는 그보다 낮은 계층의 동작들을 가능하게 하는,

방법.

청구항 8

제 1 항에 있어서,

상기 제 1 디바이스는, 상기 제 2 디바이스에 관하여 자율적(autonomous) Wi-Fi 다이렉트 그룹 운영자(owner)를 포함하는,

방법.

청구항 9

제 8 항에 있어서,

상기 제 2 디바이스와 통신하는 동안 부재 통지(notice of absence)를 발행하는 것을 억제함으로써, 레거시(legacy) Wi-Fi 다이렉트 클라이언트들과의 호환가능성을 유지하는 단계를 더 포함하는,

방법.

청구항 10

제 1 항에 있어서,

상기 제 1 디바이스에서, WPS(Wi-Fi Protected Setup) 발견 동작을 통해 상기 제 2 디바이스를 발견하는 단계를 더 포함하는,

방법.

청구항 11

제 1 항에 있어서,

상기 EAP 교환 이후 4-웨이 핸드쉐이크(four-way handshake) 동작을 수행하는 단계; 및

널(null) PIN(personal identification number)을 사용하여 WPS(Wi-Fi Protected Setup) 인증(authentication) 및 구성 동작을 수행하는 단계를 더 포함하는,

방법.

청구항 12

제 1 항에 있어서,

상기 EAP 교환은 패스워드만을 사용하는 EAP(EAP-pwd) 교환을 포함하고,

상기 방법은,

상기 EAP 교환과 연관된 MSK(master session key)의 일부에 기초하여 PIN(personal identification

number)을 결정하는 단계; 및

상기 PIN을 사용하여 WPS(Wi-Fi Protected Setup) 인증 및 구성 동작을 수행하는 단계를 더 포함하는,

방법.

청구항 13

제 12 항에 있어서,

상기 MSK의 일부는, 상기 MSK의 10개의 최소 유효 바이트(least significant byte)들을 포함하는,

방법.

청구항 14

제 1 항에 있어서,

상기 EAP 교환은 암호화된 키를 이용하는 EAP(EAP-eke) 교환을 포함하는,

방법.

청구항 15

제 1 항에 있어서,

상기 EAP 교환은 WPS(Wi-Fi Protected Setup) 실패에 의해 트리거되는,

방법.

청구항 16

제 1 항에 있어서,

상기 제 1 디바이스에서, 상기 제 2 디바이스를 발견하기 위해, 상기 제 2 디바이스와 연관된 SSID(service set identification), 상기 제 2 디바이스와 연관된 디바이스 식별자 또는 이들의 결합을 브로드캐스트하는 단계를 더 포함하는,

방법.

청구항 17

제 1 항에 있어서,

상기 적어도 하나의 애플리케이션 계층 크리덴셜은 웹사이트에서 사용자 계정과 연관된 로그인 정보에 대응하는,

방법.

청구항 18

방법으로서,

제 1 디바이스에서, 상기 제 1 디바이스가 무선 로컬 영역 네트워크(WLAN)에 연결되지 않고 제 2 디바이스가 상기 WLAN에 연결되는 동안, 보안 크리덴셜을 수신하는 단계;

상기 제 1 디바이스가 상기 WLAN에 연결되지 않고 상기 제 2 디바이스가 상기 WLAN에 연결되는 동안 그리고 확장가능한 인증 프로토콜(EAP) 교환 동안 상기 제 1 디바이스에서, 상기 보안 크리덴셜이 상기 제 1 디바이스에 저장된 저장 보안 크리덴셜과 매칭하는지를 결정하는 단계;

상기 제 1 디바이스에서, 상기 제 1 디바이스가 상기 WLAN에 연결되지 않고 상기 제 2 디바이스가 상기 WLAN에 연결되는 동안, 상기 EAP 교환을 사용하여 상기 제 2 디바이스로 보안 채널을 설정하는 단계;

상기 제 2 디바이스로부터 상기 보안 채널을 통해 상기 제 1 디바이스에서, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 수신하는 단계;

상기 제 1 디바이스에서, 상기 적어도 하나의 크리덴셜을 사용하여 상기 WLAN으로의 연결을 설정하는 단계;

상기 제 1 디바이스에서, 상기 제 2 디바이스로부터 적어도 하나의 애플리케이션 계층 크리덴셜을 수신하는 단계 - 상기 적어도 하나의 애플리케이션 계층 크리덴셜은 상기 제 1 디바이스가 상기 WLAN 외부의 네트워크로 액세스하게 하는 것을 가능하게 함 -; 및

상기 저장 보안 크리덴셜을 상기 적어도 하나의 애플리케이션 계층 크리덴셜의 적어도 일부로 대체하는 단계를 포함하는,

방법.

청구항 19

제 18 항에 있어서,

상기 수신된 보안 크리덴셜이 상기 저장 보안 크리덴셜과 매칭하지 않을 때, 상기 EAP 교환을 종료하는 단계를 더 포함하는,

방법.

청구항 20

제 18 항에 있어서,

상기 저장 보안 크리덴셜은 계층-2 크리덴셜이고, 상기 적어도 하나의 애플리케이션 계층 크리덴셜은 계층-7 크리덴셜인,

방법.

청구항 21

제 18 항에 있어서,

상기 WLAN을 통해, 상기 적어도 하나의 애플리케이션 계층 크리덴셜을 사용하여 상기 WLAN 외부의 네트워크에 액세스하는 단계를 더 포함하는,

방법.

청구항 22

방법으로서,

제 1 디바이스에서, WPS(Wi-Fi Protected Setup) 발견 동작 동안 제 1 메시지를 제 2 디바이스에 전송하는 단계; 및

상기 제 1 디바이스에서, 상기 WPS 발견 동작에 후속하는 WPS 인증 및 구성 동작 동안 제 2 메시지를 상기 제 2 디바이스에 전송하는 단계를 포함하고,

상기 제 2 메시지는 패스워드를 사용하는 확장가능한 인증 프로토콜(EAP) (EAP-pwd) 교환과 연관된 데이터를 포함하고,

상기 데이터는 상기 제 2 디바이스가 무선 로컬 영역 네트워크(WLAN)에 액세스하는 것을 가능하게 하는 적어도 하나의 링크 계층 크리덴셜 및 상기 제 2 디바이스가 상기 WLAN 외부의 네트워크에 액세스하는 것을 가능하게 하고 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 포함하는,

방법.

청구항 23

방법으로서,

제 1 디바이스에서, 상기 제 1 디바이스가 무선 로컬 영역 네트워크(WLAN) 연결되고 제 2 디바이스가 상기 WLAN에 연결되지 않은 동안, WPA2-PSK(Wi-Fi Protected Access 2 Pre-shared Key) 교환을 사용하여 상기 제 2 디바

이스로의 보안 채널을 설정하는 단계;

상기 제 1 디바이스에서, 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 수신하는 단계;

상기 제 2 디바이스가 상기 WLAN에 연결하는 것을 가능하게 하기 위해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 디바이스로 전송하는 단계; 및

상기 제 2 디바이스가 상기 WLAN 외부의 네트워크로 액세스하는 것을 가능하게 하기 위해, 상기 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 보안 채널을 통해 상기 제 2 디바이스로 전송하는 단계를 포함하는,

방법.

청구항 24

제 23 항에 있어서,

상기 WPA2-PSK 교환과 연관된 PMK(pairwise master key)의 일부에 기초하여 PIN(personal identification number)을 결정하는 단계; 및

상기 PIN을 사용하여 WPS(Wi-Fi Protected Setup) 인증 및 구성 동작을 수행하는 단계를 더 포함하는,

방법.

청구항 25

제 24 항에 있어서,

상기 PMK의 일부는 상기 PMK의 10개의 최소 유효 바이트들을 포함하는,

방법.

청구항 26

제 23 항에 있어서,

Wi-Fi 다이렉트 발견 동작을 통해 상기 제 2 디바이스를 발견하는 단계를 더 포함하는,

방법.

청구항 27

장치로서,

프로세서; 및

상기 프로세서에 커플링되는 메모리를 포함하고,

상기 메모리는,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되고 제 2 장치가 상기 WLAN에 연결되지 않은 동안, 확장가능한 인증 프로토콜(EAP) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하고;

상기 제 2 장치가 상기 WLAN에 연결하는 것을 가능하게 하기 위해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하도록 송신기에 지시하고; 그리고

상기 제 2 장치가 상기 WLAN 외부의 네트워크로 액세스하는 것을 가능하게 하기 위해, 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하도록 상기 송신기에 지시하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장하는,

장치.

청구항 28

장치로서,

프로세서; 및

상기 프로세서에 커플링되는 메모리를 포함하고,

상기 메모리는,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되지 않고 제 2 장치가 상기 WLAN에 연결되는 동안 그리고 확장가능한 인증 프로토콜(EAP) 교환 동안, 상기 제 2 장치로부터 수신된 보안 크리덴셜이 상기 장치에 저장된 저장 보안 크리덴셜과 매칭하는지를 결정하고;

상기 장치가 상기 WLAN에 연결되지 않고 상기 제 2 장치가 상기 WLAN에 연결되는 동안, 상기 EAP 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하고;

상기 WLAN과 연관되는 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로부터 수신하고;

상기 적어도 하나의 크리덴셜을 사용하여 상기 WLAN으로의 연결을 설정하고;

적어도 하나의 애플리케이션 계층 크리덴셜을 상기 제 2 장치로부터 수신하고 - 상기 적어도 하나의 애플리케이션 계층 크리덴셜은 상기 장치가 상기 WLAN 외부의 네트워크로 액세스하는 것을 가능하게 함 -; 그리고

상기 저장 보안 크리덴셜을 상기 적어도 하나의 애플리케이션 계층 크리덴셜의 적어도 일부로 대체하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장하는,

장치.

청구항 29

장치로서,

프로세서; 및

상기 프로세서에 커플링되는 메모리를 포함하고,

상기 메모리는,

WPS(Wi-Fi Protected Setup) 발견 동작 동안 제 1 메시지를 제 2 장치에 전송하도록 송신기에 지시하고; 그리고

상기 WPS 발견 동작에 후속하는 WPS 인증 및 구성 동작 동안 제 2 메시지를 상기 제 2 장치에 전송하도록 상기 송신기에 지시하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장하고,

상기 제 2 메시지는 패스워드를 사용하는 확장가능한 인증 프로토콜(EAP) (EAP-pwd) 교환과 연관된 데이터를 포함하고,

상기 데이터는 상기 제 2 장치가 무선 로컬 영역 네트워크(WLAN)에 액세스하는 것을 가능하게 하는 적어도 하나의 링크 계층 크리덴셜 및 상기 제 2 장치가 상기 WLAN 외부의 네트워크로 액세스하는 것을 가능하게 하고 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 포함하는,

장치.

청구항 30

장치로서,

프로세서; 및

상기 프로세서에 커플링되는 메모리를 포함하고,

상기 메모리는,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되고 제 2 장치가 상기 WLAN에 연결되지 않은 동안,

WPA2-PSK(Wi-Fi Protected Access 2 Pre-shared Key) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하고;

상기 제 2 장치가 상기 WLAN에 연결하는 것을 가능하게 하기 위해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하도록 송신기에 지시하고; 그리고

상기 제 2 장치가 상기 WLAN 외부의 네트워크로 액세스하는 것을 가능하게 하기 위해, 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하도록 상기 송신기에 지시하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장하는,

장치.

청구항 31

장치로서,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되고 제 2 장치가 상기 WLAN에 연결되지 않은 동안, 확장가능한 인증 프로토콜(EAP) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하기 위한 수단; 및

상기 제 2 장치가 상기 WLAN에 연결하는 것을 가능하게 하기 위해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하기 위한 수단을 포함하고,

상기 전송하기 위한 수단은, 상기 제 2 장치가 상기 WLAN 외부의 네트워크로 액세스하는 것을 가능하게 하기 위해, 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하도록 구성되는,

장치.

청구항 32

장치로서,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되지 않고 제 2 장치가 상기 WLAN에 연결되는 동안 그리고 확장가능한 인증 프로토콜(EAP) 교환 동안, 상기 제 2 장치로부터 수신된 보안 크리덴셜이 상기 장치에 저장된 저장 보안 크리덴셜과 매칭하는지를 결정하기 위한 수단;

상기 장치가 상기 WLAN에 연결되지 않고 상기 제 2 장치가 상기 WLAN에 연결되는 동안, 상기 EAP 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하기 위한 수단;

상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로부터 수신하기 위한 수단 - 상기 설정하기 위한 수단은 상기 적어도 하나의 크리덴셜을 사용하여 상기 WLAN으로의 연결을 설정하고, 상기 수신하기 위한 수단은 상기 장치가 상기 WLAN 외부의 네트워크로 액세스하는 것을 가능하게 하는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 제 2 장치로부터 수신하도록 구성됨 -; 및

상기 저장 보안 크리덴셜을 상기 적어도 하나의 애플리케이션 계층 크리덴셜의 적어도 일부로 대체하기 위한 수단을 포함하는,

장치.

청구항 33

장치로서,

제 1 메시지 및 제 2 메시지를 생성하기 위한 수단; 및

전송하기 위한 수단을 포함하고,

상기 전송하기 위한 수단은,

WPS(Wi-Fi Protected Setup) 발견 동작 동안 상기 제 1 메시지를 제 2 장치에 전송하고; 그리고

상기 WPS 발견 동작에 후속하는 WPS 인증 및 구성 동작 동안 상기 제 2 메시지를 상기 제 2 장치에 전송하도록 구성되고,

상기 제 2 메시지는 패스워드를 사용하는 확장가능한 인증 프로토콜(EAP) (EAP-pwd) 교환과 연관된 데이터를 포함하고,

상기 데이터는 상기 제 2 장치가 무선 로컬 영역 네트워크(WLAN)에 액세스하는 것을 가능하게 하는 적어도 하나의 링크 계층 크리덴셜 및 상기 제 2 장치가 상기 WLAN 외부의 네트워크에 액세스하는 것을 가능하게 하고 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 포함하는,

장치.

청구항 34

장치로서,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되고 제 2 장치가 상기 WLAN에 연결되지 않은 동안, WPA2-PSK(Wi-Fi Protected Access 2 Pre-shared Key) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하기 위한 수단; 및

상기 제 2 장치가 상기 WLAN에 연결하는 것을 가능하게 하기 위해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하기 위한 수단을 포함하고,

상기 전송하기 위한 수단은, 상기 제 2 장치가 상기 WLAN 외부의 네트워크에 액세스하는 것을 가능하게 하고 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하도록 구성되는,

장치.

청구항 35

명령들을 포함하는 컴퓨터 판독가능한 매체로서,

상기 명령들은 실행될 때, 장치로 하여금,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되고 제 2 장치가 상기 WLAN에 연결되지 않은 동안, 확장가능한 인증 프로토콜(EAP) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하고;

상기 제 2 장치가 상기 WLAN에 연결하는 것을 가능하게 하기 위해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하고; 그리고

상기 제 2 장치가 상기 WLAN 외부의 네트워크에 액세스하는 것을 가능하게 하고 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하게 하는,

컴퓨터 판독가능한 매체.

청구항 36

명령들을 포함하는 컴퓨터 판독가능한 매체로서,

상기 명령들은 실행될 때, 장치로 하여금,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되지 않고 제 2 장치가 상기 WLAN에 연결되는 동안 그리고 확장가능한 인증 프로토콜(EAP) 교환 동안, 상기 제 2 장치로부터 수신된 보안 크리덴셜이 상기 장치에 저장된 저장 보안 크리덴셜과 매칭하는지를 결정하고;

상기 장치가 상기 WLAN에 연결되지 않고 상기 제 2 장치가 상기 WLAN에 연결되는 동안, 상기 EAP 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하고;

상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로부터 수신하고;

상기 적어도 하나의 크리덴셜을 사용하여 상기 WLAN으로의 연결을 설정하고;

상기 장치가 상기 WLAN 외부의 네트워크에 액세스하는 것을 가능하게 하는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 제 2 장치로부터 수신하고; 그리고

상기 저장 보안 크리덴셜을 상기 적어도 하나의 애플리케이션 계층 크리덴셜의 적어도 일부로 대체하게 하는,

컴퓨터 판독가능한 매체.

청구항 37

명령들을 포함하는 컴퓨터 판독가능한 매체로서,

상기 명령들은 실행될 때, 장치로 하여금,

WPS(Wi-Fi Protected Setup) 발견 동작 동안 제 1 메시지를 제 2 장치에 전송하게 하고; 그리고

상기 WPS 발견 동작에 후속하는 WPS 인증 및 구성 동작 동안 제 2 메시지를 상기 제 2 장치에 전송하게 하고,

상기 제 2 메시지는 패스워드를 사용하는 확장가능한 인증 프로토콜(EAP) (EAP-pwd) 교환과 연관된 데이터를 포함하고,

상기 데이터는 상기 제 2 장치가 무선 로컬 영역 네트워크(WLAN)에 액세스하는 것을 가능하게 하는 적어도 하나의 링크 계층 크리덴셜 및 상기 제 2 장치가 상기 WLAN 외부의 네트워크에 액세스하는 것을 가능하게 하고 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 포함하는,

컴퓨터 판독가능한 매체.

청구항 38

명령들을 포함하는 컴퓨터 판독가능한 매체로서,

상기 명령들은 실행될 때, 장치로 하여금,

상기 장치가 무선 로컬 영역 네트워크(WLAN)에 연결되고 제 2 장치가 상기 WLAN에 연결되지 않은 동안, WPA2-PSK(Wi-Fi Protected Access 2 Pre-shared Key) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하고;

상기 제 2 장치가 상기 WLAN에 연결하는 것을 가능하게 하기 위해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하고; 그리고

상기 제 2 장치가 상기 WLAN 외부의 네트워크에 액세스하는 것을 가능하게 하기 위해, 사용자 입력을 통해 사용자에 의해 제공되는 적어도 하나의 애플리케이션 계층 크리덴셜을 상기 보안 채널을 통해 상기 제 2 장치로 전송하게 하는,

컴퓨터 판독가능한 매체.

발명의 설명

기 술 분 야

[0001] 본 특허 출원은 2012년 4월 17일자로 출원된, 공동 소유되는 미국 가특허 출원 제61/625,627호로부터의 우선권을 주장하고, 상기 미국 가특허 출원의 내용들은 그 전체가 인용에 의해 본원에 명백하게 포함된다.

[0002] 본 개시는 무선 네트워크들 및 무선 디바이스들에 관한 것이다.

배 경 기 술

[0003] 기술의 진보들은 더 소형이고 더 강력한 컴퓨팅 디바이스들을 창출해왔다. 예를 들어, 소형이고, 경량이며, 사용자들이 휴대하기 쉬운 휴대용 무선 전화들, 개인용 디지털 보조기(PDA)들 및 페이징 디바이스들과 같은 무선 컴퓨팅 디바이스를 포함하는 다양한 휴대용 개인 컴퓨팅 디바이스들이 현재 존재한다. 더 구체적으로, 셀룰러 전화들 및 인터넷 프로토콜(IP) 전화들과 같은 휴대용 무선 전화들은 무선 네트워크들을 통해 음성 및 데이터 패킷들을 통신할 수 있다. 많은 이러한 무선 전화들은 최종 사용자들에게 강화된 기능을 제공하기 위해서 추가 디바이스들을 포함한다. 예를 들어, 무선 전화는 또한, 디지털 스틸 카메라, 디지털 비디오 카메라, 디지털 리코더 및 오디오 파일 플레이어를 포함할 수 있다. 또한, 이러한 무선 전화들은 인터넷에 액세스하는데 사용될

수 있는, 웹 브라우저 애플리케이션과 같은 소프트웨어 애플리케이션들을 실행할 수 있다. 이로써, 이 무선 전화들은 현저한 컴퓨팅 능력들을 포함할 수 있다.

[0004] 무선 디바이스는 WPS(Wi-Fi Protected Setup)를 통해 무선 로컬 영역 네트워크(wireless local area network: WLAN)에 연결할 수 있다. 통상적으로, WPS는 PIN(personal identification number) 모드에서 또는 푸쉬-버튼(push-button) 모드에서 수행된다. PIN 모드에서, 액세스 포인트(AP)에 연결될 무선 디바이스의 사용자는, 연결을 가능하게 하기 위해서 (예를 들어, 키패드를 통해) 무선 디바이스에 또는 (예를 들어, 웹 포털을 통해) 액세스 포인트(AP)에 PIN을 입력할 수 있다. 푸쉬-버튼 모드에서, 사용자는 연결을 가능하게 하기 위해서 무선 디바이스 상의 물리적 버튼을 그리고 AP 상의 대응하는 물리적 버튼을 푸쉬할 수 있다. 그러나, 이러한 푸쉬 버튼들 또는 PIN의 물리적 입력을 수신하기 위한 능력을 가지지 않는 디바이스들은 무선 네트워크에 조인(join)가능하지 않을 수 있다.

발명의 내용

[0005] 일부 디바이스들은 설계 또는 비용 제약들로 인하여 물리적 입력을 수신가능하지 않을 수 있다. 예를 들어, 특정 디바이스들은, 네트워크 인터페이스를 통해 제어되며 임의의 입력 인터페이스들(예를 들어, 버튼들, 키보드들 등) 또는 출력 인터페이스들(예를 들어, 디스플레이들)을 포함하지 않는 "헤드리스(headless)" 디바이스들일 수 있다. 게다가, 헤드리스 디바이스의 사용자는 WLAN 연결을 설정하는데 사용되는 크리덴셜(credential)들(예를 들어, SSID(service set identifier), 패스프레이즈(passphrase) 및/또는 보안 키)을 알지 못할 수 있다. 본 명세서에 설명된 시스템들 및 방법들은 유리하게, 이러한 헤드리스 무선 디바이스들(뿐만 아니라 다른 무선 디바이스들)이 WLAN에 조인하는 것을 가능하게 할 수 있다.

[0006] 예를 들어, 홈 WLAN에 이미 연결된 모바일 디바이스(예를 들어, 사용자의 모바일 폰)는 무선 디바이스(예를 들어, 헤드리스 무선 디바이스)가 WLAN에 연결하는 것을 가능하게 할 수 있다. 초기에, 모바일 디바이스는 무선 디바이스와의 보안 채널을 생성할 수 있다. 특정 구현들에서, 보안 채널은 EAP(extensible authentication protocol), WPA(Wi-Fi protected access) 또는 이들의 변형들을 사용하여 생성될 수 있다. 보안 채널이 생성된 이후, 모바일 디바이스는 무선 디바이스가 WLAN에 연결하는 것을 가능하게 하기 위해서 WLAN 크리덴셜(들)을 무선 디바이스에 제공할 수 있다. 모바일 디바이스는 또한, 추가 정보 및 크리덴셜들을 무선 디바이스에 제공할 수 있다. 예를 들어, 모바일 디바이스는, 무선 디바이스가 애플리케이션 계층 크리덴셜을 사용하여 외부 네트워크 또는 다른 디바이스에 액세스할 수 있도록 애플리케이션 계층 크리덴셜(예를 들어, 인터넷 웹사이트에 대한 어카운트 정보)을 제공할 수 있다.

[0007] 특정 실시예에서, 방법은, 제 1 디바이스에서, 상기 제 1 디바이스가 WLAN에 연결되고 제 2 디바이스가 상기 WLAN에 연결되지 않은 동안, EAP 교환을 사용하여 상기 제 2 디바이스로의 보안 채널을 설정하는 단계를 포함한다. 상기 방법은 또한, 상기 제 2 디바이스가 상기 WLAN에 연결하는 것을 가능하게 하기 위해서, 상기 보안 채널을 통해 상기 제 2 디바이스로, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 전송하는 단계를 포함한다. 예시적인 예에서, 제 1 디바이스는 모바일 폰일 수 있고, 제 2 디바이스는 헤드리스 디바이스일 수 있다.

[0008] 다른 특정 실시예에서, 방법은, 제 1 디바이스(예를 들어, 헤드리스 디바이스)에서, 상기 제 1 디바이스가 WLAN(예를 들어, 모바일 폰)에 연결되지 않고 제 2 디바이스(예를 들어, 모바일 폰)가 상기 WLAN에 연결되는 동안, EAP 교환을 사용하여 상기 제 2 디바이스로의 보안 채널을 설정하는 단계를 포함한다. 상기 방법은 또한, 상기 제 1 디바이스에서 상기 보안 채널을 통해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 수신하는 단계를 포함한다. 상기 방법은, 상기 제 1 디바이스에서, 상기 적어도 하나의 크리덴셜을 사용하여 상기 WLAN으로의 연결을 설정하는 단계를 더 포함한다.

[0009] 또 다른 특정 실시예에서, 방법은, 제 1 디바이스에서, WPS 발견 동작 동안 제 1 메시지를 제 2 디바이스에 전송하는 단계를 포함한다. 상기 방법은 또한, 상기 제 1 디바이스에서, 상기 WPS 발견 동작 이후의 WPS 인증 및 구성 동작 동안 제 2 메시지를 상기 제 2 디바이스에 전송하는 단계를 포함한다. 상기 제 2 메시지는 패스워드를 사용하는 EAP(EAP-pwd) 교환과 연관된 데이터를 포함한다.

[0010] 또 다른 특정 실시예에서, 방법은, 제 1 디바이스에서, 상기 제 1 디바이스가 WLAN에 연결되고 제 2 디바이스가 상기 WLAN에 연결되지 않은 동안, WPA2-PSK(Wi-Fi Protected Access 2 Pre-shared Key) 교환을 사용하여 상기 제 2 디바이스로의 보안 채널을 설정하는 단계를 포함한다. 상기 방법은 또한, 상기 제 2 디바이스가 상기 WLAN에 연결하는 것을 가능하게 하기 위해서, 상기 보안 채널을 통해 상기 제 2 디바이스로, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 전송하는 단계를 포함한다.

[0011] 또 다른 특정 실시예에서, 장치는, 프로세서, 및 상기 프로세서에 커플링되는 메모리를 포함하고, 상기 메모리는, 상기 장치가 WLAN(wireless local area network)에 연결되고 제 2 장치가 상기 WLAN에 연결되지 않은 동안, EAP(extensible authentication protocol) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장한다. 상기 메모리는 또한, 상기 제 2 장치가 상기 WLAN에 연결하는 것을 가능하게 하기 위해서, 상기 보안 채널을 통해 상기 제 2 장치로, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 전송하도록 송신기를 지시(direct)하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장한다.

[0012] 또 다른 특정 실시예에서, 장치는, 프로세서, 및 상기 프로세서에 커플링되는 메모리를 포함하고, 상기 메모리는, 상기 장치가 WLAN(wireless local area network)에 연결되지 않고 제 2 장치가 상기 WLAN에 연결되는 동안, EAP(extensible authentication protocol) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장한다. 상기 메모리는 또한, 상기 보안 채널을 통해, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 수신하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장한다. 상기 프로세서는 상기 적어도 하나의 크리덴셜을 사용하여 상기 WLAN으로의 연결을 설정하도록 추가로 구성된다.

[0013] 또 다른 특정 실시예에서, 장치는, 프로세서, 및 상기 프로세서에 커플링되는 메모리를 포함하고, 상기 메모리는, WPS(Wi-Fi Protected Setup) 발견 동작 동안 제 1 메시지를 제 2 장치에 전송하도록 송신기를 지시하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장한다. 상기 메모리는 또한, 상기 WPS 발견 동작 이후의 WPS 인증 및 구성 동작 동안 제 2 메시지를 상기 제 2 장치에 전송하도록 상기 송신기를 지시하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장한다. 상기 제 2 메시지는 패스워드를 사용하는 EAP(extensible authentication protocol)(EAP-pwd) 교환과 연관된 데이터를 포함한다.

[0014] 또 다른 특정 실시예에서, 장치는, 프로세서, 및 상기 프로세서에 커플링되는 메모리를 포함하고, 상기 메모리는, 상기 장치가 WLAN(wireless local area network)에 연결되고 제 2 장치가 상기 WLAN에 연결되지 않은 동안, WPA2-PSK(Wi-Fi Protected Access 2 Pre-shared Key) 교환을 사용하여 상기 제 2 장치로의 보안 채널을 설정하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장한다. 상기 메모리는 또한, 제 2 디바이스가 상기 WLAN에 연결하는 것을 가능하게 하기 위해서, 상기 보안 채널을 통해 상기 제 2 장치로, 상기 WLAN과 연관된 적어도 하나의 크리덴셜을 전송하도록 송신기를 지시하기 위한, 상기 프로세서에 의해 실행가능한 명령들을 저장한다.

[0015] 개시된 실시예들 중 적어도 하나에 의해 제공된 하나의 특정한 이점은 제 2 디바이스(예를 들어, 헤드리스 디바이스)가 무선 네트워크에 연결하는 것을 가능하게 하는 제 1 디바이스(예를 들어, 모바일 디바이스)의 능력이다.

[0016] 본 개시의 다른 양상들, 이점들 및 특징들은, 다음의 섹션들: 도면의 간단한 설명, 발명을 실시하기 위한 구체적인 내용 및 특허청구범위를 포함하는 전체 출원의 검토후 명백해질 것이다.

도면의 간단한 설명

[0017] 도 1은 디바이스가 WLAN에 액세스하는 것을 가능하게 하도록 동작가능한 시스템의 특정 실시예를 예시하기 위한 도면이다.

도 2는 디바이스가 EAP 교환을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 것과 연관된 메시징에 대한 특정 실시예를 예시하기 위한 래더 다이어그램(ladder diagram)이다.

도 3은 디바이스가 EAP-pwd 교환으로 생성된 PIN을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 것과 연관된 메시징에 대한 특정 실시예를 예시하기 위한 레더 다이어그램이다.

도 4는 디바이스가 PIN-기반 WPS 실패 이후 EAP 교환을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 것과 연관된 메시징에 대한 특정 실시예를 예시하기 위한 레더 다이어그램이다.

도 5는 디바이스가 EAP-pwd 교환을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 것과 연관된 메시징에 대한 특정 실시예를 예시하기 위한 레더 다이어그램이다.

도 6은 디바이스가 WPA2-PSK 교환으로 생성된 PIN을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 것과 연관된 메시징의 특정 실시예를 예시하는 레더 다이어그램이다.

도 7은 도 2-4의 메시징에 따른, 도 1의 모바일 디바이스에서의 동작 방법의 특정 실시예를 예시하기 위한 흐름도이다.

도 8은 도 2-4의 메시징에 따른, 도 1의 헤드리스 디바이스에서의 동작 방법의 특정 실시예를 예시하기 위한 흐름도이다.

도 9는 도 5의 메시징에 따른, 도 1의 시스템에서의 동작 방법의 특정 실시예를 예시하기 위한 흐름도이다.

도 10은 도 6의 메시징에 따른, 도 1의 시스템에서의 동작 방법의 특정 실시예를 예시하기 위한 흐름도이다.

도 11은 다른 디바이스가 WLAN에 액세스하는 것을 가능하도록 동작가능한 컴포넌트들을 포함하는 통신 디바이스의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 도 1은 디바이스(예를 들어, 예시적인 헤드리스 디바이스(120))가 WLAN(140)에 액세스하는 것을 가능하도록 구성가능한 시스템(100)의 특정 실시예를 예시하기 위한 도면이다. 시스템(100)은 또한, 모바일 디바이스(110) 및 액세스 포인트(AP)(130)를 포함한다. 특정 실시예에서, WLAN(140)은 AP(130)를 통해 외부 네트워크(150)와 선택적으로 통신하는 고객 전제(premise)(예를 들어, 가정 또는 사무실) 무선 네트워크일 수 있다. 예를 들어, 외부 네트워크(150)는 인터넷일 수 있고 그리고/또는 서버들과 같은 인터넷-액세스가능한 컴퓨팅 디바이스들을 포함할 수 있다.

[0019] 모바일 디바이스(110)는 모바일 전화, 휴대용 컴퓨팅 디바이스, 태블릿 컴퓨팅 디바이스, PDA(personal digital assistant), 휴대용 미디어 플레이어 또는 이들의 임의의 결합일 수 있다. 모바일 디바이스(110)는 하나 또는 둘 이상의 WLAN 크리덴셜들(105)을 사용하여 WLAN 연결(103)을 통해 AP(130)에 연결될 수 있다. (예를 들어, 이전에 완료된 WPS(Wi-Fi protected setup) 동작 동안) 사용자(102)에 의해 또는 AP(130)에 의해 WLAN 크리덴셜(들)(105)이 제공될 수 있다. 모바일 디바이스(110)는 WPS 셋업을 위해서 내부 레지스트라(registrar)를 호스팅할 수 있으며, Wi-Fi 다이렉트와 호환가능할 수 있는데, 이는 모바일 디바이스(110)가 AP(130)의 사용없이 다른 Wi-Fi 디바이스들과 통신하는 것을 가능하게 할 수 있다. 모바일 디바이스(110)는 모바일 디바이스(110)의 메모리에 WLAN 크리덴셜(들)(105)을 저장할 수 있다. 특정 실시예에서, WLAN 크리덴셜(들)(105)은 SSID(service set identifier), 패스프레이즈, 보안 키 또는 이들의 임의의 결합을 포함한다.

[0020] 헤드리스 디바이스(120)는 네트워크 인터페이스(예를 들어, 무선 네트워크 인터페이스)를 포함하지만 입력 디바이스(버튼들, 키보드들 등) 또는 출력 인터페이스들(예를 들어, 디스플레이들)을 포함하지 않는 디바이스일 수 있다. 따라서, 헤드리스 디바이스(120)는 직접적으로 물리적 입력을 통해서가 아니라 오직 다른 디바이스와의 통신을 통해서만 구성가능할 수 있다. 헤드리스 디바이스(120)는 또한, Wi-Fi 다이렉트와 호환가능할 수 있다. 특정 실시예에서, 헤드리스 디바이스(120)는 SEP 2.0-호환가능한 디바이스와 같은 SEP(smart energy profile)-호환가능한 디바이스이다. SEP 2.0-호환가능할 수 있는 예시적인 디바이스들은 가정용 전자기기들(예를 들어, 세탁기, 드라이어, 냉장고 등) 및 센서들(예를 들어, 연기 탐지기들)을 포함하지만, 이에 제한되는 것은 아니다.

[0021] 동작 동안, 사용자(102)는 헤드리스 디바이스(120)를 네트워킹된 환경에 도입할 수 있다. 예를 들어, 사용자(102)는 헤드리스 디바이스(120)(예를 들어, 혈압계)를 구매하여, 헤드리스 디바이스(120)를 가정으로 가져올 수 있다. 사용자(102)는 모바일 디바이스(110)(예를 들어, 사용자의 스마트 폰)를 사용하여, 헤드리스 디바이스(120)가 WLAN(140)에 연결하는 것을 가능하게 하도록 헤드리스 디바이스(120)를 프로그래밍할 수 있다. 특정한 실시예에서, 사용자(102)는 헤드리스 디바이스(120)를 구성하기 위해서 애플리케이션을 다운로드하고 그리고/또는 이 애플리케이션을 모바일 디바이스(110)에 인스톨할 수 있다.

[0022] 모바일 디바이스(110)는 WPS 발견 동작 동안 Wi-Fi 다이렉트 연결을 통해 헤드리스 디바이스(120)를 발견할 수 있다. 특정 실시예에서, 모바일 디바이스(110)는 자율적(autonomous) Wi-Fi 다이렉트 그룹 운영자(owner)로서의 헤드리스 디바이스(120)를 나타내고, 헤드리스 디바이스(120)는 다이렉트 클라이언트로서 역할을 한다. 모바일 디바이스(110)는, 모바일 디바이스(110)가 헤드리스 디바이스(120)에 연결하는 것을 가능하게 하기 위해서 (예를 들어, 헤드리스 디바이스(120)의 제조자에 의해 제공되는) 디폴트 SSID(service set identification), (예를 들어, 헤드리스 디바이스(120)의 제조자에 의해 제공되는) 헤드리스 디바이스(120)와 연관된 디바이스 식별자 또는 이들의 결합을 브로드캐스트할 수 있다. 헤드리스 디바이스(120)는 파워 업 시, 디폴트 SSID에 의해 식별되는 네트워크를 탐색하여 이를 연결하도록 프로그래밍될 수 있다. 헤드리스 디바이스(120) 및 모바일 디

바이스(110)가 Wi-Fi 다이렉트를 통해 연결된다면, 사용자(102)는 모바일 디바이스(110)가 헤드리스 디바이스(120)에 액세스하게 하도록, 헤드리스 디바이스(120)와 연관된 디폴트 보안 크리덴셜(108)(예를 들어, 사용자이름, 패스워드, 패스프레이즈, PIN 또는 이들의 임의의 결합)을 모바일 디바이스(110)에 입력할 수 있다.

[0023] 디폴트 보안 크리덴셜(108)은 헤드리스 디바이스(120)의 명령 메뉴얼 또는 패키징(packaging)으로부터 또는 헤드리스 디바이스(120) 그 자체로부터(예를 들어, 헤드리스 디바이스(120) 상의 스티커로부터) 획득될 수 있다. 대안적으로, 사용자(102)는 헤드리스 디바이스(120)에 특정된 고유한 URL(uniform resource locator)을 통해 제조자의 웹사이트로부터 애플리케이션을 다운로드하여 실행시킬 수 있는데, 여기서 애플리케이션은 디폴트 보안 크리덴셜(108)을 포함한다. 예를 들어, 고유한 URL은 헤드리스 디바이스(120) 상의 패키징, 명령 메뉴얼 또는 스티커에 포함될 수 있다. 대안적 실시예들에서, 모바일 디바이스(110)는 디폴트 보안 크리덴셜(108)을 결정하기 위해서 헤드리스 디바이스(120)와 연관된 그래픽 정보(예를 들어, 바 코드)를 스캔하거나, 그렇지 않으면 캡처할 수 있다. 특정 실시예에서, 디폴트 보안 크리덴셜(108)은 계층-2(예를 들어, OSI(Open Systems Interconnect) 링크 계층) 크리덴셜이고 그리고/또는 헤드리스 디바이스(120)에서의, 계층-2 또는 그보다 낮은 계층의 동작들을 가능하게 한다.

[0024] 모바일 디바이스(110)는 EAP 교환(예를 들어, EAP 802.1X 교환, EAP-pwd 교환 또는 암호화된 키를 이용하는 EAP 교환(EAP-eke)), WPA2-PSK 교환 또는 이들의 임의의 결합을 사용하여 보안 채널(104)을 설정하기 위해서 디폴트 보안 크리덴셜(108)을 헤드리스 디바이스(120)로 송신할 수 있다. 헤드리스 디바이스(120) 디폴트 보안 크리덴셜(108)이 저장된 (예를 들어, 헤드리스 디바이스(120)의 메모리에 저장된) 디폴트 보안 크리덴셜(122)과 매칭하는지 여부를 결정할 수 있다. 디폴트 보안 크리덴셜(108)이 저장된 디폴트 보안 크리덴셜(122)과 매칭하지 않으면, 헤드리스 디바이스(120)는 EAP 교환을 종료할 수 있다. 디폴트 보안 크리덴셜(108)이 저장된 디폴트 보안 크리덴셜(122)과 매칭하면, EAP 교환이 완료될 수 있고, 보안 채널(104)이 설정될 수 있다. 모바일 디바이스(110)는 WLAN 크리덴셜(들)(105)을 보안 채널(104)을 통해 헤드리스 디바이스(120)로 송신할 수 있다. 그 다음, 헤드리스 디바이스(120)는 WLAN 크리덴셜(들)(105)을 사용하여 AP(130)를 통해 WLAN(140)에 연결할 수 있고, 그에 의해 WLAN 연결(106)이 설정된다.

[0025] 추가적으로, 사용자(102)는 애플리케이션 계층 크리덴셜(124)을 모바일 디바이스(110)를 통해 헤드리스 디바이스(120)로 제공할 수 있는데, 여기서 애플리케이션 계층 크리덴셜(124)은 헤드리스 디바이스(120)가 외부 네트워크(150)로의 연결(107)을 설정하는 것을 가능하게 한다. 예를 들어, 사용자(102)는 병원의 웹사이트에서의 사용자(102)의 계정(account)과 연관된 로그인 정보를 모바일 디바이스(110)에 입력할 수 있고, 모바일 디바이스(110)는 혈압계가 혈압 측정치들(blood pressure readings)을 병원 웹사이트에 업데이트할 수 있도록 이러한 로그인 정보를 혈압계와 같은 헤드리스 디바이스(120)로 전송할 수 있다.

[0026] 특정 실시예에서, 애플리케이션 계층 크리덴셜(124)은 계층-7(예를 들어, OSI(Open Systems Interconnect) 애플리케이션 계층) 크리덴셜이고 그리고/또는 헤드리스 디바이스(120)에서의, 계층-7 또는 그보다 낮은 계층의 동작들을 가능하게 한다. 헤드리스 디바이스(120)(예를 들어, 혈압계)는 헤드리스 디바이스(120) 내의 메모리에 애플리케이션 계층 크리덴셜(124)을 저장할 수 있다. 특정 대안적인 실시예에서, 헤드리스 디바이스(120)는, 애플리케이션 계층 크리덴셜(124)이 계층-2 동작들(예를 들어, WLAN(140)과의 연결을 셋업하는 것)뿐만 아니라 계층-7 동작들(예를 들어, 데이터를 외부 네트워크(150)로 전송하는 것) 둘 모두에 대하여 이후에 사용될 수 있도록, 그리고 사용자(102)가 단지 헤드리스 디바이스(120)와 연관된 한 세트의 크리덴셜들만을 기억할 필요가 있도록, 저장된 디폴트 보안 크리덴셜(122) 중 적어도 일부를 애플리케이션 계층 크리덴셜(124)로 대체할 수 있다.

[0027] 모바일 디바이스(110)는 계획된 파워-다운 기간을 다른 디바이스들에 통지하기 위해 "부재 통지(notice of absence)" 메시지를 전송하도록 구성될 수 있지만, 모바일 디바이스(110)가 Wi-Fi 다이렉트를 통해 헤드리스 디바이스(120) 또는 다른 이러한 디바이스들에 연결되는 동안, 모바일 디바이스(110)는 이러한 "부재 통지" 메시지들을 발행하는 것이 억제된다. "부재 통지" 메시지들의 발행의 억제에 의해, 모바일 디바이스(110)는, "부재 통지" 메시지들을 해석하기 위해, 장착되지 않은 레거시 Wi-Fi 다이렉트 클라이언트들과의 호환가능성을 유지한다.

[0028] 따라서, 시스템(100)은, 디바이스(예를 들어, 모바일 디바이스(110))가, WLAN(예를 들어, WLAN(140))에 액세스하도록 다른 디바이스(예를 들어, 헤드리스 디바이스(120))를 돕는 것을 가능하게 할 수 있다. 시스템(100)은 또한, 단일 세트의 보안 크리덴셜들을 사용하여 계층-2 및 계층-7 동작들의 관리를 가능하게 할 수 있어서, 더 단순한 디바이스 관리 방식을 야기할 수 있다. 헤드리스 디바이스(120)는 단지 예시를 위한 것이라는 점이 주

목되어야 한다. 모바일 디바이스(110)는 또한, 다른 타입들의 무선 디바이스들이 WLAN(140)에 연결하는 것을 가능하게 할 수 있다. 예를 들어, 모바일 디바이스(110)(예를 들어, 모바일 폰)는 넌(non)-헤드리스 디바이스(예를 들어, 태블릿 컴퓨터, 게임 콘솔 또는 다른 모바일 폰)가 WLAN(140)에 연결하는 것을 가능하게 할 수 있다.

[0029] 도 2는 등록자(enrollee)(220)가 EAP 교환을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 모바일 디바이스(210)와 연관된 메시징에 대한 특정 실시예를 예시하기 위한 레더 다이어그램이며, 일반적으로 200으로 표기된다. 예시적인 실시예에서, 모바일 디바이스(210)는 도 1의 모바일 디바이스(110)일 수 있고, 등록자(220)는 도 1의 헤드리스 디바이스(120)일 수 있다.

[0030] 동작 동안, 모바일 디바이스(210) 및 등록자(220)는 먼저, WPS 발견 동작(230)에 관여할 수 있다. WPS 발견 동작(230) 동안, 모바일 디바이스(210) 및 등록자(220)는 다양한 WPS 발견 메시지들(232)을 교환할 수 있다. WPS 발견 메시지들(232)에 기초하여, 모바일 디바이스(210)는 등록자(220)가 WPS-가능하다고 결정할 수 있다. 발견 동작(230)의 세부사항들은 도 5를 참조하여 추가로 설명된다.

[0031] WPS 발견 동작(230) 이후, 모바일 디바이스(210)는 디폴트 크리덴셜(예를 들어, 도 1의 디폴트 보안 크리덴셜(108))을 사용하여 EAP 교환(240)을 통해 등록자(220)와의 보안 채널을 설정할 수 있다. 특정 실시예에서, EAP 교환(240)은 EAP 802.1X 교환이다. 모바일 디바이스(210) 및 등록자(220)는 또한, 4-웨이 핸드쉐이크(handshake)(250)를 수행할 수 있는데, 이 동안은, 하나 또는 둘 이상의 암호화 키들이 생성되며, 모바일 디바이스(210)와 등록자(220) 사이에서 교환될 수 있다. 특정 실시예에서, 4-웨이 핸드쉐이크(250)는 WPA2 4-웨이 핸드쉐이크이다. 모바일 디바이스(210) 및 등록자(220)는 WPS 인증 및 구성 동작(280)에 관여할 수 있다. WPS 인증 및 구성 동작(280) 동안, 모바일 디바이스(210) 및 등록자(220)는 널(null) PIN(예를 들어, 공개 PIN)을 사용하여 하나 또는 둘 이상의 WPS 인증 및 구성 메시지들(282)을 교환할 수 있다. 하나 또는 둘 이상의 WLAN 크리덴셜들(예를 들어, 도 1의 WLAN 크리덴셜(들)(105))은, 등록자가 WLAN에 액세스하는 것을 가능하게 하기 위해서 모바일 디바이스(210)로부터 등록자(220)로 송신될 수 있다. 또한, 모바일 디바이스(210)는, 등록자(220)가 외부 네트워크(예를 들어, 도 1의 외부 네트워크(150))에 액세스하는 것을 가능하게 하기 위해서 애플리케이션 계층 크리덴셜(290)(예를 들어, 도 1의 애플리케이션 계층 크리덴셜(124))을 등록자(220)에게 제공할 수 있다.

[0032] EAP 802.1X 교환(240) 및 4-웨이 핸드쉐이크(250)가 보안 채널을 설정하는 단지 하나의 예로서 제공된다는 점이 주목되어야 한다. 모바일 디바이스(210)는 다양한 다른 기법들을 통해 등록자(220)와의 보안 채널을 설정할 수 있다. 예를 들어, 도 3은 등록자(220)가 EAP-pwd 교환(340)에 기초하여 생성된 PIN을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 모바일 디바이스(210)와 연관된 메시징에 대한 특정 실시예(300)를 예시하기 위한 레더 다이어그램이며, 일반적으로 300으로 표기된다.

[0033] 특정 실시예에서, MSK(master session key)는 EAP-pwd 교환(340) 동안 생성된다. 모바일 디바이스(210) 및 등록자(220)는 각각, 350 및 352에서 도시된 바와 같이, MSK의 일부를 사용하여 WPS PIN을 생성할 수 있다. WPS PIN은 도 2의 NULL PIN 대신에 WPS 인증 및 구성 동작(280) 동안 사용될 수 있다. 특정 실시예에서, MSK의 10개의 최소 유효 바이트 바이트(least significant byte)들은 WPS PIN으로서 사용된다.

[0034] 도 4는 등록자(220)가 PIN-기반 WPS 동작의 실패(430) 이후 도 2의 EAP 교환을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 모바일 디바이스(210)와 연관된 메시징에 대한 특정 실시예를 예시하기 위한 레더 다이어그램이며, 일반적으로 400으로 표기된다.

[0035] 예를 들어, 도 2의 WPS 발견 동작(230) 대신에 또는 도 2의 WPS 발견 동작(230)과 더불어, 모바일 디바이스(210) 및 등록자(220)는 PIN-기반 WPS를 완료하려고 시도할 수 있다. 그러나, PIN-기반 WPS는 (예를 들어, 부정확한 PIN이 제공되는 것 또는 어떠한 PIN도 제공되지 않는 것으로 인하여) 실패할 수 있다. 이 실패(430)는 도 2의 EAP 교환(240) 및 4-웨이 핸드쉐이크(250)를 사용하여 등록자(220)와의 보안 채널을 설정하도록 모바일 디바이스(210)를 트리거(trigger)할 수 있다.

[0036] 도 5는 등록자(220)가 EAP-pwd 교환을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 모바일 디바이스(210)와 연관된 메시징에 대한 특정 실시예를 예시하기 위한 레더 다이어그램이며, 일반적으로 500으로 표기된다.

[0037] 모바일 디바이스(210) 및 등록자(220)는 WPS 발견 동작(230)을 수행할 수 있다. WPS 발견 동작(230) 동안, 모바일 디바이스(210)는 등록자(220)와 다수의 메시지들(예를 들어, 도 5에서 1-10으로 표기된 메시지들)을 교환할 수 있다. 예를 들어, 모바일 디바이스(210)는 비컨 메시지 M1을 등록자(220)에게 송신할 수 있다. 이에 응

답하여, 등록자(220)는, 모바일 디바이스(210)로부터 등록자(220)로의 프로브 응답 메시지 M3을 트리거하는 프로브 요청 메시지 M2를 모바일 디바이스(210)로 송신할 수 있다. 등록자(220)는 등록자(220)로부터의 인증 응답 메시지 M5를 트리거하는 인증 요청 메시지 M4를 모바일 디바이스(210)로 송신하는 것을 진행할 수 있다. 연관 요청 메시지 M6, 연관 응답 메시지 M7, 근거리 네트워크를 통한 EAP 시작(EAPOL-시작) 메시지 M8, EAP-요청/아이덴티티 메시지 M9 및 EAP-요청/아이덴티티 메시지 M10은 또한, 도시된 바와 같이 교환될 수 있다.

[0038] WPS 발견 동작(230) 이후, 모바일 디바이스(210) 및 등록자(220)는 EAP-pwd 교환을 사용하여 WPS 인증 및 구성 동작(580)에 관여할 수 있다. 예를 들어, 모바일 디바이스(210)는 WPS 인증 및 구성 동작(580)의 시작을 시그널링하기 위해서 EAP-요청 메시지 M11을 등록자(220)에게 송신할 수 있다. 등록자(220)는 EAP-pwd-ID/요청 메시지 M12를 모바일 디바이스(210)로 송신할 수 있고, 모바일 디바이스(210)는 EAP-pwd-ID/응답 메시지 M13으로 응답할 수 있다. 모바일 디바이스(210) 및 등록자(220)는, EAP-pwd-커밋(commit)/요청 메시지 M14, EAP-pwd-커밋/응답 메시지 M15, EAP-pwd-확인/요청 메시지 M16 및 EAP-pwd-확인/응답 메시지 M17을 교환한 이후, MSK를 컴퓨팅할 수 있다. 특정 실시예에서, SEP 2.0 클라이언트 인증 GUID(globally unique identifier)는 EAP-요청 메시지 M18을 통해 등록자(220)로부터 모바일 디바이스로 전송된다. 모바일 디바이스(210)는 링크 계층(L2) 크리덴셜(예를 들어, 도 1의 WLAN 크리덴셜(들)(105)) 및/또는 애플리케이션 계층(L7) 크리덴셜(예를 들어, 도 1의 애플리케이션 계층 크리덴셜(124))을 EAP-응답 메시지 M19를 통해 등록자(220)에게 송신할 수 있다.

[0039] 도 6은 등록자(220)가 WPA2-PSK 교환(640) 동안 생성된 PIN을 사용하여 WLAN에 액세스하는 것을 가능하게 하는 모바일 디바이스(210)와 연관된 메시징에 대한 특정 실시예를 예시하기 위한 레더 다이어그램이다.

[0040] 도 2의 WPS 발견 동작(230) 대신에, 모바일 디바이스(210) 및 등록자(220)는 Wi-Fi 다이렉트 발견 동작(630)을 수행할 수 있는데, 이는 다양한 Wi-Fi 다이렉트 발견 메시지들(632)을 교환하는 것을 포함할 수 있다. 특정 실시예에서, 모바일 디바이스(210)는 등록자(220)에 대하여 자율적 Wi-Fi 다이렉트 그룹 운영자(GO)로서의 역할을 한다. 모바일 디바이스(210)는 WPA2-PSK 교환(640)을 사용하여 등록자(220)와의 보안 채널을 설정할 수 있다. PMK(pairwise master key)는 WPA2-PSK 교환(640) 동안 생성될 수 있고, 모바일 디바이스(210) 및 등록자(220)는, 650 및 652에 도시된 바와 같이, WPS PIN으로서 PMK의 일부(예를 들어, 10개의 최소 유효 바이트들)를 사용할 수 있다. 모바일 디바이스(210) 및 등록자(220)는 WPS PIN을 사용하여 WPS 인증 및 구성 동작(280)에 관여할 수 있다.

[0041] 따라서, 도 2-6은 모바일 디바이스(210)와 등록자(220)(예를 들어, 헤드리스 디바이스) 사이의 보안 채널을 셋업하는 다양한 예들을 예시한다. 보안 채널은, 등록자(220)가 WLAN 및 외부 네트워크에 각각 연결하는 것을 가능하게 하는 WLAN 크리덴셜(들) 및 애플리케이션 계층 크리덴셜(들)을 등록자(220)에게 제공하기 위해서 모바일 디바이스(210)에 의해 사용될 수 있다.

[0042] 도 7은 도 2-4의 메시징에 따른, 도 1의 모바일 디바이스(110)에서의 동작 방법(700)의 특정 실시예를 예시하기 위한 흐름도이다.

[0043] 방법(700)은 702에서, 제 1 디바이스(예를 들어, 모바일 폰)가 WLAN(wireless local area network)에 연결되고 제 2 디바이스(예를 들어, 헤드리스 디바이스)가 WLAN에 연결되지 않은 동안, EAP(extensible authentication protocol) 교환을 사용하여 제 1 디바이스와 제 2 디바이스 사이의 보안 채널을 설정하는 단계를 포함할 수 있다. 예를 들어, 도 1에서, 모바일 디바이스(110)는, 모바일 디바이스(110)가 WLAN(140)에 연결되고 헤드리스 디바이스(120)가 WLAN(140)에 연결되지 않은 동안, 디폴트 보안 크리덴셜(108)을 사용하여 헤드리스 디바이스(120)와의 보안 채널(104)을 설정할 수 있다.

[0044] 방법(700)은 또한, 704에서, 제 2 디바이스가 WLAN에 연결하는 것을 가능하게 하기 위해서, 보안 채널을 통해 제 1 디바이스로부터 제 2 디바이스로, WLAN과 연관된 적어도 하나의 크리덴셜을 전송하는 단계를 포함할 수 있다. 예를 들어, 도 1에서, 모바일 디바이스(110)는 헤드리스 디바이스(120)가 WLAN(140)에 연결하는 것을 가능하게 하기 위해서 WLAN 크리덴셜(들)(105)을 헤드리스 디바이스(120)에 전송할 수 있다. 그 다음, 헤드리스 디바이스(120)는 WLAN 크리덴셜(들)(105)을 사용하여 WLAN 연결(106)을 설정할 수 있다.

[0045] 도 8은 도 2-4의 메시징에 따른, 도 1의 헤드리스 디바이스(120)에서의 동작 방법(800)의 특정 실시예를 예시하기 위한 흐름도이다.

[0046] 방법(800)은 802에서, 제 1 디바이스가 WLAN에 연결되지 않고 제 2 디바이스가 WLAN에 연결되는 동안, 제 1 디바이스에서 EAP 교환 동안 제 2 디바이스로부터 보안 크리덴셜을 수신하는 단계를 포함할 수 있다. 예를 들어,

도 1에서, 헤드리스 디바이스(120)는, 헤드리스 디바이스(120)가 WLAN(140)에 연결되지 않고 모바일 디바이스(110)가 WLAN(140)에 연결되는 동안, 모바일 디바이스(110)로부터 보안 채널(104)을 통해 디폴트 보안 크리덴셜(108)을 수신할 수 있다.

[0047] 방법(800)은 또한, 804에서, 수신된 크리덴셜이 저장된 크리덴셜과 매칭하는지 여부를 결정하는 단계를 포함할 수 있다. 예를 들어, 도 1에서, 헤드리스 디바이스(120)는 디폴트 보안 크리덴셜(108)이 저장된 디폴트 보안 크리덴셜(122)과 매칭하는지 여부를 결정할 수 있다. 수신된 크리덴셜이 저장된 크리덴셜과 매칭하지 않는다면, 방법(800)은 806에서, EAP 교환을 종료하는 단계를 포함할 수 있다. 수신된 크리덴셜이 저장된 크리덴셜과 매칭한다면, 방법(800)은 808에서, EAP 교환을 완료하는 단계 및 제 1 디바이스와 제 2 디바이스 사이의 보안 채널을 설정하는 단계를 포함할 수 있다. 예를 들어, 도 1에서, EAP 교환이 완료될 수 있고, 보안 채널(104)이 설정될 수 있다.

[0048] 방법(800)은 810에서, 제 2 디바이스로부터 보안 채널을 통해, WLAN과 연관된 적어도 하나의 크리덴셜을 수신하는 단계를 더 포함할 수 있다. 예를 들어, 도 1에서, 헤드리스 디바이스(120)는 모바일 디바이스(110)로부터 보안 채널(104)을 통해 WLAN 크리덴셜(들)(105)을 수신할 수 있다. 방법(800)은 812에서, 제 1 디바이스에서, 적어도 하나의 크리덴셜을 사용하여 WLAN으로의 연결을 설정하는 단계를 포함할 수 있다. 예를 들어, 도 1에서, 헤드리스 디바이스(120)는 WLAN 크리덴셜(들)(105)을 사용하여 WLAN(140)으로의 WLAN 연결(106)을 설정할 수 있다.

[0049] 방법(800)은 또한, 814에서, 제 2 디바이스로부터 적어도 하나의 애플리케이션 계층 크리덴셜을 수신하는 단계를 포함할 수 있다. 예를 들어, 도 1에서, 헤드리스 디바이스(120)는 모바일 디바이스(110)로부터 애플리케이션 계층 크리덴셜(124)을 수신할 수 있다. 방법(800)은 816에서, 저장된 보안 크리덴셜을 적어도 하나의 애플리케이션 계층 크리덴셜의 적어도 일부로 대체하는 단계를 더 포함할 수 있다. 예를 들어, 도 1에서, 헤드리스 디바이스(120)는 저장된 디폴트 보안 크리덴셜(122)의 적어도 일부를 애플리케이션 계층 크리덴셜(124)로 대체할 수 있다. 대안적인 실시예에서, 디폴트 크리덴셜과 더불어, 애플리케이션 계층 크리덴셜이 저장된다.

[0050] 방법(800)은 818에서, WLAN을 통해, WLAN 외부의 네트워크에 액세스하기 위해서 적어도 하나의 애플리케이션 계층 크리덴셜을 사용하는 단계를 포함할 수 있다. 예를 들어, 도 1에서, 헤드리스 디바이스(120)는 애플리케이션 계층 크리덴셜(124)을 사용하여 외부 네트워크(150)에 액세스할 수 있다.

[0051] 도 9는 도 5의 메시징에 따른, 도 1의 시스템(100)에서의 동작 방법(900)의 특정 실시예를 예시하기 위한 흐름도이다.

[0052] 방법(900)은 902에서, WPS 발견 동작 동안 제 1 디바이스로부터 제 2 디바이스로 적어도 하나의 제 1 메시지를 전송하는 단계를 포함한다. 예를 들어, 도 5를 참조하면, 모바일 디바이스(210)는 WPS 발견 동작(230) 동안 등록자(220)와 메시지들 M1-M10을 교환할 수 있다.

[0053] 방법(900)은 또한, 904에서, WPS 인증 및 구성 동작 동안 제 1 디바이스로부터 제 2 디바이스로 적어도 하나의 제 2 메시지를 전송하는 단계를 포함할 수 있다. 적어도 하나의 제 2 메시지는 EAP-pwd 교환과 연관된 데이터를 포함할 수 있다. 예를 들어, 도 5를 참조하면, 모바일 디바이스(210) 및 등록자(220)는 메시지들 M11-M19에 대응하는 EAP-pwd 교환을 사용하여 WPS 인증 및 구성 동작(580)을 수행할 수 있다.

[0054] 도 10은 도 6의 메시징에 따른, 도 1의 시스템(100)에서의 동작 방법(1000)의 특정 실시예를 예시하기 위한 흐름도이다.

[0055] 방법(1000)은 1002에서, 제 1 디바이스가 WLAN에 연결되고 제 2 디바이스가 WLAN에 연결되지 않은 동안, WPA2-PSK 교환을 사용하여 제 1 디바이스와 제 2 디바이스 사이의 보안 채널을 설정하는 단계를 포함한다. 예를 들어, 도 6을 참조하면, 모바일 디바이스(210)는 WPA2-PSK 교환(640)을 사용하여 등록자(220)와의 보안 채널을 설정할 수 있다. 방법(1000)은 또한, 1004에서, 제 2 디바이스가 WLAN에 연결하는 것을 가능하게 하기 위해서, 제 1 디바이스로부터 제 2 디바이스로 보안 채널을 통해, WLAN과 연관된 적어도 하나의 크리덴셜을 전송하는 단계를 포함할 수 있다. 특정 실시예에서, 적어도 하나의 WLAN 크리덴셜은 도 1의 WLAN 크리덴셜(들)(105)일 수 있다. 그 다음, 헤드리스 디바이스(120)는 WLAN 크리덴셜(들)(105)을 사용하여 WLAN 연결(106)을 설정할 수 있다.

[0056] 도 11은 통신 디바이스(1100)의 블록도이다. 일 실시예에서, 통신 디바이스(1100) 또는 이의 컴포넌트들은, 도 1의 모바일 디바이스(110), 도 2-6의 모바일 디바이스(210) 또는 이들의 임의의 결합을 포함하거나, 이들에 포함된다. 추가로, 도 7 및 9-10에서 설명된 방법들 전부 또는 일부는 통신 디바이스(1100) 또는 이의 컴포넌트

들에서, 또는 통신 디바이스(1100) 또는 이의 컴포넌트들에 의해, 수행될 수 있다. 통신 디바이스(1100)는 메모리(1132)에 커플링되는 프로세서(1110), 이를테면, 디지털 신호 프로세서(DSP)를 포함한다.

[0057] 메모리(1132)는 명령들(1160)을 저장하는 비-일시적 유형의 컴퓨터 판독가능한 그리고/또는 프로세서 판독가능한 저장 디바이스일 수 있다. 명령들(1160)은 본 명세서에 설명된 하나 또는 둘 이상의 기능들 또는 방법들, 이를테면, 도 7 및 9-10을 참조하여 설명된 방법들을 수행하기 위해서 프로세서(1110)에 의해 실행가능할 수 있다. 메모리(1132)는 또한, 하나 또는 둘 이상의 WLAN 크리덴셜들(1190)(예를 들어, 도 1의 WLAN 크리덴셜(들)(105)), 디폴트 크리덴셜(1192)(예를 들어, 도 1의 저장된 디폴트 보안 크리덴셜(122)), 및/또는 애플리케이션 계층 크리덴셜(1194)(예를 들어, 도 1의 애플리케이션 계층 크리덴셜(124))을 저장할 수 있다.

[0058] 도 11은, 통신 디바이스(1100)가 또한, 프로세서(1110) 및 디스플레이 디바이스(1128)에 커플링되는 디스플레이 제어기(1126)를 포함할 수 있다는 것을 나타낸다. 코더/디코더(CODEC)(1134)는 또한, 프로세서(1110)에 커플링될 수 있다. 스피커(1136) 및 마이크로폰(1138)은 CODEC(1134)에 커플링될 수 있다. 도 11은 또한, 무선 제어기(1140)가 프로세서(1110)에 커플링될 수 있음 – 무선 제어기(1140)는 트랜시버(1150)를 통해 안테나(1142)와 통신함 – 을 표시한다. 따라서, 무선 제어기(1140), 트랜시버(1150) 및 안테나(1142)는 통신 디바이스(1100)에 의해 무선 통신을 가능하게 하는 무선 인터페이스를 표현할 수 있다. 예를 들어, 통신 디바이스(1100)가 도 1의 모바일 디바이스(110)인 경우, 이러한 무선 인터페이스는, 도시된 바와 같이, 헤드리스 디바이스(120) 또는 AP(130)와 통신하기 위해서 사용될 수 있다. 통신 디바이스(1100)는 다수의 무선 인터페이스들을 포함할 수 있는데, 여기서 서로 다른 무선 네트워크들은 서로 다른 네트워킹 기술들 또는 네트워킹 기술들의 결합들을 지원하도록 구성된다.

[0059] 특정 실시예에서, 프로세서(1110), 디스플레이 제어기(1126), 메모리(1132), CODEC(1134), 무선 제어기(1140) 및 트랜시버(1150)는 시스템-인-패키지 또는 시스템-온-칩 디바이스(1122)에 포함된다. 특정 실시예에서, 입력 디바이스(1130) 및 파워 서플라이(1144)는 시스템-온-칩 디바이스(1122)에 커플링된다. 더욱이, 특정 실시예에서, 도 11에 예시된 바와 같이, 디스플레이 디바이스(1128), 입력 디바이스(1130), 스피커(1136), 마이크로폰(1138), 안테나(1142) 및 파워 서플라이(1144)는 시스템-온-칩 디바이스(1122) 외부에 있다. 그러나, 디스플레이 디바이스(1128), 입력 디바이스(1130), 스피커(1136), 마이크로폰(1138), 안테나(1142) 및 파워 서플라이(1144) 각각은 시스템-온-칩 디바이스(1122)의 컴포넌트, 이를테면, 인터페이스 또는 제어기에 커플링될 수 있다.

[0060] 통신 디바이스(1100)의 하나 또는 둘 이상의 컴포넌트들 또는 이와 유사한 컴포넌트들은 또한, 헤드리스 디바이스, 이를테면, 도 1의 헤드리스 디바이스(120), 도 2-6의 등록자(220) 또는 이들의 임의의 결합에 통합될 수 있다. 예를 들어, 도 1의 헤드리스 디바이스(120) 및 도 2-6의 등록자(220)는 무선 제어기, 트랜시버, 안테나, 프로세서 및 도 8의 방법을 수행하기 위해서 프로세서에 의해 실행가능한 명령들을 저장하는 메모리를 포함할 수 있다.

[0061] 설명된 실시예들과 함께, 장치는, 장치가 WLAN에 연결되고 제 2 장치가 WLAN에 연결되지 않은 동안, EAP 교환을 사용하여 제 2 장치로의 보안 채널을 설정하기 위한 수단을 포함할 수 있다. 예를 들어, 설정하기 위한 수단은, 도 1의 모바일 디바이스(110)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 프로세서), 도 2-6의 모바일 디바이스(210)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 프로세서), 도 11의 프로세서(1110), 무선 제어기(1140), 트랜시버(1150), 안테나(1142), 보안 채널을 설정하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다. 제 1 장치는 또한, 제 2 장치가 WLAN에 연결하는 것을 가능하게 하기 위해서, 보안 채널을 통해 제 2 장치로, WLAN과 연관된 적어도 하나의 크리덴셜을 전송하기 위한 수단을 포함할 수 있다. 예를 들어, 전송하기 위한 수단은, 도 1의 모바일 디바이스(110)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 송신기), 도 2-6의 모바일 디바이스(210)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 송신기), 도 11의 무선 제어기(1140), 트랜시버(1150), 안테나(1142), 데이터를 전송하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다.

[0062] 특정 실시예에서, 제 1 장치는 또한, 보안 크리덴셜을 표시하는 입력을 수신하기 위한 수단을 포함한다. 예를 들어, 수신하기 위한 수단은, 도 1의 모바일 디바이스(110)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 수신기), 도 2-6의 모바일 디바이스(210)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 수신기), 도 11의 무선 제어기(1140), 트랜시버(1150), 안테나(1142), 데이터를 수신하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다.

[0063] 다른 장치는, 장치가 WLAN에 연결되지 않고 제 2 장치가 WLAN에 연결되는 동안, 제 2 장치로의 보안 채널을 설

정하기 위한 수단을 포함할 수 있다. 예를 들어, 설정하기 위한 수단은, 도 1의 헤드리스 디바이스(120)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 프로세서), 도 2-6의 등록자(220)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 프로세서), 무선 제어기, 트랜시버, 안테나, 보안 채널을 설정하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다. 장치는 또한, 제 2 장치로부터 보안 채널을 통해, WLAN과 연관된 적어도 하나의 크리덴셜을 수신하기 위한 수단을 포함할 수 있다. 설정하기 위한 수단은 적어도 하나의 크리덴셜을 사용하여 WLAN으로의 연결을 설정하도록 구성된다. 예를 들어, 수신하기 위한 수단은, 도 1의 헤드리스 디바이스(120)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 수신기), 도 2-6의 등록자(220)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 수신기), 무선 제어기, 트랜시버, 안테나, 데이터를 수신하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다.

[0064] 특정 실시예에서, 장치는 보안 크리덴셜을 저장하기 위한 수단을 포함한다. 예를 들어, 저장하기 위한 수단은, 도 1의 헤드리스 디바이스(120)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 메모리), 도 2-6의 등록자(220)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 메모리), 데이터를 저장하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다.

[0065] 다른 장치는 제 1 메시지 및 제 2 메시지를 생성하기 위한 수단을 포함할 수 있다. 예를 들어, 생성하기 위한 수단은, 도 1의 모바일 디바이스(110)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 프로세서), 도 2-6의 모바일 디바이스(210)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 프로세서), 도 11의 프로세서(1110), 메시지들을 생성하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다. 장치는 또한, 전송하기 위한 수단을 포함할 수 있는데, 여기서 전송하기 위한 수단은, WPS 발견 동작 동안 적어도 제 1 메시지를 제 2 디바이스로 전송하고, WPS 발견 동작 이후의 WPS 인증 및 구성 동작 동안 제 2 메시지를 제 2 디바이스로 전송하도록 구성된다. 제 2 메시지는, 단지 EAP-pwd만을 사용하는 EAP 교환과 연관된 데이터를 포함할 수 있다. 예를 들어, 전송하기 위한 수단은, 도 1의 모바일 디바이스(110)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 송신기), 도 2-6의 모바일 디바이스(210)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 송신기), 도 11의 무선 제어기(1140), 트랜시버(1150), 안테나(1142), 데이터를 전송하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다.

[0066] 다른 장치는, 장치가 WLAN(wireless local area network)에 연결되고 제 2 장치가 WLAN에 연결되지 않은 동안, 보안 채널을 설정하기 위한 수단을 포함할 수 있다. 예를 들어, 보안 채널을 설정하기 위한 수단은, 도 1의 모바일 디바이스(110)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 프로세서), 도 2-6의 모바일 디바이스(210)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 프로세서), 도 11의 프로세서(1110), 무선 제어기(1140), 트랜시버(1150), 안테나(1142), 보안 채널을 설정하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다. 장치는 또한, 제 2 디바이스가 WLAN에 연결하는 것을 가능하게 하기 위해서, 보안 채널을 통해 제 2 장치로, WLAN과 연관된 적어도 하나의 크리덴셜을 전송하기 위한 수단을 포함할 수 있다. 예를 들어, 전송하기 위한 수단은, 도 1의 모바일 디바이스(110)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 송신기), 도 2-6의 모바일 디바이스(210)의 하나 또는 둘 이상의 컴포넌트들(예를 들어, 송신기), 도 11의 무선 제어기(1140), 트랜시버(1150), 안테나(1142), 데이터를 전송하도록 구성되는 하나 또는 둘 이상의 다른 디바이스들, 또는 이들의 임의의 결합을 포함할 수 있다.

[0067] 개시된 실시예들 중 하나 또는 둘 이상은, 통신 디바이스, 고정 위치 데이터 유닛, 모바일 위치 데이터 유닛, 모바일 폰, 셀룰러 폰, 컴퓨터, 태블릿, 휴대용 컴퓨터 또는 데스크탑 컴퓨터를 포함할 수 있는 시스템 또는 장치로 구현될 수 있다. 추가적으로, 시스템 또는 장치는, 셋탑 박스, 엔터테인먼트 유닛, 네비게이션 디바이스, 개인용 디지털 보조기(PDA), 모니터, 컴퓨터 모니터, 텔레비전, 튜너, 라디오, 위성 라디오, 뮤직 플레이어, 디지털 뮤직 플레이어, 휴대용 뮤직 플레이어, 비디오 플레이어, 디지털 비디오 플레이어, 디지털 비디오 디스크(DVD) 플레이어, 휴대용 디지털 비디오 플레이어, 데이터 또는 컴퓨터 명령들을 저장 또는 리트리브하는 임의의 다른 디바이스 또는 이들의 결합을 포함할 수 있다. 다른 예시적인 비-제한적 예로서, 시스템 또는 장치는, 원격 유닛들, 이를테면, 모바일 폰들, 핸드-헬드 개인 통신 시스템(PCS) 유닛들, 휴대용 데이터 유닛들, 이를테면, 개인용 데이터 보조기들, 글로벌 포지셔닝 시스템(GPS) 가능 디바이스들, 네비게이션 디바이스들, 고정 위치 데이터 유닛들, 이를테면, 검침 장비(meter reading equipment) 또는 데이터 또는 컴퓨터 명령들을 저장 또는 리트리브하는 임의의 다른 디바이스, 또는 이들의 임의의 결합을 포함할 수 있다. 도 1-11 중 하나 또는 둘 이상은 본 개시의 교시들에 따른 시스템들, 장치들 및/또는 방법들을 예시할 수 있지만, 본 개시는 이 예시된 시스템들, 장치들 및/또는 방법들에 제한되는 것은 아니다. 본 개시의 실시예들은, 메모리를 포함하는 집적 회로, 프로세서 및 온-칩 회로를 포함하는 임의의 디바이스에서 적합하게 사용될 수 있다.

[0068] "제 1", "제 2" 등과 같은 표기를 사용하는 본 명세서에서의 엘리먼트에 대한 임의의 지칭은 일반적으로 이러한 엘리먼트들의 양 또는 순서를 제한하지 않는다는 것이 이해되어야 한다. 오히려, 이러한 표기들은 둘 또는 셋 이상의 엘리먼트들 또는 엘리먼트의 인스턴스들을 구별하는 편리한 방법으로서 본 명세서에서 사용될 수 있다. 따라서, 제 1 및 제 2 엘리먼트들에 대한 지칭은 단지 두 개의 엘리먼트들만이 사용될 수 있다는 것 또는 제 1 엘리먼트가 어떤 방식으로 제 2 엘리먼트에 선행하여야 한다는 것을 의미하지 않는다. 또한, 별도의 언급이 없는 한, 한 세트의 엘리먼트들은 하나 또는 둘 이상의 엘리먼트들을 포함할 수 있다.

[0069] 본 명세서에서 사용되는 바와 같이, "결정하는"이라는 용어는 매우 다양한 동작들을 포함한다. 예를 들어, "결정하는"은 계산하는, 컴퓨팅하는, 프로세싱하는, 유도하는, 조사하는, 검색(예를 들어, 표, 데이터베이스 또는 또 다른 데이터 구조에서 검색)하는, 확인하는 등을 포함할 수 있다. 또한, "결정하는"은 수신하는(예를 들어, 정보를 수신하는), 액세스하는(예를 들어, 메모리 내의 데이터에 액세스하는) 등을 포함할 수 있다. 또한, "결정하는"은 해결하는, 선정하는, 선택하는, 설정하는 등을 포함할 수 있다. 게다가, 본 명세서에서 사용되는 바와 같은 "채널 폭"은 특정 양상들에서 대역폭을 포함할 수 있거나 또는 이러한 대역폭으로 또한 지칭될 수 있다.

[0070] 본 명세서에서 사용되는 바와 같이, 항목들의 리스트 중 "적어도 하나"를 지칭하는 문구는 단일 멤버들을 포함하여, 이러한 항목들의 임의의 결합을 지칭한다. 일례로서, "a, b, 또는 c 중 적어도 하나"는 a, b, c, a-b, a-c, b-c 및 a-b-c를 커버하도록 의도된다.

[0071] 다양한 예시적인 컴포넌트들, 블록들, 구성들, 모듈들, 회로들 및 단계들이 일반적으로 이들의 기능적 관점에서 위에서 설명되었다. 이러한 기능이 하드웨어로 구현되는지, 또는 프로세서 실행가능한 명령들로 구현되는지는 특정한 애플리케이션 및 전체 시스템 상에 부과되는 설계 제약들에 의존한다. 추가적으로, 위에서 설명된 방법들의 다양한 동작들은 다양한 하드웨어 및/또는 소프트웨어 컴포넌트(들), 회로들 및/또는 모듈(들)과 같은 동작들을 수행할 수 있는 임의의 적합한 수단에 의해 수행될 수 있다. 일반적으로, 도 1-11에서 예시되는 임의의 동작들은 동작들을 수행할 수 있는 대응하는 기능적 수단에 의해 수행될 수 있다. 당업자들은 설명된 기능을 각각의 특정한 애플리케이션에 대하여 다양한 방식들로 구현할 수 있지만, 이러한 구현 결정들이 본 개시의 범위를 벗어나게 하는 것으로 해석되어서는 안 된다.

[0072] 당업자들은, 본 개시와 관련하여 설명되는 다양한 예시적인 논리 블록들, 구성들, 모듈들, 회로들 및 알고리즘 단계들이 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적회로(ASIC), 필드 프로그래머블 게이트 어레이(FPGA) 또는 프로그래머블 논리 디바이스(PLD), 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들(예를 들어, 전자 하드웨어), 프로세서에 의해 실행되는 컴퓨터 소프트웨어, 또는 본 명세서에 설명된 기능들을 수행하도록 설계된 이들의 임의의 결합으로 구현 또는 수행될 수 있다는 것을 추가로 인식할 것이다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 상업적으로 이용가능한 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 디바이스들의 결합, 예를 들어 DSP 및 마이크로프로세서의 결합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 또는 둘 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0073] 하나 또는 둘 이상의 양상들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 결합으로 구현될 수 있다. 소프트웨어로 구현되는 경우, 상기 기능들은 컴퓨터 판독가능한 매체 상에 하나 또는 둘 이상의 명령들 또는 코드로서 저장될 수 있다. 컴퓨터 판독가능한 매체들은 컴퓨터 판독가능한 저장 매체들, 및 한 장소에서 다른 장소로 컴퓨터 프로그램 데이터의 이전을 가능하게 하는 임의의 매체를 포함하는 통신 매체들을 포함한다. 저장 매체들은 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체들일 수 있다. 제한이 아닌 예로서, 이러한 컴퓨터 판독가능한 저장 매체들은 RAM(random access memory), ROM(read-only memory), PROM(programmable read-only memory), EPROM(erasable PROM), EEPROM(electrically erasable PROM), 레지스터(들), 하드 디스크, 이동가능한 디스크, CD-ROM(compact disc read-only memory), 다른 광 디스크 저장소, 자기 디스크 저장소, 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 저장하는데 사용될 수 있고, 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 대안적으로, 컴퓨터 판독가능한 매체들(예를 들어, 저장 매체)은 프로세서에 통합될 수 있다. 프로세서 및 저장 매체는 ASIC(application-specific integrated circuit)에 상주할 수 있다. ASIC는 컴퓨팅 디바이스 또는 사용자 단말에 상주할 수 있다. 대안적으로, 프로세서 및 저장 매체는 컴퓨팅 디바이스 또는 사용자 단말에서 개별 컴포넌트들로서 상주할 수 있다.

[0074] 또한, 임의의 연결(connection)이 컴퓨터 판독가능한 매체로 적절히 지칭된다. 예를 들어, 소프트웨어가 웹사

이트, 서버, 또는 다른 원격 소스로부터 동축 케이블, 광섬유 케이블, 꼬임 쌍선, 디지털 가입자 라인(DSL), 또는 적외선, 라디오, 및 마이크로파와 같은 무선 기술들을 사용하여 송신되는 경우, 동축 케이블, 광섬유 케이블, 꼬임 쌍선, DSL, 또는 적외선, 라디오, 및 마이크로파와 같은 무선 기술들이 매체의 정의에 포함된다. 본 명세서에서 사용되는 디스크(disk 및 disc)는 컴팩트 디스크(disc)(CD), 레이저 디스크(disc), 광 디스크(disc), 디지털 다목적 디스크(disc)(DVD) 및 플로피 디스크(disk)를 포함하며, 여기서 디스크(disk)들은 통상적으로 데이터를 자기적으로 재생하지만, 디스크(disc)들은 레이저들을 이용하여 광학적으로 데이터를 재생한다. 따라서, 일부 양상들에서, 컴퓨터 판독가능한 매체는 비-일시적 컴퓨터 판독가능한 매체(예를 들어, 유형의 매체들)를 포함할 수 있다. 또한, 일부 양상들에서, 컴퓨터 판독가능한 매체는 일시적 컴퓨터 판독가능한 매체(예를 들어, 신호)를 포함할 수 있다. 위의 것의 결합들 또한 컴퓨터 판독가능한 매체들의 범위 내에 포함되어야 한다.

[0075] 본 명세서에 개시된 방법들은 하나 또는 둘 이상의 단계들 또는 동작들을 포함한다. 방법 단계들 및/또는 동작들은 청구항들의 범위로부터 벗어나지 않고 서로 교환될 수 있다. 다시 말해서, 단계들 또는 동작들의 특정 순서가 특정되지 않는 한, 특정 단계들 및/또는 동작들의 순서 및/또는 사용은 본 개시의 범위로부터 벗어나지 않고 변경될 수 있다.

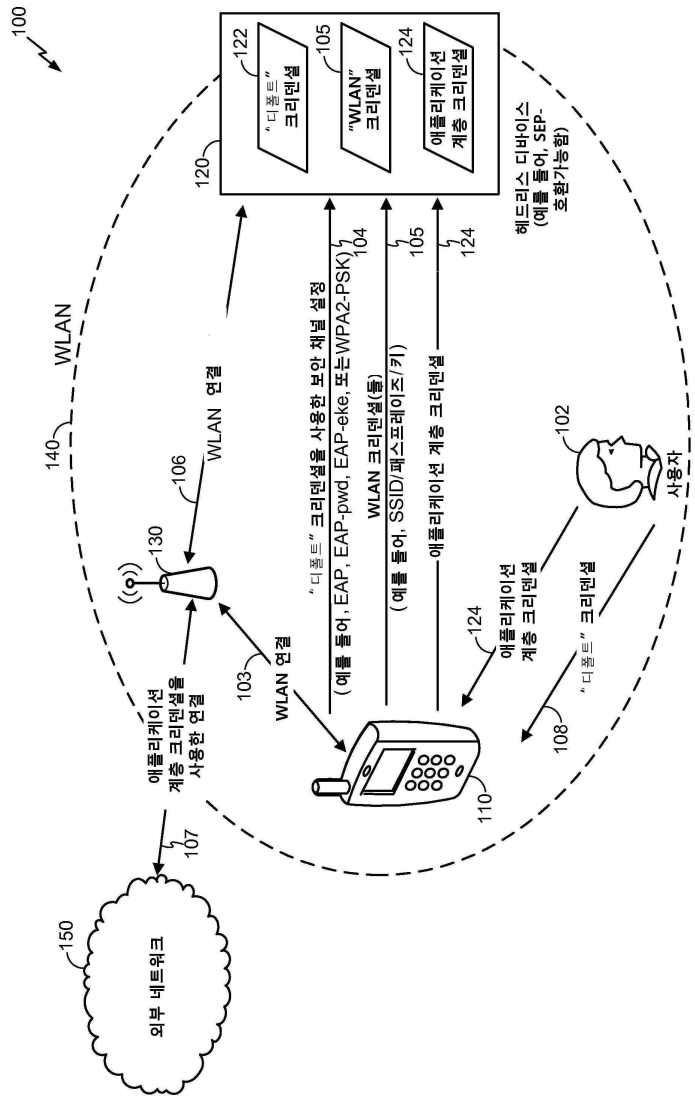
[0076] 따라서, 특정 양상들은 본 명세서에서 제시된 동작들을 수행하기 위한 컴퓨터 프로그램 물건을 포함할 수 있다. 예를 들어, 컴퓨터 프로그램 물건은 명령들이 저장된(그리고/또는 인코딩된) 컴퓨터 판독가능한 저장 매체를 포함할 수 있으며, 명령들은 본 명세서에 설명된 동작들을 수행하기 위해서 하나 또는 둘 이상의 프로세서들에 의해 실행가능하다. 컴퓨터 프로그램 물건은 패키징 재료를 포함할 수 있다.

[0077] 추가로, 본 명세서에 설명된 방법들 및 기법들을 수행하기 위한 모듈들 및/또는 다른 적절한 수단은 적용가능한 경우, 사용자 단말 및/또는 기지국에 의해 다운로드되고 그리고/또는 그렇지 않으면 획득될 수 있다는 것이 인식되어야 한다. 대안적으로, 본 명세서에 설명된 다양한 방법들은 저장 수단(예를 들어, RAM, ROM 또는 물리적 저장 매체, 이를테면, 컴팩트 디스크(CD))을 통해 제공될 수 있다. 더욱이, 본 명세서에 설명된 방법들 및 기법들을 제공하기 위한 임의의 다른 적합한 기법이 이용될 수 있다. 본 개시의 범위는 위에서 예시된 정확한 구성 및 컴포넌트들로 제한되지 않는다는 것이 이해될 것이다.

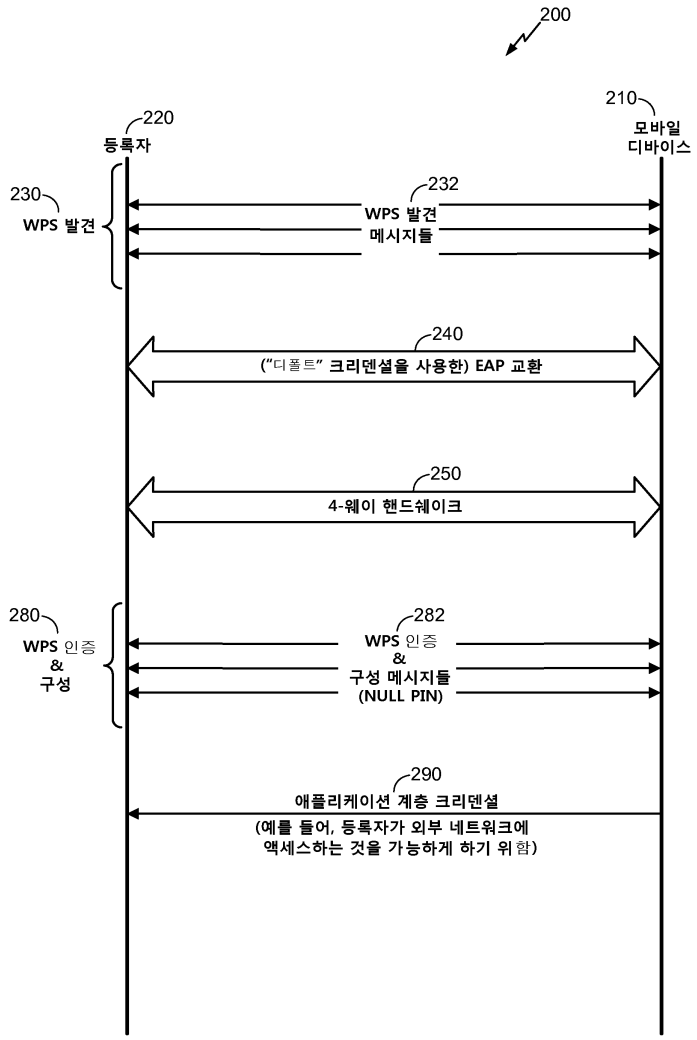
[0078] 개시된 실시예들의 이전의 설명은 당업자가 개시된 실시예들을 실시하거나 또는 이용할 수 있도록 제공된다. 위의 설명은 본 개시의 양상들에 관련되지만, 본 개시의 다른 양상들이 본 개시의 기본적 범위를 벗어나지 않고 고안될 수 있고, 그 범위는 다음의 청구항들에 의해 결정된다. 본 개시 또는 청구항들의 범위로부터 벗어나지 않으면서 다양한 변경들, 변화들 및 변형들이 본 명세서에 설명된 실시예들의 배열, 동작 및 세부사항들에서 이루어질 수 있다. 따라서, 본 개시는 본 명세서에서의 실시예들에 제한되는 것으로 의도되는 것이 아니라, 다음의 청구항들 및 이의 등가물들에 의해 정의되는 바와 같은 원리들 및 신규한 특징들과 일치하는 가능한 가장 넓은 범위를 따를 것이다.

도면

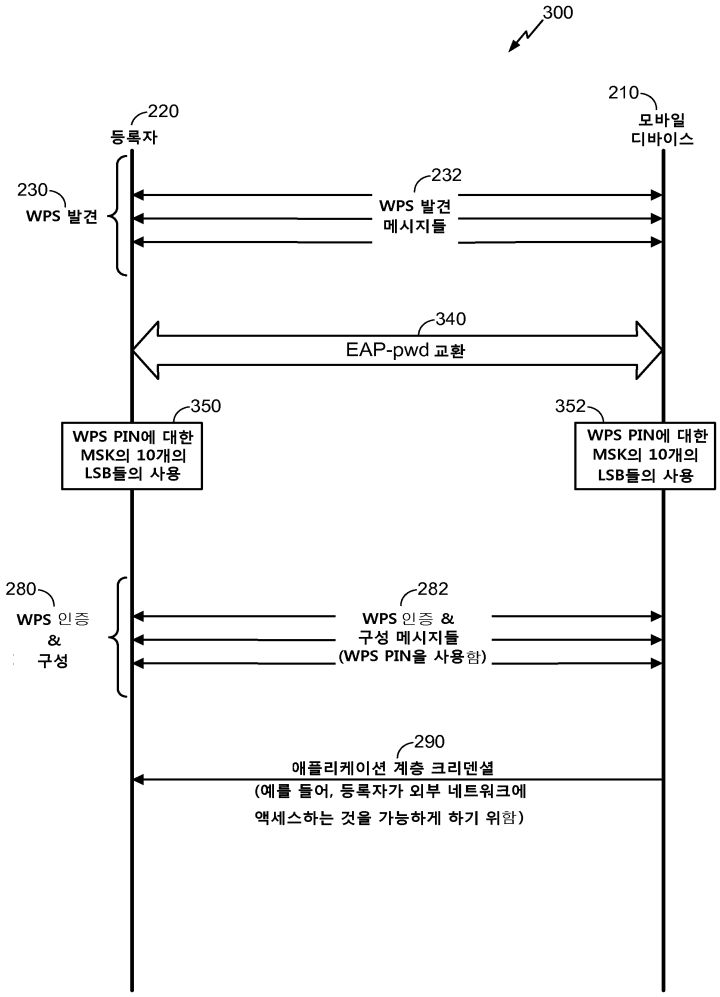
도면1


100
120
122
"디폴트" 크리덴셜
105
"WLAN" 크리덴셜
124
애플리케이션 계층 크리덴셜
헤드리스 디바이스 (예를 들어, SEP-호환가능함)
WLAN
140
106
WLAN 연결
130
"디폴트" 크리덴셜을 사용한 보안 채널 설정
(예를 들어, EAP, EAP-pwd, EAP-eke, 또는 WPA2-PSK)
104
WLAN 크리덴셜(들)
(예를 들어, SSID/패스프레이즈/키)
105
애플리케이션 계층 크리덴셜
124
102
사용자
애플리케이션 계층 크리덴셜을 사용한 연결
103
WLAN 연결
124
애플리케이션 계층 크리덴셜
"디폴트" 크리덴셜
108
110
107
150
외부 네트워크

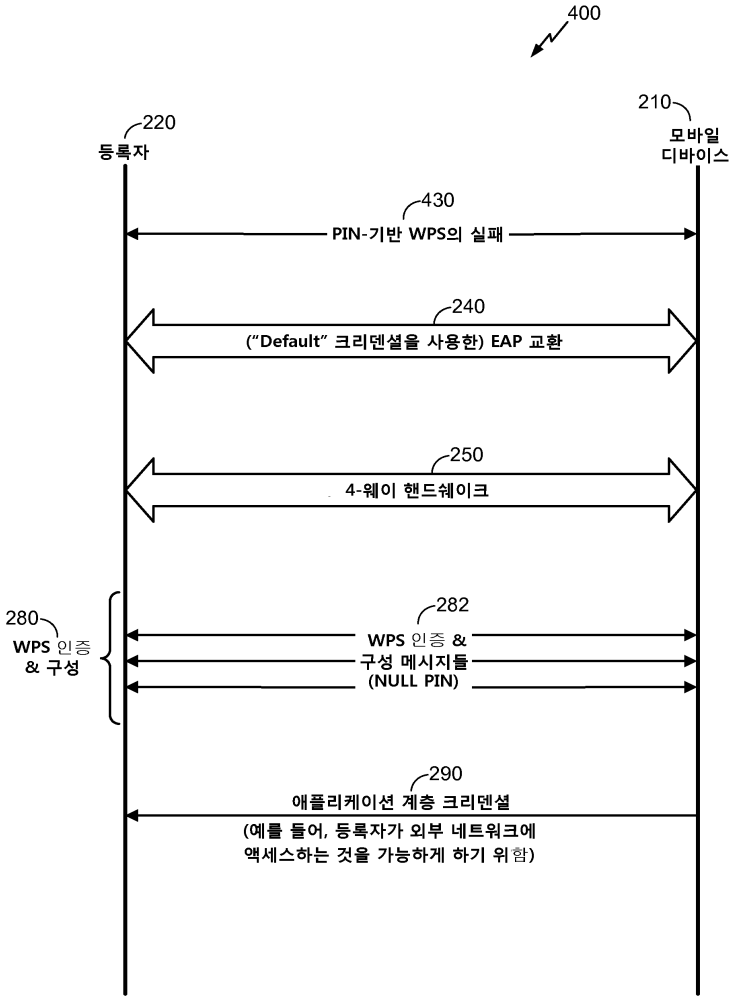
도면2


200
210
모바일
디바이스
220
등록자
230
WPS 발견
232
WPS 발견
메시지들
240
("디폴트" 크리덴셜을 사용한) EAP 교환
250
4-웨이 핸드쉐이크
280
WPS 인증
&
구성
282
WPS 인증
&
구성 메시지들
(NULL PIN)
290
애플리케이션 계층 크리덴셜
(예를 들어, 등록자가 외부 네트워크에
액세스하는 것을 가능하게 하기 위함)

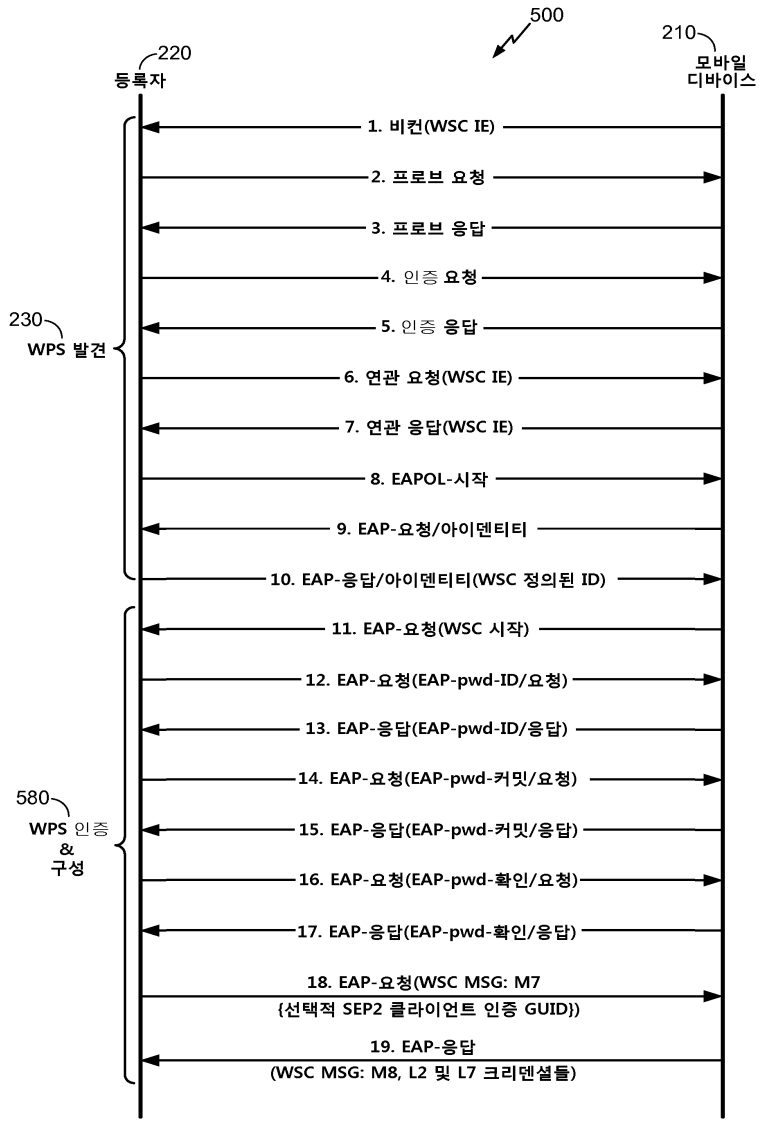
도면3


300
210
모바일
디바이스
220
등록자
230
WPS 발견
232
WPS 발견
메시지들
340
EAP-pwd 교환
350
WPS PIN에 대한
MSK의 10개의
LSB들의 사용
352
WPS PIN에 대한
MSK의 10개의
LSB들의 사용
280
WPS 인증
&
구성
282
WPS 인증 &
구성 메시지들
(WPS PIN을 사용함)
290
애플리케이션 계층 크리덴셜
(예를 들어, 등록자가 외부 네트워크에
액세스하는 것을 가능하게 하기 위함)

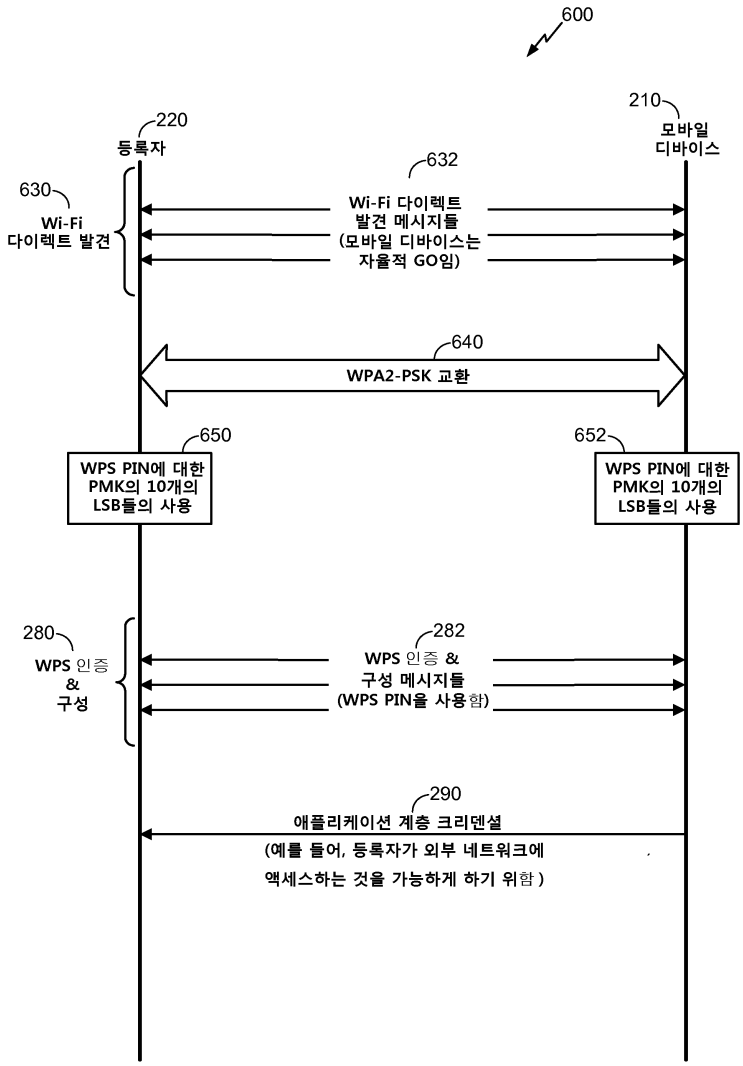
도면4


400
210
모바일
디바이스
220
등록자
430
PIN-기반 WPS의 실패
240
("Default" 크리덴셜을 사용한) EAP 교환
250
4-웨이 핸드쉐이크
280
WPS 인증
& 구성
282
WPS 인증 &
구성 메시지들
(NULL PIN)
290
애플리케이션 계층 크리덴셜
(예를 들어, 등록자가 외부 네트워크에
액세스하는 것을 가능하게 하기 위함)

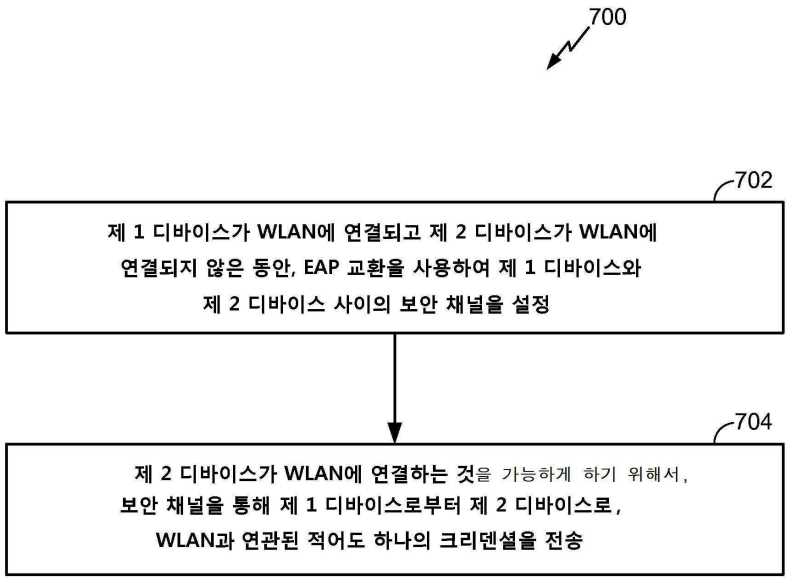
도면5


500
210
모바일 디바이스
220
등록자
230
WPS 발견
580
WPS 인증 & 구성
1. 비컨(WSC IE)
2. 프로브 요청
3. 프로브 응답
4. 인증 요청
5. 인증 응답
6. 연관 요청(WSC IE)
7. 연관 응답(WSC IE)
8. EAPOL-시작
9. EAP-요청/아이덴티티
10. EAP-응답/아이덴티티(WSC 정의된 ID)
11. EAP-요청(WSC 시작)
12. EAP-요청(EAP-pwd-ID/요청)
13. EAP-응답(EAP-pwd-ID/응답)
14. EAP-요청(EAP-pwd-커밋/요청)
15. EAP-응답(EAP-pwd-커밋/응답)
16. EAP-요청(EAP-pwd-확인/요청)
17. EAP-응답(EAP-pwd-확인/응답)
18. EAP-요청(WSC MSG: M7
{선택적 SEP2 클라이언트 인증 GUID})
19. EAP-응답
(WSC MSG: M8, L2 및 L7 크리덴셜들)

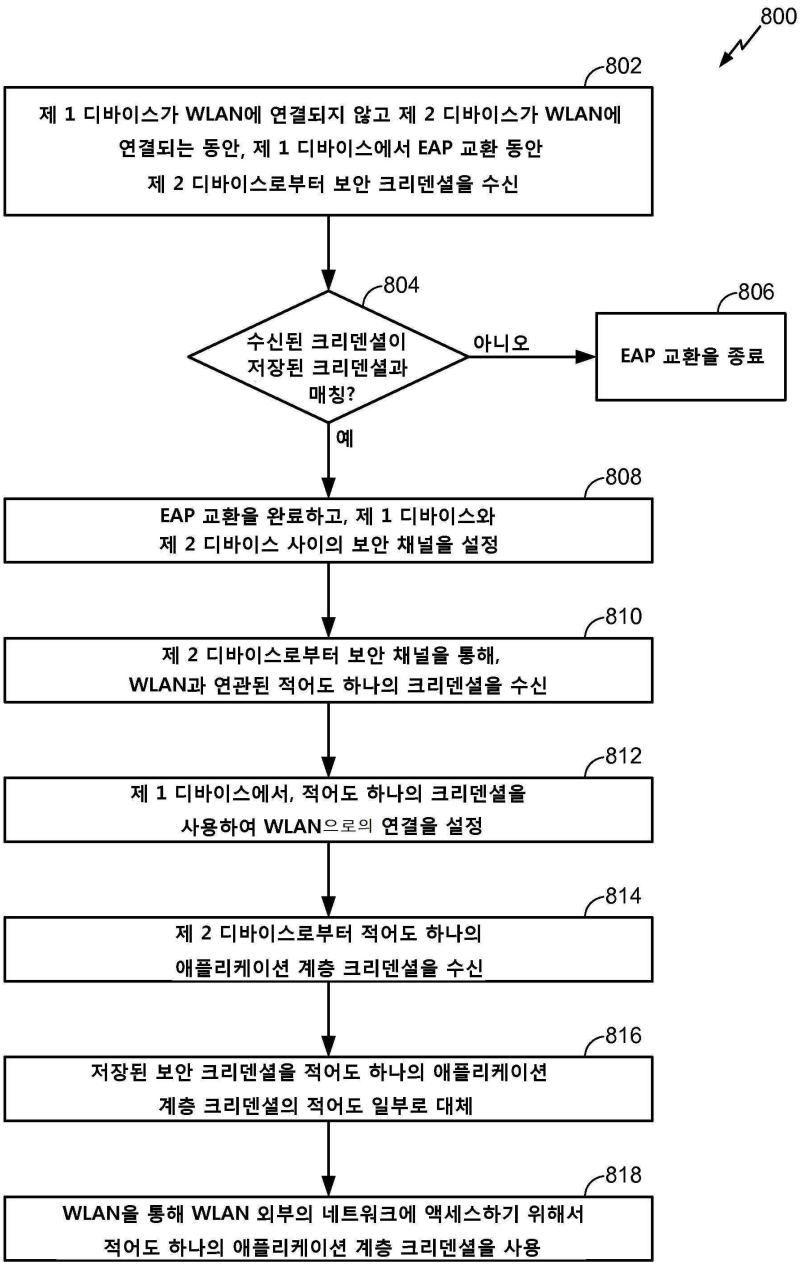
도면6


600
210
모바일
디바이스
220
등록자
632
630
Wi-Fi
다이렉트 발견
Wi-Fi 다이렉트
발견 메시지들
(모바일 디바이스는
자율적 GO임)
640
WPA2-PSK 교환
650
652
WPS PIN에 대한
PMK의 10개의
LSB들의 사용
WPS PIN에 대한
PMK의 10개의
LSB들의 사용
280
WPS 인증
&
구성
282
WPS 인증 &
구성 메시지들
(WPS PIN을 사용함)
290
애플리케이션 계층 크리덴셜
(예를 들어, 등록자가 외부 네트워크에
액세스하는 것을 가능하게 하기 위함)

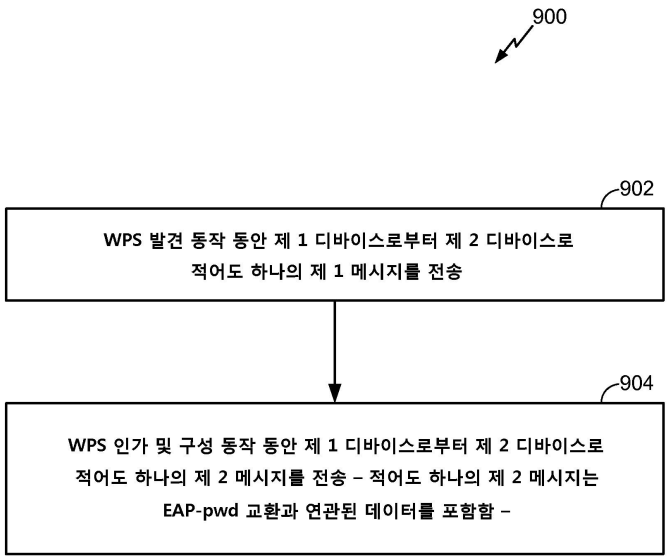
도면7


700
702
제 1 디바이스가 WLAN에 연결되고 제 2 디바이스가 WLAN에 연결되지 않은 동안, EAP 교환을 사용하여 제 1 디바이스와 제 2 디바이스 사이의 보안 채널을 설정
704
제 2 디바이스가 WLAN에 연결하는 것을 가능하게 하기 위해서, 보안 채널을 통해 제 1 디바이스로부터 제 2 디바이스로, WLAN과 연관된 적어도 하나의 크리덴셜을 전송

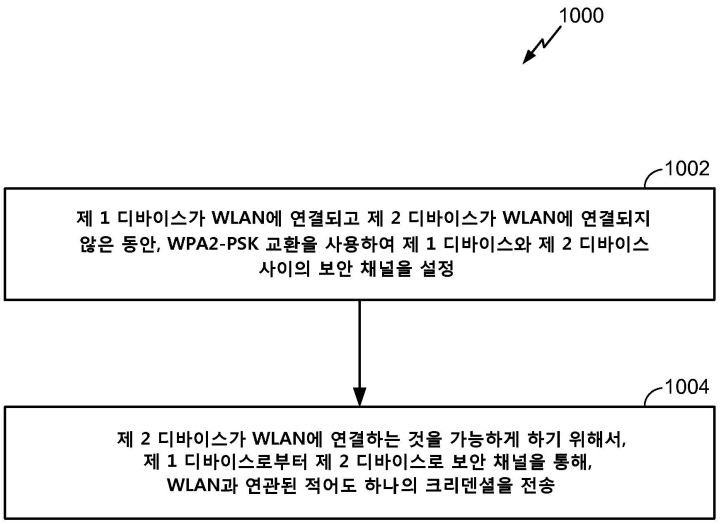
도면8


800
802
제 1 디바이스가 WLAN에 연결되지 않고 제 2 디바이스가 WLAN에 연결되는 동안, 제 1 디바이스에서 EAP 교환 동안 제 2 디바이스로부터 보안 크리덴셜을 수신
804
수신된 크리덴셜이 저장된 크리덴셜과 매칭?
아니오
806
EAP 교환을 종료
예
808
EAP 교환을 완료하고, 제 1 디바이스와 제 2 디바이스 사이의 보안 채널을 설정
810
제 2 디바이스로부터 보안 채널을 통해, WLAN과 연관된 적어도 하나의 크리덴셜을 수신
812
제 1 디바이스에서, 적어도 하나의 크리덴셜을 사용하여 WLAN으로의 연결을 설정
814
제 2 디바이스로부터 적어도 하나의 애플리케이션 계층 크리덴셜을 수신
816
저장된 보안 크리덴셜을 적어도 하나의 애플리케이션 계층 크리덴셜의 적어도 일부로 대체
818
WLAN을 통해 WLAN 외부의 네트워크에 액세스하기 위해서 적어도 하나의 애플리케이션 계층 크리덴셜을 사용

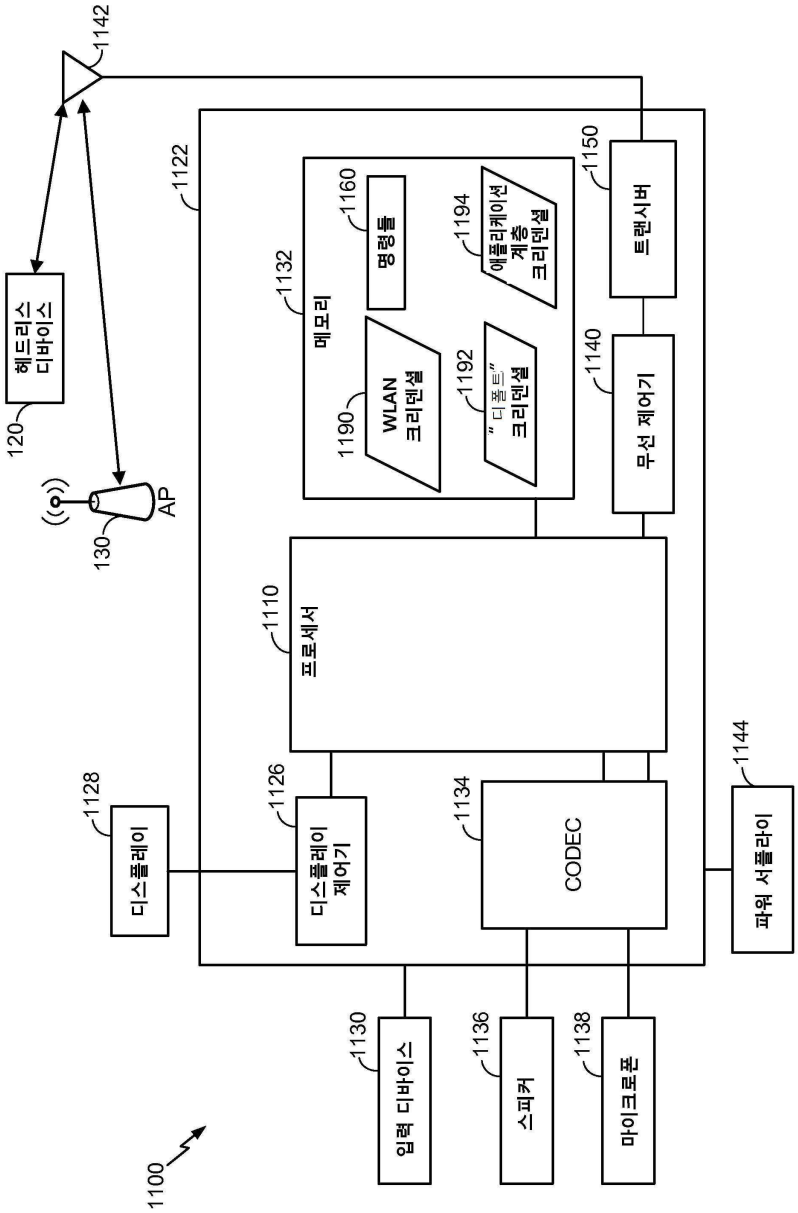
도면9


900
902
WPS 발견 동작 동안 제 1 디바이스로부터 제 2 디바이스로
적어도 하나의 제 1 메시지를 전송
904
WPS 인가 및 구성 동작 동안 제 1 디바이스로부터 제 2 디바이스로
적어도 하나의 제 2 메시지를 전송 – 적어도 하나의 제 2 메시지는
EAP-pwd 교환과 연관된 데이터를 포함함 –

도면10


1000
1002
제 1 디바이스가 WLAN에 연결되고 제 2 디바이스가 WLAN에 연결되지
않은 동안, WPA2-PSK 교환을 사용하여 제 1 디바이스와 제 2 디바이스
사이의 보안 채널을 설정
1004
제 2 디바이스가 WLAN에 연결하는 것을 가능하게 하기 위해서,
제 1 디바이스로부터 제 2 디바이스로 보안 채널을 통해,
WLAN과 연관된 적어도 하나의 크리덴셜을 전송

도면11



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 28

【변경전】

상기 제 WLAN 외부의 네트워크로

【변경후】

상기 WLAN 외부의 네트워크로

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 28

【변경전】

상기 제 보안 채널을 통해

【변경후】

상기 보안 채널을 통해